

Contribuição Data Privacy Brasil - Tomada de Subsídios Direitos dos Titulares

Eduarda Costa

Eduardo Mendonça

Johanna Monagreda

Julia Mendonça

Paula Guedes

Pedro Martins

Pedro Henrique Santos

Introdução

O seguinte documento tem por objetivo contribuir com a tomada de subsídios iniciada pela Autoridade Nacional de Proteção de Dados em 2 de fevereiro de 2024 com objetivo de receber contribuições da sociedade acerca de temas chave na elaboração da norma sobre direitos dos titulares de dados pessoais.

Em sua missão de colaborar com a construção da cultura de proteção de dados no Brasil, a Data Privacy Brasil elaborou o presente documento com considerações iniciais a respeito das perguntas elaboradas pela Autoridade.

São Paulo, 14 de março de 2024.

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (“ANPD”)

Coordenação-Geral de Normatização

Ref.: Consulta à Sociedade sobre o Guia de Anonimização e Pseudonimização

A ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO (“ANBC”), pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Avenida das Nações Unidas, n.º 14.401, Conjuntos 502 e 503, Cidade de São Paulo, Estado de São Paulo, é uma entidade que reúne os bureaus atuantes no território brasileiro, com o objetivo de representar o setor de bureaus de crédito no país, inclusive junto a agentes internacionais, incentivar a educação financeira e colaborar para a criação de um ambiente legal e regulatório que permita à gestão de crédito contribuir ativamente com a economia brasileira.

Em 30 de janeiro de 2024, a ANPD disponibilizou, por meio da Plataforma “Participa + Brasil”,¹ Consulta à Sociedade² acerca do seu Estudo Preliminar sobre Anonimização e Pseudonimização para Proteção de Dados (“Estudo Preliminar”), a fim de coletar contribuições de profissionais da área, agentes de tratamento, titulares, setor acadêmico e da sociedade em geral. A consulta pretende alinhar a atuação regulatória da Autoridade às melhores práticas em matéria de anonimização e pseudonimização de dados pessoais.

Nessa oportunidade, a ANBC vem apresentar a sua contribuição à ANPD, reiterando seus cumprimentos pela iniciativa de consultar e colher subsídios de todos os setores interessados com vistas a contribuir para a atuação da Autoridade em torno do tema.

* * *

¹ ANPD. “Consulta à Sociedade - Estudo Preliminar - Anonimização e pseudonimização para proteção de dados”. Disponível em: <<https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonizacao-e-pseudonizacao-para-protacao-de-dados>>. Acesso em: 21.02.2024.

² ANPD. “ANPD abre consulta à sociedade sobre o Guia de Anonimização e Pseudonimização”. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonizacao-e-pseudonizacao>>. Acesso em: 21.02.2024.



Brasília, 2 de abril de 2024.

À Autoridade Nacional de Proteção de Dados - ANPD

Assunto: Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT) à Tomada de Subsídios sobre os direitos dos titulares.

Fundada em 27 de novembro de 1962, a Associação Brasileira de Emissoras de Rádio e Televisão – ABERT é uma sociedade civil sem fins econômicos, de duração indeterminada, constituída por empresas de radiodifusão autorizadas a funcionar no País. Tem como principal objetivo a defesa da liberdade de expressão, em todas as suas formas, bem como dos interesses das emissoras de radiodifusão, suas prerrogativas como executoras de serviços de interesse público, assim como seus direitos e garantias.

Neste contexto, a ABERT gostaria de contribuir para a consulta pública da ANPD sobre os direitos dos titulares¹. Na visão da entidade, os seguintes pontos merecem especial atenção e devem ser revistos, de forma a aperfeiçoar a minuta de regulação proposta:

I. Relacionamento entre o controlador e o titular

a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

Os prazos fixados na Lei nº 12.527/2011, a Lei de Acesso à Informação (LAI), consideram o atendimento por órgãos e entidades da Administração Pública a pedidos formulados por cidadãos a respeito de informações contidas em registros e documentos, processos administrativos, relatórios sobre uso de recursos públicos, resultados de auditoria, entre outras. O atendimento a requerimentos fundados na LAI leva, portanto, na maior parte das vezes, a que os responsáveis pelo funcionamento de um balcão de atendimento ao

¹ Disponível em: <https://www.gov.br/participamaisbrasil/consulta-a-sociedade-sobre-os-direitos-dos-titulares>



REFERÊNCIA: TOMADA DE SUBSÍDIOS PARA NORMA SOBRE DIREITOS DOS TITULARES DE DADOS PESSOAIS

REFERÊNCIA: TOMADA DE SUBSÍDIOS PARA NORMA SOBRE DIREITOS DOS TITULARES DE DADOS PESSOAIS

ENTIDADE CONTRIBUINTE: ASSOCIAÇÃO DAS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) E DE TECNOLOGIAS DIGITAIS ("BRASSCOM")

PRAZO: 03/04/2024

I. RELACIONAMENTO ENTRE O CONTROLADOR E O TITULAR

a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

Primeiramente, é importante destacar que, no que se refere aos incisos I e II do artigo 19 da LGPD, já existem prazos estabelecidos para a resposta do controlador. Assim, no que diz respeito à confirmação da existência ou acesso aos dados, a ANPD apenas poderia desviar dos prazos ali estabelecidos no caso de setores específicos, como prevê o §4º do artigo 19. Quanto aos demais direitos previstos nos incisos III a IX do artigo 18, de fato é necessário que haja uma elucidação em relação ao prazo para seu atendimento.

A proposta de seguir os prazos da Lei nº 12.527/2011 é inadequada, considerando as diferentes lógicas subjacentes aos direitos estabelecidos por essa lei e pela LGPD. Enquanto a LGPD visa possibilitar que um titular específico exerça seus direitos em relação aos seus dados pessoais perante o controlador, a LAI tem o objetivo de regular o acesso a informações públicas. Assim, no contexto da LGPD, o controlador precisa primeiro garantir a autenticação do titular, o que envolve uma série de procedimentos (como a confirmação da identidade e a verificação do meio de exercício do direito, incluindo se é feito por meio de procurador), impactando o tempo necessário para atender a esses direitos. Essa realidade não se aplica à LAI.

Além disso, os prazos previstos pela LAI (20 dias, com a possibilidade de prorrogação por mais dez dias, conforme previsto pelo caput do artigo 11 e seu §2º) são demasiadamente exíguos para o atendimento dos direitos previstos nos incisos III a IX do artigo 18 da LGPD. Nesse sentido, destaca-se que o GDPR estabelece, em seu artigo 12.1, que os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Assim, recomenda-se que a ANPD siga o prazo estabelecido pelo *GDPR*, ou seja, de 30 (trinta dias), podendo haver

DIREITO DOS TITULARES

Documento elucidativo elaborado pela Brasscom com os desafios os quais os controladores de dados pessoais têm se deparado quando da operacionalização de pedido de acesso ou exercício dos direitos pelos titulares

Brasília (DF), 07 de fevereiro de 2022

A Brasscom, Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais (TIC) e de Tecnologias Digitais, entidade sem fins lucrativos de representatividade nacional, e que congrega algumas das mais dinâmicas e inovadoras empresas de TIC alinhadas com a Era Digital.

O envolvimento da Brasscom em discussões atinentes à proteção de dados pessoais há muito se situa como uma das prioridades da Associação, que tem acompanhado todo o desenvolvimento do processo legislativo desde o momento embrionário da Lei Geral de Proteção de Dados Pessoais, quando ainda anteprojeto de lei, e participado ativamente com contribuições relevantes para o notável resultado equilibrado da norma.

Nesse sentido, a Brasscom inequivocamente reconhece os direitos dos titulares criados pela LGPD¹ como pilar essencial do arcabouço legislativo sobre dados pessoais no Brasil, sem os quais a efetividade da tutela, almejada pela Lei, seria comprometida. Entretanto, apesar da essencialidade desses direitos à pessoa humana, tais direitos não são absolutos pelo que seu exercício precisa ser adequadamente direcionado para que o ordenamento jurídico como um todo possa ser respeitado.

Deste modo e com o intuito de viabilizar seu cumprimento adequado por parte do setor empresarial, a Brasscom compartilha, com esta respeitável Autoridade Nacional de Proteção de Dados, documento elucidativo dos desafios e incertezas com as quais os controladores de dados pessoais têm se deparado quando da operacionalização de um pedido de acesso ou exercício dos outros direitos pelos titulares para, na sequência e se apoiando em exemplos de autoridades de proteção de dados internacionais, como a ICO², o CNIL³, a AEPD⁴, do Reino Unido, da França e da Espanha, respectivamente, propor sugestões ao endereçamento dessas questões visando ao atendimento de tais direitos com a devida segurança jurídica.

1. DA NECESSIDADE DA VERIFICAÇÃO DA AUTENTICIDADE DO TITULAR QUANDO DO EXERCÍCIO DOS DIREITOS PREVISTOS NO ARTIGO 18 DA LGPD

Uma das principais questões que geram dúvidas nos controladores no âmbito da implementação dos direitos dos titulares decorre da necessidade de verificação da autenticidade do titular antes de responder a qualquer direito por ele exercido. Esse aspecto afeta diretamente o prazo que o controlador tem para atender o pedido de exercício do direito, na medida em que, após o recebimento de um pedido e visando a adoção das melhores medidas de segurança, deve certificar a identidade do titular para responder à pessoa adequada, evitando, assim, a ocorrência de incidentes de segurança.

¹ Artigo 18 da LGPD.

² *Information Commissioner's Officer* (Reino Unido)

³ *Commission Nationale Informatique & Libertés* (França)

⁴ *Agencia Española de Protección de Datos* (Espanha)

03/04/2024 - BigDataCorp - Tomada de Subsídios - Direitos dos Titulares

Pergunta	Resposta
Bloco I - Relacionamento entre o controlador e o titular	
a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?	Entende-se que o prazo de 20 dias prorrogáveis por mais 10 dias do art. 11 da Lei nº 12.527/2011 ("LAI") seria razoável para o atendimento, pelos agentes de tratamento do setor privado, dos direitos dos titulares previstos na LGPD, com exceção do que diz respeito a eventuais requisições relacionadas especificamente à confirmação de existência e acesso aos dados pessoais pelos titulares (art. 18, I e II). Isso porque o art. 19 da LGPD prevê expressamente que a confirmação de existência ou o acesso aos dados pessoais serão providenciados, mediante requisição do titular, (i) em formato simplificado, imediatamente; ou (ii) por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular. Não obstante, considerando a complexidade que pode revestir o atendimento de direitos dessa natureza, é razoável que a possibilidade de prorrogação por mais 10 dias do prazo legal de 15 dias também seja prevista pela ANPD para essas hipóteses. Adicionalmente, sugere-se que a ANPD preveja algum mecanismo segundo o qual, desde que mediante razões justificadas e previsão de data para conclusão do atendimento dos direitos pelo controlador, os prazos totais de 25 dias para o atendimento dos direitos previstos no art. 18, I e II da LGPD e 30 dias para o atendimento dos demais direitos previstos na LGPD possam ser excedidos. Nesse cenário excepcional, a adoção das medidas para atender os direitos dos titulares deverá ser iniciada dentro do prazo total previsto, mas com possibilidade de prazo adicional para conclusão do atendimento, diante de eventuais particularidades do modelo de negócio do controlador e/ou das características específicas da solicitação ou do tratamento em discussão (por exemplo, em caso de eventuais solicitações de exercício do direito de portabilidade, que possam atrair complexidades técnicas e a necessidade de atuação de terceiros para sua efetivação). Por fim, independentemente dos prazos adotados, é necessário que qualquer regulação ou orientação sobre

CONTRIBUIÇÕES B/LUZ – TOMADA DE SUBSÍDIOS SOBRE DIREITOS DOS TITULARES

**Atenção ao limite de 2100 caracteres para cada resposta.*

I. Relacionamento entre Controlador e Titular

- a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

O artigo 11 da Lei nº 12.527 prevê que o acesso a informações, quando solicitado, deve ser **imediato**. Caso não seja possível, a entidade que receber o pedido deverá, em até 20 dias, atender à solicitação, podendo prorrogar por mais 10 dias, mediante justificativa. Contudo, a aplicação dessa lógica aos direitos previstos na LGPD tornaria inviável o atendimento de tais direitos pelas empresas.

A LGPD abrange direitos com diferentes níveis de complexidade. Um atendimento imediato pode ser impraticável, especialmente quando as solicitações dos titulares exigem análises detalhadas dos dados, envolvimento de diferentes áreas e consultas a terceiros.

É necessário estabelecer que a LGPD e a LAI possuem contextos distintos. Enquanto a LAI visa a transparência do governo, a LGPD visa a proteção dos direitos dos titulares, requerendo abordagens adequadas às suas particularidades. Os interesses protegidos pela LGPD, demandam prazos diferenciados para garantir a proteção de direitos dos titulares, com a aplicação de procedimentos prévios de autenticação de identidade, e os interesses do setor privado, com a avaliação a respeito da eventual violação dos segredos comerciais da empresa.

É razoável, portanto, argumentar que a aplicação dos prazos da LAI não é adequada para a LGPD. Em vez disso, outras legislações internacionais oferecem prazos mais flexíveis e adaptados à complexidade das solicitações dos titulares de dados. A *California Consumer Privacy Act*¹ prevê um prazo de 45 dias para responder às solicitações dos titulares, enquanto o GDPR² e a *PIPEDA*³ do Canadá estabelecem um prazo de 30 dias, todos prorrogáveis por tempo igual. Essa flexibilidade é crucial para lidar com solicitações complexas de forma eficiente e garantir o respeito aos direitos dos titulares sem comprometer a operacionalidade das empresas.

¹ California Consumer Privacy Act (CCPA). Seção 1798.130(a)(2) (A). Disponível em: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.8

² União Europeia. Regulamento (UE) 2016/679 (GDPR). (GDPR). Artigo 12, item 3. Disponível em: <https://gdpr-info.eu/art-12-gdpr/>

³ Personal Information Protection and Electronic Documents Act (PIPEDA) Parte 1. Item 7.4 (3). Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>

A Associação Brasileira das Empresas do Mercado de Fidelização (“ABEMF”), vem apresentar os seus comentários aos quesitos levantados pela ANPD na tomada de subsídio sobre os direitos dos titulares¹, elaboradas considerando as particularidades e os interesses do setor de fidelização.

I. Relacionamento entre o controlador e o titular

Q- a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

R- Ao nosso entender, não.

De forma geral, os prazos previstos na Lei em questão variam entre 5-20 dias. Embora esses prazos possam ser exequíveis em sistemas centralizados (que tende a ser o caso da maioria dos órgãos da administração pública, que detêm atividades específicas e concentradas em alguns sistemas), tendem a ser inadequados para entes privados, que, inclusive pela necessidade de inovação para se manterem no mercado, têm sistemas e bases de dados diversos, em produção ou em teste, desempenhando atividades relevantes ao negócio, nos quais os dados pessoais do titular podem circular e, por isso mesmo, precisam ser verificados para o atendimento às solicitações dos titulares.

Diante disso, para que as companhias tenham segurança nas respostas, é fundamental que prazo adequado seja concedido, sob pena de tornar inviável o atendimento com assertividade, especialmente para pequenas e médias empresas, que têm maior dificuldade para automatizar os processos de atendimento de direitos. Justamente por isso, o legislador europeu estabeleceu o prazo de 1 mês, prorrogável por até 3 meses, nos termos do art. 12(3), do GDPR, o que recomendamos seja seguido como referência por esta Autoridade, fixando o prazo de, no mínimo, um mês.

Q- b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

R- Entendemos que os seguintes critérios relevantes podem ser razoavelmente tomados em consideração:

- **O grau de abstração do pedido:** pedidos com escopo mais concreto tendem a ser mais facilmente (e mais rapidamente) atendidos do que pedidos com escopo demasiadamente abrangentes e abstratos. Quanto mais específica e limitada a solicitação, menor tende a ser o prazo necessário a atendê-la.
- **O termo inicial deveria ser contado a partir da validação da identidade do titular:** em atenção ao princípio da segurança (art. 6º, VI, da LGPD), o atendimento de solicitações de direito deve ser precedido de prévia validação da identidade do titular, por intermédio de processo de autenticação razoável (ex. solicitação de cópia de documento, validação biométrica...). Deste modo, é recomendável que o termo inicial do prazo se opere após a comprovação, pelo titular, de sua identidade – nesse sentido já se posicionam alguns códigos de conduta setoriais, como a SARB 25, da FEBRABAN.

¹ Disponível em <https://www.gov.br/participamaisbrasil/consulta-a-sociedade-sobre-os-direitos-dos-titulares>. Último acesso em 19.02.2024

São Paulo, 3 de abril de 2024.

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

normatizacao@anpd.gov.br

Ref.: Tomada de Subsídios sobre os direitos dos titulares

Prezados,

A **Associação Brasileira de Instituições de Pagamentos ("ABIPAG")**, inscrita no CNPJ/MF sob o nº26.425.404/0001-10, vem respeitosamente à presença desta Autoridade Nacional de Proteção de Dados ("**ANPD**") e em completude às sugestões realizadas na plataforma Participa + Brasil apresentar manifestação com suas contribuições.

A ABIPAG é uma associação setorial do mercado de meios de pagamento eletrônicos formada por instituições de pagamento e instituições financeiras. Nesse sentido, suas contribuições possuem como foco o melhor interesse do titular de dados e estão direcionadas à realidade do mercado de meios de pagamento.

I. SUMÁRIO EXECUTIVO

A ABIPAG apresenta abaixo propostas de aprimoramento orientadas pela abordagem baseada em riscos, com o intuito de garantir práticas mais benéficas aos usuários, aos agentes de tratamento e aos encarregados:

Prazos de respostas: propõe-se que a contagem dos prazos de atendimento aos titulares esteja alinhada ao Código de Processo Civil (contagem em dias úteis), bem como seja assegurada convergência com as práticas internacionais — em especial o General Data Protection Regulation ("GDPR") — garantindo que haja previsibilidade e segurança jurídica para o titular e para os agentes.

Autonomia das organizações: entende-se relevante que cada organização, considerando seu porte e características do tratamento de dados pessoais realizado, tenha autonomia para adaptar o formato de atendimento dos titulares dos dados às suas especificidades.

São Paulo, 02 de abril de 2024.

REFERÊNCIA: TOMADA DE SUBSÍDIOS PARA NORMA SOBRE DIREITOS DOS
TITULARES DE DADOS PESSOAIS

REFERÊNCIA: TOMADA DE SUBSÍDIOS PARA NORMA SOBRE DIREITOS DOS
TITULARES DE DADOS PESSOAIS

ENTIDADE CONTRIBUINTE: CÂMARA BRASILEIRA DA ECONOMIA DIGITAL
("CÂMARA-E.NET")

I. RELACIONAMENTO ENTRE O CONTROLADOR E O TITULAR

a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

Em relação aos prazos para resposta do controlador em relação aos direitos exercidos pelos titulares no moldes dos incisos I e II do artigo 19 da LGPD, é preciso que se considere que tais prazos estão legalmente estabelecidos. No que se refere aos demais direitos listados nos incisos III a IX, para fins de segurança jurídica, de fato é imprescindível uma orientação mais clara da ANPD não só quanto aos prazos em si, mas também em relação à sua contagem.

Quanto à sugestão de adotar os prazos da LAI, há uma distinção fundamental entre os propósitos das leis, que deve ser considerada. Enquanto a LGPD visa garantir que os titulares de dados exerçam uma série de direitos em relação aos seus dados pessoais, a LAI trata do acesso a informações públicas. Portanto, encargos decorrem dessa distinção, como a necessidade de verificação da identidade do titular, entre outros procedimentos técnicos e administrativos necessários para o cumprimento da LGPD, que inevitavelmente afetam o tempo necessário para atender a esses direitos, o que não se aplica à LAI.

Nesse sentido, os prazos estipulados pela LAI podem ser considerados insuficientes para o atendimento dos direitos mencionados nos incisos III a IX do artigo 18 da LGPD, ainda mais porque são contados em dias corridos, como regra. Em contraste, o General Data Protection Regulation ("GDPR") estabelece, em seu artigo 12 (3), que os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos.

Assim, uma saída regulatória ao tema seria adotar os prazos estabelecidos pelo GDPR como inspiração. Contudo, para serem mais compatíveis com a forma de contagem brasileira, que seja previsto em formato de dias: 30 dias a partir do dia útil seguinte ao dia em que houver o recebimento de pedido legítimo, prorrogando-se para o dia seguinte o fim do prazo que caia em feriados ou finais de semanas.

Como destacado, a Câmara-e.net entende que a contagem deve se dar em dias úteis, com início no dia útil subsequente ao momento em que há o recebimento de um pedido legítimo, o que significa que: (i) houve autenticação do titular; (ii) o pedido de titular é suficientemente claro (muitas vezes os titulares fazem pedidos genéricos que impossibilitam o atendimento e exigem

a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

NDA

b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

Devem os agentes de tratamento, buscar o célere atendimento, quiçá nos mesmos 15 dias previstos para os direitos de informação e de acesso.,"615484": "Evitar o acúmulo de função do encarregado de proteção de dados responsável pelo canal de atendimento. ","615485": "Sim. A distribuição da responsabilidade civil do operador de dados pessoais no caso de incidente de privacidade com lesão ao titular, se dá de acordo com o estágio da operação em que residiu a falha, sendo que poderá haver solidariedade entre controlador e operador em determinadas hipóteses","615486": "Sim","615487": "Sim, evitar o acúmulo de função do encarregado de proteção de dados em ambos os setores. ","615491": "Não","615492": "Nome, número de telefone e e-mail","615489": "A respeito da responsabilidade e do ressarcimento de danos, o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar ao titular dos dados, dano patrimonial, moral, individual ou coletivo, violando as normas da LGPD, estará obrigado a repará-lo. ","615490": "Nome e número de telefone","615494": "Nome, CNPJ, número de telefone, e-mail e endereço. ","615493": "sim","615502": "Setor de tecnologia da informação - OSI","615501": "políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação no Poder Executivo","615505": "os padrões tecnológicos a serem aplicados no governo passam por quatro níveis, a saber: Adotado (A), Recomendado (R), Em Transição (T) e Em Estudo (E).","615503": "sim","615504": "sim .. 15 dias","615511": "Prazo de armazenamento","615514": "Dados sensíveis","615513": "caráter técnico, operacional e esforço desproporcional ","615512": "Não utilização da base legal consentimento ","615517": "A resposta a qualquer requisição formulada por titular depende da aptidão da organização em precisar quais dados pessoais detém sobre o específico titular requisitante e onde estes dados estão localizados, inclusive se em mais de um local e em diferentes formatos (físico e/ou digital), e, finalmente, possuir um processo que forneça a resposta à requisição, de preferência de forma padronizada. ","615516": "sim","615518": "sim","615523": "Sim","615521": "A não utilização desses dados em qualquer situação ","615617": "um ato decisório realizado por meio de mapeamento de perfis, mediante qualquer forma de tratamento automatizado de dados pessoais, para avaliar aspectos pessoais relativos a uma pessoa singular","615618": "direito de revisão","615619": "De forma real, qual seria o real interesse violado","615620": "segredos comercial e industrial."

{“615450”: “Entendemos que o prazo deve ser de até 30 dias corridos, ou seja, mais amplo que a LAI. Quando houver muito volume, sugerimos uma ampliação do prazo a ser definida pelo controlador conforme o caso concreto, volume das operações na forma art. 50, par. 2º. A esse respeito, vale lembrar o art. 12, inciso 3 do GDPR, que estabelece o mesmo prazo e a possibilidade de prorrogação até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Deve ser lembrado que o atendimento aos titulares não pode inviabilizar o exercício da atividade econômica (art. 2º, V e VI da LGPD). Além disso, a LAI demanda a transparência ativa (art. 9º) em grau muito mais profundo que os agentes privados, que em muitos casos devem proteger o sigilo das informações como, por exemplo, as trabalhistas. Logo, enquanto na LAI o portal da transparência irá satisfazer a maior parte dos interesses por informações, os agentes privados terão que prestar informações mediante requisição, e por isso deve ser considerado um prazo mais elástico para não prejudicar os agentes de pequeno e médio porte.”, b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? “Entendemos, naturalmente, que a declaração simplificada deve conter menos itens do que aqueles requisitos da declaração completa (art. 19, II). A declaração simplificada seria utilizada quando o titular pedir apenas um aspecto do direito de acesso ou confirmação de existência. Podemos citar como exemplo a situação em que o titular pede informações apenas sobre o rastreamento do seu IP ou e-mail para receber propaganda.”, “615484”: “Como operadoras de planos de saúde sem fins lucrativos não podemos deixar de mencionar o modelo adotado na Resolução Normativa n. 395 da ANS, arts. 5º e 7º, que trata da necessidade de atendimento presencial e telefônico. No caso da proteção de dados, entendemos que o atendimento deverá ocorrer preferencialmente ou por telefone ou por e-mail, gerando mais dinâmica no acesso. Também poderá ser fornecido um atendimento via portal ou presencial ao titular. Em termos de estruturação do canal de atendimento, citamos a RN n. 323 da ANS, que trata da ouvidoria, e que traz requisitos importantes como: a) vinculação ao representante legal da operadora, respeitada a estrutura organizacional de cada operadora; b) a designação de pessoa para exercício da atividade de ouvidor, não cumulável com a atividade de gestão do atendimento ao beneficiário da operadora, ressalvada a hipótese do art. 8º; c) a constituição de equipe de trabalho, capaz de atender o fluxo de demandas, com dedicação exclusiva para exercício na unidade; d) a instituição de canal ou de canais específicos para atendimento. Claro que tudo isso deve levar em conta o porte econômico do agente de tratamento, assim como faz a referida entidade (Art. 8º).”, “615485”: “Muito embora não sejam responsáveis diretos, os operadores devem auxiliar/consultar o controlador no exercício dos atendimentos, principalmente em caso de dúvida ou omissão contratual. Esta é uma diretriz clara do art. 50, caput, da LGPD.”, “615486”: “Em primeiro lugar, é importante destacar que nem toda organização se submete a relação de consumo, ainda que preste serviços às pessoas naturais. Nessa linha, o Superior Tribunal de Justiça já decidiu que não se aplica o CDC às autogestões (Súmula 608 do STJ). Mesmo que não se aplique tal normativo às autogestões, entendemos que as questões relativas à qualidade do atendimento previstas na lei do SAC podem ser aproveitadas pela ANPD como, por exemplo, o registro e o fornecimento de um número de protocolo, assim como os prazos de retorno administrativo (não confundir com a resposta a requisição).”, “615487”: “Mais uma vez, mencionamos o modelo estabelecido pelas RNs 323 e 395 da ANS. Delineamos maiores explicações em nosso FAQ (<https://unidas.org.br/faq-lgpd/>), principalmente na parte

que trata do encarregado de proteção de dados."615491": "Sim, por exemplo, quando o provocado não é o agente de tratamento, ou em outras hipóteses como, por exemplo, quando não é possível confirmar a identidade do solicitante (§ 4º, do art. 18 da LGPD). Além disso, havendo canais claros ao titular, é possível negar o direito à confirmação, a nosso ver, quando o titular não utiliza o meio adequado para a solicitação (p. ex., envia para o endereço errado em relação ao informado no aviso de privacidade). Há, ainda, situações em que a solicitação já foi respondida, mas o titular reitera o mesmo pedido de confirmação para criar um imbróglio (má-fé)."

"615492": "Entendemos que as informações necessárias são o nome (razão social e fantasia), dados de contato (para a requisição), e o CNPJ."

"615489": "A nosso ver, com base no art. 5º, VII e art. 50, caput, ambos da LGPD, o operador deverá direcionar para o controlador as requisições e fornecer o apoio necessário para a resposta."

"615490": "Entendemos que, como a LGPD é um tema transversal, esse assunto deveria ser tratado com os diversos setores, dentre os quais regulados e não regulados. Nos setores regulados, já existem informações de transparência ativa que são exigidas pelos órgãos reguladores aos controladores. Por exemplo, na saúde suplementar existe a RN 509 da ANS, que trata da disponibilização do conteúdo mínimo obrigatório de informações referentes aos planos no portal do beneficiário. Nos setores regulados que já exigem a transparência ativa, a declaração simplificada deveria ser suprida com base nas exigências dos diversos órgãos reguladores. Nos setores não regulados, a declaração deve ser inferior àqueles requisitos da declaração completa (art. 19, II), razão pela qual entendemos que, nestes casos, a declaração simplificada poderá ocorrer quando o titular pede apenas um aspecto do direito de acesso ou confirmação de existência. Exemplo: o titular pede informações apenas sobre o rastreamento do seu IP ou e-mail para receber propaganda."

"615494": "Entendemos que as informações que devem ser exibidas independentemente de requerimento são aquelas previstas no art. 9 da LGPD, com destaque para situações objeto de tratamento automatizado capazes de afetar os interesses do titular (art. 20 da LGPD). Na saúde suplementar, a declaração simplificada sobre o direito de confirmação de existência e de acesso deve ser satisfeita com as informações já disponíveis no portal do beneficiário (art. 7º da RN 509 da ANS)."

"615493": "Sim, conforme previsto na própria LGPD."

"615502": "Entendemos que ao tratar sobre a portabilidade de dados, o setor bancário teria maturidade avançada por conta open banking (Resolução BCB nº 206, de 22/3/2022). A telefonia possui a portabilidade de números (Resolução nº 73/1998 da Anatel). A saúde suplementar, muito embora possua o padrão TISS (RN 501), que estabelece um padrão de troca de informações, ainda possui muitas dificuldades em relação a portabilidade de dados, a começar pelos dados de prontuário, pois há operadoras de planos de saúde que possuem rede própria de atendimento (clínicas e hospitais). Como o modelo brasileiro de prontuário é segregado (cada estabelecimento possui o seu obedecendo às normas do CFM), existe ainda um grande problema de interoperabilidade dos dados de prontuário, que aos poucos tem sido combatido com iniciativas como a Rede Nacional de Dados de Saúde – RNDs."

"615501": "Como dito acima, dentro da saúde, por exemplo, cada setor possui um padrão de troca de informações como, por exemplo, o TISS. Contudo, esses padrões estabelecidos não abarcam todo o setor. Então, inicialmente, o desafio para a saúde é a diversidade de mercado e de agentes, o que se diferencia dos setores bancários e de telefonia. Além disso, existe o desafio de uma linguagem padrão e de porte tecnológico para implementação de uma portabilidade plena. Existem muitos agentes com porte econômico completamente diferente. Por exemplo, pequenos consultórios terão dificuldade com a portabilidade."

"615505": "Os componentes do padrão TISS são um bom exemplo para garantir a interoperabilidade (art. 6º da RN 501 da ANS), quais sejam: I –

organizacional; II - conteúdo e estrutura; III - representação de conceitos em saúde; IV - segurança e privacidade; e V - comunicação. Recomendamos, ainda, os trabalhos da ANS a respeito deste tema: https://www.gov.br/ans/pt-br/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-2013-tiss/PadroTISS_ComponenteOrganizacional_202207.pdf e <https://www.gov.br/ans/pt-br/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-2013-tiss/janeiro-2024.>","615503":"Sim, entendemos que sim, sob pena de ser exigido demasiado esforço ao agente.","615504":"Sim, diante das complexidades e dificuldades dos diversos setores, sendo impossível a ANPD estabelecer uma regra única sem graves impactos. O prazo deverá ser definido por meio de reuniões entre a ANPD e os principais agentes do setor na forma do art. 50, caput, da LGPD.","615511":"Inicialmente, a indicação deve ser de iniciativa do próprio titular, seja por meio de contato espontâneo, seja por meio de campanhas de atualização cadastral. Ao indicar um dado como inexato, incompleto ou desatualizado, o titular deve indicar a correção juntamente com os documentos comprobatórios, se aplicável, para a correção, conforme podemos adotar por analogia com base no art. 4º da Lei do Habeas Data. Além disso, a ANPD pode usar como referência procedimentos de outros órgãos reguladores como a retificação do SIB da ANS.","615514":"Principalmente situações em que forem afetados direitos de terceiros. Como exemplo, podemos citar os casos de elegibilidade de dependentes em planos de saúde. Nesses casos, as operadoras de planos de saúde têm exigido documentos comprobatórios da informação como, por exemplo, a apresentação de certidão de casamento (RN 557 da ANS). Outro exemplo são situações que afetam direitos nos contratos, por exemplo, o comprovante de residência para algumas situações contratuais. Contudo, mudanças simples como a de um telefone não demandarão documentos, caso comprovada a identidade do titular de dados.","615513":"Entendemos que deve ser avaliado caso a caso de acordo com o porte econômico e as capacidades tecnológicas de uma organização. Vamos pensar, por exemplo, em uma associação que realiza eventos. Nesse evento temos patrocinadores, expositores, prestadores de serviço de tecnologia, logística, segurança, dentre vários outros. Vamos imaginar que o nome ou um sobrenome de um participante tenha sido redigido de forma equivocada, mas que o erro seja tão insignificante que não impeça a entrada no evento, ou que não traga nenhum prejuízo ao titular. Nesta hipótese não faria sentido o esforço em comunicar todos os terceiros que possuem o dado incorreto apenas para comunicar a retificação.","615512":"Sim, naquelas situações em que a legislação não permite a correção no documento, mas sim uma anotação, caso a informação inserida não seja correta. A legislação também pode limitar a anotação apenas a determinados agentes (Res. 1.827 do CFM). Exemplo, no prontuário médico, dados cadastrais podem ser atualizados, contudo, o conteúdo dos procedimentos não está sujeito a correção pelo titular, pois apenas os profissionais de saúde podem anotar no documento, de acordo com aquilo que eles entendem que ocorreu. ","615517":"Não. Entendemos que o titular, como agente possivelmente leigo, deve ter o direito de fazer o requerimento independentemente de justificativa, cabendo ao agente de tratamento negá-lo, caso exista impedimento lícito no cumprimento. Porém, isso não deve permitir ao titular utilizar-se da má-fé, por exemplo, reiterando requerimento já realizado sucessivas vezes, ou realizando o mesmo requerimento com outras palavras. Entendemos que nesse caso deverá ser aplicada uma regra similar ao inciso 5 do art. 12 do GDPR, devendo o titular pagar uma taxa caso o pedido seja reiterado injustificadamente.","615516":"Como o art. 13 e o art. 16 deixam claro que a anonimização afasta a aplicação da LGPD e a necessidade de eliminação, entendemos que sim.","615518":"O agente deverá interromper imediatamente o tratamento. Entendemos que a expressão “em caso de descumprimento ao disposto nesta Lei”

se trata de situações em que não é mais justificável a hipótese de tratamento adequada, ou que o tratamento não utilizou a hipótese correta. Desse modo, há que se aplicar a proporcionalidade no caso concreto (art. 27 da Res. 4 da ANPD) para que seja verificada a necessidade ou não de punição ao agente de tratamento. ";615523": "Conforme entendimento europeu não necessariamente, se o agente possui outra hipótese de tratamento (finalidade) que justifique a utilização do mesmo dado (art. 17, I, alínea b, e III, do GDPR). Nessa linha, um dos exemplos dado pelas Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/679 é a necessidade de conservação dos dados. Vale destacar que o art. 16 da LGPD permite a conservação dos dados em algumas hipóteses como o cumprimento de obrigação legal e regulatória.";615521": "Entendemos que deve ser aplicado o que dispõe as Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/679, ou seja, "[...] se o consentimento for retirado, todas as operações de tratamento de dados baseadas nesse consentimento e que ocorreram antes da retirada do consentimento – e em conformidade com o RGPD – permanecem lícitas. Contudo, o responsável pelo tratamento deve parar as ações de tratamento em causa. Caso não exista qualquer outro fundamento jurídico que justifique o tratamento (p. ex. continuação da conservação) dos dados, estes devem ser apagados pelo responsável pelo tratamento";615617": "Decisão automatizada, nos termos das Diretrizes sobre tomada de decisões individuais automatizadas e criação de perfis para efeitos do Regulamento 2016/679, é a decisão tomada por meios tecnológicos. Uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é a capacidade de tomar decisões por meios tecnológicos sem envolvimento humano. Na última situação, a tecnologia toma a decisão final sem participação humana (ex. uma câmera de velocidade que aplica multas). Na área de saúde um exemplo é a utilização de sistemas que fazem a leitura de diretrizes de utilização - DUT, conforme regras da ANS, para negar ou autorizar procedimentos médicos.";615618": "Entendemos que deve ocorrer um prejuízo comprovado ao titular, seja em seu patrimônio ou em sua vida (incluindo direitos da personalidade). Ex: o titular deixou de receber um empréstimo.";615619": "O primeiro desafio é a explicação sobre os critérios da decisão, o que não é tarefa fácil considerando titulares leigos. O segundo desafio, a nosso ver, é conferir esta transparência ao titular sem violar segredos comerciais e/ou industriais.";615620": "Sim, quando não se enquadrarem na hipótese no art. 20, ou seja, não constituírem decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses do titular. Em outras palavras, o caso pode envolver uma decisão não tomada unicamente com base em tratamento automatizado ou não afetar o interesse do titular, como exemplo decisões baseadas em normas regulamentadoras do segmento. Nesta hipótese, é possível a negativa."

{ "615450": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); Primeiramente, importante destacar que o atendimento aos direitos dos titulares não é tarefa trivial e pode ser bastante complexo. Adotar prazos similares aos da Lei n. 12.527/2011, também conhecida como Lei de Acesso à Informação - LAI, pode ser desafiador em face das diferenças específicas entre o tratamento de dados pessoais e o acesso à informação pública. Nesse sentido, entendemos necessário que seja estipulado prazo compatível com a complexidade no caso dos direitos dos titulares, a exemplo do prazo semelhante previsto no GDPR (1 mês prorrogável até 2 meses a contar do recebimento do pedido). O prazo previsto na LAI poderia ser considerado como prazo mínimo a ser adotado pela ANPD, mas entendemos pertinente que a ANPD regule prazos maiores do que os previstos na LAI, especialmente no caso de setores que tratam grandes volumes de dados, como é o caso do financeiro, e no caso de controladores de maior porte. Assim, consideramos que o prazo deveria ser de, no mínimo, 30 dias, prorrogáveis por mais 30 dias.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como

previstos nos incisos I e II do caput do art. 19 da LGPD?: "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); Primeiramente, reforçamos que o prazo de 15 dias previsto no art. 19, II, da LGPD não deve ser diminuído em nenhuma hipótese pela regulamentação, dada a sabida complexidade que envolve o atendimento aos direitos de acesso e confirmação de tratamento. Assim, os prazos diferenciados a serem oportunamente definidos pela ANPD devem ser maiores do que o prazo de 15 dias (vide os nossos comentários ao item anterior) e sua definição pode levar em consideração alguns critérios, tais como os indicados a seguir: (i) o pedido do titular e a sua complexidade, inclusive a natureza dos dados, quantidade/volume de dados, período e a complexidade dos tratamentos de dados pessoais que, inclusive, podem envolver outras partes (como operadores) e diversas fontes; (ii) a quantidade de solicitações recebidas pelo controlador, ressaltando que há ferramentas atualmente no mercado que automatizam o envio de grandes números de solicitações individuais de titulares ao controlador ao mesmo tempo ou em blocos, gerando maior complexidade no atendimento das solicitações; (iii) setores que lidam com quantidade relevante de dados e de titulares, como é o caso do setor financeiro, entre outros; (iv) o porte dos agentes, considerando que agentes de maior porte podem lidar com maior complexidade decorrente do atendimento aos direitos dos titulares.", "615484": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); A definição do canal de contato e do seu formato devem ficar a critério do controlador, que pode aproveitar canais já existentes, ou ter um ou mais canais próprios para exercício dos direitos a depender da sua estrutura ou do tipo de relacionamento com o titular (por exemplo, se já é cliente ou não, se é colaborador ou não etc.). Da mesma forma, o formato do canal deve ficar a critério do controlador (meios digitais, como plataforma com área logada, atendimento telefônico, e-mail etc.). O mínimo é que o canal garanta a comunicação com o controlador e o recebimento da demanda pelo controlador, além da possibilidade de verificação da identidade do titular pelo controlador. Outros fatores que podem ser levados em conta são: fácil acesso e divulgação do canal de acordo com o previsto na LGPD, clareza nas informações fornecidas ao titular, segurança, possibilidade de registro e acompanhamento das solicitações e capacitação do canal para atender às solicitações dos titulares. ", "615485": "Contribuição enviada em nome da Federação

Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); Entendemos que os operadores de dados possuem responsabilidade de cooperar com os controladores no atendimento dos direitos dos titulares, principalmente, no que diz respeito ao tratamento de dados pessoais que esteja sobre sua atribuição. Nesse sentido, sua cooperação abrange o auxílio, tempestivo, aos controladores, subsidiando-os com dados pessoais ou com informações sobre o tratamento dos dados do titular, além de atenderem às instruções do controlador caso seja necessário concretizar alguma ação relativa ao atendimento de algum direito (como, por exemplo, a exclusão de dados, quando for cabível). Também é responsabilidade dos operadores repassar aos controladores requisições que venham a receber dos titulares, além de manter as informações atualizadas sobre a guarda dos dados que estejam sob sua responsabilidade. Porém, entendemos que os operadores não devem atender ou responder diretamente ao titular sem a anuência ou orientação nesse sentido pelo controlador, pois a obrigação de atendimento dos direitos é do controlador e os operadores podem compartilhar informações incorretas ou incompletas sobre o tratamento dos dados pessoais.";"615486": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); Muito embora haja pontos nas normas do SAC já adotados de forma semelhante na LGPD (como atendimento gratuito e sem ônus ao consumidor), entendemos que a adoção de diretrizes e procedimentos análogos ao Serviço de Atendimento ao Consumidor ("SAC") não seriam aplicáveis no caso de atendimento aos direitos dos titulares, considerando a temática e a especificidade de solicitações atreladas aos direitos dos titulares. Além disso, entendemos que diversos critérios previstos no caso do SAC seriam de difícil implementação, ou mesmo inváveis considerando o contexto de dados pessoais, por exemplo: disponibilidade de um canal de atendimento 24h (art.4º); criação de canal para acesso ao histórico das reclamações (art.12); atendimento telefônico obrigatório (art. 4º, §2º), o acesso inicial ao atendente não será condicionado ao fornecimento prévio de dados pelo consumidor (art. 4º, §4º) etc. Por isso, acreditamos que o canal de atendimento do encarregado deve ser formatado de acordo com as diretrizes e peculiaridades de cada instituição. Além disso, entendemos que tais requisitos não foram trazidos pela LGPD.";"615487": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS); É bastante complexo definir um modelo como paradigma, considerando que há diversos modelos de atendimento possíveis e diferentes perfis de controladores e de setores específicos. Além disso, as características do canal podem variar de acordo com o tipo de relacionamento que o controlador possui com o titular, que pode ser direto ou não. Assim, muito embora haja modelos que se mostram eficientes, como o atendimento em formato digital aos titulares, inclusive por meio de "área logada", por exemplo, ou o fornecimento de reportes mais enxutos de forma mais rápida, com a possibilidade de complementação ou esclarecimento de dúvidas se necessário, entendemos que não deve haver uma definição de paradigma ou modelo único, cabendo a cada controlador adotar a solução mais adequada ao seu ambiente e estrutura. Não obstante, no que se refere ao atendimento simultâneo de grande volume de solicitações, é possível a adoção de chatbots utilizando recursos de inteligência artificial, com intuito de automatizar o atendimento ao cliente final, momento em que caberia às equipes o atendimento das questões mais específicas e complexas realizadas em horário comercial, em qualquer caso, com prazo adequado para resposta. Finalmente, outro ponto importante a ser levado em consideração é a segurança do canal, permitindo a verificação da identidade do titular.";"615491": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões

de Crédito e Serviços (ABECS); Entendemos ser possível a negativa ao direito de confirmação da existência do tratamento no caso de atos ilícitos e prevenção a fraudes e quando não for possível validar a identidade do titular, inclusive de seus representantes, pois há o risco de disponibilização de informações para quem não seja o titular, ou mesmo para fraudadores ou pessoas mal intencionadas. Também entendemos possível a negativa no caso de situações de cumprimento de obrigação legal/regulatória atreladas a combater a lavagem de dinheiro e o terrorismo que podem vedar o fornecimento de informações a esse respeito ao titular. ","615492":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Importante destacar que o conceito de uso compartilhado não é claro na LGPD e gera dúvidas sobre o seu alcance e interpretação. De qualquer forma, entendemos que não é qualquer situação de compartilhamento que deve ser considerada como uso compartilhado. Além disso, não é tarefa trivial que o controlador, especialmente considerando o dinamismo das operações de tratamento, o volume de dados e de agentes de tratamento envolvidos, tenha a informação disponível e extremamente granular, titular a titular, de todos os compartilhamentos realizados especificamente no contexto de uso compartilhado, ainda mais para informar nos curtos prazos de atendimento a direitos dos titulares. A informação relevante para fins atendimento aos direitos do titular são os tipos ou categorias de entidades com as quais pode ser realizado o uso compartilhado de dados, sem que seja necessário informar especificamente esses controladores. Se o titular tiver dúvidas específicas, o controlador pode esclarecer, na medida em que for possível e viável, fornecendo o nome do controlador. Ademais, o fornecimento de informação sobre controladores no contexto de uso compartilhado de dados não deve ferir o segredo empresarial, que também é passível de proteção. ","615489":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que os operadores de dados possuem responsabilidade de cooperar com os controladores no atendimento dos direitos dos titulares, principalmente, no que diz respeito ao tratamento de dados pessoais que esteja sobre sua atribuição. Nesse sentido, sua cooperação abrange o auxílio, tempestivo, aos controladores, subsidiando-os com dados pessoais ou com informações sobre o tratamento dos dados do titular, além de atenderem às instruções do controlador caso seja necessário concretizar alguma ação relativa ao atendimento de algum direito (como, por exemplo, a exclusão de dados, quando for cabível). Também é responsabilidade dos operadores repassar aos controladores requisições que venham a receber dos titulares, além de manter as informações atualizadas sobre a guarda dos dados que estejam sob sua responsabilidade. Porém, entendemos que os operadores não devem atender ou responder diretamente ao titular sem a anuência ou orientação nesse sentido pelo controlador, pois a obrigação de atendimento dos direitos é do controlador e os operadores podem compartilhar informações incorretas ou incompletas sobre o tratamento dos dados pessoais. ","615490":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Cada controlador dispõe de dados diferentes para compor a declaração em formato simplificado. Com isso, entendemos que, minimamente, deverão ser apresentados os dados pessoais referentes ao relacionamento do titular com o controlador e por esse coletados, como os dados cadastrais (por exemplo, CPF, nome completo, número de documento de identificação, endereço, telefone, e-mail etc.), assim como informações mínimas sobre o tratamento de dados, ressalvadas as informações protegidas por sigilo. ","615494":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). As informações

mínimas sobre o tratamento de dados pessoais fornecidas sem requerimento seriam aquelas sobre as principais finalidades de tratamento e tipos de dados pessoais que podem ser tratados. Referidas informações são objeto dos avisos/políticas de privacidade divulgadas pelos controladores. Os critérios e procedimentos usados no caso de decisões automatizadas devem ser fornecidas quando solicitado pelo titular, conforme previsto no art. 20, §1º, da LGPD. ","615493":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que sim. Ainda, observando a autonomia privada das instituições, muito embora o formato da transmissão da informação possa ser escolhido pelo titular, entendemos que o mais apropriado é que o controlador defina o meio que atenderá os direitos, como o digital, que é o mais comum, podendo o titular solicitar a via impressa. É também possível que o formato digital fornecido permita que o titular imprima o documento, caso assim deseje. ","615502":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). A implementação de portabilidade diretamente entre agentes de tratamento mostra-se extremamente complexa, mesmo em setores que já possuem iniciativas que possuam algum tipo de semelhança. Como exemplo dessas iniciativas, citamos as regulamentações do setor financeiro relacionadas à portabilidade de determinados produtos, como consignado, financiamento e outras operações de crédito, além do Open Finance, que viabiliza o compartilhamento de dados dos clientes entre as instituições financeiras participantes (por exemplo, a Resolução BCB 4292/2013, a Resolução CMN n. 5.057/2022, além da Resolução Conjunta nº. 1 e outras relacionadas ao Open Finance). Também como exemplo, citamos a portabilidade numérica de telefonia fixa e móvel no setor de telecomunicações. Muito embora existam iniciativas com alguns pontos de semelhança, entendemos que os desafios da portabilidade de dados diretamente entre agentes são grandes e que nenhum setor estaria totalmente maduro para a sua implementação. Ademais, entendemos que não há maturidade para a portabilidade de dados diretamente entre controladores de setores distintos. De qualquer forma, tendo em vista sua complexidade e potenciais impactos, é importante que qualquer iniciativa de portabilidade específica em setores regulados seja regulamentada também pelo órgão regulador do respectivo setor econômico, inclusive considerando as regulamentações já existentes sobre o tema de modo a otimizar a adoção de soluções já existentes, considerando o que já está implementado como suficiente e dentro do escopo de portabilidade de dados, evitando-se ônus desproporcionais aos agentes do setor. Ainda, entendemos também possível considerar a implementação de soluções mais simples para a portabilidade entre agentes do mesmo setor. Finalmente, destacamos alguns pontos importantes sobre o escopo de dados considerando tanto o direito de acesso, quanto o de portabilidade. No Recital 68 do GDPR, o direito de portabil","615501":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Os desafios são inúmeros e extremamente complexos. Vão desde a definição de padrões comuns de escopo e de dados e de participantes, compatibilidade tecnológica, padrão de conexão entre sistemas/ferramentas e padrões e requisitos técnicos de implementação, como medidas de segurança e aquelas relacionadas à integridade dos dados. Ainda, adicionam-se as dificuldades, ônus e custos elevados relacionados à implementação em si, considerando também o esforço nada desprezível para que os dados e arquivos sejam convertidos em formato padrão. A experiência com iniciativas semelhantes mostra que os obstáculos são inúmeros e que a implementação tem impactos grandes nos controladores, não sendo, de forma alguma, um tema simples. ","615505":"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN)

e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Padronização é algo bastante complicado de se alcançar, ainda mais considerando a enorme diversidade de controladores dos mais variados setores e graus de maturidade. Entendemos que o mais recomendável seria não definir padrões específicos, mas caso se pretenda delimitar alguns a título de orientação aos agentes de tratamento, os formatos mais simples e acessíveis deveriam ser priorizados. Colocar complexidade pode criar barreiras e ônus desproporcionais aos controladores. Por exemplo, o formato PDF é um padrão amplamente utilizado e de fácil manuseio tanto pelos controladores, quanto pelos titulares de dados. Outros formatos que podem ser considerados são XML, CSV ou JSON. Como mencionado na resposta acima, há outros fatores que podem impactar, como escopo de dados, garantindo que os conceitos e termos sejam os mesmos e protocolos de comunicação."

"615503": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que sim, tendo em vista que o direito à portabilidade deve ser considerado plenamente satisfeito quando o agente de tratamento disponibiliza os dados pessoais a seu titular para que este possa, caso assim deseje, transferir seus dados para outro agente de tratamento, em atendimento à autonomia e ao controle do titular sobre os seus dados pessoais."

"615504": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Sim, entendemos possível e razoável a definição de padrões de interoperabilidade específicos pelo setor privado relacionadas a certas atividades econômicas para fins de portabilidade. A autorregulação, que inclusive pode ser implementada por meio de associações comerciais ou empresas certificadoras, pode ser um instrumento importante para esse fim. Qualquer prazo que venha a ser definido para tal propósito não deve ser inferior a 24 meses, podendo ser prorrogado."

"615511": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Um dado pode estar incorreto, inexato ou desatualizado quando, por exemplo, há mudança de algum dado cadastral (o titular muda de endereço, telefone, nome completo, e-mail para contato etc.) ou mesmo quando um dado é atribuído a determinado titular erroneamente. Além disso, podem ser assim considerados os dados sem verificação/atualização dos dados, assim como a ausência de informação e/ou informação incompleta/incorreta, além daquelas que não identifiquem um titular corretamente. Importante ressaltar que, muitas vezes, a atualização dessas informações depende também de informação e comprovação pelo próprio titular."

"615514": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). O titular pode sempre exercer o direito à correção, mas para a sua implementação, é necessária a comprovação ou verificação com documentos e/ou informações (como, por exemplo, comprovação de endereço, outros dados cadastrais ou de titularidade de algum bem ou direito). Além disso, o titular deve ser devidamente identificado e autenticado para exercer os seus direitos, além de comprovar a veracidade das informações. Ainda, pode haver situações em que pessoas mal intencionadas queiram se fazer passar pelo titular de dados para alterar propositadamente dados pessoais, para fins ilícitos. Além disso, quando a atividade de tratamento for verificação de identidade ou detecção de fraude, a manutenção de dados pode ser essencial."

"615513": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). O disposto no art. 18, §6 é bastante complexo de ser implementado por diversos motivos. Um deles é o atendimento "de maneira imediata" que é difícil, ou mesmo inviável de se implementar na prática. Além disso, o conceito de uso compartilhado traz

dificuldades de interpretação e de delimitação acerca de sua aplicabilidade, pois o texto da LGPD não é claro. De qualquer forma, nos parece que não é qualquer compartilhamento que deve ser considerado como uso compartilhado. Outros fatores que podem ser considerados para avaliar a impossibilidade ou esforço desproporcional são: (i) o uso compartilhado pode ter ocorrido há muito tempo e o controlador pode não ter mais contato com o outro controlador; (ii) a quantidade de controladores com os quais o uso compartilhado foi realizado poderia inviabilizar a sua comunicação; (iii) a viabilidade prática e os custos e recursos necessários para processamento da comunicação; (iv) a infraestrutura tecnológica e o impacto na operação do controlador; (v) a complexidade e o volume de dados pessoais tratados. Importante ressaltar que a obrigação do controlador se resume ao envio da comunicação, mas não há ingerência ou responsabilidade em relação às providências que serão, ou não, adotadas pelo outro controlador."

615512:"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Sem prejuízo de outras situações, entendemos ser possível a negativa ao direito de correção nos casos em que: (i) não é possível identificar o titular para o exercício dos seus direitos; (ii) o titular não comprove a alteração do referido dado pessoal e/ou o controlador não consiga meios para comprovação/verificação de que o dado informado seja válido e correto; (iii) quando a atividade de tratamento for verificação de identidade ou detecção de fraude; (iv) quando o controlador identificar se tratar de pedido não realizado pelo titular ou em casos de fraude; (v) quando o dado pessoal informado pelo titular for incorreto ou seja fornecido de forma propositadamente incorreta pelo titular; (vi) se o pedido é manifestamente infundado, como por exemplo, se o titular claramente não tem intenção de exercer seu direito de retificação, mas pretende obter algum benefício da organização ou declara que a intenção do pedido é causar entraves ou perturbações à organização ou a colaboradores específicos da instituição; (vii) o titular envia sistematicamente grandes volumes de solicitações ao controlador com a intenção de causar entraves ou interrupções, inclusive repetindo o conteúdo de pedidos anteriores já atendidos. Tais situações dependem das circunstâncias particulares e devem ser analisadas caso a caso pelo controlador."

615517:"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos ser necessária a fundamentação e demonstração por parte do titular na solicitação de atendimento dos seus direitos, considerando que a fundamentação para os pedidos de anonimização, bloqueio, eliminação e oposição é necessária para a compreensão do pedido pelo controlador, que deve avaliar se o pedido é cabível ou não. Isso porque, muitas vezes o titular realiza o pedido com base em sua mera percepção pessoal sobre a desnecessidade, excessividade ou desconformidade do tratamento, sem real embasamento ou por desconhecimento de alguma obrigação legal ou outra necessidade do controlador que justifique o tratamento. Assim, diante da alegação sobre a desnecessidade, excessividade ou desconformidade do tratamento, o titular deve fundamentar e justificar sua alegação, assim como o controlador deve fundamentar o respectivo tratamento."

615516:"Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos ser possível que a anonimização e a eliminação de dados sejam adotadas de forma alternativa, considerando inclusive o previsto no art.16, IV da LGPD em que os dados pessoais poderão ser conservados para uso exclusivo do controlador. Ademais, o controlador deverá avaliar qual dos procedimentos seria mais recomendável, considerando a necessidade de manutenção ou não dos dados pessoais, cumprimento de obrigações legais, custos, etc."

615518:"Contribuição enviada em nome da Federação Brasileira de Bancos

(FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que se a oposição ao tratamento de dados pessoais do titular for considerada legítima pelo controlador ou pela autoridade competente, o controlador deverá cessar o tratamento daqueles dados pessoais em relação às finalidades para as quais foram considerados desnecessários, excessivos ou em desconformidade com a LGPD, e seguir com a exclusão, anonimização ou bloqueio, se aplicável, nos termos da LGPD e nos limites técnicos da atividade. Ressalta-se que o tratamento de dados pessoais para outras finalidades pode ser preservado."

"615523": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que não é necessário eliminar os dados apenas em razão da revogação consentimento. Isso porque, como o próprio art. 8º, §5º, da LGPD determina, são ratificados os tratamentos realizados sob o amparo anteriormente manifestado enquanto não houver requerimento de eliminação. Além disso, os dados podem ser tratados com fundamento em outra base legal que justifique a sua manutenção ou tratamento, inclusive para cumprimento de obrigações legais e regulatórias ou para exercício regular de direitos, por exemplo. Ademais, mesmo no caso do consentimento, os dados pessoais referentes a um tratamento de dados também poderão ser mantidos nas hipóteses do Art.16 da LGPD."

"615521": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Após o requerimento de eliminação dos dados pessoais tratados com base no consentimento revogado, o controlador deverá observar o disposto nos artigos 15, III, e 16, da LGPD, tanto para proceder à eliminação dos dados, observado o âmbito e nos limites técnicos das atividades, quanto para fundamentar a guarda dos dados (art.16), se for o caso. Importante também avaliar se a eliminação dos dados pessoais pode causar algum impacto na prestação dos serviços ao titular ou se há outras bases legais aplicáveis ao tratamento dos dados pessoais."

"615617": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que ambos os conceitos foram utilizados com o mesmo significado no art. 20 da LGPD para se referir a decisões tomadas unicamente com base em tratamentos automatizados. De qualquer forma, importante diferenciar as decisões automatizadas das informações/dados pessoais considerados para a tomada de tal decisão."

"615618": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Não obstante o disposto no art. 4º, §2º, da Resolução CD/ANPD nº 02/22, que trazem critérios interpretativos sobre tratamentos de dados pessoais que possam afetar significativamente interesses do titular, entendemos que um dos principais critérios para determinar quando um interesse está sendo efetivamente afetado é a própria identificação de prejuízos de fato relevantes e a gravidade do impacto sobre direitos fundamentais do titular. Não é razoável que qualquer decisão automatizada seja passível de revisão, devendo tal fato ocorrer no caso de interesses relevantes e sobre os quais a decisão possa de fato afetar significativamente."

"615619": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Com o aumento da utilização de tecnologias, como a inteligência artificial, em diversos setores da sociedade para facilitar as tomadas de decisão automatizada, nos parece que os desafios práticos estarão atrelados à eventual maior complexidade da forma de tomada de decisão e dos fatores levados em consideração para tanto, bem como ao maior volume de decisões que possam vir a ser tomadas unicamente com base em tratamento automatizado (sempre considerando as que de fato possam afetar significativamente os interesses do titular e eventual dificuldade nessa definição na

prática), o que pode gerar maior demanda e complexidade operacional para implementar processos práticos de revisão, os quais, a critério do controlador, podem ser tanto de forma também automatizada (unicamente ou não), como com intervenção humana. Outro ponto a ser levado em consideração é a própria definição das decisões que estariam sujeitas à revisão. A título de exemplo, o documento "Guidelines on Automated individual decision-making and Profiling" do Grupo de Trabalho EDPB / WP 29, traz como desafio prático determinar o nível de intervenção humana em um processo automatizado para considerar se o processo ou decisão foi realmente tomada "exclusivamente com base no tratamento automatizado de dados pessoais". Se há um nível de envolvimento humano no processo, então a decisão não foi tomada apenas com base no tratamento automatizado de dados pessoais e não ensejaria o direito à revisão previsto no art. 20, da LGPD. ",615620": "Contribuição enviada em nome da Federação Brasileira de Bancos (FEBRABAN) e Associação Brasileira de Cartões de Crédito e Serviços (ABECS). Entendemos que o controlador pode negar o direito de revisão sobre decisões automatizadas, sem prejuízo de outras situações, quando: (i) não for possível validar a identidade do titular; (ii) não se tratar de decisão automatizada; (iii) a decisão não puder afetar significativamente interesses do titular; (iv) a decisão estiver atrelada a fatos com origem ilícita, como, por exemplo quando a decisão automatizada for fundamentada em razões de fraude; (v) a revisão exponha segredo empresarial ou exija esforço/custo/tempo desproporcional. De qualquer forma, importante pontuar que a revisão da decisão não necessariamente implicará na mudança da decisão tomada, mas apenas que houve uma revisão dessa decisão a pedido do titular."

{ "615450": "É imprescindível que no estabelecimento de prazos pela ANPD, dentro do contexto dos dados pessoais, a Autoridade leve em consideração a necessidade de respostas mais imediatas e prazos mais curtos, tendo em vista a demanda por um atendimento personalizado quando falamos em proteção de dados pessoais uma vez que há regulamentação específica disposta, qual seja, a LGPD.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "Podemos considerar como critérios: Natureza dos Dados Violados; Extensão da Violação; a Gravidade dos Danos Potenciais; Complexidade das solicitações; as Circunstâncias Específicas; Cooperação com a ANPD; a finalidade e urgência; e, o Histórico de Conformidade. Esses critérios podem orientar as organizações na avaliação da gravidade e urgência de uma violação de dados, ajudando na aplicação dos prazos estipulados pela LGPD de maneira diferenciada de acordo com a natureza do incidente.", "615484": "Podem ser consideradas como características essenciais àquelas que possuem o objetivo de assegurar transparência na comunicação, acessibilidade, clareza e eficiência na troca de informações, respeitando os princípios da privacidade e proteção de dados, incluindo um atendimento rápido, horários de atendimento estendidos até às 20h durante a semana, com a possibilidade de um atendimento diferenciado aos finais de semana, a segurança da informação, simplicidade do canal, canais diversificados, treinamento de agentes, registro de atividades, atualizações e melhorias constantes.", "615485": "Sim, os operadores têm responsabilidade na concretização dos direitos dos titulares dos dados, uma vez que realizam o tratamento de dados em nome dos controladores, sendo contratados por estes para realizar atividades específicas de processamento de dados, sendo que, além dos operadores toda a cadeia de agentes relacionados devem estar cientes e cumprindo com os direitos dos titulares. Ao pensarmos em maneiras para cooperação entre os operadores e controladores, temos o estabelecimento de contratos, compartilhamento de informações, treinamento e conscientização, segurança da informação, notificação de incidentes, registro de atividades, auditorias, monitoramento e atualização de informações.", "615486": "O Serviço de Atendimento ao Consumidor (SAC) tem o objetivo de garantir o atendimento eficiente e transparente aos consumidores. Ocorre que a aplicação direta dessas diretrizes para o exercício dos direitos do titular de dados pessoais pode não ser totalmente adequada tendo em vista alguns motivos, quais sejam, exemplificativamente: o tratamento diferenciado por tipo (meio) de canal de atendimento (telefone, e-mail, chat) uma vez que no contexto de proteção de dados pessoais há uma necessidade de uniformidade no atendimento (mesmos prazos, por exemplo); prazos mais longos para resposta, sendo que no contexto dos dados pessoais há necessidade de respostas mais imediatas e prazos mais curtos; e, atendimento personalizado que é demandado quando se fala em proteção de dados pessoais e há uma regulamentação específica.", "615487": "Sim, um modelo de atendimento que poderia servir como paradigma para lidar com grandes volumes de demandas com economicidade é o sistema de atendimento ao cliente via chatbots e automação de processos. Tanto o setor privado quanto o setor público têm adotado cada vez mais soluções de inteligência artificial (IA) e automação para melhorar a eficiência e reduzir os custos operacionais no atendimento ao cliente ou cidadão. Esses sistemas são capazes de lidar com um grande volume de demandas de forma rápida, escalável e econômica. Além disso, oferecem vantagens como: Disponibilidade 24/7; Respostas Imediatas; Redução de Custo; Escalabilidade; Personalização; e, Análise de Dados. ", "615491": "Sim. Existem hipóteses em que esse direito pode ser

excepcionalmente negado desde que estejam respaldadas em determinadas disposições legais como, por exemplo: Sigilo Profissional ou Comercial; Garantia da Defesa em Processos Judiciais ou Administrativos; Impossibilidade de Confirmação da sua existência em virtude de motivos técnicos ou legais; e, Preservação da Segurança Nacional ou Ordem Pública como, por exemplo, em situações emergenciais. Nestes casos, a negativa deverá ser clara e fundamentada. ";615492": "As informações que devem ser apresentadas de maneira clara, acessível e compreensível para os titulares a fim de identificarem os controladores, podendo ser: Identificação do Controlador Principal e de Controladores Adicionais, se houver (ex. Razão social, CNPJ, Contatos); Finalidades do Tratamento; Base Legal para o Tratamento; os Dados Compartilhados; Informações de Contato dos Controladores; Possibilidade de Revogação do Consentimento; e, Transferências Internacionais se for o caso.";615489": "Transparência e Colaboração com o Controlador; Execução de Instruções do Controlador; Colaboração em Solicitações de titulares; Manutenção de registros; Segurança da Informação; Notificação de Incidentes; Participação e Colaboração em avaliações de impacto à proteção de dados pessoais; Treinamento e Conscientização. ";615490": "Finalidade do Tratamento; Forma e Duração do Tratamento; Identificação do Controlador e/ou Controladores se houver mais de um; Informações de Contato do Encarregado (DPO); Formas de Contato para Respostas a Solicitações dos Titulares; Informações sobre Compartilhamento; Direitos dos Titulares; e, Informações sobre Consentimento. Entretanto, por se tratar de um relatório simplificado, todas essas informações devem ser levadas em consideração de forma ponderada a fim de não exigir um detalhamento muito amplo e perder a sua finalidade.";615494": "Poderiam ser citadas aqui as mesmas informações que já foram detalhadas nas respostas às perguntas b & d. ";615493": "Sim, a disponibilização dos dados pessoais em formato digital e em papel, conforme escolhido pelo titular, pode ser considerada uma forma de satisfazer o direito de acesso previsto na Lei Geral de Proteção de Dados (LGPD), desde que ocorra em um formato acessível e legível.";615502": "Podemos citar como exemplo o setor de Telecomunicações, tendo em vista que as empresas de telecomunicações frequentemente lidam com a portabilidade de dados de clientes ao migrar entre provedores de serviços. Existem regulamentações específicas nesse setor que abordam a transferência de dados do titular. Além disso temos o setor da Tecnologia da Informação (TI), uma vez que as empresas de tecnologia geralmente têm maturidade em processos e tecnologias que facilitam a portabilidade de dados. Podemos observar isto em plataformas de redes sociais, serviços de e-mail e outros serviços online.";615501": "Existência de múltiplos padrões; Garantia da segurança e privacidade; o Volume e a Velocidade de dados quando pensamos em transferência eficiente de grandes conjuntos de dados em tempo real, a segurança envolvida na transferência dos dados compartilhados, bem como a automatização dos processos e a comunicação entre as organizações.";615505": "Podemos destacar a importância de padronização desde formatos de dados até protocolos de comunicação, passando mais além sobre padrões de segurança e criptografia, sendo inclusive apropriado que a Autoridade Nacional de Proteção de Dados (ANPD) disponha de um portal que facilite a padronização das informações visando uma maior segurança no processo de interoperabilidade. Ao pensarmos na criação de um portal único para lançamento de informações, isso poderá proporcionar à Autoridade Nacional de Proteção de Dados (ANPD) o aprimoramento de seus regulamentos através da observância a respeito da maturidade de todos os setores diante do tratamento de dados, conseguindo estabelecer tendências diferente para cada setor da economia. Importante levar em consideração a diferenciação com a qual poderá ser tratada cada setor a partir de critérios objetivos, tal como, o volume de dados. Dito tudo isso, tal medida ainda reforça a

missão institucional da ANPD de assegurar a mais ampla e correta observância da LGPD no Brasil e, nessa medida, garantir a devida proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade dos indivíduos."615503": "Sim, podemos considerar como adequado, uma vez que o direito à portabilidade de dados dá ao titular o poder de receber suas informações pessoais de um agente de tratamento e transmiti-las para outro, facilitando a mobilidade dos dados entre diferentes prestadores de serviços. Se o agente de tratamento for capaz de fornecer todos os dados pessoais do titular de forma interoperável, conforme previsto nas regulamentações, isso geralmente atende às expectativas do titular e aos requisitos da lei."615504": "O prazo considerado razoável pode variar dependendo do contexto e da complexidade do setor em questão. Idealmente, deve-se buscar um equilíbrio entre a necessidade de implementação eficaz e a garantia de que as organizações tenham tempo suficiente para realizar as adaptações necessárias, sendo fundamental a atuação da Autoridade Nacional de Proteção de Dados (ANPD) para garantir que o prazo seja estabelecido em observância aos princípios e diretrizes estabelecidos pelas leis de proteção de dados conforme disposto no art. 40 da LGPD. Dentro deste contexto entendemos que os padrões de interoperabilidade devem ser definidos pelo setor público, tendo em vista a atuação da ANPD como órgão regulador."615511": "Neste contexto podemos considerar os critérios objetivos a partir da definição de cada um deles, veja-se: I) Incompleto: campos obrigatórios não preenchidos e/ou informações essenciais ausentes; II) Inexato: discrepância com fontes confiáveis e/ou erro de digitação ou transcrição; e, III) Desatualizado: informações temporalmente sensíveis e/ou falha na atualização regular, inclusive mediante o uso de comparações considerando os períodos em análise."615514": "Em geral, a simples declaração do titular pode ser suficiente para o exercício do direito à correção de dados pessoais. Entretanto, a vontade do titular para que determinado dado possa ser corrigido, poderá encontrar obstáculos por motivos técnicos que impossibilitem a retificação, quando as informações fornecidas não correspondem à finalidade; quando o dado não é preciso ou ainda quando faltam informações suficientes à identificação do titular. No setor de telecomunicações temos como exemplos de que a declaração não é suficiente nos seguintes casos: Alteração de nome, endereço e em virtude de questões referente à troca de titularidade dos serviços, uma vez que essas circunstâncias demandam apresentação de documentos e não somente a declaração de vontade."615513": "O artigo 18, § 6º, da Lei Geral de Proteção de Dados (LGPD) no Brasil trata da impossibilidade ou do esforço desproporcional para a correção, anonimização, bloqueio ou eliminação de dados pessoais. Nesse contexto, ao avaliar a impossibilidade ou o esforço desproporcional, alguns critérios objetivos podem ser considerados, tais como a natureza e o volume de dados, a complexidade técnica, custo financeiro e os recursos disponíveis."615512": "Podemos citar como exemplo as mesmas situações em que a simples declaração do titular não seria suficiente para o exercício do direito à correção, uma vez que ao mesmo tempo elas podem ser insuficientes para a retificação, elas podem ser utilizadas como justificativa para negativa da retificação. Podemos tomar como exemplo as suspeitas de fraude, o que acarretariam na negativa de retificação. Sendo que, inclusive neste caso, a negativa deve estar baseada em uma explicação clara e transparente devidamente justificada sobre essa impossibilidade do controlador ao titular."615517": "Não, tendo em vista que cabe ao controlador a justificativa do motivo do não atendimento à solicitação, uma vez que é o controlador quem possui o conhecimento técnico necessário."615516": "Sim, em casos de uso dos dados internamente como, por exemplo, para acompanhamentos de relatórios internos, como nos casos de cancelamentos, inadimplências, etc. Inclusive podemos adotar a técnica da pseudonimização quando

necessária e alternativamente à anonimização e eliminação.”;615518”:”Ocorreria o encerramento do tratamento de dados pessoais com o consequente envio do relatório final ao titular comprovando a exclusão dos dados pessoais, ou seja, a comprovação de que foram realizadas as devidas tratativas para o caso em questão.”;615523”:”Não, a revogação do consentimento não implica necessariamente na necessidade e/ou na solicitação de exclusão dos dados uma vez que a solicitação de exclusão precisa ser expressa neste sentido, com base no § 5º, do artigo 18, da LGPD que dispõe: “O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.””;615521”:”Impossibilidade do uso dos dados pessoais por exemplo, para uso interno do controlador, seja para fins de pesquisas de satisfação, análise de relatórios e da persona sendo o caso, ainda que de forma anonimizada ou pseudonimizada.”;615617”:”Uma decisão automatizada refere-se a um processo no qual as decisões são tomadas com o auxílio de sistemas automatizados, sem intervenção humana direta significativa, ou seja, poderá haver intervenção de atendimento humano parcial. Já uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é um cenário específico em que uma decisão é resultante exclusivamente do processamento automatizado de dados pessoais, sem a intervenção de uma pessoa na tomada de decisão.”;615618”:”Os critérios poderão ser, entre outros: Natureza do interesse; Impacto significativo em um interesse; se há alguma restrição na autonomia e na liberdade; se a decisão ou a prática acarreta em discriminação; a vulnerabilidade do titular, suas expectativas e o Nível de controle do titular.”;615619”:”Entendemos que dentro do contexto de proteção de dados pessoais há a necessidade de um atendimento personalizado, uma vez que estamos diante de um tema com regulamentação específica e que demanda maior celeridade na resolução das demandas, especificamente quando se fala em estabelecimento e cumprimento de prazos.”;615620”:”Em regra não. A regra deverá ser de não negar o direito de revisão e, excepcionalmente se houver motivo para negativa, esta negativa deverá ser clara e justificada. Reforçamos que as hipóteses de negativa quanto ao direito de correção já respondido anteriormente, poderá ser aqui aplicado, desde de que haja justificativa clara e fundamentada.”

{ "615450": "Confederação Nacional do Comércio de Bens, Serv e Turismo - CNC: A Lei 12.527/2011 foi criada para regular o acesso a informações no âmbito do setor público. Embora a solicitação por meio de sites oficiais esteja contemplada em tal Lei, na prática, muitas vezes exige-se que o titular se desloque a um local específico e especializado para fazer quaisquer tipos de requisições aos órgãos públicos. No entanto, no contexto do setor privado, em que os direitos dos titulares serão predominantemente solicitados por meio de plataformas online, como uma plataforma de gestão de requisições dos direitos dos titulares (DSAR), portal de privacidade ou por e-mail, é essencial considerar o volume de solicitações que as organizações podem receber e considerar suas capacidades e estruturas para gerenciar essas solicitações. O setor de comércio no Brasil conta com milhões de empresas ativas, sendo essencial considerar a pluralidade de realidades ao delimitar quais exigências são razoáveis para o atendimento dos direitos dos titulares. Com infraestruturas adequadas, por exemplo, é possível atender prontamente alguns direitos do titular, como o de confirmação de tratamento, mas devido à complexidade envolvida, o mesmo não seria possível em outras modalidades de direitos. O artigo 11, § 1º da Lei de Acesso à Informação estabelece que o órgão público deve resolver o atendimento dentro de um prazo não superior a 20 dias, prorrogável por mais 10 dias (art. 16), o que pode servir como referência inicial para estabelecer prazos razoáveis no contexto do atendimento amplo aos direitos dos titulares no setor privado. No Reino Unido, o ICO determinou em guia que as organizações devem responder a uma solicitação dentro de um mês do recebimento da solicitação, podendo ser prorrogado por até dois meses se a solicitação for considerada complexa. Assim, entendemos que, de modo a abranger a realidade de diferentes setores e portes de agentes de tratamento, bem como garantir que o atendimento de direitos dos titulares seja efetivo, os prazos propostos pela ICO podem servir como boa referência à ANPD.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Confederação Nacional do Comércio de Bens, Serv e Turismo-CNC: Ao definir prazos para atendimento às requisições feitas pelos titulares, seja em formato simplificado ou por meio de declaração completa, o principal critério a ser observado é a quantidade de informações que será prestada em cada situação, como demonstrado a seguir: - Declaração simplificada (art. 19, I): Deve abranger apenas a indicação dos dados de cadastro e as categorias dos demais dados tratados, sem necessidade, neste momento, de enumerá-los. - Declaração clara e completa (art. 19, II): Deve abranger não só a indicação das categorias de dados tratados, mas a indicação de todos os dados pessoais tratados, inclusive os inferidos, com especial atenção à manutenção do segredo comercial e de negócio. Tem-se que a declaração completa é mais complexa e, segundo o EDPB (European Data Protection Board), a complexidade de um pedido varia conforme as circunstâncias específicas de cada situação. Diversos fatores são levados em conta, incluindo a extensão dos dados gerenciados pelo controlador, o método de armazenamento dos dados — especialmente quando sua recuperação é desafiadora (por exemplo, quando os dados são dispersos por várias unidades da organização) —, a aplicação de isenções (como informações sobre outros titulares de dados ou dados confidenciais) e a necessidade de esforço adicional para tornar as informações compreensíveis. Organizações que lidam com um grande volume da população, como companhias aéreas, operadoras telefônicas, instituições financeiras e outros provedores de serviços ao público em geral, enfrentam naturalmente um aumento significativo no número de requisições que recebem. Esse cenário, influenciado tanto pelo tipo

de serviço prestado quanto pela amplitude da clientela atendida, tem impacto direto na disponibilidade de recursos necessários para gerenciar o fluxo de solicitações. Portanto, os prazos estabelecidos para atender a essas demandas devem considerar essas variáveis, a fim de garantir um atendimento eficaz e em conformidade com as expectativas dos titulares."

"615484": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: - Divulgação: Assegurar que o acesso ao Portal de Privacidade e/ou Aviso de Privacidade seja facilmente visível na experiência do usuário, com o Canal de Atendimento claramente identificado e acompanhado de instruções claras sobre como utilizá-lo. - Informação: Informar o titular sobre seus direitos conforme previstos no art. 18, LGPD, para que possa exercer a autodeterminação informativa. - Linguagem e Formato: Utilizar linguagem clara e acessível para garantir que as informações sejam compreendidas facilmente pelo titular e prestar informações em formato inteligível, que não demande conhecimento prévio para acessar a resposta. - Procedimento: Estruturar fluxos de atendimento e estabelecer prazos para o atendimento das requisições de acordo com a legislação vigente e mantendo a transparência com o titular em relação aos passos do atendimento. Por exemplo, ao receber uma solicitação, acusar recebimento e apontar ao titular o prazo estimado para retorno. - Recursos: Disponibilizar internamente recursos tecnológicos e humanos necessários para operacionalizar o canal de atendimento de forma eficiente. - Autenticação da identidade: Garantir que a pessoa que solicita acesso aos dados seja de fato o titular destes, evitando assim violações dos direitos de terceiros, como o compartilhamento indevido de dados. - Gratuito: os direitos dos titulares devem ser exercidos sempre de forma gratuita. Eventualmente, a ANPD poderá avaliar exceções relacionadas ao abuso de direito pelo titular, em que o excesso despropositado de solicitações gerar onerosidade ao controlador. - Registro: É fundamental que os protocolos de atendimento sejam devidamente registrados e armazenados internamente pela organização. Essa prática assegura a disponibilidade desses registros para futuras fiscalizações e/ou reclamações, promovendo transparência e fornecendo evidências claras das interações com os clientes ou usuários. A ANPD pode recomendar prazos específicos de armazenamento para informações destinadas a esse fim."

"615485": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim, há responsabilidade dos operadores na concretização dos direitos dos titulares. Obrigações e responsabilidades dos operadores no que tange ao atendimento dos direitos dos titulares, bem como sua colaboração com os controladores, são pilares essenciais da relação entre as partes. Além de estas obrigações serem definidas via contrato entre os agentes de tratamento, é interessante que a ANPD reforce a importância dessa colaboração. A ANPD já estabelece diretrizes em seu próprio Guia Orientativo Agentes de Tratamento (pg 17), ressaltando a importância de o operador seguir as orientações do controlador de forma abrangente. Destaca-se a relevância desse suporte no contexto do atendimento aos direitos dos titulares. Cabe ao operador fornecer as informações requisitadas pelo controlador que estiverem em seu poder e/ou informar sobre as solicitações dos titulares feitas diretamente a este, dentro dos prazos estipulados no contrato. Assim os operadores devem: a) Oferecer toda a assistência necessária (técnica, organizacional, logística, etc.) para que os controladores possam atender às solicitações dos titulares dos dados dentro dos prazos legais. Isso inclui a implementação de sistemas e procedimentos que facilitem o acesso, a retificação, a exclusão ou a portabilidade dos dados. b) Notificar o controlador em prazo adequado para que as medidas cabíveis possam ser tomadas, incluindo a notificação às autoridades supervisoras e aos titulares dos dados, quando necessário; c) Manter registros das atividades de tratamento de dados sob sua responsabilidade, contribuindo para a transparência e facilitando a auditoria pelo controlador ou autoridades

competentes. d) Garantir que as pessoas autorizadas a tratar os dados pessoais se comprometam a respeitar a confidencialidade ou estejam sob uma obrigação legal de confidencialidade.";"615486": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Não é apropriado equiparar as diretrizes estabelecidas para o atendimento de SAC, conforme previsto no Decreto nº 11.034/2022, ao atendimento dos direitos dos titulares, conforme estabelecido na LGPD. Entendemos que, em especial, as seguintes disposições trazidas no Decreto não seriam aplicáveis: a) Art. 4º e Art. 5º: Embora o canal online de atendimento deva estar disponível para envio de requisições a qualquer hora e todos os dias, a exigência de múltiplos canais e atendimento contínuo pode ser impraticável devido à complexidade e custos de segurança para proteção de dados. Além disso, o atendimento telefônico para os direitos dos titulares previstos na LGPD não se equiparam às tratativas no âmbito da legislação consumerista, já que as demandas exigem análise, compreensão e avaliação, conforme exigido pela legislação. b) Art. 13: Os prazos estabelecidos pela legislação de SAC são exíguos e não são adequados para lidar com as requisições previstas pela LGPD, que são mais complexas e, em diversas situações, exigem mais tempo para serem atendidas. c) Art. 14: Os direitos garantidos pela LGPD dizem respeito aos dados pessoais dos titulares e não à qualidade dos serviços prestados.";"615487": "---";"615491": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: A confirmação da existência do tratamento pode ser negada em algumas situações excepcionais, como: a) Segredo de negócio, quando a confirmação da existência do tratamento de dados pessoais poderia revelar informações que constituem segredo de negócio da empresa, comprometendo sua vantagem competitiva no mercado; b) Durante o curso de investigação e auditorias internas, quando essa divulgação possa prejudicar o desfecho dos trabalhos; c) Casos onde a confirmação possa atrapalhar um exercício de um direito (p.ex. direito de defesa em uma ação trabalhista); d) Quando a confirmação puder afetar os direitos de privacidade ou outras liberdades fundamentais de outra pessoa; e) Quando o controlador estiver submetido a uma norma de sigilo; e) Quando a informação puder colocar em risco a defesa e a segurança nacional ou a segurança do Estado e da sociedade; f) Se uma solicitação for claramente ou obviamente irrazoável, considerando-se desproporcional em relação ao ônus ou custos envolvidos no seu atendimento; g) Casos em que as solicitações se referem a informações ou a atividades de tratamento que obviamente não fazem parte das operações de tratamento do controlador. Para determinar se uma solicitação é manifestamente excessiva, é necessário avaliar se ela é claramente irrazoável. Isso deve ser baseado na proporcionalidade da solicitação em relação ao ônus ou custos envolvidos no tratamento da solicitação. Deve-se levar em consideração todas as circunstâncias da solicitação, incluindo: a natureza das informações solicitadas; o contexto da solicitação e o relacionamento entre o controlador e o indivíduo; se a recusa em fornecer as informações ou mesmo reconhecer se a empresa as detém pode causar danos substanciais ao indivíduo; os recursos disponíveis.";"615492": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: As informações relevantes a serem fornecidas aos titulares para a identificação dos controladores, são: (i) Na identificação do controlador: informações básicas, claras e precisas sobre a identidade do controlador responsável pelo tratamento dos dados pessoais do titular, como nome ou razão social da organização, bem como os meios de contato. (ii) Compartilhamento de dados: a indicação do setor empresarial em que o compartilhamento é realizado juntamente com a respectiva finalidade deve bastar para que o titular tenha satisfeito seu direito à transparência. Isso se justifica pois o excesso de detalhamento em relação as informações prestadas pode gerar efeito contrário ao esperado.";"615489": "Confederação Nacional do Comércio de Bens, Serviços e Turismo

- CNC: Os operadores têm a responsabilidade de cooperar com os controladores para garantir que os titulares dos dados possam exercer seu direito de obter informações sobre o tratamento de dados pessoais, seja por eventual: (i) Cooperação e suporte no recebimento da solicitação e encaminhamento ao controlador, ou ao menos no redirecionamento do titular para o canal de atendimento do controlador que é responsável pela atividade; (ii) Fornecimento de informações ao controlador que auxiliem na elaboração de resposta ao titular de dados, pois o operador normalmente saberá os detalhes de como a atividade ocorre; (iii) Facilitação na localização e recuperação dos dados para atender solicitações dos titulares, especialmente quando o tratamento de dados ocorrer em seu ambiente; (iv) Documentação das atividades de tratamento e visibilidade para o controlador acerca de qualquer alteração ou intercorrência no tratamento.";"615490": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: A declaração em formato simplificado deve conter três componentes distintos, para estar de acordo com o direito de acesso: a) Confirmação sobre a existência de tratamento dos dados do titular; b) Indicação da categoria de dados pessoais, e; c) Finalidade do tratamento.";"615494": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Para garantir a transparência e o direito à informação no âmbito de decisões automatizadas, as informações mínimas sobre o tratamento consistem na indicação de: - Categoria de dados tratada; e - Respectiva finalidade do tratamento. A partir dessas informações, o titular tem plena condição de exercer sua autodeterminação informativa para, caso queira, solicitar informações mais detalhadas sobre o tratamento, nos termos do que prevê o artigo 20 e § 1º da LGPD.";"615493": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim, poderia ser considerado satisfeito. Segundo diretrizes internacionais, como as da EDPB, os agentes de tratamento responsáveis pelo atendimento ao direito não são obrigados a fornecer as informações de outra forma além daquela solicitada pelo titular. No entanto, os formatos podem variar dependendo dos próprios dados pessoais a serem fornecidos e da forma de contato normalmente mantida entre titular e controlador. Por exemplo, para relações usualmente mantidas em ambiente virtual, o formato digital via portal de privacidade, e-mails ou área logada pode ser suficiente. Já para arquivos de voz, pode ser necessário restringir apenas o envio por e-mail (como gravações de áudio relacionadas a protocolos de atendimento realizados, uma vez que o arquivo de voz do titular dos dados em si pode ser considerado um dado pessoal). Pode haver, então, em casos específicos, um acordo entre o agente de tratamento e o titular para determinar o melhor formato e tipo de transferência que satisfaça ambas as partes.";"615502": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: No Brasil, é possível identificar alguns setores que, em razão da matéria e de regulamentação setorial já existente, já possuem mais maturidade para implementação do direito de portabilidade, previsto pelo artigo 18, V da LGPD, quais sejam: 1) Setor Bancário/Financeiro: O setor bancário/financeiro é altamente apto para implementar o direito de portabilidade da LGPD devido à sua experiência em tecnologias avançadas, como o Open Banking/Finance. A robusta estrutura tecnológica permite a transferência segura de dados entre instituições, facilitada pela padronização de APIs e protocolos de segurança. Isso promove transparência, interoperabilidade e oferece aos clientes mais opções e controle sobre seus dados. O movimento em direção ao Open Banking/Finance demonstra o compromisso do setor em facilitar a portabilidade de dados, promovendo concorrência e atendendo às exigências da LGPD. 2) Saúde Suplementar: Na mesma linha, o setor de saúde suplementar alcançou um nível de maturidade significativo no que diz respeito à transferência de dados pessoais. Com o surgimento do Open Health, semelhante ao conceito de Open Banking, visa-se simplificar o acesso aos dados da ANS disponíveis

no Portal Brasileiro de Dados Abertos por meio de softwares e aplicativos. 3) Telecomunicações: O setor de telecomunicações, embora tenha infraestrutura para o tratamento de dados pessoais, ainda está explorando a portabilidade entre operadoras, isso porque, no âmbito de sua prestação de serviço a portabilidade se assemelha ao direito de acesso em si. Logo é necessário maior maturidade do setor e aprofundamento de discussões para que haja consenso acerca do formato da portabilidade. A portabilidade na telefonia é regulamentada pela Resolução nº 460/2007 da ANATEL, contudo, é importante ressaltar que a portabilidade de dados pessoais difere da portabilidade de serviços. Enquanto a primeira transmite os dados para um novo provedor, a segunda permite que o usuário troque de fornecedor mantendo o mesmo número de telefone."615501": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Os desafios tecnológicos para implementação de um padrão de interoperabilidade para o direito de portabilidade são diversos e abrangentes. Eles envolvem a complexidade das operações, a diversidade de formatos de dados e metadados, bem como as ferramentas e protocolos de comunicação adotados pelo mercado de cada setor e indústria, incluindo ainda medidas de segurança e criptografia aplicadas na operacionalização. A integração de APIs e softwares heterogêneos também pode representar obstáculos significativos."615505": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Para garantia da interoperabilidade na implementação do direito de portabilidade de dados pessoais entre empresas é essencial que algumas especificações técnicas sejam compatíveis, como: - Formato dos arquivos, de modo a garantir a consistência na estruturação dos dados; - Ferramentas utilizadas devem ser compatíveis entre os diferentes sistemas; - Protocolos de comunicação devem ser definidos para que os sistemas sigam padrões ao enviar e receber dados pela rede, assegurando uma comunicação confiável e eficiente; - Medidas mínimas de segurança e criptografia devem ser aplicadas durante o processo de transferência; - APIs e softwares de integração utilizados devem ser compatíveis; e - Devem ser implementados padrões para metadados e dados para garantia de compreensão entre os sistemas e plataformas, bem como na leitura desses dados por máquinas."615503": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim, uma vez que haverá um padrão mínimo que permitirá aos agentes de tratamento receptores dos dados lerem e integrarem as informações em seus próprios sistemas, sem impactos negativos aos titulares. Ao compararmos com o GDPR, espera-se que os controladores transfiram os dados pessoais em um formato interoperável. Entretanto, não há uma imposição direta de obrigações aos outros controladores para que suportem esses formatos, em razão da variedade de formatos e padrões existentes no mercado. Portanto, a ANPD e os órgãos reguladores específicos de cada setor (se houver) devem colaborar para promover o diálogo entre as empresas e a autorregulação do mercado, com foco na eficácia e na garantia do direito do titular dos dados."615504": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: É não apenas razoável, mas também necessário permitir que o setor privado participe da definição de padrões de interoperabilidade para a portabilidade de dados, especialmente em setores específicos ou que já se beneficiam de outras iniciativas que possam trazer luz para essa questão. Essa colaboração reflete o reconhecimento de que a diversidade de perspectivas pode enriquecer e aprimorar os padrões e práticas de interoperabilidade. Na União Europeia, essa cooperação é valorizada e incentivada como parte dos esforços para promover a interoperabilidade em todos os setores e indústrias. O WP29, por exemplo, incentivava fortemente a cooperação entre as partes interessadas da indústria e associações comerciais para desenvolver um conjunto comum de padrões e formatos interoperáveis que atendam aos requisitos do direito à portabilidade de dados. Essa questão também foi

abordada pelo European Interoperability Framework (EIF), que estabeleceu uma abordagem acordada para a interoperabilidade de organizações que desejam fornecer conjuntamente serviços públicos. Dentro desse contexto, o framework especifica um conjunto de elementos comuns, como vocabulário, conceitos, princípios, políticas, diretrizes, recomendações, padrões, especificações e práticas. Em relação ao prazo, ele deve ser definido de forma a permitir um processo colaborativo e inclusivo, levando em consideração a complexidade das questões envolvidas e a necessidade de um resultado abrangente e sustentável."

"615511": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Os critérios objetivos que podem ser considerados para interpretação dos termos são: 1) Dados incompletos: - Ausência de informações essenciais; - Falta de elementos de identificação; - Campos obrigatórios não preenchidos; - Informações parciais ou fragmentadas; - Inconsistência dos dados pessoais. 2) Dados inexatos: - Fontes de dados não confiáveis; - Erros de processamento de dados. 3) Dados desatualizados: - Informações antigas que já não correspondem mais à realidade; - Obsoletos para a finalidade tratada."

"615514": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Com base nas diretrizes internacionais sobre o tema, a simples declaração do titular poderia não ser suficiente para o exercício do direito à correção em situações nas quais: a. A precisão dos dados não pode ser verificada de forma objetiva apenas com base na declaração do titular. Isso inclui casos em que os dados refletem registros oficiais ou informações que requerem validação por meio de documentação adicional ou provas; b. Se a correção dos dados puder prejudicar investigações oficiais, a proteção da segurança pública, a segurança nacional ou os direitos e liberdades de terceiros. Nesses casos, deve ser avaliada a necessidade de equilibrar o direito à correção com outros princípios fundamentais, incluindo a segurança jurídica e a prevenção de fraudes; c. Em situações em que a correção dos dados pessoais envolva dados sensíveis ou que possam ter repercussões legais ou financeiras significativas para o titular ou para terceiros; d. Se a solicitação for considerada manifestamente infundada ou excessiva. Por exemplo, se um titular faz repetidos pedidos de correção, mas a empresa já investigou e considera as informações precisas, e o titular continua a fazer pedidos baseados em alegações não comprovadas."

"615513": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Os critérios que podem ser considerados como esforço desproporcional são: a) Custo necessário para atender à solicitação é significativamente alto em relação ao tamanho e aos recursos financeiros da organização; b) Necessidade de mobilizar recursos técnicos significativos que a organização não possui ou que exigiriam um esforço desproporcional para serem implementados; c) Atendimento à solicitação impactaria de forma significativa as operações cotidianas da organização, prejudicando sua capacidade de executar suas funções básicas; d) Volume ou complexidade dos dados solicitados é tal que tornaria o processo de recuperação e fornecimento impraticável dentro de um período razoável; e) Solicitações repetidas pelo mesmo titular ou solicitações em massa que impõem uma carga administrativa desproporcional. Alguns exemplos: situações que envolvem a utilização de serviços de armazenamento em nuvem estrangeiros, que mantêm servidores em diversos países. Nesses casos, a comunicação para correção, eliminação, anonimização ou bloqueio dos dados pode ser considerada inviável devido à complexidade de suas operações, ao grande volume de dados que gerenciam e à escala global de suas operações, bem como à diversidade de regulamentações em diferentes jurisdições. Outro caso de esforço irrazoável seria realizar essa providência em dados históricos ou constantes de backups."

"615512": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Em comparação com o contexto europeu, é importante notar que a solicitação de correção pode ser recusada se a empresa considerar os dados

tratados como "precisos/adequados", ou seja, se entender que não há necessidade de correção. Também em situações de alteração de dados, mas necessidade de manutenção de dados anteriores para fins de histórico. Além disso, o direito à correção pode ser negado se a solicitação for considerada manifestamente infundada ou excessiva. Por exemplo, de acordo com o ICO, órgão regulador do Reino Unido, se um titular faz repetidos pedidos de correção, mas a empresa já investigou e considera as informações precisas, e o titular continua a fazer pedidos baseados em alegações não comprovadas, o pedido pode ser recusado por ser manifestamente infundado, e o titular deve ser notificado com a justificativa adequada."

"615517": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim. O titular deve fornecer contexto ou justificativa que fundamente seu pedido no momento da requisição, mostrando a desnecessidade dos dados. Isso garante um equilíbrio entre obrigação e diligência, permitindo que as requisições sejam avaliadas à luz da LGPD e possibilitando às empresas compreender os titulares, melhorar seus serviços e alinhar seus atendimentos de forma eficaz."

"615516": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim, embora as implicações das operações sejam diferentes para as empresas, a eliminação implica na exclusão total dos dados pessoais tratados, sem retenção de qualquer informação relacionada, enquanto a anonimização preserva dados que podem ser usados para outros propósitos, mas sem vínculo com o titular original. A manutenção dessas informações possibilita o estímulo às atividades econômicas e aprimora a governança interna das organizações, além de estar em consonância com o artigo 16 da LGPD. No que diz respeito aos titulares, a anonimização satisfaz seus objetivos. Ainda, a anonimização pode ser adotada alternativamente em casos em que houver dificuldades operacionais de eliminação dos dados pessoais tratados. O processo robusto e adequado de anonimização poderá ser utilizado para demonstrar que o agente de tratamento cumpriu, satisfatória e alternativamente, a providência que, em última instância, tinha como objetivo interromper o tratamento de dados que identificasse os titulares."

"615518": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Caso o titular se oponha ao tratamento de dados realizado com base em uma das hipóteses de dispensa de consentimento, e essa oposição seja considerada legítima, o controlador deverá interromper a operação de tratamento, a menos que consiga justificá-la com base em outra fundamentação legal. No entanto, mesmo diante da possibilidade de a oposição legítima do titular estar fundada em tratamento de dados em descumprimento da LGPD, isso não deveria, por si só, configurar infração para fins de aplicação de sanções administrativas perante a ANPD. Isso porque o nível de exigência, comprovação e apuração deve ser mais elevado, devendo ser respeitado o trâmite de apuração da ocorrência garantindo a ampla defesa do agente de tratamento. Ademais, espera-se que a ANPD possa auxiliar os agentes de tratamento na tarefa de adequar suas atividades de tratamento, abrindo prazo para essa adequação no caso concreto - promovendo, assim, o incremento de maturidade da cultura de proteção de dados no Brasil e a atuação responsiva da autoridade - e não que aplique sanções a partir de situações isoladas e que podem ser pontuais."

"615523": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Não necessariamente. Cada situação é única, pois, embora os controladores tenham a obrigação de excluir os dados tratados com base no consentimento, a própria LGPD traz o direito de exclusão separado do direito de revogação. Em certos casos, portanto, o controlador poderá continuar tratando os mesmos dados pessoais com base em outra hipótese legal, especialmente quando se tratar de conjunto de dados que são tratados para diferentes finalidades legítimas e amparadas pela lei. Nesse sentido, para que os dados pessoais sejam eliminados após a revogação do consentimento, o titular dos dados deve fazer uma

solicitação específica para a eliminação, conforme o art. 18, VI, da LGPD. Nesse caso, o controlador deve avaliar a solicitação e proceder com a eliminação, salvo se houver outra base legal que justifique a retenção dos dados. Ainda, após a revogação do consentimento, é possível a manutenção dos dados necessários para garantir que a atividade de tratamento ocorrerá sem os dados do titular que revogou o consentimento (ex.: titular revoga autorização para receber propaganda e pede eliminação de seus dados. O agente de tratamento mantém o registro de que aquela pessoa não quer receber propaganda, e apaga os demais dados).";615521": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Como regra geral, se o consentimento for revogado, todas as operações de tratamento de dados que eram baseadas nele e ocorreram antes de sua retirada permanecem legais; no entanto, o controlador deve interromper as ações de tratamento futuras. Se não houver outra base legal justificando o tratamento (para outras finalidades ou que justifiquem o armazenamento), eles devem ser excluídos pelo controlador. Caso os dados pessoais tratados com base no consentimento do titular tenham sido compartilhados com terceiros, o controlador deve comunicar esses terceiros sobre a revogação do consentimento, bem como sobre o requerimento de eliminação, para que eles também cessem o tratamento e eliminem os dados.";615617": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: A decisão automatizada abrange diversos processos operados automaticamente, nos quais a máquina toma decisões durante o processo. Geralmente, essas decisões envolvem questões técnicas de tecnologia da informação, com parâmetros inicialmente inseridos por intervenção humana. Por outro lado, as decisões tomadas unicamente com base em tratamentos automatizados são programadas para analisar dados e chegar a um resultado, avaliando parâmetros gerados por algoritmos e/ou machine learning. Essas decisões podem ter efeitos legais ou significativos para os titulares de dados, sem a intervenção direta de humanos no processo decisório.";615618": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Um interesse está sendo efetivamente afetado quando uma decisão tem repercussões tangíveis na vida do titular, influenciando seu status legal, direitos ou liberdades individuais. Isso implica que a decisão tem um impacto substancial em suas circunstâncias, comportamento ou escolhas, podendo inclusive excluir ou discriminar tais indivíduos. De modo geral, é fundamental considerar se a decisão afeta significativamente o titular em relação a sua: (i) Situação financeira; (ii) Saúde; (iii) Reputação; (iv) Oportunidades de emprego; (v) Comportamento; ou (vi) Escolhas. Por exemplo, a negação automática de um benefício social previsto em lei com base no perfil do indivíduo, a rejeição automática de uma solicitação de crédito online ou até mesmo práticas de recrutamento automatizadas são casos em que os interesses do titular são diretamente afetados. Deve-se, portanto, avaliar até que ponto a decisão pode impactar o titular em termos de suas circunstâncias financeiras, saúde, reputação, oportunidades de emprego, comportamento e escolhas.";615619": "Confederação Nacional do Comércio de Bens, Serv e Turismo-CNC: - A transparência pode ser desafiadora na revisão de decisões que afetam os titulares dos dados, especialmente quando essas decisões são baseadas em algoritmos complexos. Explicar esses algoritmos de maneira compreensível para os titulares dos dados, sem comprometer informações sigilosas e segredos de negócio, é um desafio, e manter a transparência requer esforço contínuo à medida que os algoritmos evoluem e são atualizados. Além disso, detalhes específicos sobre os algoritmos devem ser protegidos devido a preocupações com propriedade intelectual e segredos comerciais; - Equilíbrio entre fornecer informações e elas serem claras, satisfatórias e de fácil entendimento pelos titulares; - Pode ser difícil determinar o que constitui um viés ou discriminação sem critérios definidos e padrões claros para avaliação. A interpretação de

vieses e discriminação pode ser subjetiva e variar entre diferentes partes interessadas, podendo gerar insegurança por parte das organizações; - As empresas precisam desenvolver sistemas e processos que permitam a operacionalização da revisão de decisões automatizadas. Em empresas com grandes volumes de dados e processos complexos de tomada de decisão automatizada, também pode ser difícil identificar e explicar precisamente como uma decisão específica foi tomada e quais dados foram considerados. Implementar e manter um processo eficiente de revisão de decisões automatizadas pode gerar custos operacionais significativos para as empresas. Isso inclui não apenas os custos relacionados à tecnologia e segurança da informação, mas também os custos associados à formação de pessoal e à gestão dos processos de revisão; - O artigo 20, LGPD estabelece que as empresas devem fornecer uma resposta ao titular dos dados dentro de um prazo razoável. Garantir que os pedidos de revisão sejam tratados dentro desse prazo pode ser um desafio, especialmente para empresas com grandes volumes de solicitações, por isso a ANPD deve levar esse fator em consideração em futura regulamentação do assunto.";"615620": "Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC: Sim, o controlador pode negar o direito de revisão sobre decisões automatizadas nas seguintes hipóteses: (i) As decisões automatizadas não impactaram de forma significativa os direitos do titular e/ou que esse impacto não tenha sido demonstrado; (ii) A revisão da decisão automatizada implica no comprometimento de segredo comercial e/ou industrial do controlador; (iii) Quando a revisão manual de decisões automatizadas for tecnicamente ou praticamente inviável devido à complexidade ou ao volume dos processos de decisão. Ainda, existe a possibilidade de fundamentação, pelo controlador, de que as decisões que foram tomadas com base em tratamento automatizado com intervenção humana determinante para o resultado não se enquadrariam estritamente na definição de decisões automatizadas. Vale notar que o regimento da LGPD é diferente daquele do GDPR, não havendo situações em que o uso de decisão automatizada é vedado ab initio."

{ "615450": "A Lei Nº 12.527/2011 ("Lei de Acesso à Informação" ou "LAI") prevê prazos para o atendimento do direito de informação para dados e/ou demais informações armazenadas por órgãos que integrem a Administração Pública Direta. Nesse sentido, ainda que os prazos previstos em lei sejam proporcionais - 20 (vinte) dias caso não seja concedido acesso imediato, prorrogável, ainda, por mais 10 (dez) dias diante de justificativa razoável do órgão responsável pelo armazenamento - há prejuízo direto na concretização de direitos dos titulares, em especial, diante das particularidades de cada setor econômico. Portanto, a ABRAFARMA entende que a adoção de um prazo único para atendimento de todas as solicitações de direitos de titulares, fixado em 15 (quinze) dias úteis, contados a partir da confirmação da identidade do titular, se demonstra como a opção normativa com maior eficiência, na medida em que: (i) decorre do prazo legal do direito de confirmação de existência de tratamento e acesso à dados (art. 19, II, LGPD); e (ii) atende ao melhor interesse do titular, posto que garante previsibilidade ao período máximo em que o titular poderá exercer seu direito, ao passo que assegura que o agente de tratamento dispõe de tempo hábil o suficiente para atender às solicitações. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?": "A ABRAFARMA entende que a definição de prazos concretos para atendimento às solicitações dos titulares deverão levar em consideração fatores como: (i) a natureza dos dados pessoais tratados para as finalidades almejadas; (ii) as condições de tratamento e a implementação de medidas necessárias para autenticação da identidade do titular e, por consequência, da legitimidade da solicitação; e (iii) as particularidades inerentes aos setores e/ou segmentos econômicos nos quais os dados pessoais são tratados. Exemplificativamente, para agentes de tratamento que atuem em segmentos que demandam o tratamento de dados pessoais sensíveis, é necessário a implementação de medidas de verificação de identificação do titular para que se evite o comprometimento e/ou a disponibilização indevida de dados pessoais. Nesse cenário, a adoção de protocolos como o envio de documento de identidade para identificação e atendimento do solicitante deverá ser considerada na contagem de prazo, haja vista que é etapa necessária para o atendimento do direito do titular. Nesse sentido, a ABRAFARMA acredita que o prazo geral de 15 (quinze) dias úteis para atendimento aos direitos dos titulares deverá ser aplicável, mas a sua contagem deve ser iniciada após a confirmação da identidade do titular pelo controlador. ", "615484": "Sem contribuições para esse tópico.", "615485": "Sem contribuições para esse tópico.", "615486": "Sem contribuições para esse tópico.", "615487": "Sem contribuições para esse tópico.", "615491": "A ABRAFARMA entende que sim. Recomenda-se que a Autoridade estabeleça regras que determinem parâmetros e/ou limites concretos para indicar a satisfação e/ou o nível de maturidade na resposta de solicitação a titulares, como forma de verificar se os direitos foram satisfatoriamente cumpridos pelo controlador e evitar potenciais sancionamentos posteriores. A exemplo, em casos em que os titulares solicitam o exercício de direitos e/ou encaminham dúvidas ao agente de tratamento por intermédio do encarregado e, após posterior esclarecimento ou exercício do direito, o titular torna a solicitar direitos que já foram atendidos e/ou esclarecimentos que já foram endereçados. Nestes cenários, somente será possível sustentar que as obrigações do controlador foram satisfatoriamente cumpridas, eximindo o agente de tratamento de potenciais obrigações residuais, a partir da verificação de atendimento satisfatório das solicitações dos titulares. Portanto, salienta-se a necessidade de orientações específicas e limites objetivos estabelecidos previamente pela ANPD a fim de

equilibrar o melhor interesse dos titulares e os esforços razoáveis dos agentes de tratamento. ","615492": "À luz das boas práticas de proteção de dados e privacidade, recomenda-se que os documentos informacionais elaborados para prestar esclarecimentos aos titulares a respeito do tratamento de seus dados, como a política de privacidade, apresentem informações suficientes para indicar ao titular a qualificação do controlador, isto é, a razão social e/ou nome fantasia da pessoa jurídica que atue como controladora de dados pessoais e seu canal de contato. Caso haja compartilhamento de dados pessoais com terceiros que igualmente atuem como controlador, seja mediante hipótese de controladoria singular ou conjunta, é recomendável que haja previsão expressa na política de privacidade para que o titular seja satisfatoriamente informado ou possua legítima expectativa de que seus dados serão compartilhados com terceiros. Nesse caso, os demais controladores poderão ser indicados a partir de sua relação contratual com o controlador responsável pela coleta dos dados - por exemplo, indicação de que os dados serão compartilhados com “parceiros comerciais”, “fornecedores”, “prestadores de serviços” ou com “demais órgãos da administração pública”, na hipótese de cumprimento de obrigação regulatória ou em dados tratados pelo Poder Público. ","615489": "Sem contribuições para esse tópico.", "615490": "A ABRAFARMA entende que no que tange à confirmação de existência de tratamento de dados pessoais o Controlador deve apenas responder um “Sim” ou “Não” para confirmar se a empresa trata dados pessoais do Titular. A solicitação de acesso aos dados, por sua vez, considerando que é uma solicitação que demanda a compilação das informações que o Controlador possui do Titular de Dados, entendemos que não entraria no prazo previsto no art. 19, I, tendo em vista que demanda esforço por parte do Controlador para geração do relatório. ","615494": "Sem contribuições para esse tópico.", "615493": "A ABRAFARMA entende que sim, seguindo as disposições relatadas no item “a” deste tópico.", "615502": "Sem contribuições para esse tópico.", "615501": "A ABRAFARMA entende que um dos desafios a ser enfrentado poderia ser a comunicação entre as empresas, levando em consideração o uso de tecnologia por cada uma delas. Por exemplo, o Controlador que enviar ou receber dados pode entender que a tecnologia utilizada por outro Controlador não seja adequada ou acesse informações confidenciais deste. Entendemos que deve haver um parâmetro mínimo de requisitos de segurança a serem utilizados (por exemplo, criptografia, envio de dados por SFTP, entre outros) e, a depender do modelo de disponibilização de dados, que as empresas não podem utilizar qualquer tipo de ferramenta, tecnologia, engenharia reversa ou qualquer outro método que viole os segredos comerciais e os direitos relativos à propriedade intelectual do Controlador que está enviando/disponibilizando os dados. ","615505": "Sem contribuições para esse tópico.", "615503": "Sem contribuições para esse tópico.", "615504": "Sem contribuições para esse tópico.", "615511": "Sem contribuições para esse tópico.", "615514": "Sem contribuições para esse tópico.", "615513": "A ABRAFARMA entende que a impossibilidade e/ou emprego de esforços desproporcionais para o atendimento às solicitações dos titulares deverão levar em consideração fatores como: (i) a natureza dos dados pessoais tratados para as finalidades almejadas; (ii) as condições de tratamento e a implementação de medidas necessárias para autenticação da identidade do titular e, por consequência, da legitimidade da solicitação; e (iii) as particularidades inerentes aos setores e/ou segmentos econômicos nos quais os dados pessoais são tratados. Exemplificativamente, para agentes de tratamento que atuem em segmentos que demandam o tratamento de dados pessoais sensíveis, é necessário a implementação de medidas de verificação de identificação do titular para que se evite o comprometimento e/ou a disponibilização indevida de dados pessoais. Nesse cenário, a adoção de protocolos como o envio de documento de identidade para

identificação e atendimento do solicitante deverá ser considerado no grau de esforço desempenhado pelo agente de tratamento para assegurar a efetividade na solicitação, de modo que a efetivação e atendimento de solicitações para certos direitos - como o de acesso aos dados pessoais tratados (art. 18, II, LGPD) - somente serão possíveis mediante apresentação de documentos que comprovem a titularidade do solicitante. ","615512": "A ABRAFARMA entende que sim. Recomenda-se que a Autoridade estabeleça regras que determinem parâmetros e/ou limites concretos para indicar a satisfação e/ou o nível de maturidade na resposta de solicitação a titulares, como forma de verificar se os direitos foram satisfatoriamente cumpridos pelo controlador e evitar potenciais sancionamentos posteriores. A exemplo, pode haver casos que o Controlador não possa efetivar a alteração de dados sem antes solicitar documentos comprobatórios (alteração de nome, sobrenome, entre outros) e entendemos que deve haver um limite em relação à este atendimento para os casos em que os titulares solicitam o exercício de direitos e/ou encaminham dúvidas ao agente de tratamento por intermédio do encarregado e, após posterior esclarecimento ou exercício do direito, o titular se recusa a apresentar os documentos necessários e torna a solicitar direitos que já foram atendidos e/ou esclarecimentos que já foram endereçados. Nestes cenários, somente será possível sustentar que as obrigações do controlador foram satisfatoriamente cumpridas, eximindo o agente de tratamento de potenciais obrigações residuais, a partir da verificação de atendimento satisfatório das solicitações dos titulares. ","615517": "A ABRAFARMA entende que a fundamentação das solicitações submetidas por titulares é necessária, na medida em que a concretização do direito deverá passar por avaliação prévia conduzida pelo controlador para verificar a possibilidade de concretização do direito, em especial, como forma de avaliar a fundamentação com base em violação à LGPD ou demais irregularidades na atividade de tratamento. Desse modo, a solicitação exclusão e/ou bloqueio não implicará na concretização efetiva do direito pelo controlador, caso a avaliação conduzida não identifique, de maneira razoável, a desconformidade da atividade de tratamento a ponto de ensejar a eliminação, anonimização ou bloqueio da atividade de tratamento, salvo em situações específicas, como a revogação ou eliminação de dados pessoais tratados com base no consentimento. ","615516": "A ABRAFARMA entende que, uma vez que os direitos de “anonimização” e “eliminação” de dados pessoais estão previstos no mesmo dispositivo legal (art. 18, IV, LGPD), caberá ao controlador optar, de maneira alternativa, por concretizar os direitos do titular a partir da implementação das medidas previstas no art. 18. Do ponto de vista prático, o exercício do direito de anonimização, bem como o exercício do direito de eliminação de dados pessoais, implicam no mesmo resultado - a interrupção do tratamento de dados pessoais que identifiquem o titular enquanto pessoa natural. A medida técnica a ser adotada deverá, portanto, ser avaliada a partir da solicitação concreta submetida pelo titular de dados pessoais, facultando ao controlador optar pela medida que melhor se adeque em face da satisfação dos interesses do titular e da promoção das atividades econômicas do controlador, respeitadas as disposições do art. 16 e da LGPD. ","615518": "Sem contribuições para esse tópico. ","615523": "A ABRAFARMA entende que o direito de revogação de consentimento (art. 18, IX, LGPD), não constitui necessariamente a obrigação de eliminação de dados pessoais tratados com base no consentimento (art. 18, VI, LGPD). Com efeito, ainda que o consentimento enquanto base legal (art. 7º, I, LGPD) fundamente o tratamento de dados pessoais para as finalidades pretendidas, a revogação do consentimento não implicará na eliminação dos dados pessoais caso o consentimento seja revogado, na medida em que o armazenamento e o posterior tratamento dos dados pessoais poderá ser amparado por base legal distinta a do consentimento, à obrigação legal ou regulatória que necessite da retenção dos dados

peçoais tratados (art. 7º, II). Ademais, as atividades de tratamento anteriormente amparadas pelo consentimento não deverão ser afetadas pela revogação, isto é, a revogação do consentimento deverá ter efeito ex-nunc, afetando apenas aos tratamentos posteriores. Além disso, nos casos em que forem aplicáveis, os dados poderão ser submetidos somente à processo de exclusão lógica, isto é, torná-los inativos nos sistemas do agente de tratamento para que não sejam objeto de novas atividades e/ou não sejam acessíveis por terceiros, incluindo a possibilidade de anonimização dos dados para fins estatísticos. Desse modo, a interrupção da atividade de tratamento com base no consentimento não necessariamente implicará a eliminação dos dados pessoais, que constitui direito apartado da revogação do consentimento. ","615521": "Sem contribuições para esse tópico. ","615617": "A ABRAFARMA entende que a decisão automatizada é aquela que um sistema ou algoritmo toma uma decisão sem intervenção humana direta. Por exemplo, um algoritmo de recomendação utilizado para recomendar produtos e/ou serviços, sem necessariamente, levar em consideração a interação e/ou dados do Titular. A decisão tomada unicamente com base em tratamento automatizado de dados pessoais, por sua vez, significa que a decisão realizada pelo sistema ou algoritmo leva em consideração a interação do Titular e suas preferências, sem qualquer intervenção ou análise humana. Por exemplo, um algoritmo de recomendação utilizado para recomendar produtos e/ou serviços, com base nas preferências, interações e dados do Titular, podendo ser desde a indicação de um serviço (filmes e músicas em streaming) até a indicação de produtos (com base nas compras realizadas pelo Titular). A diferença principal entre a “decisão automatizada” e a “decisão tomada unicamente com base em tratamento automatizado de dados pessoais” é a utilização de informações relacionadas ao Titular dos Dados para executar o algoritmo. ","615618": "Sem contribuições para esse tópico. ","615619": "A ABRAFARMA entende que os desafios para implementar o direito de revisão das decisões automatizadas, são: • Tempo e tecnologias necessárias: A revisão de decisões automatizadas pode exigir tempo para analisar a lógica do algoritmo e recursos que podem exigir um esforço desproporcional, tanto por parte dos Controladores de Dados quanto dos Titulares Dos Dados. Neste sentido, estamos diante de um desafio em termos de alocação de tecnologias para atendimento da solicitação e capacidade de resposta adequada às solicitações de revisão, incluindo funcionários treinados, por parte do Controlador, para lidar com essas solicitações e sistemas para rastrear e documentar o processo de revisão. Neste ponto, importante salientar que, a depender do esforço, é possível que seja necessário a solicitação de prazo adicional para o cumprimento do Direito do Titular, levando em consideração às complexidades tecnológicas atuais; • Desafios técnicos: A implementação do direito de revisão pode trazer, também, desafios técnicos, especialmente quando se trata de algoritmos ou sistemas de computação de difícil compreensão ou de novas tecnologias. Para que o Controlador possa garantir que seus sistemas identifiquem de forma rápida a decisão automatizada, pode ser necessário investimentos em infraestrutura e tecnologia. ","615620": "Sem contribuições para esse tópico."

{ "615450": "CNseg: A Lei nº 12.527/2011 (Lei de Acesso à Informação) estabelece que, não sendo possível conceder o acesso imediato à informação, a solicitação deverá ser atendida em prazo não superior a vinte dias (art. 11, §1º), prorrogável por mais dez dias (art. 11, §2º). A LGPD, por sua vez, com relação ao atendimento ao direito de confirmação de tratamento ou acesso aos dados pessoais por meio de declaração clara e completa, prevê que o controlador dispõe do prazo de até quinze dias (art. 19, II). Pois bem. Analisando a questão sob a perspectiva do setor de seguros, que realiza o tratamento de um volume significativo de dados, esses prazos parecem insuficientes, principalmente para o atendimento de solicitações mais complexas (como a de retificação, por exemplo). Desta forma, para que seja exequível, sugerimos o prazo de até trinta dias para o atendimento aos direitos do titular, com a possibilidade de, em casos de maior complexidade, esse prazo ser prorrogado por igual período. A título de demonstração da razoabilidade do prazo que está sendo proposto, cumpre informar que no âmbito do RGPD o prazo para atendimento da solicitação do titular no exercício de seus direitos é de um mês, prorrogável por até dois meses, verbis: “Art. 12. Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados.(...). 3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos art. 15º a 20º, sem demora injustificada e no prazo de um mês a contar da data de recepção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de recepção do pedido. Se o titular dos dados apresentar o pedido por meios eletrônicos, a informação é, sempre que possível, fornecida por meios eletrônicos, salvo pedido em contrário do titular”(sem grifos no original)".b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:"CNseg: Dentre os critérios que deveriam ser levados em consideração pela ANPD, sugerimos os seguintes: (i) o porte do agente de tratamento; (ii) o volume de dados tratados; (iii) o setor de atuação do agente de tratamento, a fim de que sejam consideradas eventuais obrigações regulatórias já existentes, evitando-se, assim, a sobreposição de normas; e (iv) a forma como o dado pessoal é tratado (se por meio físico ou digital)."; "615484": "CNseg: Para que seja efetivo, o canal de atendimento deve observar a forma de comunicação já usualmente utilizada entre o titular e o agente de tratamento. Também é preciso estabelecer mecanismos para confirmar que aquele que pretende exercer o direito é realmente o titular do dado pessoal (art. 6º, VII, LGPD). É importante que haja prazos objetivos, expressos e inequívocos a serem cumpridos, para que o controlador se guie ao realizar a ponderação e opte pela opção mais benéfica. Entende-se que os atributos de um Canal de Atendimento são os indicados abaixo: • Acesso facilitado e simplificação na localização do Canal: o link, página ou telefone de acesso não podem estar ocultos e o titular não deve ter dificuldades para chegar ao Canal de Atendimento. Sempre que possível, oferecer diferentes opções de contato; • Transparência e clareza nas informações: informações claras e simples, indicando o que é o Canal de Atendimento e a que ele se destina. Caso os direitos sejam exercidos por diversos meios, a exposição precisa demonstrar quais são eles, de modo indicativo e, se possível, usando ícones e pictogramas. É recomendável, ainda nesta página de informações, apresentar quais são os prazos praticados pelo controlador, os serviços oferecidos e os que não são atendidos, neste caso com o direcionamento do titular a algum outro canal

mais apropriado; • Validação de identidade: é preciso que o titular seja informado quanto à necessidade de validação de sua identidade na apresentação da solicitação, de modo a garantir que as informações de um titular não sejam expostas a terceiro estranho à relação; • Registro e rastreamento: o Canal de Atendimento deve ter sistemas adequados para registrar e rastrear as interações, garantindo que as solicitações sejam devidamente registradas, acompanhadas e respondidas dentro dos prazos estabelecidos; • Protocolo de recebimento: o Canal de Atendimento deve indicar um protocolo de recebimento, a fim de que o titular entenda que sua reclamação foi recebida e será analisada dentro do prazo praticado pelo Controlador. "615485":CNseg: Considerando o que dispõe o art. 18, caput, da LGPD, entendemos que a obrigação de atender aos direitos dos titulares é exclusiva do controlador, não podendo ser estendida para o operador. Apesar disso, julgamos adequado que o operador coopere com o controlador para o cumprimento dessa obrigação. Uma vez que o operador executa a atividade de tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD), reúne condições para auxiliar o controlador no atendimento das demandas dos titulares dos dados. Nesse sentido, nos parece pertinente que a ANPD recomende aos agentes de tratamento, como medida de boa prática, que estabeleçam contratualmente o dever de cooperação para atender aos direitos dos titulares. "615486":CNseg: Com a entrada em vigor da LGPD, as empresas já passaram por adequações de estrutura e houve a criação de um canal de atendimento específico para as finalidades da LGPD. Cabe mencionar que o atendimento aos direitos dos titulares não é um atendimento de nível 1 de um call center ou SAC. Parece-nos inapropriado adotar as diretrizes do Decreto do SAC, considerando: • Disponibilidade e ininterrupção 24x7 (art. 4º, caput): faz sentido em termos de atendimento ao consumidor, que está diante de serviços e produtos para uso e sobre os quais pode incidir certo senso de urgência. Em termos de atendimento ao titular de dados, não parece razoável demandar do Controlador essas duas obrigações, sobretudo se se considerar que para certos direitos o prazo de atendimento já é de 15 dias; • Obrigatoriedade de atendimento telefônico (art. 4º, §2º): a depender do porte da organização, o atendimento ao titular de dados pode ser feita por áreas de backoffice (como o escritório de Privacidade), e não por áreas de atendimento. A obrigatoriedade de disponibilização de canal telefônico imporia um ônus desnecessário ao controlador que tem uma operação perfeitamente atendida por canais remotos como e-mails e formulários; • Impossibilidade de exigência de dados pessoais (art. 4, §4º): o fornecimento de dados pelo controlador é condição necessária para a validação de identidade e única forma de materializar o disposto no art. 18, §3º da LGPD, garantindo-se que o acesso aos dados pessoais seja fornecido somente àqueles que são os efetivos titulares; • Prazo de atendimento (art. 13): o prazo de 7 dias corridos é demasiado curto para a complexidade dos direitos atendidos. Não obstante, seria viável a adoção de previsões que levem em conta o porte dos agentes de tratamento, como estipulado no art. 1º, parágrafo único da referida norma. "615487":CNseg: Entendemos que cada Controlador tem a liberdade de determinar, de modo autônomo, um modelo de atendimento a ser adotado, considerando o volume de dados tratados, a realidade de seus sistemas operacionais e informativos, os locais em que dados pessoais podem estar armazenados, sua capacidade operacional ou a capacidade dos Canais de Atendimento e a complexidade de suas atividades de tratamento. O estabelecimento de um modelo único poderia estabelecer exigência desproporcional ao agente de tratamento de pequeno porte, por exemplo, caso seja um processo muito complexo, ou simplificar demais o processo para controladores com grandes volumes que precisam estabelecer meios e métodos próprios para operacionalizar esta atividade. "615491":CNseg: Entendemos que sim. Para coibir o abuso de direito, reputamos

legítimo que o controlador deixe de atender pedidos infundados ou excessivos, nos mesmos moldes do que estabelece a RGPD, cujo artigo 12º/5, “b” preconiza o seguinte: “5. As informações fornecidas nos termos dos artigos 13.º e 14.º e quaisquer comunicações e medidas tomadas nos termos dos artigos 15.º a 22.º e 34.º são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode: (...) ou b) Recusar-se a dar seguimento ao pedido”. Embora a LGPD não possua dispositivo com previsão semelhante, é possível compreender, à luz do princípio da boa-fé, que o controlador não está obrigado a atender pedidos abusivos. Desta forma, nos parece que, em situações específicas, em que o pedido for infundado ou excessivo, o controlador poderá negar a solicitação. Além disso, julgamos que seria igualmente possível ao controlador negar o direito de confirmação em situações excepcionais para: (i) evitar prejuízo a investigações ou processos judiciais; ou (ii) preservar direitos e liberdade de terceiros. Por exemplo, tratamento de dados realizados para fins de prevenção e combate à fraude em seguros, tanto na área securitária quanto na bancária, podem ser negativamente impactados pela confirmação do tratamento a determinado titular de dados que seja sujeito de tais medidas e investigações que, frise-se, têm natureza legítima, reconhecida, inclusive, no âmbito da União Europeia. Outra hipótese seria, também, que o fornecimento de solicitações de órgãos públicos ou de terceiros no exercício regular de seus direitos também venham a ser prejudicados com a confirmação de um tratamento de dados por solicitação de determinado titular. “,”615492”:“CNseg: Para viabilizar que o titular identifique o(s) agente(s) responsável(is) pelo tratamento de seus dados pessoais, devem lhe ser fornecidas informações contendo razão social, CNPJ e nome pela qual a empresa é conhecida publicamente. “,”615489”:“CNseg: Todas as responsabilidades do operador são obrigações contratuais que o vinculam ao Controlador, dentre as quais as obrigações de respeitar as regras da LGPD em seu âmbito de atuação, as obrigações de observar os princípios da LGPD, notadamente os princípios da segurança e da prevenção, as obrigações de observar meios seguros de compartilhamento de informações, de observar as diretrizes de confidencialidade, integridade e disponibilidade dos dados pessoais sob sua guarda. “,”615490”:“CNseg: Entendemos que a declaração em formato simplificado deve conter informações sobre os tipos de dados (por exemplo, o nome, o CPF, o e-mail do titular de dados, o endereço residencial), considerando a contextualização do aviso de privacidade já disponibilizado pela companhia em seus canais de comunicação.”,”615494”:“CNseg: Entendemos que as informações mínimas sobre o tratamento de dados pessoais que devem ser disponibilizadas pelo controlador são aquelas mencionadas no art. 9º da LGPD, ou seja: (i) a finalidade do tratamento; (ii) a forma e a duração do tratamento, observados os seus segredos comercial e industrial; (iii) a sua identidade (nome e CPF/CNPJ) e o seu contato; (iv) o meio de comunicação com o encarregado; (v) o compartilhamento de dados e a respectiva finalidade; (vi) a responsabilidade dos agentes que realizarão o tratamento; (vii) os direitos dos titulares; e (viii) se o tratamento de dados pessoais é condição para o fornecimento de produto ou de serviço. No que diz respeito aos critérios e procedimentos utilizados para a decisão automatizada, são informações que só deverão ser disponibilizadas ao titular se houver solicitação, exatamente como estabelece o art. 20, § 1º, da LGPD. E nesses casos, caberá ao controlador avaliar quais informações poderão ser disponibilizadas para garantir, de um lado, a transparência quanto à lógica do tratamento que é realizado, e, de outro lado, a preservação dos seus segredos de negócio. “,”615493”:“CNseg: Observada a forma como os dados já são tratados (forma física ou digital), entendemos que sim. Sem prejuízo de o titular poder solicitar do controlador informações

complementares a respeito do tratamento, é possível que queira apenas acessar os seus próprios dados. Desta forma, entendemos possível considerar a disponibilização dos dados pessoais como suficiente para atender ao direito de acesso. Cabe mencionar que pode ser dada essa opção de escolha, caso a empresa possua ambos os formatos. Nesta era digital, poucas empresas têm mantido o atendimento em papel. Logo, se a empresa já realiza o atendimento de solicitações de forma digital, este é o meio de atendimento que deve ser utilizado. Além disso, o recebimento em formato físico pode trazer riscos de segurança em relação ao envio e não ser um formato tão célere quando comparado ao envio em formato digital.

","615502": "CNseg: No âmbito do setor de seguros, o tema ainda está sendo tratado conforme regulamentação do CNSP/Susep no que diz respeito ao OPIN. Nos termos do art. 55-J, XXIII da LGPD, deverá a ANPD articular-se com autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação, para não haver sobreposição regulatória ou para que não seja estabelecido encargo regulatório exagerado.

","615501": "CNseg: Dentre os desafios que se pode antever, citamos a padronização de formatos de dados pessoais, algoritmos validadores/regras, compatibilidade entre os diversos sistemas com linguagens diversas, garantia de segurança, privacidade e gestão de identidade e acesso, integração entre os sistemas legados, além de custos e eventuais investimentos em novas adaptações.

","615505": "CNseg: No âmbito do setor de seguros, o tema ainda está sendo tratado conforme regulamentação do CNSP/Susep no que diz respeito ao OPIN. Nos termos do art. 55-J, XXIII da LGPD, deverá a ANPD articular-se com autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação, para não haver sobreposição regulatória ou para que não seja estabelecido encargo regulatório exagerado.

","615503": "CNseg: Inicialmente, registramos o nosso entendimento no sentido de que o direito à portabilidade não abrange “todos” os dados pessoais do titular, devendo ser excluídos do escopo desse direito, por exemplo, os dados derivados e inferidos pelo controlador. Feita essa ressalva, entendemos que a disponibilização ao titular de seus dados pessoais portáveis (como por exemplo, os dados fornecidos pelo próprio titular) deve ser considerada como medida suficiente para atender ao direito à portabilidade.

","615504": "CNseg: Sim, é razoável que os setores se autorregulem neste aspecto. Os prazos para a definição dos padrões devem considerar conversas entre ANPD e representantes de cada setor para que os desafios dos entes participantes sejam considerados e o impacto operacional/financeiro seja levado em consideração.

","615511": "CNseg: Sugerem-se os seguintes critérios: • Completude: por este critério, é considerado incompleto o dado pessoal que não possui todos os elementos que tornam possível a identificação do indivíduo a que ele se refere. Exemplo: um CPF contendo 10 dígitos, endereço ao qual faltam número e complemento, endereço eletrônico cuja identificação de provedor está fora do padrão internacional, documento de identidade que foge ao padrão adotado pelo órgão expedidor. Com esses elementos, o dado pessoal seria inapto a gerar a identificação de um indivíduo; • Exatidão/precisão: por este critério, um dado deve ser considerado inexato quando não descrever a verdade dos fatos, quando for impreciso, falso ou que não retornar nenhum resultado àquele que o pesquisa. Neste sentido, o nome de registro civil pode ser considerado um dado inexato para pessoas transgênero, assim como o sexo atribuído ao nascimento. Essas situações podem se perpetuar em bancos de dados públicos e privados (exemplos: dados de secretaria de saúde ou de educação); • Atualização: leva em conta as modificações sofridas pelo dado ao longo do tempo, por diversos fatores, e que tornam a informação imprecisa e/ou incapaz de gerar uma identificação acurada do titular de dados. Neste sentido, é importante destacar que

há dados pessoais que estão sujeitos a perecimento conforme a passagem do tempo e outros que não estão. Dados pessoais que compõem os chamados identificadores governamentais, como CPF, PIS, PASEP, passaporte, número de registros profissionais, data de nascimento, número de certificado de reservista são dados pessoais que não estão sujeitos a mudanças geradas pelo tempo, ao passo que título de eleitor (em caso de transferência), nome, estado civil e informações de contato, podem ser objeto de desatualização em bancos de dados e sistemas de cadastros. Deve-se ainda levar em consideração que é obrigação do próprio titular manter seus dados atualizados. ","615514": "CNseg: Em casos de alteração de dados relacionados à identificação ou qualificação do titular, como o nome, mudança para estado civil, números de identificação geral (RG, CPF, CNH), domicílio e demais dados pessoais que possam impactar no atendimento aos direitos dos titulares. ","615513": "CNseg: Para avaliar a impossibilidade ou o esforço desproporcional para fins de aplicação do art. 18, § 6º, da LGPD, sugerimos que sejam considerados os seguintes critérios: (i) o tempo decorrido desde a data em que ocorreu o compartilhamento dos dados; (ii) os recursos materiais e humanos que deverão ser empregados; (iii) o volume de dados tratados; (iv) o porte do agente de tratamento; (v) a utilidade que a providência resultará para o titular; (vi) a quantidade de agentes de tratamento envolvidos e, (vii) se o titular possui ou não relação com o agente de tratamento. A exemplo do setor de seguros, o volume de dados pessoais é significativo, além de haver milhares de agentes de tratamento envolvidos, como os corretores. Logo, as seguradoras não deveriam ser obrigadas a comunicar a atualização dos dados pessoais dos titulares para os corretores, já que estes já possuem relação direta com o titular. ","615512": "CNseg: Entendemos que sim. Em determinadas situações a retificação da informação dependerá de prévia adoção de outros procedimentos específicos. A título de exemplo, pode-se mencionar a hipótese em que um titular queira retificar o seu sobrenome em um determinado cadastro. Ainda que seja possível para esse titular demonstrar que a informação está incorreta, decorrente de um erro material constante em seu assentamento de registro civil, a retificação do dado dependerá da prévia correção da informação nos órgãos oficiais, que, no caso deste exemplo, teria que seguir o procedimento previsto na Lei nº 6.015/73. Ou seja, ainda que a informação esteja, de fato, incorreta, não caberá ao controlador realizar a retificação nesse caso hipotético, pois dependerá da prévia retificação em órgãos oficiais, de acordo com o procedimento estabelecido por lei. Também entendemos que seria descabido acolher o pedido de retificação se o dado, ainda que desatualizado, for útil para a finalidade específica do tratamento. Pode-se imaginar, a título de exemplo, o registro do histórico de saúde de um titular. É possível que algumas informações, mesmo que desatualizadas, sejam necessárias e relevantes para permitir um adequado atendimento médico. Sendo assim, desde que haja motivação idônea, que deverá ser informada ao titular pelo controlador, entendemos possível negar o direito de correção em algumas situações específicas. Entende-se ainda que nos casos identificados em políticas internas de prevenção à fraude é possível não atender imediatamente pedidos de correção de dados pessoais, uma vez que tais pedidos e consequentes alterações têm potencial de causar danos ao titular de dados, justificando, com isso, a exigência de apresentação de documentos comprobatórios. ","615517": "CNseg: O titular deve motivar o pedido e explicar por que considera que os dados sejam desnecessários ou se mostrem excessivos ou porque o tratamento está em violação legal. ","615516": "CNseg: Sim. Considerando que dados anonimizados de forma adequada não são mais considerados dados pessoais, entendemos que qualquer relação com o titular foi encerrada, gerando o mesmo efeito da eliminação, mas permitindo que a companhia tenha alternativas de adequação do seu ambiente e geração de valor sobre dados

agregados.";"615518": "CNseg: Restando caracterizada hipótese de tratamento irregular, o controlador deverá adotar providências internas para adequação do tratamento.";"615523": "CNseg: Entendemos que não. A eliminação do dado pessoal não é uma consequência inevitável da revogação do consentimento. Conforme expressamente estabelece o art. 18, VI, da LGPD, o titular tem o direito de solicitar a eliminação dos dados pessoais tratados com o seu consentimento, “exceto nas hipóteses previstas no art. 16” da lei. Ou seja, mesmo que haja a revogação do consentimento, ainda assim os dados pessoais poderão ser conservados para: (i) cumprimento de obrigação legal ou regulatória do controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Também será possível continuar o tratamento de dados pessoais após a revogação do consentimento do titular, desde que seja possível respaldá-lo em outra base legal (arts. 7º e/ou 11 da LGPD).";"615521": "CNseg: Em regra, os tratamentos já realizados não poderão ser afetados pela revogação do consentimento, sob pena de não se observar o que estabelece o § 5º, do art. 8º da LGPD. Na hipótese de revogação do consentimento, os dados só terão que ser eliminados se houver requerimento expresso do titular nesse sentido e, ainda assim, desde que não reste configurada nenhuma hipótese que autorize o controlador a conservar esses dados, exatamente como dispõe o art. 16 da LGPD.";"615617": "CNseg: Uma decisão automatizada ocorre quando uma escolha ou determinação é realizada por sistema automatizado, como um algoritmo ou inteligência artificial, sem a intervenção humana direta. Já uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é aquela em que a determinação é feita exclusivamente com base na análise de dados pessoais por meio de algoritmos ou processos automatizados, sem a participação humana na tomada da decisão.";"615618": "CNseg: Para fins de aplicação do art. 20, sugere-se adotar a interpretação de que o interesse do titular só restará efetivamente afetado quando a decisão lhe causar prejuízo. Ou seja, o primeiro critério é o efeito negativo da decisão na esfera jurídica do titular. O segundo critério é a relevância. Não deverá ser qualquer interesse do titular que seja contrariado que desencadeará o direito de revisão; há de se observar a razoabilidade e a proporcionalidade.";"615619": "CNseg: As implantações de automação permitem que a companhia gere escala e agilidade para os seus clientes. O atendimento destes objetivos corresponde a uma definição de regras de negócio e a um volume expressivo de titulares afetados, o que torna a revisão um desafio operacional pelo volume e um impacto no negócio significativo, o que pode mitigar os benefícios gerados pela automação, gerando ainda investimento de recursos financeiros e humanos. A revisão das decisões não impede que as empresas avaliem aspectos como qualidade de dados que possam afetar o resultado da automação e o impacto no titular.";"615620": "CNseg: Entendemos que sim. O direito à revisão nasce para o titular quando a decisão é tomada unicamente de forma automatizada. A contrario sensu, havendo outros parâmetros que embasam a decisão, é possível que o controlador negue o direito à revisão por falta de respaldo legal. Além disso, para coibir o abuso de direito, reputamos legítimo que o controlador deixe de atender à solicitação de revisão infundada ou excessiva. Também julgamos que, ao menos em tese, seria igualmente possível ao controlador negar o direito de revisão em situações excepcionais, relacionadas à preservação do interesse público ou para resguardar direitos e liberdade de terceiros. Por exemplo: tratamentos automatizados que identificam padrões indicativos de prática de lavagem de dinheiro que deveriam ser comunicados

aos órgãos competentes, possibilitar a revisão, e mais do que isso, impedir que a comunicação seja realizada até que a revisão ocorra pode prejudicar o interesse público. "

{"615450": "Para abordar as questões de prazos, sejam eles úteis ou corridos, é necessário levar em consideração para empresas privadas a capacidade de se adequarem, segue sugestões em relação ao LAI até 20 dias prorrogável por mais 10 dias: 1. Especificação do Tipo de Prazo: é importante especificar claramente se o prazo é contado em dias úteis ou corridos. Isso evita interpretações divergentes. 2. Prazo Base com Possibilidade de Prorrogação: Estabelecer um prazo inicial, como os 20 dias úteis previstos na LAI, com a possibilidade de prorrogação. No entanto, diferentemente da LAI, que prevê uma única prorrogação por mais 10 dias, poderia ser considerado um modelo mais flexível, onde a prorrogação possa ser feita por até três vezes, desde que devidamente justificada. Isso consideraria as particularidades do tratamento de dados e as dificuldades de adaptação das empresas. 3. Critérios para Prorrogação: Definir critérios claros para a prorrogação do prazo. Esses critérios podem incluir a complexidade da solicitação, a necessidade de consultas a terceiros ou a localização dos dados solicitados dentro de grandes conjuntos de dados. A justificativa para cada prorrogação deveria ser comunicada ao titular dos dados de forma transparente. 4. Mecanismo de Revisão e Feedback: Implementar um mecanismo pelo qual os titulares dos dados possam receber atualizações regulares sobre o status de suas solicitações, especialmente se uma prorrogação do prazo for necessária. 5. Período de Transição: Considerar um período de transição onde prazos mais longos possam ser aplicáveis, dando às empresas tempo para se adaptarem completamente às exigências da LGPD. Após esse período, os prazos poderiam ser gradualmente reduzidos à medida que as práticas de gestão de dados e atendimento às solicitações se tornassem mais eficientes. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Formato Simplificado (2 dias) sem análise profunda: 1. Confirmar tratamento: Fornecer confirmação de forma direta, sem análise detalhada. 2. Transparência sobre consentimento: Explicar obtenção, não consentimentos e revogação de forma simples. 3. Informar não ser agente de tratamento: Comunicar papel da organização de maneira direta. 4. Finalidade específica do tratamento: Comunicar finalidades de forma concisa. 5. Informação de tratamento automatizado: Confirmar existência e explicar de modo simples. Formato Detalhado: 1. Acesso aos dados: Identificar e recuperar dados específicos, considerando sistemas complexos. 2. Correção: Verificar solicitação e atualizar dados nos registros da organização. 3. Anonimização, bloqueio ou eliminação: Realizar alterações solicitadas com cuidado. 4. Portabilidade: Coletar e preparar dados em formato específico, considerando sistemas de TI. 5. Eliminação: Identificar e remover dados relevantes de forma segura. 6. Informação de compartilhamento e finalidade: Revisar acordos e políticas. 7. Oposição de tratamento: Avaliar solicitações considerando bases legais. 8. Forma e duração do tratamento: Detalhar processos e prazos. 9. Cópia: Emitir cópias em formato seguro. 10. Relação de dados: Levantar dados nos sistemas da organização. 11. Hipótese de tratamento: Esclarecer as hipóteses legais. Para atrasos no atendimento: 1. Comunicação clara: Informar o titular sobre atrasos e explicar o motivo. 2. Justificativa detalhada: Fornecer razões específicas e identificar causas raiz. 3. Novo prazo: Estabelecer novo prazo realista. Para atendimentos antecipados – Boa Fé: 1. Comunicação proativa: Informar o titular sobre o atendimento antes do prazo. 2. Boa prática e transparência: Destacar atendimentos antecipados como boas práticas. 3. Feedback do titular: Considerar feedback para melhorar processos. 4. Análise interna: Utilizar casos como estudos de caso para melhorias futuras. ","615484": "As características essenciais de um canal de atendimento para assegurar essa

efetividade são: 1. Acessibilidade: O canal de atendimento facilmente acessível, sem barreiras ou complicações que possam desencorajar o contato, garantindo que titulares com diferentes preferências e capacidades possam comunicar-se eficazmente. 2. Clareza e Compreensibilidade: A comunicação através do canal deve ser clara e compreensível para os titulares dos dados. 3. Resposta Rápida: É essencial para a correção tempestiva de dados inexatos ou desatualizados, em conformidade com o princípio da qualidade dos dados. 4. Segurança e Privacidade: Os canais de atendimento devem implementar medidas de segurança para verificação da identidade do titular. 5. Registro e Documentação: É importante que os canais de atendimento mantenham registros das interações com os titulares. 6. Feedback e Melhoria Contínua: O canal deve permitir e encorajar o feedback dos titulares sobre a experiência de atendimento. 7. Capacitação da Equipe: As equipes responsáveis pelo atendimento devem ser bem informadas e capacitadas sobre a LGPD e os direitos dos titulares, garantindo que possam fornecer informações precisas e orientações adequadas.

;"615485": "Sim, na minha opinião o atendimento ao titular deveria ser de responsabilidade do agente que interage diretamente com o mesmo. Quando se trata de interação direta e atendimento aos titulares de dados, a entidade que mantém contato direto com o titular desempenha um papel crucial na efetivação dos direitos dos titulares.

1. Princípio da Transparência e Acessibilidade: Quando a entidade que mantém contato direto com o titular é responsável por atender às suas solicitações, isso naturalmente facilita um processo mais transparente e acessível. 2. Eficiência na Resposta: A entidade com contato direto geralmente possui mais contexto sobre as interações com o titular e, portanto, está em uma posição melhor para entender e processar suas solicitações de forma eficiente e eficaz. 3. Clareza na Comunicação: Titulares de dados podem não estar sempre cientes da distinção técnica entre controladores e operadores. A responsabilidade pelo atendimento direto das solicitações pelo ente com quem o titular tem interação direta simplifica a comunicação e torna o processo menos confuso para o titular, promovendo uma melhor experiência do usuário. Essa prática é eficaz e alinhada com os princípios de proteção de dados ao designar a responsabilidade pelo atendimento direto aos titulares para a entidade ou pessoa que tem contato direto com eles. Isso melhora a maneira como as operações diárias são conduzidas, tornando mais fácil para os titulares dos dados acessarem informações sobre como seus dados estão sendo usados, garantindo transparência no processo e, ao mesmo tempo, melhorando a eficácia na proteção dos direitos desses titulares.

;"615486": "Desafios na Implementação de Canais de Atendimento: - Verificação Segura da Identidade do Solicitante: Um aspecto crítico no atendimento é a capacidade de verificar de forma segura e eficaz a identidade do solicitante. - Proteção dos Dados Durante Todo o Processo: Garantir a proteção e a segurança dos dados pessoais durante todo o processo de atendimento ao titular. Isso inclui proteger os dados contra acesso, divulgação ou alteração não autorizados, bem como contra perda, destruição ou dano acidental.

1. Canais de Comunicação: Análise de Necessidades: análise cuidadosa de suas capacidades, do perfil de seus titulares de dados e do volume de solicitações para determinar os canais de atendimento mais adequados. Canal Único ou Múltiplos Canais: a empresa pode optar por manter um canal único de atendimento eficiente ou oferecer múltiplos canais. 2. Transparência, facilidade e agilidade: Propõe-se um canal unificado de comunicação para receber e tratar todas as solicitações inicialmente, independentemente de sua classificação na LGPD, visando remover obstáculos iniciais ao acesso. Isso simplifica o início do pedido para todos os titulares, independentemente de seu conhecimento da lei. Após identificar a necessidade específica da solicitação, a empresa fornece informações detalhadas sobre prazos e procedimentos relevantes, atendendo à exigência de transparência da LGPD de

forma contextualizada e diretamente relevante para o solicitante, evitando sobrecarregá-lo com informações genéricas.

3. Estrutura de Atendimento O Encarregado atender diretamente a todas as solicitações pode ser inviável em organizações grandes ou com alto volume de demandas. Uma estratégia baseada em volume pode ser adotada, com equipes especializadas de atendimento ao titular, supervisionadas pelo Encarregado. Isso agiliza o processo, permitindo que o Encarregado foque em questões mais complexas e regulatórias. Deixando sempre o contato do Encarregado disponível.

","615487":":","615491":":Proteção de Direitos de 3os: Se a confirmação puder revelar informações relacionadas a terceiros, e essas informações estiverem sob a proteção de direitos como a privacidade, propriedade intelectual ou segredos comerciais. exemplo: Quando um titular solicita acesso a suas imagens nas quais aparece junto com outras pessoas. Mesmo borrando os rostos das outras pessoas para cumprir a solicitação, a identidade desses indivíduos pode ser inferida ou reconhecida pelo solicitante, especialmente considerando que, na maioria das vezes, o solicitante conhece as pessoas na imagem. Elementos como o contexto da imagem, localização, data ou características particulares podem gerar a identificação indireta.

Prevenção à Fraude e Proteção ao Consumidor: Quando houver suspeita que a solicitação é fraudulenta ou uma tentativa de enganar. Por exemplo, se houver razões para acreditar que a solicitação foi feita por alguém que não é o titular, a empresa poderia se recusar a confirmar a existência de tratamento até que a identidade do solicitante seja adequadamente verificada.

Conflitos com obrigações contratuais/legais: Casos em que a confirmação poderia colocar a empresa em conflito com obrigações contratuais ou legais, especialmente em setores altamente regulados. Por exemplo, regulamentações específicas de setores como o financeiro, saúde ou jurídico podem impor restrições ao compartilhamento de informações, exigindo das empresas uma avaliação cuidadosa antes de confirmar o tratamento de dados pessoais.

Proteção e melhor interesse da criança/adolescente (idosos, indígena, proteção a vítimas): Em situações onde a segurança ou o bem-estar do menor possa estar em risco, a proteção integral do menor deve prevalecer sobre outros direitos e interesses. Exemplo: situações de suspeita de abuso tanto físico quanto psicológico ou mesmo trabalho escravo. Ao negar acesso a dados pessoais, a empresa deve basear sua decisão na lei e estar pronta para explicar e justificar essa decisão de forma transparente.

","615492":":","615489":":","615490":":","615494":":","615493":":Estratégias deve considerar diferentes capacidades organizacionais: 1. Empresas com capacidade para oferecer ambos os Formatos. 2. Empresas com capacidade limitada a um único formato: especialmente pequenas e médias empresas (PMEs) com recursos limitados. A escolha do formato disponível deve ser claramente comunicada aos titulares dos dados, explicando as razões da limitação de formato, sempre buscando garantir a segurança e a integridade dos dados fornecidos. 3. Variação conforme o tipo de dado e/ou volume: situações onde o formato de dos dados possa depender do tipo de dado pessoal em questão (por exemplo, dados sensíveis que exigem maiores precauções de segurança), a empresa deve especificar as condições sob as quais cada tipo de dado será acessível.

Transparência e Comunicação com o Titular: ¿ Detalhar em seus avisos de privacidade ou em comunicações específicas as opções de formato disponíveis para o acesso aos dados, incluindo quaisquer limitações ou condições aplicáveis. ¿ Providenciar justificativas claras e baseadas em critérios legítimos para quaisquer restrições no formato de disponibilização dos dados. ¿ Assegurar que os titulares dos dados estejam cientes de seus direitos e de como podem exercê-los dentro das opções de formato disponibilizadas pela empresa.

","615502":":","615501":":","615505":":","615503":":","615504":":","615511":":","615514":":","615513":":","615512":":Sim, por exemplo quando necessidade de Consistência:, se o tratamento

de dados necessitar que as informações estejam consistentes com documentos oficiais ou registros governamentais — por exemplo, para processos de verificação de identidade, operações financeiras ou cumprimento de obrigações regulatórias específicas, o controlador deve negar temporariamente a correção até que a alteração do nome seja oficialmente reconhecida pelos órgãos competentes.

,"615517":",","615516":",","615518":",","615523":",","615521":",","615617":",","615618":",","615619":",","615620":","

{ "615450": "MANIFESTAÇÃO OI S.A: Tendo em vista que a Lei de Acesso à Informação prevê o fornecimento de informações de maneira imediata, sem a necessidade de formalização de pedido ou em até 20 dias, prorrogável por mais 10 dias, entendemos que os prazos adotados poderiam ir no mesmo sentido, considerando que: • Há direitos que podem ser atendidos de forma imediata, como o de confirmação, por exemplo conforme melhor evidenciado na resposta subsequente; • A possibilidade de dilação de prazo é bem-vinda, na medida em que poderá abarcar o atendimento a demandas mais complexas; • Conforme pontuado pela ANPD no texto introdutório, prazos pré-estabelecidos dão sensação de maior segurança ao titular ao mesmo tempo que o seu cumprimento demonstra o comprometimento do controlador com a análise da demanda. É necessário ponderar, todavia, que o referido prazo só deve ser contabilizado a partir da confirmação da identidade dos titulares, quando aplicável, considerando principalmente que as principais plataformas de atendimento aos direitos dos titulares somente dão início ao atendimento após a confirmação dessa etapa. Além disso, podem existir outros direitos, previstos em legislações diversas, mas conexas com o tema de proteção de dados. Nesses casos devem ser observados os prazos específicos eventualmente específicos em tais normas. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "MANIFESTAÇÃO OI S.A: Considerando os arranjos sistêmicos, o volume de dados pessoais que podem ser tratados por agentes de tratamento, bem como as etapas operacionais para a) validação da identidade de titulares de dados; b) formatação da resposta à solicitação de acesso pelo titular, é preciso cautela na interpretação do inciso I do art. 19 da LGPD. Em primeiro lugar é importante recordar que o caput do art. 19 menciona dois direitos distintos, são eles: 1) confirmação da existência e 2) acesso aos dados pessoais. Muito embora a redação do artigo seja um tanto confusa, não nos parece distante da realidade interpretar que o art. 19, I se refira ao direito de “confirmação de existência do tratamento de dados pessoais” e o inciso II; ao direito de acesso. E isso se deve muito à expressão “imediatamente”, a qual, pelos pontos trazidos nessa manifestação, é praticamente impossível de se operacionalizar. Nessa senda, boa prática seria entender que a disponibilização imediata do direito à confirmação de existência seria suprida desde a publicação de “avisos de Privacidade” íntegros e aderentes aos ditames do art. 9º da LGPD, ao passo que ao disponibilizar informações como dados pessoais tratados, finalidades e categorias de titulares de dados já se tornaria possível inferir pela confirmação (ou não) do tratamento de dados de determinado titular (de maneira imediata, como preconiza o art. 19, II) Por outro lado, caso seja a intenção o recebimento da cópia dos dados pessoais que eventualmente sejam tratados pelo agente de tratamento, agora sim, estaríamos à luz do art. 19, II, prevendo-se tempo hábil para resposta segura (vide o encargo de autenticação da identidade do titular) e completa (vide as questões prático-operacionais para localização de dados, formatação de resposta e retorno efetivo ao titular de dados). ", "615484": "MANIFESTAÇÃO OI S.A: Independente do formato do atendimento a ser realizado, se por caixa departamental ou com o apoio de ferramentas, o canal de atendimento a direitos dos titulares deve ser acessível e transparente, ou seja, de fácil utilização e ser de clara disponibilização aos titulares, como, por exemplo, disponível no site oficial do agente de tratamento ou em seu Aviso de Privacidade. Essa clareza e disponibilidade são importantes, pois, uma vez empregadas, devem ser levadas em consideração no momento da reclamação de titulares, caso esses entrem em contato com outros canais de atendimento do agente de tratamento, como o SAC, por exemplo. O

que se pretende dizer é, considerando a obrigação legal de disponibilidade de canal específico, é imperioso que o titular entre em contato apenas com essa via para a resolução de seus direitos previstos da LGPD, bem como que a ANPD apenas considere como contato prévio os atendimentos realizados por esse canal em específico. ";615485": "MANIFESTAÇÃO OI S.A: Primeiramente, é preciso destacar que todos os operadores, pelo menos no que se refere ao seu quadro de colaboradores, serão controladores em algum tratamento de dados realizado. Nesse sentido, entende-se que todos os agentes de tratamento devem possuir canal de atendimento de direitos operante. Adicionalmente, ressalta-se que o operador, enquanto agente de tratamento subordinado aos comandos do controlador, pode vir a auxiliá-lo no cumprimento de suas obrigações, inclusive no atendimento aos direitos dos titulares. A maneira como essa cooperação ocorrerá, no entanto, depende de fatores como (i) o contexto do tratamento, (ii) o tipo de atividade exercida pelo operador e (iii) dos protocolos definidos entre as Partes. Assim, considerando a pluralidade de cenários possíveis, restringir a cooperação dos operadores a determinadas condutas pode acabar por deixar de fora aspectos específicos. Nesse sentido, entendemos que a via contratual e os demais protocolos entre as sejam capazes endereçar, não apenas as particularidades de cada contexto, mas também as próprias decisões do Controlador a fim de melhor atender aos direitos dos titulares. ";615486": "MANIFESTAÇÃO OI S.A: Por tratar de tema específico, o canal de atendimento aos direitos dos titulares demanda a tratativa por profissionais especializados no tema, o que não ocorre no atendimento feito pelo SAC. Como consequência e até mesmo pelo volume inferior de demandas, a equipe de atendimento aos titulares tende a ser reduzida, se comparada com o atendimento ao consumidor o qual, por vezes, é composto até mesmo por dezenas de equipes terceirizadas. Nesse sentido, importar diretrizes de atendimento com escopo e nível de especialização diverso seria trazer obrigações não apenas onerosas, mas desproporcionais aos agentes de tratamento de dados. Adicionalmente, ao contrário do pretendido pela Autoridade, o efeito de tal medida pode esvaziar o atendimento aos titulares, ou seja, no afã de atender a diretrizes como as destacadas abaixo, os agentes de tratamento podem incorporar os direitos dos titulares no seu atendimento SAC o que pode acabar prejudicando a experiência do mais interessado, o titular, na medida em que, na tentativa de massificar os atendimentos, esses não serão mais realizados por equipe especializadas, mas sim por operadores generalistas. Como reforço ao ponto acima, vale recordar que a LGPD é expressa ao entregar ao Encarregado pelo tratamento de dados pessoais a responsabilidade de interlocutor entre o agente de tratamento e o titular de dados, o que nos referenda o ideal de especialidade exigida nesse atendimento. Em decorrência desse contexto, os agentes de tratamento investiram fortemente para a construção e solidificação de equipes e procedimentos especializados no atendimento aos direitos dos titulares. Ir em sentido oposto, com a equiparação dessa interlocução com o titular com demandas de cunho completamente diverso, pode resultar na fragilização desses times especializados e, em última medida, gerar o deterioramento do tema dentro desses ambientes, impactando diretamente o cuidado com os dados pessoais e os seus titulares. Assim, conclui-se desde de já que não devem ser adotadas quaisquer diretrizes do Decreto SAC. ";615487": "MANIFESTAÇÃO OI S.A: Sim, o próprio protocolo de atendimento às solicitações de titulares já empregadas pelos agentes de tratamento. Assim, é necessário que a ANPD, com o intuito de verificar as práticas comumente adotadas, não priorize uma forma em detrimento de outras, mas realize estudo com o objetivo de apresentar uma gama de possibilidades de atendimento, considerando o que já é feito no mercado e, principalmente, fatores como volume de dados, tipo de tratamento e porte dos agentes. Isso, porque diferentemente de outros temas, nos quais a inexistência

de manifestação ou orientação por parte da Autoridade acaba por gerar um vácuo de efetividade, o atendimento às solicitações de titulares de dados já é uma realidade posta e imposta aos agentes de tratamento. Nesse sentido, é imperioso que, antes da publicação de qualquer material orientativo ou – quiçá, regulatório sobre o tema, a ANPD se debruce sobre as práticas já adotadas pelos Controladores brasileiros, de modo a entender e aproveitar aquilo que já está sendo implementado na prática.

;"615491": "MANIFESTAÇÃO OI S.A.: Tendo em vista que nenhum direito é absoluto, é imprescindível que sejam estabelecidas hipóteses de negativa por parte dos agentes de tratamento, a fim de que seja dada maior segurança jurídica a determinadas operações, além de reduzir eventuais atritos junto aos titulares de dados pessoais. Nesse mesmo sentido, vale ressaltar que as limitações a serem estipuladas não importam em afronta aos direitos e liberdades fundamentais dos titulares, muito pelo contrário. A definição desse cenário de maneira pré-estabelecida evitará o não atendimento por parte dos agentes de maneira desarrazoada. Nesse sentido, no que se refere ao direito de confirmação, entendemos ser possível indicar alguns cenários de negativa, para além do segredo industrial:

- Proteção de direitos e liberdades de outros titulares de dados pessoais: há hipóteses de solicitação que podem afetar dados de outros titulares e, por conseguinte, o atendimento a esse direito pode ser limitado. Como exemplo, é possível citar uma limitação no atendimento para defender os direitos e as liberdades de terceiro através de um inquérito administrativo e/ou processo disciplinar ou investigação de alegações de assédio no local de trabalho.
- Atividades de Supervisão: em atividades como auditorias e investigações, é possível que a confirmação do tratamento possa prejudicar o êxito dos trabalhos.
- Sigilo profissional: profissionais como médicos e advogados, possuem o dever de sigilo profissional e, nesse sentido, podem não conseguir atender ao direito de confirmação, sob o risco de infração de outras determinações legais.

;"615492": "MANIFESTAÇÃO OI S.A.: No que tange à identificação dos controladores, considerando que as informações a serem disponibilizadas pelos agentes de tratamento visam oportunizar ao titular o exercício de seus direitos e o acesso a informações sobre eventual tratamento de dados pessoais realizado, a disponibilização desse tipo de conteúdo nos sites institucionais pode ser adequada, na medida em que esses apresentam a empresa, seus propósitos e metas. Em resumo, o que se pretende dizer é que não é preciso, principalmente considerando a variedade de porte de agentes, que essas informações estejam engessadas em um formato específico, como o Aviso de Privacidade por exemplo, desde que esse conteúdo esteja de fácil acesso. No que se refere a informações sobre o compartilhamento, em um primeiro momento, é preciso ter cautela na disponibilização desses dados, uma vez que há tópicos relevantes a serem observados, como o segredo industrial, a alta rotatividade de terceiros e a própria segurança dos dados do titular. Explica-se:

- Segredo industrial;
- Rotatividade de terceiros (fornecedores);
- Segurança dos titulares;

À vista do exposto, conclui-se ser possível atender ao direito previsto e, ao mesmo tempo, resguardar os demais pontos críticos por meio da indicação das categorias de empresas que podem receber dados e as respectivas finalidades. Casos excepcionais poderiam ser informados numa segunda camada de atendimentos ao titular, se necessário. Por fim, objetivando dirimir quaisquer dúvidas, o atendimento a esse direito a partir da divulgação das categorias das empresas não importa em falta de controle sobre quais são os agentes com os quais o controlador compartilha dados, isso porque essa governança já é realizada a partir de outro instrumento, o ROPA.

;"615489": "MANIFESTAÇÃO OI S.A.: Assim como o exposto na pergunta I.d, primeiramente, é preciso destacar que todos os operadores, pelo menos no que se refere ao seu quadro de colaboradores, serão controladores em algum tratamento de dados realizado. Nesse sentido, entende-se que todos os agentes de

tratamento devem possuir canal de atendimento de direitos operante. Adicionalmente, resalta-se que o operador, enquanto agente de tratamento subordinado aos comandos do controlador, pode vir a auxiliá-lo no cumprimento de suas obrigações, inclusive no atendimento aos direitos dos titulares. A maneira como essa cooperação ocorrerá e quais responsabilidades serão estabelecidas, no entanto, dependem de fatores como (i) o contexto da atividade de tratamento, (ii) do tipo de atividade exercida pelo operador e (iii) dos protocolos definidos entre as Partes. Assim, considerando a pluralidade de tratamentos possíveis, restringir a cooperação dos operadores a determinadas condutas pode acabar por deixar de fora aspectos específicos. Nesse sentido, entendemos que a via contratual e os demais protocolos entre as são capazes endereçar, não apenas as particularidades de cada contexto, mas também as próprias decisões do Controlador a fim de melhor atender aos direitos dos titulares.

","615490": "MANIFESTAÇÃO OI S.A.: Considerando os arranjos sistêmicos, o volume de dados pessoais que podem ser tratados por agentes de tratamento, bem como as etapas operacionais para a) validação da identidade de titulares de dados; b) formatação da resposta à solicitação de acesso pelo titular, é preciso cautela na interpretação do inciso I do art. 19 da LGPD. Em primeiro lugar é importante recordar que o caput do art. 19 menciona dois direitos distintos, são eles: 1) confirmação da existência e 2) acesso aos dados pessoais. Muito embora a redação do artigo seja um tanto confusa, não nos parece distante da realidade interpretar que o art. 19, I se refira ao direito de “confirmação de existência do tratamento de dados pessoais” e o inciso II; ao direito de acesso. E isso se deve muito à expressão “imediatamente”, a qual, pelos pontos trazidos nessa manifestação, é praticamente impossível de se operacionalizar. Nessa senda, boa prática seria entender que a disponibilização imediata do direito à confirmação de existência seria suprida desde a publicação de “avisos de Privacidade” íntegros e aderentes aos ditames do art. 9º da LGPD, ao passo que ao disponibilizar informações como dados pessoais tratados, finalidades e categorias de titulares de dados já se tornaria possível inferir pela confirmação (ou não) do tratamento de dados de determinado titular (de maneira imediata, como preconiza o art. 19, II) Por outro lado, caso seja a intenção o recebimento da cópia dos dados pessoais que eventualmente sejam tratados pelo agente de tratamento, agora sim, estaríamos à luz do art. 19, II, prevendo-se tempo hábil para resposta segura (vide o encargo de autenticação da identidade do titular) e completa (vide as questões prático-operacionais para localização de dados, formatação de resposta e retorno efetivo ao titular de dados). No que se refere às informações mínimas, pela multiplicidade de tratamentos possíveis, entendemos que esse deve ser um rol a ser acordado de maneira setorial. Agir contrariamente pode trazer obrigações impossíveis (ausência de tratamento dos dados listados).","615494": "MANIFESTAÇÃO OI S.A.: A fim de atender aos princípios da transparência e do direito à informação, o Aviso de Privacidade, disponibilizado no site oficial dos controladores, pode ser o meio pelo o qual os titulares conseguirão obter informações mínimas sobre o tratamento de seus dados pessoais. Todavia, tendo em vista a pluralidade de tratamentos possíveis, incluindo aqueles que envolvem processos de decisões automatizadas, entende-se que a definição de rol mínimo de informações deva ser analisado com cautela, sendo factível fornecê-lo como recomendação/boa-prática, a depender dos casos em concreto. Feita essa ressalva, entende-se que no conjunto de informações mínimas ao titular possam estar presentes tópicos como: • Glossário, com a definição dos principais termos trazidos pela LGPD; • Canal de Atendimento ao Direito dos Titulares; • Esclarecimento sobre como os dados são tratados, coletados e compartilhados; • Informações sobre o armazenamento, como local e período de retenção; • Indicação sobre as medidas de segurança adotadas; Por fim, ressalva-se que ainda não é possível concluir sobre quais

seriam as informações básicas a serem disponibilizadas quando falamos em decisões automatizadas, tendo em vista a atual falta de consenso sobre um passo anterior e fundamental, a definição do que seriam tais decisões. Assim, conclui-se que é preciso o avanço do amadurecimento do tema antes de qualquer imposição de obrigação nesse sentido.

","615493": "MANIFESTAÇÃO OI S.A.: Sim. É preciso destacar que, especificamente no direito de acesso, não há qualquer obrigação legal de fornecimento de dados de maneira que esses sejam interoperáveis. É preciso levar em consideração, ainda, que o atendimento ao referido direito de forma diversa que não em formato digital pode implicar custos desproporcionais aos agentes de tratamento, a depender do volume de solicitações recebidas. Assim, a fim de garantir proporcionalidade, entende-se que o formato de atendimento ao direito deve ser correspondente à sua coleta, ou seja, apenas deveria ser recomendado a disponibilização em papel, por exemplo, caso a coleta dos dados seja feita de mesmo modo.

","615502": "MANIFESTAÇÃO OI S.A.: Conforme esclarecido no Código de Boas Práticas publicado, o setor de telecomunicações regulamentou o seu processo de portabilidade numérica por meio do Regulamento Geral da Portabilidade – RGP (Resolução nº 460/2007). Essa é uma importante iniciativa regulatória que se encontra alinhada com as discussões deste Código e com a LGPD. O procedimento existente permite a portabilidade dos dados entre prestadores de serviço, a pedido do titular, para que esse não fique vinculado a um determinado serviço por conta da ausência dessa previsão. No caso das prestadoras de serviços de telefonia, a migração do número de telefone do titular, e a consequente migração do contrato de prestação de serviços, possibilita a completa interoperabilidade dos serviços de telefonia há anos, se tratando de iniciativa verdadeiramente inovadora. Nesse sentido, a portabilidade numérica executada pelas prestadoras pode ser considerada um importante precursor do art. 18, V, da LGPD, cumprindo com a função pretendida pelo referido dispositivo legal. Para que a portabilidade numérica ocorra, é necessário que o titular de dados solicite o serviço, passando por processos de provisão, notificação, validação, nos termos descritos no art. 32 do RGP, o que implica em troca de informações entre a prestadora doadora e a prestadora receptora, além da Entidade Administradora (ABR Telecom) e a própria Anatel.

","615501": "","615505": "","615503": "MANIFESTAÇÃO OI S.A.: Sim.

","615504": "MANIFESTAÇÃO OI S.A.: Sim, considerando a variedade de contextos a depender de cada setor.

","615511": "MANIFESTAÇÃO OI S.A.: Devem ser considerados para os conceitos acima, definições que envolvam os seguintes pontos:

- Dados incompletos: dados que não contêm todas as informações necessárias para cumprir o propósito para o qual foram coletados. Exemplo: dado de endereço sem a informação de CEP. Ou, ainda, número de telefone sem os quatro últimos dígitos.
- Dados inexatos: dados com erros, como de digitação ou de entrada de dados. Exemplo: números invertidos ou letras trocadas.
- Dados desatualizados: dados que não refletem o contexto atual do titular de dados pessoais.

","615514": "MANIFESTAÇÃO OI S.A.: Como qualquer outro direito, aqueles exercidos pelo titular também não são absolutos. Assim, a princípio é preciso ter como premissa a impossibilidade nos casos em que a correção pode implicar em feitos significativos, como para o próprio titular ou para a prestação dos serviços. Dentre eles, podemos citar:

- Ausência de envio de documentação comprobatória de identidade ou negativa de participação de quaisquer etapas de verificação de identidade. Nesse caso, esses procedimentos visam garantir a segurança dos dados pessoais e autodeterminação do titular e, por esse motivo, não seria factível atender o direito sem, antes, confirmar a titularidade do solicitante;
- Impossibilidade de alteração de determinados dados, os quais costumeiramente são utilizados como chave de identificação única dos titulares, como código de cliente ou número de contrato, por exemplo.
- Informações históricas como dados de

compras e outras informações contratuais armazenadas para fins de exercício regular de direitos e cumprimento de obrigações legais. ","615513": "MANIFESTAÇÃO OI S.A: Primeira-mente, é preciso destacar que o rol a ser definido precisa ter caráter exemplificativo, ou seja, é possível que o controlador entenda como desproporcional determinado atendimento fora dos critérios trazidos, desde que realize a devida fundamentação. Perpassado esse ponto, entendemos que os critérios abaixo podem ser considerados para avaliar a impossibilidade ou o esforço desproporcional:

- Custo financeiro e tecnológico: se o custo financeiro e/ou tecnológico necessário para comunicar toda a cadeia de agente envolvida no tratamento for muito elevado em relação aos recursos disponíveis da empresa, isso poderia ser considerado um impeditivo.
- Complexidade da solicitação: se estivermos diante de uma solicitação que envolva vários agentes de tratamento, na casa de dezenas, por exemplo, uma solicitação de correção de dados pessoais poderia ser considerada um esforço desproporcional.
- Impacto nas operações do controlador: tendo em vista o potencial de solicitações de direitos dos titulares e a multiplicidade de agentes com os quais os dados podem ser compartilhados na atual economia data driven, o impacto às operações do controlador e à equipe de privacidade devem ser considerados. Informar, por exemplo, acerca do pedido de exclusão para toda a complexa rede de parceiros de um bureau de crédito, por exemplo, pode sobrecarregar as operações do negócio e as demais atividades da equipe dedicada à proteção dos dados pessoais. Adicionalmente, é imperioso destacar que todos os critérios acima ficam ainda mais pungentes quando verificamos que a determinação prevista no art. 18, § 6º requer cumprimento imediato o que, além de extremamente difícil na prática, ainda traz a insegurança jurídica no que tange a sua aferição. Por fim, deve-se relembrar que a grande maioria dos tratamentos realizados pelos agentes de tratamento atualmente (muitas vezes o core do negócio) tiveram a sua concepção muito antes do advento da LGPD. Assim, estruturar um fluxo comunicacional nesses casos pode gerar impacto demasiado aos controladores.

","615512": "MANIFESTAÇÃO OI S.A: Assim como pontuado na questão IV.b, como qualquer outro direito, aqueles exercidos pelo titular também não são absolutos. Assim, a princípio é preciso ter como premissa a impossibilidade nos casos em que a correção pode implicar em feitos significativos, como para o próprio titular ou para a prestação dos serviços. Dentre eles, podemos citar:

- Ausência de envio de documentação comprobatória de identidade ou negativa de participação de quaisquer etapas de verificação de identidade. Nesse caso, esses procedimentos visam garantir a segurança dos dados pessoais e autodeterminação do titular e, por esse motivo, não seria factível atender o direito sem, antes, confirmar a titularidade do solicitante;
- Impossibilidade de alteração de determinados dados, os quais costumeiramente são utilizados como chave de identificação única dos titulares, como código de cliente ou número de contrato, por exemplo.
- Informações históricas como dados de compras e outras informações contratuais armazenadas para fins de exercício regular de direitos e cumprimento de obrigações legais.

","615517": "MANIFESTAÇÃO OI S.A: Sim. Ao contrário do que se possa afirmar, a necessidade de fundamentação por parte do titular não significa qualquer tipo de barreira ao exercício de seus direitos, mas sim uma etapa fundamental, a qual auxiliará o agente de tratamento:

- i. No entendimento da percepção do titular;
- ii. Na elaboração do retorno mais claro e adequado, a depender do contexto relatado pelo solicitante;
- iii. Na avaliação da pertinência da solicitação. Em sendo o caso de ser pertinente, a fundamentação auxiliará o agente adotar as medidas técnicas adequadas para a remediação. Vale fazer a ressalva de que essa fundamentação não se traduz, necessariamente, na comprovação da ilegalidade, mas sim em sua demonstração/indicação, para que, desse modo, o Controlador possa responder a contento e a própria ANPD compreenda melhor a

48

acima, é possível citar decisões que afetem as circunstâncias financeiras de alguém, como sua elegibilidade para crédito; decisões que afetam o acesso a serviços de saúde; decisões que negam oportunidades de emprego ou que os coloquem em séria desvantagem; ou decisões que afetam o acesso à educação, por exemplo, admissões universitárias. Em suma, assim como defendido pelo WP29, em suas Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, para considerar que determinado interesse está sendo afetado, é necessário que a decisão tomada de maneira automatizada afete direitos legais do titular, como, por exemplo, de acesso à saúde ou à educação. "615619": "MANIFESTAÇÃO OI S.A: O cenário de utilização de inteligência para a realização de decisões automatizadas cresce e se altera a cada dia. Assim, a priori é preciso destacar como primeiro desafio implementar regras mínimas de atendimento a esse direito, quando o contexto pode ser tão diverso. Além dessa primeira adversidade, é possível destacar outros entreves práticos ao atendimento do referido direito, como: • Opacidade algorítmica: ou seja, há casos em que nem mesmo quem desenvolveu a inteligência é capaz de compreender, com amplitude, como determinados algoritmos operam, fazem escolhas ou chegam a conclusões específicas; • Dificuldades na explicabilidade: em razão de ser um tema extremamente técnico, os agentes de tratamento possuem o desafio de serem transparentes de maneira inteligível ao titular de dados; • Sigilo: como sempre levantado quando o tema é suscitado, é imprescindível ponderar acerca do desafio de garantir a transparência e informações aos titulares sem que esse retorno afete o segredo de negócio e, até mesmo, a segurança dos dados dos próprios titulares. • Complexa cadeia de atores de IA: o desenvolvimento de uma inteligência artificial costumeiramente envolve uma intrincada cadeia de agentes, cada um responsável por etapas específicas de formação da tecnologia. Assim, a tarefa do Controlador em atender a solicitações do gênero envolverá todas os entreves expostos acima, multiplicados pela variedade desses agentes. "615620": "MANIFESTAÇÃO OI S.A: Quando as indagações do titular tiverem o potencial de impactar o segredo de negócio ou a segurança de seus dados pessoais. É imperioso ressaltar que a revisão não tem, por si só, o condão de alterar as decisões tomadas de maneira automatizadas, mas apenas de revisá-las a partir da indagação do titular. Tendo em vista que a grande maioria dos titulares não possui conhecimento técnico na área é necessário que a ANPD faça esse esclarecimento nos materiais e posicionamentos a respeito do tema. "

{ "615450": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): A lei 12.527/11 traz o prazo de 20 dias (artigo 11, parágrafo 1º), prorrogável por mais 10 dias (parágrafo 2º, desde que mediante justificativa expressa, da qual será cientificado o requerente. Vale apontar que o art. 12, item 3 do GDPR, prevê prazo de um mês a contar da data de recepção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento deverá informar o titular sobre a prorrogação e os motivos da demora de atender o prazo inicial de 30 dias. Ambos os prazos acima são mais razoáveis e trazem ao setor privado a possibilidade de responder em prazo maior, já que em determinados tratamentos de dados, a cadeia de agentes de tratamento de dados pode ser extensa. Entendemos ainda que a resposta, ainda que simplificada, não necessariamente deve ser imediata. Sugerimos a adoção do prazo mínimo de 30 (trinta) dias para qualquer situação. ", b.

Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Os prazos dispostos nos incisos I e II do artigo 19 são exclusivos para a confirmação de existência ou acesso a dados pessoais. Portanto, não significa os prazos para atendimento de demais requerimentos dos Titulares. Prazos para atendimento de requisições dos Titulares conforme sugestão no item (a) acima. I – Imediatamente não é um prazo factível a depender do tamanho da empresa e da cadeia de tratamento de dados. Entendemos que as entidades devem possuir, ao menos, um prazo de 5 (cinco) dias úteis para confirmar a existência ou não do tratamento de dados, exceto em circunstâncias excepcionais, onde direitos fundamentais dos titulares de dados forem violados. Definição do que é simplificado. Trata-se de somente confirmar se os dados são ou não tratados pela entidade? Entendemos que sim.

II – Considerar o tamanho da empresa e a cadeia de tratamento dos dados. Isso pode levar um tempo até a entidade ter todas as informações e 15 dias pode ser um prazo exíguo. Sugerimos a adoção de prazos superiores conforme resposta anterior. ", "615484": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): É importante que a ANPD reconheça a liberdade que o controlador possui para estabelecer o canal que irá utilizar para atendimento de direitos dos titulares, em conformidade com as obrigações e melhores práticas de segurança da informação que o controlador está sujeito. O controlador deve direcionar o titular que exercer seus direitos pelo canal incorreto para este canal único, bem como só serão considerados válidos os pedidos efetuados pelo canal indicado pelo controlador. Além disso, deve ressaltar a identificação do controlador, suas informações de contato e a forma de validação da identidade do titular Assim, entendemos que o canal deve ser acessado formalmente e preferencialmente por escrito para registrar o contato entre o titular dos dados e a entidade. Se o atendimento for realizado por um humano, sugerimos que seja nos dias úteis e em horário comercial. Em caso de atendimento eletrônico (ex.: chatbot), o atendimento poderá ser 24hs, mas, o prazo de atendimento deve iniciar no primeiro dia útil subsequente a abertura do chamado. ", "615485": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): A responsabilidade do operador deve ser limitada ao escopo do seu tratamento de dados, ou seja, desde que dentro da lei e tenha seguido as instruções do controlador, ele não deve ser responsável pela concretização do atendimento dos direitos dos titulares. No entanto, o operador deve ter obrigação de cooperar com o controlador, prestando as informações e documentos necessários referente aos dados pessoais no atendimento dos direitos dos titulares de dados, sendo que

os limites e obrigações de cooperação do operador de dados pessoais sejam estabelecidos contratualmente com o controlador. ","615486":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Entendemos que o controlador deve ter a liberdade de escolha do canal que irá utilizar para atendimento de direitos dos titulares. Obrigar as empresas a ter um SAC para atendimento dos direitos dos titulares de dados vai onerar substancialmente as empresas. A forma de comunicação entre o Titular de Dados e cada entidade deve ser definida pela própria empresa e, preferencialmente, por escrito. Empresas que já tenham SAC estabelecido podem usar, como liberalidade, este canal. Adicionalmente, via de regra esses canais são empresas terceirizadas, ou seja, mais uma entidade na cadeia de tratamento dos dados pessoais. ","615487":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Entendemos ser importante que a ANPD reconheça a liberdade que o controlador possui para estabelecer o canal que irá utilizar para atendimento de direitos dos titulares, em conformidade com as obrigações e melhores práticas de segurança da informação que o controlador está sujeito. ","615491":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615492":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Razão Social, CNPJ, site institucional e meio de contato. ","615489":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): A ANPD deve reiterar que a obrigação de efetivar o atendimento de direitos dos titulares é do controlador. A responsabilidade do operador deve ser limitada ao escopo do seu tratamento de dados, ou seja, desde que dentro da lei e tenha seguido as instruções do controlador, ele não deve ser responsável pela concretização dos direitos dos titulares. O Titular de dados não deve ter acesso ao Operador para obter informações sobre o tratamento de seus dados pessoais. O atendimento ao Titular deve se concentrar no controlador dos dados, ou seja, àquele a quem compete a tomada de decisões sobre o tratamento. No entanto, o operador deve ter obrigação de cooperar com o controlador dos dados pessoais no atendimento dos direitos dos titulares de dados. ","615490":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): CONTRIBUIÇÃO CONTROLADAS: Como a legislação impõe que a declaração em formato simplificado seja efetivada imediatamente (neste documento propomos que o prazo seja de até 5 (cinco) dias úteis, a ideia do legislador é que o direito seja viabilizado de forma ágil. Desta forma, propomos que a declaração simplificada possua apenas a confirmação (SIM/NÃO) do tratamento. ","615494":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): As informações mínimas que devem ser repassadas sobre o tratamento de dados pessoais, independente de requerimento, são as previstas no artigo 9º da LGPD. Quanto à transparência em relação aos critérios e procedimentos utilizados para a decisão automatizada, é fundamental que a autoridade traga um conceito de “decisão automatizada”, nos termos propostos no item “a” do Bloco VII, e que este contemple efetivamente um aspecto decisório que tenha impacto real na vida do titular de dados, bem como que a transparência se dê em conformidade com a proteção ao segredo comercial e propriedade intelectual do controlador. ","615493":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Sim. A forma de disponibilização da informação, desde que mantenha a sua segurança e confidencialidade, pode ser disponibilizada em formato físico ou digital. No entanto, entendemos que a escolha não deve ser do Titular, já que a segurança da informação é algo importante de governança de cada empresa e cabe à esta decidir a forma de disponibilização dessa informação para manter não somente está governança e rastreabilidade. Importante ressaltar que o formato de disponibilização dos dados deve ser proporcional, não implicando em esforço desproporcional ao controlador dos dados, bem como deve considerar os meios de contato normalmente mantidos entre o

titular e o controlador. ","615502":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615501":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615505":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615503":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615504":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615511":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615514":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Entendemos que as entidades devem buscar a confirmação oficial de que o titular que busca a correção de determinada informação é, de fato, o proprietário daquelas informações. Então, a simples declaração não pode ser considerada como suficiente para o exercício do direito à correção. Para os casos de operações de tratamento de dados pessoais que os dados não sejam fornecidos pelo próprio titular, este deverá apresentar documentação que comprove a veracidade do dado que pretende corrigir. Além disso, para situações que a simples declaração pareça inverídica (ex: fornecimento de e-mails manifestamente temporários, preenchimentos aleatórios como "1234567, acbdefg, etc""), "615513":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): O esforço desproporcional deve ser analisado faticamente, como por exemplo o porte do controlador de dados, o número de agentes de tratamento envolvidos, a nacionalidade destes agentes de tratamento envolvidos e os meios de contato disponíveis, bem como o relacionamento existente entre estes controladores. Esforço desproporcional, no contexto de fornecer informações ao titular de dados sobre o tratamento de dados pessoais, geralmente se refere a uma situação em que o custo, a complexidade ou o tempo necessários para fornecer essas informações são considerados excessivos em relação aos benefícios para o titular dos dados ou em relação aos requisitos legais ou regulamentares. Em outras palavras, se o esforço necessário para fornecer as informações supera razoavelmente o benefício ou a necessidade dessas informações para o titular dos dados, pode ser considerado desproporcional. Por exemplo, se um conjunto de dados for muito grande e complexo, ou se os custos associados à busca e fornecimento dessas informações forem excessivamente altos, pode ser considerado desproporcional exigir que o controlador forneça todas as informações solicitadas. Nessas situações, os controladores de dados podem buscar maneiras alternativas de cumprir suas obrigações de transparência, como fornecer informações de forma mais resumida ou simplificada, ou fornecer informações sobre como os titulares dos dados podem acessar suas próprias informações de forma mais autônoma. No entanto, é importante ressaltar que o conceito de "esforço desproporcional" pode variar dependendo do contexto e das leis de proteção de dados aplicáveis. ","615512":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Sim. O controlador pode se negar a apresentar qualquer informação quando: (i) não conseguir comprovar que o titular requerente é de fato o proprietário desses dados; (ii) Se o controlador comprovar que os dados contestados são precisos e não estão sujeitos a correção (iii) Se a correção dos dados contestados resultar na mudança da base legal ou da finalidade para o tratamento desses dados e não houver uma base legal adequada para a correção; (iv) caso o titular exerça o direito de correção de forma abusiva, por exemplo, realizando solicitações frequentes e infundadas; (v) quando a correção tem potencial de risco ao titular e sua acurácia não puder ser comprovada. ","615517":"CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Entendemos que o tratamento dos dados pessoais por uma empresa ou entidade é realizado de forma fundamentada e de acordo com um dos incisos do artigo 7º da Legislação. Nesse sentido, entendemos que

não é uma liberalidade exclusiva do titular determinar eventual desnecessidade, excessividade, desconformidade ou descumprimento legal. Todos esses itens devem ser fundamentados e comprovados. No entanto, o atendimento deve seguir sendo uma liberalidade, também fundamentada pelo Controlador. O não atendimento do requerimento, desde que justificado, ainda é uma liberalidade do Controlador. ","615516": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Sim. Como a anonimização retira o caráter pessoal de um dado, este pode ser adotado alternativamente à eliminação, conforme definido pelo controlador dos dados. ","615518": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): As tratativas para atendimento ao direito dos titulares se dá exclusivamente entre o controlador e o titular, sendo que a decisão final sobre a continuidade do tratamento deve ser tomada pelo próprio Controlador. Caso o titular não concorde com o tratamento, poderá intermediar tais tratativas por meio do mecanismo “Petição do Titular Contra o Controlador” junto a ANPD. A legitimidade da alegação não deverá implicar necessariamente a aplicação de sanções, visto que estas deverão seguir o procedimento administrativo aplicável, com garantia do contraditório e ampla defesa. ","615523": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): A revogação do consentimento não necessariamente leva à obrigação de eliminação dos dados pessoais. A revogação do consentimento, como mais uma base legal, leva a empresa a não mais tratar os dados conforme autorização anteriormente concedida. No entanto, se a empresa tiver outra base legal que justifique o tratamento dos dados pessoais, ainda que para a mesma finalidade, o tratamento poderá continuar a acontecer. Caso disponível o controlador poderá enquadrar a operação de tratamento em outra base legal aplicável. ","615521": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): O artigo 8 dispõe que o consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. A revogação também deve seguir o mesmo formato, ou seja, expresso e por escrito. No entanto, a revogação do consentimento não necessariamente leva à eliminação dos dados pessoais tratados. A manutenção dos dados e seu tratamento dependerá do fundamento legal e governança do controlador, a existência de outra base legal válida para o tratamento, , como também a existência de obrigações regulatórias, exercício regular de direitos, etc.. ","615617": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Decisão automatizada: Na decisão automatizada um sistema informatizado toma autonomamente e sem supervisão ou revisão de um ser humano. Decisão tomada unicamente com base em tratamento automatizado de dados pessoais: um ser humano toma uma decisão, tomando como fundamento para essa decisão um tratamento automatizado de dados pessoais (scores, inteligência artificial, motores de decisão, etc). Imprescindível que a ANPD faça essa distinção de conceitos, concentrando os esforços de regulamentação na decisão automatizada. ","615618": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): sem contribuições. ","615619": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Dentre as dificuldades para implementação da revisão de decisões automatizadas estão: (a) A distinção clara para o titular de dados dos casos que se tratam de decisões automatizadas de dados pessoais e decisões tomadas unicamente com base no tratamento automatizado de dados pessoais; (b) A tradução para termos simples e compreensíveis para o titular de dados, considerando a compreensão do “homem médio” de lógicas matemáticas e algoritmos que sustentam sistemas de aprendizado de máquina e inteligência artificial; (c) A proteção do segredo comercial, propriedade intelectual e segredos de negócio ao efetivar este direito. ","615620": "CONTRIBUIÇÃO ABES (Associação Brasileira das Empresas de Software): Sim, quando não se enquadrar nas condicionantes para o

exercício de revisão de decisões automatizadas, quais sejam: a) quando não se tratar de uma decisão automatizada; b) quando esta não for o único critério decisório utilizado; c) quando a decisão automatizada não impactar os interesses do titular ou definam o perfil pessoal, profissional, de consumo, de crédito ou os aspectos da personalidade do titular.

"

{ "615450": "-", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? - "615484": "O canal deve estar disponível em local de fácil acesso, cuja finalidade seja indubitável ao titular. Recomenda-se que haja possibilidade da efetivação do atendimento tanto de forma eletrônica quanto de forma física, a fim de que aqueles que tenham dificuldades com o mundo digital não deixem de ser atendidos ou tenham seus direitos suprimidos. O atendimento ao titular de dados deve ser realizado de forma clara, simples e objetiva, de modo que não haja dúvidas quanto à resposta pretendida. O canal de atendimento deve, ainda, conter o nome do DPO (encarregado de dados) responsável pelo agente de tratamento em questão e uma outra forma de contato, caso necessário. Ademais, o canal de atendimento deve preocupar-se em verificar a identidade do titular, coletando os mínimos dados necessários para responder de forma efetiva a solicitação, nos termos do artigo 6º, inciso III, da LGPD, tais como nome, e-mail, 3 primeiros dígitos do CPF e telefone, evitando o envio de cópias de documentos, fotos do titular portando sua documentação e uso de tecnologias que possibilitam captura de biometria. É necessário, ainda, disponibilizar o rol de direitos expressos no art. 18, da LGPD. Para melhor compreensão do agente de tratamento, sugere-se, ainda que o canal indague a relação do titular com o agente de tratamento, bem como se a solicitação é para ele ou para terceiro. Deve haver, ainda, preocupação com a confirmação de identidade do titular: o titular receberá no e-mail cadastrado um token, devendo confirmar a solicitação realizada. A partir disso, o agente de tratamento deve conferir se o e-mail descrito no formulário é o mesmo e-mail que o titular deixou como forma de contato em sua base de dados. Em caso negativo, o pedido deve ser negado, sendo respondido ao titular que os dados cadastrados não são os mesmos. Caso os dados sejam correspondentes, o agente de tratamento deve responder a solicitação de forma clara, precisa e objetiva, evitando termos técnicos e respostas automáticas que pouco auxiliam na efetivação do direito solicitado. "615485": - "615486": - "615487": "O Canal de Atendimento ao Titular de Dados, conectado à plataforma Privacidade&Você é um modelo que pode ser seguido e é utilizado por mais de 3 mil empresas e órgãos públicos (https://www.privacidade.com.br/portal-de-privacidade?token=c319342ef39f3dda91b50332c0abacd8&site_url=https%3A%2F%2Fimmunizesys-tem.com%2F). A partir de um selo físico e digital chamado de “Canal de Comunicação LGPD”, o agente de tratamento o disponibiliza em seu local de preferência. O titular de dados poderá solicitar seu atendimento preenchendo formulário com os dados mínimos, tais como nome, e-mail, 3 primeiros dígitos do CPF e telefone. Evita-se o envio de cópias de documentos, fotos do titular portando documentação e uso de tecnologias que capturam biometria - coleta de dados excessiva. Sugere-se, ainda, que o canal indique a relação do titular com o agente de tratamento, bem como se a solicitação é para ele ou para terceiro, comprovando vínculo/autorização. O modelo ora descrito é hábil para atender volume expressivo de titulares de dados, conciliando tecnologia e conhecimento humano. O titular receberá, de forma automática, no e-mail cadastrado, um token, devendo confirmar a solicitação realizada. O agente de tratamento também deve conferir se o e-mail descrito no formulário é o e-mail que o titular deixou como forma de contato em sua base de dados (uso de IA). Em caso negativo, caso o e-mail do titular ou telefone ou 3 primeiros dígitos do CPF não estejam de acordo com a base de dados do agente de tratamento, o pedido deve ser negado ou pode haver cancelamento automático, caso o e-mail não seja validado. A IA também realiza respostas automáticas para determinados tipos de pedidos (legitimidade,

por exemplo), mas sempre há a validação humana que confirma a resposta. A IA também pode ser usada para detectar pedidos semelhantes, gerando respostas automáticas, que sempre passam pelo crivo humano para garantir que o titular está sendo respondido de forma satisfatória. Toda essa operação, ocorre dentro de um único sistema, garantido maior rastreabilidade."

615491":"-","615492":"-","615489":"-","615490":"-","615494":"-","615493":"-","615502":"-","615501":"-","615505":"-","615503":"-","615504":"-","615511":"-","615514":"-","615513":"-","615512":"-","615517":"-","615516":"-","615518":"-","615523":"-","615521":"-","615617":"-","615618":"-","615619":"-","615620":"-"

{ "615450": "O prazo de 20 dias, prorrogáveis por mais 10 dias parece ser plausível. 30 dias consecutivos parecem razoáveis. Sugere-se prazos diferenciados e/ou possibilidade de prorrogações, considerando conjuntamente: - modelos de negócio B2C e B2B, pois as bases de dados dos negócios B2C tendem a ser mais integradas, facilitando a busca. Já os negócios B2B podem ter mais públicos de interesse com diversos tamanhos e diferentes bases de dados não integradas; - tamanho das empresas, por conta do volume das bases de dados; - inciso do art. 18, LGPD, pois acesso completo, correção, anonimização, bloqueio ou eliminação e portabilidade podem ser mais complexos; - entes públicos e privados, por conta de seguimentos de atuação, públicos diversos, flexibilidade de recursos etc. A depender dessas considerações, o prazo poderia ser acrescido de mais dias. Sugere-se mais 5 dias a depender de cada critério. Portanto, mais 20 dias ao todo, chegando-se ao prazo máximo de 50 dias consecutivos. Quando da efetiva regulamentação, sugere-se esclarecer os prazos de atendimento, início e fim da contagem de prazo e possibilidade de prorrogação. Qualidade e formato de resposta deveriam ser objeto de orientação para padronizar e facilitar, inclusive, portabilidade e entendimento dos titulares. Sugere-se um prazo global e não prorrogável - 50 dias consecutivos. Isso facilitará eventual customização de sistemas. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "- modelos de negócio B2C e B2B; - existência ou não de bases de dados integradas; - quantidade e tamanho dos públicos de interesse do controlador; - natureza da atividade final prestada pelo controlador a justificar o tratamento dos dados pessoais; - tamanho das empresas, por conta do volume das bases de dados; - inciso do art. 18, LGPD, pois acesso completo, correção, anonimização, bloqueio ou eliminação e portabilidade podem ser mais complexos; - entes públicos e privados, por conta de seguimentos de atuação, públicos diversos, flexibilidade de recursos etc. - quantidade de mão de obra disponível ao controlador para atender as demandas do art. 18, LGPD; - quantidade de dados pessoais tratados; e - quantidade de solicitações simultâneas previstas nos incisos I e II do art. 19 da LGPD. Sugere-se um prazo global e não prorrogável para ambos os incisos - 50 dias consecutivos. Isso facilitará eventual customização de sistemas. ", "615484": "• Obrigatoriedade de autenticação dos titulares para acesso ao canal; • Segurança da informação na interação entre titular e agente de tratamento; • Não solicitar muitas informações para fazer a demanda, pedindo apenas aquelas necessárias para autenticação; • Solicitar o mínimo de cópia de documentos para autenticação; • Segurança da informação interna ao agente de tratamento, permitindo a interação segura entre as diversas áreas do agente de tratamento para o atendimento ao titular; • Sistema permitir interação entre titular e agente de tratamento e vice-versa, incluindo a possibilidade de inserir anexos; • Acessibilidade: o canal deve ser facilmente identificado no aviso de privacidade ou nas formas de comunicação do ente; • Transparência: canal de atendimento deve fornecer informações claras sobre como entrar em contato, o propósito do canal e os prazos de resposta esperados; • Transparência ativa: fornecer no aviso de privacidade informações por público de interesse quanto à finalidade, prazo e segurança; • Qualidade: informações precisas e completas, em formato facilmente inteligível; • Permitir controle de prazo. ", "615485": "Sim, baseando-se nos art. 18, §3º; 39, 42, 44 e 49 da LGPD. Cabe ao operador que receber a requisição do titular informar a este que tal requisição será respondida pelo controlador caso esse seja o detentor das informações essenciais do tratamento. Ao ser demandado pelo controlador para apoio ao atendimento de demanda, responder tempestivamente para que o

controlador observe o prazo legal, com a qualidade e prazo avençados entre os agentes de tratamento. A depender da natureza do tratamento e a previsão contratual existente, se o operador tiver todas as informações necessárias para atender as demandas dos titulares (finalidade, hipótese legal, natureza dos dados pessoais tratados e duração do tratamento), deve responder diretamente aos titulares com a qualidade e prazo orientado pelo controlador. Este pode solicitar periodicamente relatório sobre tais atendimentos.

","615486": "Apenas as diretrizes relativas à qualidade do atendimento poderiam servir de insumo para regulamentação. A parte de garantia de registro numérico do protocolo é possível se o atendimento for feito em sistema, podendo ser gerado automaticamente, mas pode não ser a realidade de muitas organizações. Questões de disponibilidade, acessibilidade, atendimento e acompanhamento das demandas precisam ser repensadas em termos de segurança da informação. "

","615487": "O modelo de atendimento da Petrobras considera todos os itens informados acima. Internamente, dispomos de normativos internos a regular o atendimento conforme itens acima. O foco na segurança começa no atendimento da demanda, que precisa de login e senha, seja da Petrobras ou pelo GOV.BR. "

","615491": "Atenção aos princípios da segurança, prevenção e responsabilização e prestação de contas previstos no art. 6º, LGPD, caso não seja possível autenticar o titular de dados (confirmar a autenticidade da identidade do solicitante e/ou de seu representante legal) ou outra previsão legal, como caso fortuito ou força maior."

","615492": "Pessoa física: nome completo, número de identificação ou CPF, meio de contato. Pessoa jurídica: razão social, CNPJ, meio de contato específico para questões de LGPD. Compartilhamento de dados: dados acima acrescidos da hipótese legal e finalidade do compartilhamento. "

","615489": "Cabe ao operador que receber a requisição do titular informar a este que tal requisição será respondida pelo controlador caso esse seja o detentor das informações essenciais do tratamento. Ao ser demandado pelo controlador para apoio ao atendimento de demanda, responder tempestivamente para que o controlador observe o prazo legal, com a qualidade e prazo avençados entre os agentes de tratamento. A depender da natureza do tratamento, se o operador tiver todas as informações necessárias para atender as demandas dos titulares (finalidade, hipótese legal, natureza dos dados pessoais tratados e duração do tratamento), deve responder diretamente aos titulares com a qualidade e prazo orientado pelo controlador. Este pode solicitar periodicamente relatório sobre tais atendimentos. Deve fornecer informações claras e transparentes aos titulares sobre como seus dados pessoais são tratados (finalidade, tipos de dados pessoais, hipótese legal, prazos de retenção dos dados) e qualquer informação relevante relativa ao tratamento dos dados. Deve prover os direitos do art. 18, LGPD. "

","615490": "• Afirmativa/negativa de tratamento de dados pessoais do titular; • dados pessoais tratados; • finalidades dos tratamentos; • agentes de tratamento. "

","615494": "Respeitando os segredos comercial e industrial e por público de interesse: • identificação do controlador; • se possível agentes de tratamento; • dados pessoais e dados pessoais sensíveis tratados; • finalidades; • possibilidade de compartilhamento de dados e sua finalidade de forma resumida; • existência de decisão automatizada envolvendo dados pessoais; • canal de contato para exercer os direitos da LGPD. "

","615493": "Sim, conforme § 2º do art. 19 da LGPD, se conjugado aos princípios da segurança, prevenção e responsabilização e prestação de contas. Caso o agente de tratamento não tenha meios de demonstrar a observância desses princípios, tanto a forma digital quanto a física não seriam condizentes com a LGPD. A disponibilização em papel não deveria ser entendida como meramente impressão seguida de postagem, mas sim como impressão segura seguida de disponibilização segura. Reconhece-se a dificuldade de disponibilização segura, especialmente se presencial, pois as disponibilidades das

instalações das entidades podem não ser de fácil acesso a todos os interessados.

","615502": "Setores B2C regulados, como planos de saúde e concessionárias de serviços públicos.", "615501": "Formato, conteúdo e protocolos padronizados conforme regulamentação dos setores. Padrões de segurança uniformes definidos pelos órgãos de regulação para o trânsito seguro dos dados. ", "615505": "Formato, conteúdo, padrões de segurança, meios para compartilhamento, garantido os requisitos de integridade, disponibilidade, confidencialidade, autenticidade, uso e utilidade do dado.", "615503": "Sim, desde que observados os princípios da segurança, prevenção responsabilização e prestação de contas. O ideal seria que a portabilidade fosse realizada tempestiva e diretamente entre os controladores envolvidos, mediante requisição comprovada do titular. ", "615504": "Em um primeiro momento sim, mas deve ser regulado ou normatizado ao menos como boas práticas. O setor privado deve ser envolvido e consultado, mas ao final e periodicamente deve haver regulamentação por parte da ANPD. ", "615511": "Considerando forma razoável e proporcional, baseando-se na finalidade do tratamento e na natureza dos dados em questão, mediante fundamentação/comprovação do titular: • Incompletude: quando não contém todas as informações necessárias para cumprir a finalidade para a qual foi coletado. • Inexatidão: quando não reflete corretamente a informação que representa (erros materiais ou imprecisão que o torna passível de entendimentos diversos). • Desatualização: quando não reflete a informação mais recente, pois houve mudanças nas informações. Mudanças informadas pelo titular ou representante legal e não contempladas ou mudanças ainda não informadas pelo titular ou representante legal. ", "615514": "Após a confirmação da identificação do titular ou de seu representante legal, quando: - houver necessidade de comprovação documental da alteração das informações; - os dados coletados /inicialmente tratados foram baseados em documentos comprobatórios. ", "615513": "• Custos e tempo necessários para a comunicação, considerando a tecnologia disponível à data do tratamento dos dados e na data do pedido. • Meios próprios lícitos (habilidades como dados, instrumentos e técnicas) disponíveis ao próprio agente de tratamento responsável pela comunicação, segundo o parâmetro de boas práticas do segmento em questão. • Elementos pertinentes do caso concreto. • Extinção da empresa ou modificação societária que implique em impossibilidade de contato. • Critérios do § 1º do art. 12, LGPD. ", "615512": "• Quando não for possível confirmar/autenticar a identidade do solicitante como o próprio titular de dados ou de seu representante legal. • Situações em que se comprovem custos e tempo não razoáveis, considerando a tecnologia disponível à data do tratamento dos dados e na data do pedido. • Ausência de meios próprios lícitos (dados, instrumentos e técnicas) disponíveis ao próprio agente de tratamento responsável pela correção, segundo o parâmetro de boas práticas do segmento em questão. • Elementos pertinentes do caso concreto. ", "615517": "Não é necessário, mas desejável. Cabe ao controlador avaliar se há fundamentos legítimos para a manutenção dos dados ou se a solicitação do titular deve ser atendida. A eventual negativa por parte do controlador deve ser justificada.", "615516": "Quando a eliminação não for possível por razões técnicas a anonimização ou o bloqueio podem ser as alternativas perseguidas. Considerando aspectos técnicos, aparentemente, o bloqueio seria mais fácil, depois a anonimização e, por fim, a eliminação. A intenção parece ser impossibilitar o uso identificado ou identificável do dado. ", "615518": "Interrupção do tratamento, a menos que haja hipótese legal a permitir a continuidade do tratamento. • Caso não haja outra hipótese legal, espera-se a eliminação. • Caso esta não seja possível, perseguir a anonimização ou o bloqueio. • Se tiver havido compartilhamento, cabe ao controlador notificar ao terceiro quanto à determinação de eliminação/bloqueio/anonimização dos dados pessoais. • Se tiver dano, verificar responsabilização. O controlador deve informar ao titular as

providências tomadas em resposta à sua solicitação de oposição, inclusive a continuidade do tratamento de forma justificada, se for este o caso. ","615523": "Não, o direito de revogar não é sinônimo do direito de solicitar eliminação. Essa deve ser solicitada expressamente pelo titular, conforme (artigo 18, VI, da LGPD, respeitadas as situações de guarda do artigo 16).","615521": "A LGPD prevê a irretroatividade da revogação do consentimento, confirmando a legitimidade do tratamento realizado baseado no consentimento válido concedido. O pedido de eliminação deve impedir novo tratamento, mas não deve ser entendido como possibilidade de desfazimento ou invalidação do que foi feito até sua revogação. Sugere-se que haja regulamentação expressa acerca das consequências e implicações fáticas da revogação seguida ou não de pedido de eliminação, quando se tratar do dado pessoal imagem (foto ou gravação), bem como voz, pois materiais produzidos legitimamente sob a égide do consentimento podem ter a circulação dali em diante proibidas, mas o que já foi liberado não teria como ser efetivamente eliminado. As consequências do efeito devem ser comunicadas pelo controlador aos terceiros com os quais compartilhou. ","615617": "A decisão automatizada é realizada por sistemas automatizados/algoritmos, com ou sem intervenção humana. A decisão tomada unicamente com base em tratamento automatizado é realizada por sistemas automatizados/algoritmos sem intervenção humana. ","615618": "• Potencial tratamento discriminatório • Potencial perda financeira • Potencial perda de oportunidade • Potencial adiamento de oportunidade • Potencial não pagamento de direito líquido e certo • Potencial retenção de pagamento de direito líquido e certo • Potencial postergação de pagamento de direito líquido e certo • Potencial perda de direitos • Potencial impacto negativa na reputação, imagem ou honra • Potencial tratamento de dados pessoais em processos administrativos ou judiciais com consequências punitivas (perda de liberdades, principalmente) • Potencial perda de confidencialidade/sigilo sobre o tratamento de dados pessoais • Potencial acesso (ilegal) a dados pessoais sensíveis • Potencial perda de controle sobre seus dados pessoais • Potencial perda do dado pessoal (eliminação, bloqueio ou anonimização) • Falha de segurança em tratamentos com decisão automatizada (exemplo: Decifração não autorizada ou algoritmo comprometido) • Potencial tratamento de dados pessoais de indivíduos em situação de vulnerabilidade (menores de idade, pacientes, trabalhadores, pessoas em sistemas prisionais etc). • Criação ou atualização de perfilamento sem finalidade objetivas ou sem prévio comunicado ao titular. Justificativa: qualquer tratamento que possa causar prejuízo ou dano, além de restrição de quaisquer direitos. Situações de perfilamento que possam ser usadas para monitoramento também devem ser cuidadosamente entendidas pelo titular, para que possa proteger seus direitos fundamentais de liberdade e de privacidade e desenvolver de forma livre sua personalidade. ","615619": "Qualidade e detalhe das informações passadas pelo controlador sobre o tema. Falta de orientação normativa sobre os parâmetros da revisão, inclusive se a revisão precisa ser conduzida por pessoas e não por nova decisão automatizada. ","615620": "Não pode negar com base nos art. 1º e 6º, LGPD. Contudo, a revisão não deveria ser entendida como sinônimo de o controlador ter que revelar segredos comercial e industrial. Nesta situação de impossibilidade por proteção dos segredos o titular poderia ter o direito de solicitar eliminação, bloqueio ou anonimização. O ônus da prova da impossibilidade de revisão caberia ao controlador e a ele também caberia comprovar como os direitos do titular foram respeitados. "

{ "615450": "A BSA | The Software Alliance (BSA) agradece a oportunidade de fornecer feedback à Autoridade Nacional de Proteção de Dados (ANPD) sobre a consulta pública para regulamentação dos direitos dos titulares de dados pessoais no âmbito da Lei de Proteção de Dados Pessoais (LGPD). Os responsáveis pelo tratamento devem dispor de, pelo menos, um mês (30 dias) para responder a qualquer pedido formulado por um titular de dados. Os controladores também devem ser autorizados a prorrogar, como a concessão de mais dois meses para uma resposta, quando apropriado. Esse prazo está alinhado com os prazos previstos em outras leis globais de proteção de dados, incluindo o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que exige que os controladores respondam às solicitações dos titulares de dados "sem demora indevida e, em qualquer caso, dentro de um mês após o recebimento", mas permite aos controladores prorrogações de dois meses. Em Cingapura, as organizações devem responder às solicitações de acesso "o mais rápido possível", mas devem informar ao indivíduo se não puderem responder a uma solicitação de acesso dentro de 30 dias. Alinhar o cronograma da LGPD para responder às solicitações de direitos dos titulares de dados com prazos reconhecidos em outras leis globais de proteção de dados pode incentivar as empresas a encaminhar as solicitações brasileiras por meio de práticas de conformidade estabelecidas e atualizadas regularmente, em vez de exigir que as empresas criem abordagens pontuais para lidar com as solicitações brasileiras. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Os controladores devem ser autorizados a identificar os critérios para a prestação de notificação simplificada nos termos do artigo 19 da LGPD. Isso é importante porque os controladores devem elaborar um aviso simplificado de forma diferente para diferentes tipos de produtos e serviços. Além disso, as empresas muitas vezes precisarão revisar seus registros para determinar se estão processando os dados pessoais de um indivíduo. Embora o artigo 19 estabeleça que os controladores devem responder a um titular de dados que exerça seu direito de confirmar a existência ou o acesso a dados pessoais "imediatamente" em um "formato simplificado", encorajamos a ANPD a reconhecer que isso não é possível em todas as circunstâncias. Por exemplo, quando um titular de dados não é um usuário registrado ou titular de conta com esse controlador, o controlador pode exigir tempo para revisar seus registros, a fim de confirmar se está processando os dados pessoais desse indivíduo. Encorajamos a ANPD a reconhecer essas circunstâncias, não exigindo que as empresas respondam imediatamente ou reconhecendo que as empresas podem cumprir essa obrigação fornecendo um aviso simplificado informando que estão revisando seus registros em resposta à solicitação do titular dos dados. ", "615484": "Os titulares dos dados devem exercer os direitos previstos na LGPD enviando uma solicitação diretamente a um controlador. Os controladores devem ser obrigados a informar os titulares dos dados sobre formas específicas de exercer esses direitos, tais como descrever o processo na política de privacidade do controlador, que deve ser tornada pública no site do controlador. É importante que a ANPD evite criar requisitos excessivamente específicos sobre os métodos pelos quais um titular de dados exerce esses direitos, devido à grande variedade de controladores que devem honrar as solicitações de direitos em uma ampla gama de produtos e serviços. Os melhores métodos de comunicação para o exercício desses direitos variam muito entre os diferentes produtos e serviços. ", "615485": "A LGPD reconhece os diferentes papéis dos controladores (que decidem como e por que coletar os dados pessoais de um titular de dados) e dos operadores (que processam dados pessoais em nome de um

controlador e sujeitos às suas instruções). Como o controlador é a empresa que decide coletar os dados pessoais de um titular de dados — e a empresa que decide como e por que esses dados são processados — os titulares dos dados devem exercer seus direitos previstos na LGPD indo diretamente a um controlador. Um operador, por sua vez, deve ser obrigado a assistir o responsável pelo tratamento no cumprimento de um pedido de direito do titular dos dados, fornecendo, na medida do possível, medidas técnicas e organizacionais adequadas. Mas os operadores não devem ser obrigados a responder diretamente ao pedido do titular dos dados. Essa estrutura está alinhada com as leis de proteção de dados e privacidade em todo o mundo. Há fortes razões de privacidade e segurança para que a ANPD garanta que os titulares dos dados exerçam seus direitos indo a um controlador, em vez de a um operador. Por exemplo, os operadores muitas vezes não analisam os dados pessoais armazenados em seus serviços — mas podem ter que revisar dados que, de outra forma, não fariam se fossem obrigados a confirmar se estão processando dados pessoais de um determinado indivíduo. Além disso, os operadores não tomam os tipos de decisões necessárias para responder aos pedidos de direitos do titular dos dados, porque responder aos pedidos requer determinar quais os campos de dados que devem ser fornecidos a um titular de dados ou se as informações que o titular dos dados procura corrigir são imprecisas. Essas decisões são tomadas pelos controladores, assim como as entidades que decidem como e por que processar os dados pessoais de um indivíduo. Incentivamos fortemente a ANPD a reconhecer a importância de os titulares de dados exercerem seus direitos indo diretamente ao controlador. ";615486": "Por gentileza, veja nossos comentários acima, em resposta à pergunta c. É importante que a ANPD não adote uma abordagem única para o método pelo qual os titulares de dados exercem direitos sob a LGPD, porque esses direitos se aplicarão a uma variedade de produtos e serviços diferentes nos quais diferentes métodos podem ser apropriados. ";615487": "Por favor, veja nossos comentários acima, em resposta à pergunta c. É importante que a ANPD não adote uma abordagem única para o método pelo qual os titulares de dados exercem direitos sob a LGPD, porque esses direitos se aplicarão a uma variedade de produtos e serviços diferentes nos quais diferentes métodos podem ser apropriados. ";615491": "Sim, os controladores não devem ser obrigados a conceder a solicitação de acesso do titular dos dados em todos os casos. Como questão inicial, este direito só deve aplicar-se se o responsável pelo tratamento tiver verificado a identidade do titular dos dados, a fim de evitar o fornecimento de dados pessoais ao indivíduo errado. Além disso, haverá uma série de circunstâncias em que a concessão de acesso não é apropriada e a ANPD deve reconhecer que os controladores não devem ser obrigados a fornecer acesso a dados pessoais em tais cenários. Estes podem incluir quando o fornecimento de acesso a dados pessoais restringir a capacidade de um responsável pelo tratamento ou do seu operador de: • Cumprir leis ou regulamentos; • Cumprir com uma investigação civil, criminal ou regulatória de uma autoridade governamental ou cooperar com agências regulatórias e de aplicação da lei; • Investigar, estabelecer, exercer, preparar ou defender reivindicações legais; • Fornecer um produto ou serviço especificamente solicitado por um consumidor; • Executar um contrato do qual o consumidor é parte, incluindo o cumprimento de uma garantia por escrito • Tomar medidas imediatas para proteger um interesse que seja essencial para a vida ou a segurança física do titular dos dados ou de outra pessoa física; • Prevenir, detectar, proteger contra ou responder a incidentes de segurança, roubo de identidade ou quaisquer atividades ilegais, ou preservar a integridade, integração ou segurança de seus sistemas; • Participar de pesquisas científicas ou estatísticas públicas ou revisadas por pares; ou • Auxiliar outro controlador, processador ou terceiro com qualquer uma dessas atividades listadas. ";615492": "Os

titulares dos dados devem exercer seu direito de acesso dirigindo-se diretamente a um controlador. O controlador deve responder ao titular dos dados com base nas informações disponíveis para esse controlador, mas não deve ser obrigado a fornecer informações relacionadas a ou em nome de outro controlador."615489": "Por favor, veja nossa resposta à pergunta I.d, acima. Tal como explicado nessa resposta, um operador não deve ser obrigado a responder a pedidos de direitos do titular dos dados. Em vez disso, os controladores – as empresas que decidem como e por que processar os dados pessoais de um indivíduo – devem ser obrigados a responder a essas solicitações, conforme reconhecido nas principais leis de proteção de dados em todo o mundo. Um operador, por sua vez, deve ser obrigado a auxiliar o controlador a atender a uma solicitação de direito do titular dos dados, fornecendo medidas técnicas e organizacionais adequadas, na medida do possível."615490": "Os artigos 18 e 19 da LGPD exigem que os controladores confirmem a existência de tratamento de dados pessoais e forneçam acesso a esses dados pessoais. Não se deve exigir que os controladores confirmem a existência do processamento de uma maneira específica, pois esse direito se aplica aos controladores que fornecem uma ampla gama de produtos e serviços - e para os quais diferentes formas de confirmação podem ser apropriadas. Portanto, recomendamos que a ANPD não exija que um aviso de "formato simplificado" inclua uma lista específica de informações, devido ao potencial de variação significativa."615494": "A BSA não pretende responder a esta pergunta."615493": "Sim. Os artigos 18 e 19 da LGPD exigem que os controladores forneçam acesso aos dados pessoais do titular dos dados. Essa obrigação deve ser considerada cumprida quando o acesso for fornecido."615502": "A BSA não pretende responder a esta pergunta."615501": "A BSA não pretende responder a esta pergunta."615505": "A BSA não pretende responder a esta pergunta."615503": "Sim. Encorajamos a ANPD a reconhecer que o direito à portabilidade pode ser satisfeito fornecendo ao titular dos dados os dados pessoais que o titular dos dados forneceu anteriormente ao controlador em um formato portátil, estruturado e legível por máquina. Isso permite que o titular dos dados transmita esses dados pessoais a outro controlador, sem levantar as questões de segurança e privacidade que podem acompanhar os pedidos de transmissão de dados pessoais diretamente a outro controlador."615504": "A BSA não pretende responder a esta pergunta."615511": "Os controladores devem exercer um julgamento independente para determinar se os dados pessoais estão incompletos, imprecisos ou desatualizados. No entanto, se um titular de dados considerar que um responsável pelo tratamento negou indevidamente o seu pedido de correção de dados pessoais, o responsável pelo tratamento deve dispor de um processo claro para que os titulares dos dados recorram dessas decisões."615514": "Os controladores devem exercer julgamento independente para determinar se devem atender à solicitação de um titular de dados para corrigir dados pessoais. Por exemplo, em alguns casos, os titulares dos dados podem tentar "corrigir" dados pessoais que sejam precisos, mas pouco favoráveis; os titulares dos dados também podem tentar "corrigir" dados de forma que possam criar oportunidades de fraude. No entanto, se um titular de dados acreditar que um controlador negou indevidamente sua solicitação de correção de dados pessoais, o controlador deverá ter um processo claro para que os titulares de dados recorram de tais determinações."615513": "Há uma série de cenários em que informar outros agentes de processamento sobre o exercício dos direitos do consumidor por um titular de dados pode ser impossível ou envolver um esforço desproporcional, conforme reconhecido pela Seção 6 do Artigo 18 da LGPD. Exemplos incluem quando a notificação a outros agentes de processamento exigiria que um controlador reidentificasse dados pessoais armazenados em formato não identificável ou exigiria que o controlador coletasse dados pessoais que, de outra

forma, não coletaria. Esses dois cenários têm o potencial de criar novos riscos à privacidade dos titulares de dados, em vez de aumentar a privacidade dos mesmos. Além disso, os controladores devem considerar fatores como o número de indivíduos envolvidos, a idade dos dados pessoais e as salvaguardas adotadas pelo controlador para determinar se um esforço é desproporcional."

"615512": "Sim, os controladores não devem ser obrigados a conceder o pedido de correção do titular dos dados em todos os casos. Numa primeira fase, este direito só deve aplicar-se se o responsável pelo tratamento tiver verificado a identidade do titular dos dados – para evitar a correção de dados que não digam respeito ao titular dos dados. Além disso, haverá uma série de circunstâncias em que a correção de dados pessoais não é apropriada. A ANPD deve reconhecer que os controladores não devem ser obrigados a corrigir dados pessoais em tais cenários, inclusive quando o fornecimento de acesso restringiria a capacidade de um controlador ou de seu operador de:

- Cumprir leis ou regulamentos;
- Cumprir uma investigação civil, criminal ou regulatória de uma autoridade governamental, ou cooperar de outra forma com agências de aplicação da lei e reguladoras;
- Investigar, estabelecer, exercer, preparar ou defender reivindicações legais;
- Fornecer um produto ou serviço especificamente solicitado por um consumidor;
- Executar um contrato do qual o consumidor seja parte, incluindo o cumprimento de uma garantia por escrito;
- Tomar medidas imediatas para proteger um interesse essencial para a vida ou a segurança física do titular dos dados ou de outra pessoa singular;
- Prevenir, detectar, proteger ou responder a incidentes de segurança, roubo de identidade ou quaisquer atividades ilegais, ou preservar a integridade ou segurança de seus sistemas;
- Envolver-se em pesquisas científicas, estatísticas públicas ou revisadas por pares; ou
- Auxiliar outro controlador, processador ou terceiro com qualquer uma dessas atividades listadas.

"615517": "A BSA não pretende responder a esta pergunta."

"615516": "A BSA não pretende responder a esta pergunta."

"615518": "A BSA não pretende responder a esta pergunta."

"615523": "Não. Os indivíduos recebem uma série de direitos previstos na LGPD e esses direitos devem ser exercidos individualmente para que os controladores possam entender claramente um pedido individual. Em alguns casos, um indivíduo pode revogar seu consentimento para que um controlador processe dados em conexão com um serviço específico. No entanto, se o controlador excluir os dados desse indivíduo, poderá impedi-lo de fornecer serviços para os quais o indivíduo não retirou o consentimento e ainda gostaria que o controlador fornecesse. Essa situação pode ser evitada se os indivíduos exercerem seus novos direitos individualmente, de modo que os controladores tenham instruções claras de um consumidor sobre o direito que ele pretende exercer."

"615521": "A LGPD dá aos titulares dos dados o direito de retirar o consentimento a qualquer momento. É importante ressaltar que o Artigo 8, Seção 5, reconhece que, uma vez que o consentimento é retirado, "o processamento realizado sob consentimento previamente dado permanece válido enquanto não houver pedido de exclusão". Encorajamos a ANPD a reconhecer que: (1) o direito de retirar o consentimento é voltado para o futuro e não invalida o tratamento realizado sob consentimento previamente dado, e (2) que os controladores devem ter aviso razoável da intenção do titular dos dados de retirar o consentimento, para que possam efetivamente implementá-lo. Essa abordagem se alinharia com outras leis globais de proteção de dados importantes. Por exemplo, de acordo com a Lei de Proteção de Dados Pessoais de Cingapura, os titulares dos dados devem dar "aviso razoável" de sua intenção de retirar o consentimento. A Comissão de Proteção de Dados Pessoais de Cingapura reconheceu que não há uma "abordagem única para todos" para um prazo específico para aviso prévio razoável, mas disse que o aviso de pelo menos 10 dias seria razoável. Da mesma forma, o Gabinete do Comissário de Informação do Reino Unido reconheceu que, se um titular de

dados retirar seu consentimento, "isso não afeta a legalidade do processamento até esse ponto". Embora alguns controladores possam ser capazes de implementar rapidamente a retirada de consentimento de um titular de dados, a ICO reconhece que os controladores podem precisar de um "pequeno atraso enquanto [eles] processam a retirada".

;"615617": "As decisões automatizadas e as decisões tomadas exclusivamente com base no tratamento automatizado de dados pessoais devem ser consideradas como aquelas sem revisão ou envolvimento humano no processo de tomada de decisão. Isso é consistente com as orientações dos principais reguladores de proteção de dados. Por exemplo, a ICO do Reino Unido explicou que "para que algo seja exclusivamente automatizado, não deve haver envolvimento humano no processo de tomada de decisão". O Grupo de Trabalho do Artigo 29, em orientação posteriormente adotada pelo Conselho Europeu para a Proteção de Dados, explicou igualmente que "a tomada de decisão exclusivamente automatizada é a capacidade de tomar decisões por meios tecnológicos sem envolvimento humano".

;"615618": "A ANPD deve criar um padrão claro para o processamento que "afeta" os interesses de um indivíduo e, portanto, é coberto por esse direito. Outras leis de privacidade importantes fazem isso aplicando um direito a decisões que produzem efeitos legais sobre um indivíduo. De acordo com o GDPR, o direito do Artigo 22 de não estar sujeito a uma decisão baseada exclusivamente na criação de perfis automatizados está vinculado se o processamento "produzir efeitos legais em relação a ele ou ela ou afetá-lo significativamente de forma semelhante".

;"615619": "A LGPD permite que os indivíduos solicitem "revisão" de decisões tomadas exclusivamente com base em processamento automatizado. Essa disposição parece contemplar a possibilidade de um controlador pedir a um ser humano que revise uma decisão, mediante solicitação de um controlador. Um problema que surgirá à medida que as empresas responderem a essas solicitações é lidar com um volume potencialmente grande de solicitações. Esse problema será exacerbado se o direito for aplicado de forma ampla, como, por exemplo, se a ANPD adotar um padrão amplo para quando se considera que uma decisão "afeta" o interesse de um indivíduo. Por outro lado, a adoção de um padrão mais restrito diminuirá o número de decisões sujeitas a esse direito, o que pode melhorar a posição das empresas para fornecer revisão humana mediante solicitação.

;"615620": "Sim, esse direito não deve se estender ao processamento que seja necessário para um contrato entre o titular dos dados e o controlador, ou ao processamento baseado no consentimento do titular dos dados, ou ao processamento autorizado por outra legislação aplicável. Agradecemos novamente por seu foco em garantir que os direitos fornecidos aos titulares de dados pela LGPD funcionem na prática. Agradecemos a oportunidade de nos envolvermos mais com a ANPD nessas importantes questões. Sinceramente. Kate Goodloe Managing Director, Policy BSA | The Software Alliance "

{ "615450": "teste fabiola", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "teste fabiola", "615484": "teste fabiola", "615485": "teste fabiola", "615486": "teste fabiola", "615487": "teste fabiola", "615491": "teste fabiola", "615492": "teste fabiola", "615489": "teste fabiola", "615490": "teste fabiola", "615494": "teste fabiola", "615493": "teste fabiola", "615502": "teste fabiola", "615501": "teste fabiola", "615505": "teste fabiola", "615503": "teste fabiola", "615504": "teste fabiola", "615511": "teste fabiola", "615514": "teste fabiola", "615513": "teste fabiola", "615512": "teste fabiola", "615517": "teste fabiola", "615516": "teste fabiola", "615518": "teste fabiola", "615523": "teste fabiola", "615521": "teste fabiola", "615617": "teste fabiola", "615618": "teste fabiola", "615619": "teste fabiola", "615620": "teste fabiola"

{ "615450": "A adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), para o atendimento aos direitos do titular de dados pessoais no setor privado, pode não ser razoável em todos os casos. Isso se deve a diferenças fundamentais entre os contextos e finalidades dessas leis. Enquanto a LAI visa garantir o acesso do público a informações públicas, muitas vezes de natureza administrativa e não pessoal, a LGPD tem como objetivo proteger os dados pessoais dos indivíduos, garantindo seus direitos à privacidade e proteção de dados. Portanto, os procedimentos e prazos para atender aos direitos dos titulares de dados pessoais devem ser adaptados à sensibilidade e complexidade desses dados, bem como à necessidade de proteger os direitos e a privacidade dos indivíduos. Em muitos casos, os prazos da LAI podem ser inadequados para lidar com solicitações de acesso, retificação, exclusão ou portabilidade de dados pessoais, especialmente considerando que esses processos envolvem a verificação da identidade do solicitante, a avaliação da legalidade do pedido e a proteção dos direitos de terceiros envolvidos. Além disso, deve-se ressaltar que os procedimentos internos das organizações privadas podem não estar preparados para lidar com solicitações de maneira tão rápida quanto os órgãos públicos. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "É importante lembrar que nem todos os direitos dos titulares podem ser atendidos imediatamente, especialmente diante da complexidade das solicitações, quantidade de requisições recebidas e recursos disponíveis para o cumprimento dessas demandas. Nesse sentido, para definir os prazos de forma diferenciada conforme previsto nos incisos I e II do art. 19 da LGPD, devem ser considerados diversos critérios: a) Complexidade do pedido - Se a solicitação envolver uma análise mais detalhada dos dados, pesquisa em múltiplos sistemas ou a consulta de fontes externas, o prazo estabelecido no inciso II pode ser mais apropriado para fornecer uma resposta completa e clara ao titular. b) Disponibilidade e acessibilidade dos dados - Se os dados do titular estão prontamente disponíveis e acessíveis pelo controlador, a resposta imediata em formato simplificado (inciso I) pode ser viável. No entanto, se os dados estão dispersos em diferentes sistemas ou requerem processos adicionais para acesso, pode ser necessário o prazo do inciso II para uma declaração completa. c) Impacto na privacidade - Avaliar o potencial impacto na privacidade dos titulares caso a solicitação não seja atendida dentro do prazo estabelecido. Se a demora na resposta pode resultar em danos significativos aos direitos dos titulares, priorizar a análise e resposta da solicitação de acordo com o inciso I. d) Urgência da solicitação - Caso a requisição do titular demande uma resposta rápida diante de caráter urgente, como em situações de emergência ou necessidade imediata de acesso aos dados, o inciso I deve ser aplicado, diante de apresentação do motivo razoável pelo titular. d) Capacidade operacional do controlador - A capacidade operacional, incluindo recursos humanos e tecnológicos disponíveis, deve ser levada em consideração. Se o controlador possui os recursos necessários para atender prontamente às solicitações dos titulares, o inciso I pode ser aplicado. Caso contrário, o prazo mais extenso do inciso II pode ser mais realista. "; "615484": "Para assegurar a efetividade na comunicação entre o titular e o agente de tratamento, algumas características essenciais devem ser consideradas, alinhadas com os princípios da LGPD: a) Transparência: assegurar que o titular seja informado em seu primeiro contato com o canal de atendimento que os dados pessoais compartilhados por ele somente serão utilizados para fins de atendimento, além de disponibilizar a Política de Privacidade para acesso do titular. A título de exemplo, deve ser veiculada

a seguinte mensagem: “Os dados pessoais que você compartilhar serão tratados unicamente para atender a sua solicitação. Suas informações pessoais serão processadas de acordo com as leis de privacidade aplicáveis, em especial, a Lei Geral de Proteção de Dados (Lei nº 13.709/18), conforme descrito na Política de Privacidade e Termos e Condições de Uso, disponíveis no site (link do documento).” b) Acessibilidade: o canal deve ser de fácil acesso, contando com time especializado para atender às solicitações dos titulares. c) Segurança: devem ser empregadas medidas robustas de segurança, como criptografia e autenticação, para evitar incidentes envolvendo vazamentos ou acessos não autorizados. d) Confidencialidade: todas as interações devem ser tratadas de forma confidencial, com garantias de que as informações compartilhadas serão utilizadas apenas para os fins autorizados pelo titular. e) Clareza: uma comunicação clara e precisa, através de linguagem simples, é importante para garantir que o titular compreenda completamente suas opções e direitos em relação ao tratamento de seus dados pessoais. f) Diligência: o agente de tratamento deve responder às solicitações do titular, fornecendo informações precisas seguindo os prazos estabelecidos pela LGPD. ”;"615485":“Embora o artigo 18 da LGPD mencione somente a responsabilidade do controlador de atender às solicitações dos titulares, em alguns casos, os operadores também desempenham um papel fundamental na cooperação para garantir o cumprimento dos direitos dos titulares. A título de exemplo, as requisições podem: (a) ser intermediadas pelos operadores; (b) exigir a colaboração dos operadores para fornecimento de detalhes nas respostas; ou (c) depender da atuação dos operadores para garantir que sejam atendidas. Dessa forma, é importante que haja disposição legal além da mera responsabilidade contratual que estabeleça ao operador a obrigatoriedade cooperação entre as partes, deixando claro que essa cooperação não afetará a posição ocupada pelos agentes de tratamento. No contexto de atendimento aos titulares, é fundamental que os operadores assumam as seguintes responsabilidades: a) Comunicação sobre recebimento de solicitação: informar imediatamente ao controlador após o recebimento de solicitações dos titulares, a fim de permitir que o controlador atenda às solicitações dentro dos prazos estabelecidos pela legislação. b) Facilitar o acesso dos titulares aos seus dados: quando necessário, os operadores devem comprometer-se a colaborar com os controladores, fornecendo todos os detalhes relevantes para garantir respostas completas e precisas às solicitações dos titulares ou autoridades competentes. c) Fornecer informações claras sobre o tratamento de dados: os operadores têm a obrigação de oferecer informações transparentes sobre como os dados dos titulares estão sendo tratados, trabalhando em estreita colaboração com os controladores para garantir a transparência e conformidade com a LGPD. d) Atender a solicitações que dependam da sua cooperação ativa: os operadores devem cooperar com os controladores para garantir que as solicitações dos titulares, como correção ou exclusão de seus dados, sejam atendidas de maneira adequada e dentro dos prazos estabelecidos pela LGPD, caso estas dependam da sua ação. ”;"615486":“Inicialmente, deve-se pontuar que o Decreto nº 11.034/2022 aplica-se a empresas reguladas por órgãos e entidades do governo federal e visa aprimorar o atendimento ao cliente ao estabelecer em seus artigos uma série de obrigações específicas para o atendimento. Embora o modelo de atendimento ao consumidor delineado pelo Decreto nº 11.034/2022 possa servir como referência, especialmente em relação aos princípios estabelecidos no art. 8º, é importante pontuar que nem todas as suas obrigações são adequadas ou aplicáveis ao atendimento relacionado à privacidade de dados pessoais. Isso se deve ao risco de impor um ônus desproporcional e custos excessivos para a manutenção dos canais de atendimento pelos agentes de tratamento, os quais se somariam às despesas de consultoria para conformidade com a LGPD. Entre as diretrizes do Decreto nº

11.034/2022 que não recomendamos a adoção, destacamos: (a) atendimento telefônico obrigatório (art. 3º, § 3º e art. 5º), incluindo atendimento por humano por pelo menos 8 horas por dia (Art. 5º, I) e opções mínimas presentes no primeiro menu, incluídas, obrigatoriamente, as opções de reclamação e de cancelamento de contratos e serviços (Art. 5º, II); (b) multicanalidade, ou seja, diversos canais integrados sendo disponibilizados; e (c) prazos do capítulo V, por diferirem dos elencados na LGPD. Além de causar um ônus desproporcional aos agentes, a justificativa para não adoção desses artigos reside na falta de compatibilidade com a LGPD em relação aos prazos estabelecidos no art. 19, bem como ao disposto no art. 41, § 1º, da LGPD. Este último exige apenas que as informações de contato estejam disponíveis, sem impor a obrigatoriedade de múltiplos canais de contato ou de atendimento telefônico. ";615487": "Um modelo de atendimento que pode servir como paradigma, tanto para agentes privados quanto para o setor público, é o adotado por algumas empresas de tecnologia e plataformas digitais, como o modelo automatizado de atendimento inicial ao cliente via chatbots. Empresas como Amazon, Google e Facebook, entre tantas outras, são exemplos das que adotam esse modelo. Essas empresas implementaram sistemas de atendimento automatizado que utilizam inteligência artificial (IA) e chatbots para lidar com uma grande variedade de consultas e solicitações dos usuários de forma rápida e eficiente. Esses chatbots são capazes de responder a perguntas frequentes, resolver problemas simples e encaminhar questões mais complexas para atendentes humanos quando necessário, lidando com volumes de demandas de forma escalável, o que os torna ideais para lidar com o crescente número de solicitações de proteção de dados. Além disso, eles oferecem uma abordagem econômica para o atendimento ao cliente, reduzindo a necessidade de recursos humanos em muitos casos. Através de respostas instantâneas e precisas, os chatbots podem fornecer informações sobre políticas de privacidade da empresa e responder de forma simples e automática que a solicitação foi recebida e será retornada em 15 dias, conforme previsto na LGPD. Eles também podem orientar os usuários sobre como exercer seus direitos de privacidade, redirecionando-os para a seção adequada. A título de exemplo, o titular pode alterar/corrigir seus dados, solicitar o direito de oposição ao recebimento de e-mail marketing ou SMS envolvendo conteúdo publicitário ou ainda, solicitar acesso ao relatório de dados pessoais em opções contidas em um menu específico da seção de privacidade. Em resumo, o modelo de atendimento ao cliente adotado por empresas de tecnologia pode ser adaptado e aplicado ao atendimento de privacidade, oferecendo eficiência, escalabilidade e economia de recursos. ";615491": "Sim. Há disposições na LGPD que podem ser utilizadas para negar o direito de confirmação da existência de tratamento de dados pessoais, entre elas: a) Falta de qualificação do solicitante: o direito de confirmação pode ser negado se o solicitante não for o titular dos dados ou não possuir representante legalmente constituído, conforme estipulado no artigo 18, § 3º da LGPD. b) Identificação equivocada do agente de tratamento: no caso específico em que há equívoco quanto ao agente de tratamento, devendo ser indicado, se possível, o agente correto, conforme previsto no artigo 18, § 4º, inciso I, da LGPD; c) Razões fáticas ou de direito impeditivas: quando houver razões de fato ou de direito que impeçam a adoção imediata da providência, conforme estabelecido no artigo 18, § 4º, inciso II, da LGPD. Além dessas hipóteses, pode-se fazer um paralelo com o artigo 12 do GDPR, que também prevê a negação de solicitações consideradas manifestamente infundadas ou manifestamente excessivas. Entre os exemplos fornecidos pelo Information Commissioner's Office (ICO) para pedidos "manifestamente infundados", destacam-se situações em que o indivíduo não possui intenção genuína de exercer seu direito de acesso, como quando busca vantagens em troca da retirada do pedido, ou se a solicitação é maliciosa e visa perturbar a organização,

incluindo declarações de má fé, acusações infundadas ou assédio sistemático. Por outro lado, o conceito de "manifestamente excessivo" refere-se a pedidos que são claramente irrazoáveis em relação aos custos ou encargos envolvidos em seu processamento. Isso é determinado considerando a natureza das informações solicitadas, o contexto da solicitação, o relacionamento entre o solicitante e a organização, o potencial impacto de recusar o acesso às informações, os recursos disponíveis da organização e se o pedido é repetitivo ou se sobrepõe a outros pedidos. Caso o controlador não possa atender à solicitação de confirmação, é fundamental que as razões para a recusa sejam claramente esclarecidas em resposta ao titular em linha com o princípio da transparência.

","615492": "Para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais, é essencial fornecer informações que permitam que o titular identifique claramente a empresa ou empresas responsáveis pelo tratamento de seus dados. Isso inclui detalhes como a razão social, número de CNPJ, endereço físico ou eletrônico para contato direto e facilitado, além do tipo de serviço prestado que justifique para o compartilhamento dos dados pessoais. Entretanto, ao lidar com informações sobre controladores e o compartilhamento de dados pessoais, é fundamental encontrar um equilíbrio adequado entre a transparência com os titulares e a proteção dos segredos comerciais e industriais das empresas envolvidas. Portanto, se houver uma justificativa válida para não fornecer detalhes específicos sobre uma empresa, é possível adotar uma abordagem mais genérica, fornecendo apenas informações sobre os dados pessoais compartilhados e a atividade principal (core business) da empresa envolvida, acompanhada da devida justificativa para limitação das informações. Isso permite que os titulares compreendam o propósito do compartilhamento de seus dados sem comprometer a confidencialidade ou a competitividade dos negócios envolvidos. Em suma, deve-se buscar um equilíbrio entre a transparência com os titulares e a proteção dos interesses comerciais legítimos, garantindo que a divulgação de informações seja estratégica e prudente para preservar a segurança e o sucesso dos negócios.

","615489": "Embora o artigo 18 da LGPD mencione somente a responsabilidade do controlador de atender às solicitações dos titulares, em alguns casos, os operadores também desempenham um papel fundamental na cooperação para garantir o cumprimento dos direitos dos titulares. A título de exemplo, as requisições podem: (a) ser intermediadas pelos operadores; (b) exigir a colaboração dos operadores para fornecimento de detalhes nas respostas; ou (c) depender da atuação dos operadores para garantir que sejam atendidas. Dessa forma, é importante que haja disposição legal além da mera responsabilidade contratual que estabeleça ao operador a obrigatoriedade de cooperação entre as partes, deixando claro que essa cooperação não afetará a posição dos agentes de tratamento. No contexto de atendimento aos titulares, é fundamental que os operadores assumam as seguintes responsabilidades: a) Comunicação sobre recebimento de solicitação: informar imediatamente ao controlador após o recebimento de solicitações dos titulares, a fim de permitir que o controlador atenda às solicitações dentro dos prazos estabelecidos pela legislação. b) Facilitar o acesso dos titulares aos seus dados: quando necessário, os operadores devem comprometer-se a colaborar com os controladores, fornecendo todos os detalhes relevantes para garantir respostas completas e precisas às solicitações dos titulares ou autoridades competentes. c) Fornecer informações claras sobre o tratamento de dados: os operadores têm a obrigação de oferecer informações transparentes sobre como os dados dos titulares estão sendo tratados, trabalhando em estreita colaboração com os controladores para garantir a transparência e conformidade com a LGPD. d) Atender a solicitações que dependam da sua cooperação ativa: os operadores devem cooperar com os controladores para garantir que as solicitações dos titulares, como correção ou exclusão de

seus dados, sejam atendidas de maneira adequada e dentro dos prazos estabelecidos pela LGPD, caso estas dependam da sua ação. "615490": "Considerando que o art. 19, I, LGPD exige uma resposta imediata em formato simplificado, entende-se que o conteúdo dessa declaração deve ser sucinto e direto. Nesse sentido, o conteúdo deve restringir-se a informação de que a solicitação será recebida e analisada pelo controlador, sendo retornada de forma completa dentro do prazo de 15 dias do art. 19, II, da LGPD. Adicionalmente, é importante que seja informado o canal de contato e o link da Política de Privacidade, documento que traz informações detalhadas sobre como os dados pessoais são tratados pela organização, incluindo os propósitos do tratamento, as medidas de segurança adotadas, os direitos dos titulares e os procedimentos para exercê-los. Ao limitar a declaração a esses pontos essenciais, garante-se que a resposta esteja em conformidade com o prazo exigido em lei, permitindo ao titular ter ciência de que sua solicitação foi recebida e será tratada adequadamente, ao mesmo tempo em que são fornecidos os meios para contato e acesso a informações adicionais sobre o tratamento de dados pessoais. A título de exemplo, segue modelo de resposta que poderia ser utilizado pelas empresas: “Olá, [nome do titular solicitante]! Recebemos sua solicitação para [explicitar o pedido]. Ela será analisada pelo nosso time e, em até 15 (quinze) dias, você receberá uma resposta completa, em linha com as disposições da Lei Geral de Proteção de Dados (Lei 13.709/18). Para saber mais como a nossa empresa realiza o tratamento de dados pessoais no âmbito de suas operações, acesse nossa Política de Privacidade [link]. Em caso de dúvidas, estamos disponíveis para atendê-lo por meio de nosso canal de atendimento: [contato@contato.com.br]. Atenciosamente, Controlador”.

"615494": "O artigo 9 da LGPD e o artigo 15 do GDPR podem ser utilizados como referência para identificar as informações mínimas que o controlador deve fornecer independentemente de requerimento, com o intuito de assegurar a transparência e o direito à informação dos titulares. De modo a aliviar o ônus sobre o controlador, destacamos entre as informações dos artigos, aquelas que consideramos as informações mínimas mais importantes, que devem ser evidenciadas independentemente de requerimento:

- a) Dados pessoais coletados - Devem ser identificados os tipos de dados pessoais que estão sendo coletados, entre eles, nome, endereço, CPF, além de outros dados específicos que sejam relevantes para a finalidade do tratamento.
- b) Finalidade do tratamento - Deve ser claramente especificado o propósito para o qual os dados pessoais estão sendo tratados. Isso inclui explicar se os dados estão sendo utilizados para fornecer um serviço específico, para cumprir uma obrigação legal, para personalização de conteúdo, entre outras finalidades cabíveis.
- c) Política de Privacidade - Deve ser disponibilizado um link para a Política de Privacidade que esclareça como os dados pessoais são tratados. Essa política deve incluir informações sobre os direitos dos titulares, os procedimentos para exercício, as medidas de segurança adotadas, entre outros aspectos relevantes para a proteção da privacidade.
- d) Contato do controlador - Deve ser fornecido um canal de comunicação através do qual os titulares possam entrar em contato com o controlador, e, caso cabível, com o Encarregado de Proteção de Dados (DPO).
- e) Procedimentos para decisão automatizada - Caso o tratamento inclua decisões automatizadas que afetem significativamente o titular, o controlador deve minimamente informar que a decisão foi tomada com base em critérios automatizados garantindo a transparência desse processo. Sobre os critérios utilizados para a tomada de decisão automatizada, entende-se que podem ser respondidos somente após a solicitação de esclarecimentos, respeitados os segredos comerciais e industriais.

"615493": "Sim, o direito de acesso pode ser considerado satisfeito quando o agente de tratamento disponibiliza os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular. O artigo 18, II da LGPD estabelece

que o titular tem o direito de acessar suas informações pessoais que estão sendo tratadas por um agente de tratamento, sem especificar um formato em que esses dados devem ser disponibilizados. Portanto, se o agente de tratamento oferece ao titular a opção de receber seus dados pessoais de acordo com a escolha do próprio titular, isso atende plenamente ao direito de acesso previsto na LGPD. Afinal, o objetivo do direito de acesso é permitir que os titulares tenham acesso fácil e eficaz às suas informações pessoais, de forma que possam verificar a precisão e a legalidade do tratamento de seus dados. ","615502": "Atualmente, alguns setores têm demonstrado maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular. Entre esses setores, destacam-se especialmente aqueles que lidam com serviços digitais e tecnologia da informação, como empresas de tecnologia, provedores de serviços de internet, plataformas de comércio eletrônico e redes sociais, já que geralmente possuem infraestrutura tecnológica robusta e sistemas de gestão de dados avançados, o que facilita a transferência de dados entre diferentes agentes de tratamento. Adicionalmente, pode-se listar os setores como saúde, financeiro e seguros como aqueles que têm avançado na implementação da portabilidade de dados, devido à necessidade de compartilhar informações entre diferentes prestadores de serviços para garantir um atendimento mais integrado e personalizado aos clientes. Ainda que o direito de portabilidade esteja previsto na LGPD e seja importante por promover a concorrência, a inovação e a personalização dos serviços, deve-se considerar que sua implementação somente será possível caso haja uma regulamentação específica da ANPD, conforme previsto nos arts. 18, V e 40 da LGPD. Essas diretrizes também devem abordar desafios específicos, como formatos de interoperabilidade, segurança, privacidade, limites, bases legais aplicáveis e obrigações dos controladores envolvidos, conforme previsto no Considerando 68 do GDPR. Por fim, ainda há que se mencionar como desafio que cada setor pode ter considerações únicas em relação à portabilidade de dados, como requisitos regulatórios específicos ou preocupações de segurança variáveis a depender do teor dos dados pessoais tratados. ","615501": "Implementar um padrão de interoperabilidade enfrenta diversos desafios tecnológicos, incluindo: a) Compatibilidade de sistemas – Integrar sistemas e aplicativos que operam em diferentes plataformas e tecnologias, de forma a garantir que os sistemas possam comunicar-se de maneira eficaz e compreender os dados trocados. b) Padronização de formatos de dados - Estabelecer formatos de dados comuns e compreensíveis por todos os sistemas, o que requer a definição de esquemas de dados claros e interoperáveis que possam ser entendidos e utilizados por todos os participantes. c) Segurança da informação – De modo a evitar incidentes, deve haver a implementação de medidas robustas de criptografia, autenticação e controle de acesso para proteger os dados contra acesso não autorizado e violações de segurança. d) Escalabilidade e desempenho - Garantir que o padrão de interoperabilidade possa lidar com grandes volumes de dados e operar de maneira eficiente em ambientes de produção é um desafio significativo. Isso requer o uso de tecnologias escaláveis e de alto desempenho, bem como a otimização contínua dos sistemas para lidar com demandas crescentes. Uma abordagem colaborativa e multidisciplinar envolvendo especialistas em tecnologia da informação, padronização de dados e gerenciamento de projetos é fundamental para que sejam superados esses desafios. ","615505": "Consoante as orientações do Information Commissioner's Office (ICO), os dados pessoais devem ser fornecidos em um formato que seja estruturado, comumente usado e legível por máquina. Embora esses termos não estejam definidos no GDPR, essas três características são relevantes para se garantir a adequação do formato escolhido. Ainda, segundo o ICO, quando nenhum formato específico for de uso comum em uma

indústria ou setor, é recomendável que os agentes de tratamento forneçam os dados pessoais usando formatos abertos, como CSV, XML e JSON, por serem formatos mais fáceis de usar ao responder a solicitações de portabilidade de dados. Para garantir a interoperabilidade, vários aspectos devem ser padronizados para garantir que os sistemas possam interoperar de maneira eficaz, permitindo a transferência de dados de forma segura, eficiente e transparente, entre eles: a) Formato de dados portáveis - Estabelecer um formato comum para os dados transferidos entre sistemas, garantindo que sejam compreensíveis e utilizáveis por diferentes plataformas e aplicativos. b) Protocolos de comunicação – Definir protocolos padronizados para a comunicação entre sistemas, permitindo que troquem informações de maneira eficiente e sem perda de dados. c) Ferramentas de conversão e migração de dados – Desenvolver ferramentas que facilitem a conversão e migração de dados entre diferentes formatos e sistemas, garantindo a portabilidade e compatibilidade dos dados. d) Documentação e diretrizes – Elaborar documentação e diretrizes detalhadas sobre o padrão de interoperabilidade, incluindo sua implementação, uso e manutenção, facilitando sua adoção e garantindo sua conformidade. Para maiores informações sobre o tema seguem acesso aos links do ICO - <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/#ib1> – e do Open Data Handbook - <https://opendatahandbook.org/guide/en/how-to-open-up-data/>).

","615503": "Sim, é adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme estabelecido no art. 18, V da LGPD. A portabilidade de dados é um direito fundamental previsto na LGPD, que permite que os titulares solicitem a transferência de seus dados pessoais de um controlador para outro, de forma fácil e segura. O formato interoperável refere-se à capacidade dos dados de serem compreendidos e utilizados por diferentes sistemas e aplicativos sem perda de informação ou funcionalidade. No entanto, é importante fazer uma ressalva de que, caso a ANPD venha a estabelecer outros requisitos em regulamentação própria sobre o tema, podem vir a ser considerados outros critérios que ainda não estão previstos na LGPD.

","615504": "Permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas pode ser uma abordagem positiva, desde que seja feito com supervisão e orientação adequadas para garantir a conformidade com os princípios de proteção de dados estabelecidos na legislação, como a LGPD. Isso porque, padrões de interoperabilidade específicos podem facilitar a transferência eficiente de dados entre diferentes sistemas e aplicativos, promovendo a concorrência e a inovação dentro de diferentes setores econômicos. No entanto, é fundamental que esses padrões sejam desenvolvidos de forma transparente, inclusiva e consultiva, envolvendo múltiplos interessados, incluindo representantes dos titulares de dados, órgãos reguladores e especialistas em privacidade. Além disso, é essencial estabelecer mecanismos de supervisão e avaliação contínua para garantir que os padrões de interoperabilidade não comprometam a privacidade e a segurança dos dados pessoais dos titulares. Isso pode incluir a revisão periódica dos padrões, a realização de auditorias independentes e a imposição de sanções em caso de violações. O prazo para estabelecer esses padrões deve ser cuidadosamente considerado para equilibrar a necessidade de implementação rápida com a garantia de que os padrões sejam robustos e eficazes. Um prazo de 12 (doze) a 24 (vinte e quatro) meses a partir da publicação do regulamento específico do tema de portabilidade pode ser razoável para desenvolver e implementar padrões de interoperabilidade. No entanto, esse prazo pode variar dependendo da complexidade das atividades econômicas envolvidas e da disponibilidade de recursos.

","615511": "Dada a ausência de definição na LGPD sobre os conceitos apresentados, torna-se fundamental

considerar critérios específicos que permitam uma avaliação objetiva da qualidade dos dados incompletos, inexatos ou desatualizados. A seguir apresentam-se os critérios que podem ser considerados para cada uma dessas classificações: a) Incompleto – Dados são considerados incompletos quando não contêm todas as informações necessárias para a finalidade pretendida, apresentando lacunas ou omissões que comprometem sua utilidade e precisão. Os critérios objetivos para identificar dados incompletos incluem a ausência de informações essenciais, como campos obrigatórios vazios ou dados relevantes faltantes. b) Inexato - Dados são considerados inexatos quando não refletem a realidade de forma precisa e correta, apresentando erros, imprecisões ou inconsistências. Os critérios objetivos para identificar dados inexatos incluem a presença de informações imprecisas, bem como a existência de divergências em relação a um conjunto completo de dados. Também se considera a falta de validação ou verificação dos dados, a utilização de fontes não confiáveis ou a manipulação indevida das informações. c) Desatualizado - Dados são considerados desatualizados quando não refletem a situação mais recente ou atualizada de um determinado contexto, estando obsoletos ou ultrapassados em relação às informações disponíveis. Os critérios objetivos para identificar dados desatualizados incluem a falta de sincronização com fontes de dados atualizadas, a ausência de registros recentes, além de ser importante considerar a relevância temporal das informações, a frequência de atualização dos dados e a disponibilidade de dados mais recentes.

,"615514": "A simples declaração do titular pode não ser suficiente para o exercício do direito à correção em algumas situações específicas. Isso ocorre principalmente em casos em que: a) Verificação da veracidade dos dados: quando a veracidade dos dados em questão não pode ser prontamente verificada, especialmente se houver informações contraditórias fornecidas pelo titular. b) Disputas ou controvérsias legais: se os dados em questão forem objeto de controvérsia ou disputa legal entre o titular e o responsável pelo tratamento dos dados, é necessário um processo mais detalhado para resolver a questão de maneira justa e imparcial. c) Impacto nos direitos de terceiros: em situações em que a correção dos dados pode afetar os direitos de terceiros ou interesses legítimos, é importante conduzir um processo mais robusto para garantir que todas as partes envolvidas sejam devidamente consideradas. d) Dúvidas sobre a identidade do solicitante: em caso de dúvidas sobre a identidade do solicitante, o controlador pode solicitar informações adicionais para verificar sua identidade, garantindo assim a segurança e a integridade do processo de correção. Em casos complexos ou controversos, pode ser necessário um processo mais formal que inclua a apresentação de evidências adicionais ou a obtenção de autorizações legais antes que a correção possa ser efetuada. Portanto, a determinação da insuficiência da simples declaração do titular para exercer o direito à correção depende da consideração da proporcionalidade, levando em conta a natureza dos dados, a existência de disputas ou interesses de terceiros, e a necessidade de um processo justo e equitativo.

,"615513": "O artigo 18, § 6º, da LGPD estabelece que o responsável pelo tratamento deve informar imediatamente aos agentes de tratamento com os quais compartilhou os dados sobre qualquer correção, eliminação, anonimização ou bloqueio dos dados, para que eles possam realizar procedimentos idênticos. No entanto, há exceções a essa regra nos casos em que essa comunicação seja comprovadamente impossível ou implique em esforço desproporcional. Para avaliar a impossibilidade ou o esforço desproporcional, os seguintes critérios objetivos podem ser considerados: a) Viabilidade técnica da comunicação - Se é tecnicamente possível para o responsável pelo tratamento informar imediatamente aos agentes de tratamento sobre as correções ou ações realizadas nos dados compartilhados. b) Esforço necessário para a comunicação - Se o esforço necessário para realizar essa comunicação é proporcional em

relação à importância e urgência das mudanças nos dados. c) Complexidade e volume dos dados compartilhados - Se a correção, eliminação, anonimização ou bloqueio dos dados compartilhados envolve uma grande quantidade de informações ou requer procedimentos complexos que dificultam a comunicação imediata. d) Impacto nas operações dos agentes de tratamento - Se a comunicação imediata das mudanças nos dados compartilhados terá um impacto significativo nas operações dos agentes de tratamento, com uma sobrecarga operacional. Portanto, a impossibilidade ou o esforço desproporcional para cumprir com as obrigações do artigo 18, parágrafo 6º, da LGPD deve ser avaliada com base na praticabilidade e razoabilidade das medidas necessárias para garantir a conformidade com a lei. De todo modo, entende-se que é ônus do controlador fazer prova desta impossibilidade, de forma a dar transparência ao titular e à autoridade reguladora em caso de procedimento fiscalizatório. "615512": "Sim. Há disposições na LGPD que podem justificar a recusa do direito de correção de dados pessoais, entre elas: a) Falta de qualificação do solicitante: Quando o solicitante não é o titular dos dados ou não possui representante legalmente constituído, conforme estipulado no artigo 18, § 3º da LGPD; b) Identificação do agente de tratamento: no caso específico em que há equívoco quanto ao agente de tratamento, devendo ser indicado, se possível, o agente correto, conforme previsto no artigo 18, § 4º, inciso I, da LGPD; c) Razões de fato ou de direito impeditivas: Quando há razões de fato ou de direito que impedem a adoção imediata da providência, conforme estabelecido no artigo 18, § 4º, inciso II, da LGPD. Além dessas hipóteses, pode-se fazer um paralelo com o artigo 12 do GDPR, que também prevê a negação de solicitações consideradas manifestamente infundadas ou excessivas. Entre os exemplos fornecidos pelo Information Commissioner's Office (ICO) para pedidos manifestamente infundados, destacam-se situações em que o indivíduo não possui intenção genuína de exercer seu direito de acesso, como quando busca vantagens em troca da retirada do pedido, ou se a solicitação é maliciosa e visa perturbar a organização, incluindo declarações de má fé, acusações infundadas ou assédio sistemático. Por outro lado, o conceito de excessivo refere-se a pedidos que repetem o conteúdo de pedidos anteriores ou se sobrepõe a outras solicitações. Independentemente da justificativa para a recusa, caso o controlador não possa atender à solicitação de confirmação, é essencial que as razões para a recusa sejam claramente esclarecidas em resposta ao titular, em linha com o princípio da transparência. "615517": "De acordo com o art. 18, IV da LGPD, o titular tem o direito de solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei. Contudo, não há qualquer exigência explícita que gere incumbência do titular provar que os dados se enquadram nessas categorias. Além disso, há que se considerar que o titular pode não ter total conhecimento sobre todos os fluxos de tratamento de seus dados pessoais pela empresa, dificultando a prova dessas alegações. A responsabilidade de provar a necessidade dos dados e a conformidade com a lei recai sobre o controlador, que por estar mais familiarizado com os procedimentos de coleta, armazenamento e uso dos dados, é quem deve determinar se as informações em questão são realmente necessárias para as finalidades do tratamento. Embora essa responsabilidade do controlador não esteja explicitamente definida na LGPD, ela é derivada do princípio da necessidade (art. 6º, III, LGPD), que exige que o tratamento de dados seja limitado ao mínimo necessário para a realização de suas finalidades, e do princípio da transparência (art. 6º, VI, LGPD), que assegura aos titulares informações claras, precisas e facilmente acessíveis sobre o tratamento. "615516": "Sim, tanto a anonimização quanto a eliminação podem ser adotadas alternativamente, considerando situações específicas. Dado que ambas as medidas afastam a incidência da LGPD, e partindo do pressuposto de que o titular não tem

conhecimento técnico para decidir entre qual medida seria mais adequada, a escolha entre as opções pode ser feita pelo controlador, dependendo das circunstâncias do caso. A anonimização é particularmente útil quando os dados são valiosos para fins estatísticos, de pesquisa ou análise, mas não são mais necessários para identificar indivíduos específicos. Por outro lado, a eliminação pode ser adotada quando os dados não são mais relevantes para as finalidades do tratamento, quando o consentimento do titular é revogado ou quando o período de retenção estabelecido pela legislação expira. Em muitos casos, a escolha do controlador entre anonimização e eliminação dependerá de uma avaliação cuidadosa das necessidades específicas do tratamento de dados, dos requisitos legais aplicáveis e das políticas internas da organização. A decisão pode ser influenciada por fatores como a finalidade original da coleta de dados, a importância dos dados para a organização e os potenciais impactos na privacidade dos indivíduos.

","615518": "Se a alegação do titular for considerada legítima, o efeito da oposição prevista no art. 18, § 2º da LGPD será o cessamento imediato do tratamento de dados realizado, que foi objeto da oposição. Isso implica que o controlador deve interromper o tratamento dos dados em questão, garantindo a proteção dos direitos e privacidade do titular. Nesse sentido, a organização não poderá mais continuar utilizando os dados para os fins especificados aos quais o titular se opôs. A título de exemplo, se um indivíduo solicita a exclusão de seus dados pessoais de um banco de dados de uma empresa de marketing digital, por ser contra o uso de seus dados em campanhas publicitárias, a empresa deve interromper imediatamente o uso dos dados desse indivíduo para fins de marketing. Por outro lado, se a alegação do titular não for considerada legítima, o controlador não precisará interromper o tratamento dos dados e poderá continuar utilizando esses dados para os fins especificados, desde que haja uma base legal que fundamente esse tratamento e que esteja em conformidade com as disposições da LGPD. A título de exemplo, o controlador pode prosseguir com o envio de e-mails sobre eventuais transações ou compras realizadas em uma plataforma de e-commerce com justificativa na base legal da execução do contrato, ainda que o titular solicite a interrupção do envio de todo e qualquer tipo de e-mail. No entanto, é importante destacar que o controlador deve esclarecer sua decisão de não acatar a oposição do titular. Isso pode envolver a demonstração de que o tratamento dos dados pode ser justificado em base legal correspondente, está em conformidade com as disposições legais da LGPD, bem como com os direitos e interesses legítimos do controlador e de terceiros envolvidos.

","615523": "A revogação do consentimento, conforme estipulado no artigo 18, IX da LGPD, não necessariamente implica na obrigação imediata de eliminar os dados pessoais tratados com justificativa nessa base legal. É fundamental considerar que o referido dispositivo legal deve ser interpretado em conjunto com outras disposições da LGPD, como o artigo 18, VI e o artigo 16. O artigo 18, VI estabelece exceções ao direito de eliminação dos dados pessoais tratados com o consentimento do titular, conforme as hipóteses previstas no artigo 16 da LGPD. Portanto, mesmo que o titular revogue seu consentimento, os dados podem ser mantidos pelo controlador em algumas situações específicas. Assim, embora o titular tenha o direito de revogar seu consentimento a qualquer momento, como previsto no artigo 8º, § 5º da LGPD, é necessário considerar as seguintes circunstâncias em que os dados podem ser retidos pelo controlador: (a) cumprimento de obrigação legal ou regulatória; (b) realização de estudos por órgão de pesquisa, garantindo, sempre que possível, a anonimização dos dados pessoais; (c) transferência a terceiros, desde que observados os requisitos de tratamento de dados estabelecidos na LGPD; ou (d) uso exclusivo pelo controlador, desde que os dados sejam anonimizados e o acesso por terceiros seja vedado. Conclui-se, portanto, que a revogação do consentimento não gera automaticamente a

obrigação de eliminar os dados pessoais, cabendo ao controlador avaliar cada situação à luz das exceções previstas na legislação. ","615521": "Com base no artigo 8º, § 5º da LGPD, quando o titular revoga seu consentimento para o tratamento de dados pessoais, os tratamentos de dados pessoais realizados com base no consentimento anteriormente manifestado pelo titular são considerados válidos e ratificados até o momento da revogação do consentimento. Embora o titular tenha o direito de exigir a eliminação dos dados pessoais também nesses casos, a revogação do consentimento não gera automaticamente a obrigação de eliminar os dados pessoais. É incumbência do controlador analisar a solicitação do titular e verificar se alguma das hipóteses previstas no art. 16 da LGPD autoriza a manutenção dos dados pessoais, tais como o cumprimento de obrigação legal ou regulatória, realização de estudos por órgão de pesquisa, transferência a terceiros, ou uso exclusivo do controlador, desde que observadas as disposições legais pertinentes. De toda forma, alinhado com o princípio da transparência, é dever do controlador comunicar ao titular sobre a efetivação da eliminação dos dados conforme requerido, e, quando não aplicável, informar sobre a impossibilidade de atender integralmente ao pedido destacando a exceção legal cabível. ","615617": "A distinção entre uma “decisão automatizada” e uma “decisão tomada unicamente com base em tratamento automatizado” de dados pessoais reside na presença ou ausência de intervenção humana no processo de tomada de decisão. a) Decisão automatizada: refere-se a uma decisão que é totalmente tomada por um sistema automatizado, sem qualquer intervenção humana direta. Isso significa que o processo de análise e decisão é conduzido exclusivamente por algoritmos ou programas de computador, com base nos dados pessoais fornecidos. Nesse caso, não há interferência ou influência humana na decisão final. b) Decisão – automatizada ou não - tomada unicamente com base em tratamento automatizado de dados pessoais: trata-se de categoria mais ampla que abrange não apenas decisões totalmente automatizadas, mas também aquelas em que o tratamento automatizado de dados desempenha um papel significativo na tomada de decisão, mesmo que haja alguma intervenção humana mínima ou periférica. Nesse sentido, o processo decisório pode envolver uma combinação de análise automatizada de dados e intervenção humana em etapas específicas, como configuração dos parâmetros do algoritmo ou revisão parcial dos resultados. No entanto, a decisão final é influenciada principalmente pelo tratamento automatizado dos dados pessoais. Em suma, enquanto a “decisão automatizada” é completamente controlada por sistemas automatizados, a “decisão tomada unicamente com base em tratamento automatizado” de dados pessoais pode envolver alguma intervenção humana periférica, mas ainda é principalmente orientada e influenciada pelo processamento automatizado de dados. ","615618": "Diante da ausência de previsão na LGPD, a ANPD deve considerar os critérios abaixo expostos ao formular diretrizes e regulamentações relacionadas à interpretação e aplicação das disposições legais sobre proteção de dados e privacidade, especialmente no que diz respeito ao direito à revisão de decisões automatizadas previsto no artigo 20 da LGPD: a) Impacto na esfera individual: um interesse é considerado afetado quando há um impacto significativo na esfera individual da pessoa, incluindo sua autonomia, liberdade, reputação e bem-estar financeiro ou emocional. b) Tomada de decisões substanciais: se uma decisão tomada com base no tratamento automatizado de dados pessoais pode influenciar substancialmente a vida ou as circunstâncias de uma pessoa, seu interesse pode ser considerado impactado. c) Perfil pessoal ou comportamental: decisões automatizadas destinadas a definir o perfil pessoal, profissional, de consumo, de crédito ou outros aspectos da personalidade de um indivíduo indicam um impacto significativo em seus interesses. d) Consequências negativas: a possibilidade de consequências negativas, como exclusão, discriminação, prejuízos

financeiros ou restrições indevidas, indica que os interesses do indivíduo estão sendo afetados. e) Falta de transparência: a falta de transparência no processo de tomada de decisão automatizada ou a ausência de controle por parte do indivíduo sobre os dados utilizados ou o resultado da decisão podem indicar um impacto negativo em seus interesses.

","615619": "Abaixo estão alguns dos principais desafios práticos para implementação do direito de revisão do art. 20 da LGPD: a) Complexidade dos algoritmos: em diversos casos, os algoritmos utilizados para tomada de decisão automatizada podem ser complexos e opacos, dificultando a compreensão de como as decisões são realmente tomadas. Essa complexidade torna desafiador para os titulares entenderem e contestarem as decisões baseadas nesses algoritmos. b) Transparência dos processos: os titulares podem ter dificuldade em obter informações claras sobre como suas informações foram usadas e quais foram os motivos por trás de uma decisão específica. c) Acesso aos dados: para contestar uma decisão automatizada, os titulares precisam ter acesso aos dados que foram utilizados para tomá-la. No entanto, nem sempre é fácil para os titulares obterem acesso a todas as informações relevantes, especialmente quando envolvem dados de terceiros ou dados sensíveis protegidos por segredo comercial. d) Recursos limitados: os titulares podem não ter os recursos necessários para contestar uma decisão automatizada, especialmente se envolver processos complexos ou exigir análises especializadas de dados, o que pode resultar em uma falta de acesso efetivo ao direito de revisão garantido pela LGPD. e) Tempo e eficiência: esse processo de revisão de decisões automatizadas pode ser demorado e exigir recursos consideráveis tanto por parte dos titulares quanto dos controladores. f) Desenvolvimento de mecanismos de revisão: é necessário desenvolver mecanismos eficazes para a revisão de decisões automatizadas que sejam acessíveis e compreensíveis para os titulares, com a criação de procedimentos claros para contestação, bem como a implementação de sistemas de suporte para facilitar o processo de revisão.

","615620": "Sim, existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas, embora isso deva ser feito de forma justificada e dentro dos limites estabelecidos pela LGPD, entre elas: a) Proteção de segredos comerciais ou industriais: as organizações têm uma justificativa sólida para proteger seus segredos comercial e industrial, já que essa abertura desmedida de informações estratégicas pode expor as organizações a riscos competitivos, minando sua capacidade de inovar e reduzindo suas vantagens no mercado. b) Garantia da segurança da informação: em situações em que a divulgação de informações relacionadas à decisão automatizada possa representar um risco significativo para a segurança da informação, o controlador pode negar o acesso ou a revisão, comprometendo a integridade do sistema, isso poderia justificar a negação do direito de revisão. b) Proteção de dados de terceiros: se a divulgação de informações relacionadas à decisão automatizada envolver dados pessoais de terceiros que não autorizaram a sua divulgação, o controlador pode negar o acesso ou a revisão para proteger a privacidade dessas partes. c) Decisões baseadas em critérios legais ou contratuais: em algumas situações, as decisões automatizadas podem ser baseadas em critérios legais ou contratuais específicos que não permitem revisão ou contestação. Por exemplo, se uma decisão automatizada for necessária para cumprir uma obrigação legal ou contratual estrita, o controlador pode não ter margem de manobra para permitir a revisão dessas decisões. d) Decisões de risco baixo ou trivial: em casos em que as decisões automatizadas têm um impacto mínimo ou trivial nos interesses do titular, o controlador pode negar o direito de revisão com base na proporcionalidade e na eficiência dos recursos envolvidos. Ao desenvolver regulamentações relacionadas ao direito de revisão de decisões automatizadas, a ANPD deve considerar

cuidadosamente esses pontos, garantindo que as exceções sejam fundamentadas e alinhadas aos princípios e objetivos da LGPD. "

{ "615450": "A ANPD deverá avaliar a criticidade da solicitação em comparação com o prazo previsto para seu atendimento, bem como, a especificidade da natureza do tratamento do dado pessoal em questão, i.e. compartilhamento com terceiros; relação operador-controlador, que podem gerar dependências de outros agentes; bem como, a complexidade do atendimento, como, por exemplo, num caso de anonimização. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: ""Sim, os prazos podem ser atendidos em até 20 dias, com prorrogação de mais 10, mediante justificativa expressa, como nos casos de algum incidente que resulte em alta demanda ou quando os dados são compartilhados em situações de controladoria conjunta e quando é necessário a identificação de operadores e suboperadores. Formato Simplificado: a resposta poderá ser feita através de templates simples ou corpo do e-mail/mensagem, sendo preferencialmente identificado dados cadastrais, sendo exclusivamente a caráter de direito da pessoa que realiza o tratamento, neste caso após a confirmação da identidade deverá ser realizado o atendimento em D+1, ou seja, em até 24 horas após a validação da identidade do titular. Declaração clara e Completa: deverá ocorrer em até 20 dias após a validação da identidade do titular, sendo em que ambos os casos a primeira resposta ao titular deverão ocorrer em até 2 dias úteis." "615484": "O canal de atendimento deverá ser simplificado cujo direcione o titular a pontos específicos de atendimento da lei de proteção de dados, dando inclusive instruções para que o titular valide sua identidade nesse momento. Não deverá conter termos complexos e trazer uma breve explicação sobre o canal, além de uma breve explicação da lei para que o titular entenda a finalidade de sua requisição, tornando as solicitações ágeis para ambos os lados. De modo que a solicitação poderá ser feita através de formulários específicos indicados no site ou canal de comunicação. Além disso, deverá contar com processos para validação da identidade do titular ou operar por via de canal logado. "615485": "Sim, entretanto, para essa definição deve ser levada em consideração a capacidade técnica do operador em efetivar a solicitação, visto que pode não possuir a ingerência necessária sobre os dados pessoais para que possa concretizar o pedido do titular, situação em que deverá se responsabilizar pela devida comunicação ao controlador correspondente, para que esse empenhe os esforços necessários para sua realização. Além disso, tal comunicação deverá ser acompanhada de previsão legal no regulamento a ser criado, bem como, deve ser definido prazo prévio para tal. "615486": "A adoção de diretrizes e procedimentos análogos ao SAC para o exercício dos direitos do titular de dados pessoais é uma boa prática que pode contribuir para a efetividade da LGPD, bem como, para contribuir para a segurança jurídica tanto do ponto de vista dos titulares, quanto dos agentes de tratamento de dados, a fim de estabelecer procedimentos documentados e assegurar o cumprimento das expectativas de ambas as partes. Entretanto, tal proceduralização deve acompanhar as particularidades e complexidades inerentes ao tratamento de dados pessoais. "615487": ""O modelo utilizado é a solicitação via formulário, onde o titular é induzido as respostas de acordo com o atendimento da LGPD, onde não demanda ônus ao agente de tratamento, ocorre que em casos excepcionais devido ao grande volume, sugere-se uma ordem de prioridades de acordo com a demanda apresentada levando em consideração a solicitação do titular, devendo ser priorizada os casos de eliminação, correção, anonimização e posteriormente confirmação. O formulário é dividido em 3 partes: I – Titular fornece os dados cadastrais para identificação e de contato (e-mail e/ou telefone).

II – O titular é induzido a responder dentro dos parâmetros da LGPD, ou seja, através de um checklist, vai responder qual(is) direito(s) ele está requerendo. III – Validação da identidade do titular, nesse momento o titular encaminha 3 fotos ao agente de tratamento que ele está solicitando seus direitos. (i) foto do documento, (ii) foto do rosto (selfie), (iii) foto segurando o documento. Há outros meios de validação, por contato via SMS, WhatsApp e ou confirmação via e-mail. tem menu de contexto." ;"615491": "Como princípio, todo pedido de titular deve ser acompanhado com a confirmação da identidade do solicitante, a fim de resguardar os dados pessoais tratados pelo agente, bem como, assegurar a existência de nexo entre o solicitante e o dado pessoal tratado. ";"615492": "sem considerações";"615489": ""O operador, na capacidade de agente que atua mediante instruções prévias e documentadas do controlador, deve ser penalizado pela não efetivação do cumprimento de uma solicitação do titular quando há necessidade de sua contribuição e o agente falhar em fornecer as informações necessárias ou não disponibilizou justificativa no caso de incapacidade do fornecimento. O operador, deve, em sua capacidade, contribuir com o controlador quando necessário para que possa responder a uma solicitação de informação sobre o tratamento de dados pessoais, empregando os esforços necessários a fim de efetivar a solicitação. Nesse mesmo sentido, a ANPD, ao regulamentar o papel do operador na efetivação de solicitações dos titulares, deverá considerar situações em que o agente operador é incapaz de responder a um pedido, dada a uma possível incapacidade técnica ou operacional à vista de não possuir a devida ingerência sobre o dado pessoal, a impossibilidade de individualizar o titular, etc. Ademais, deverá ser levada em consideração os limites de responsabilidade da atuação sobre a gestão do processo de tratamento de dados pessoais por cada agente de tratamento. Por fim, a resposta do operador deve ser realizada mediante requisição em formato detalhada ou simplificado." ;"615490": ""- Categoria do dado pessoal tratado (i.e. ""Nome"""); e - O próprio dado pessoal tratado (i.e. ""Paulo Silva""").";"615494": "Confirmação de tratamento de dados pessoais e dados públicos ou que não gerem danos ao titular, como nome e idade. ";"615493": "O formato digital deverá ser o mais aceitável, apenas em casos específicos deverá ser tratado o dado em papel, muitas vezes o dado em papel poderá ser enviado por meio de carta, visto que nem sempre o titular ou o agente de tratamento é encontrado com fácil acesso, forçando o uso dos correios, sendo assim, a entrega da carta com os dados passa a ser mais um tratamento de riscos com um específico operador que independe do titular para realizar suas funções, além do mais os dados físicos são considerados um grande risco a incidente, tendo em vista a sua facilidade de destruição acidental ou não. ";"615502": "sem considerações";"615501": "sem considerações";"615505": "sem considerações";"615503": "sem considerações";"615504": "sem considerações";"615511": "Erros de digitação, erros crassos e critérios formais. Dados desatualizados estão de acordo com a atualização do titular, por exemplo, no caso de alteração de residência é necessário primeiro o informe do autor, posteriormente a atualização em tempo hábil. ";"615514": "Situações em que a solicitação do titular seja feita frente a um agente operador ou; situações em que o dado pessoal tenha sido recepcionado por outro agente controlador (controladoria conjunta), ocasião em que o titular deve ser orientado a postular sua solicitação frente ao controlador original e possuidor da fonte do dado pessoal questionado. ";"615513": "sem considerações";"615512": "Sim, quando ocorre necessidade de apresentação de documento oficial, ou seja, quando a correção pende de decisão judicial ou alteração formal em cartório, respeitando todos os trâmites formais. ";"615517": "Não há necessidade, uma vez que após a solicitação do titular, é o controlador que irá determinar e fundamentar se a solicitação poderá ser acatada ou não. ";"615516": "Sim. A anonimização pode ser uma alternativa a eliminação de dados pessoais,

garantida a irreversibilidade da identificação do titular. ";615518": "sem considerações";615523": "Não. Deverá ser levado em consideração a obrigatoriedade do agente de tratamento em reter os dados, à vista da necessidade de cumprir com uma determinação legal; seu legítimo interesse na retenção dos dados; e seu direito em reter os dados, como, por exemplo, para fins de defesa em procedimentos judiciais e não judiciais. Ademais, a revogação do consentimento deverá impactar tão somente tratamentos futuros, não atingindo tratamentos retroativos, a não ser que assim solicitado pelo titular. Nesse sentido, devem ser levadas em consideração as demais bases legais que possam legitimar a manutenção desses dados na base de dados do agente de tratamento. ";615521": "A revogação do consentimento deverá impactar tão somente tratamentos futuros, não atingindo tratamentos retroativos, a não ser que assim solicitado pelo titular. A eliminação dos dados não poderá ser feita por completo e imediato uma vez que existiu algum vínculo entre controlador ou titular, a determinação da eliminação dos dados dos titulares é algo pouco provável a jurisdição brasileira, podendo os dados serem armazenados em uma "base fria" onde há apenas o armazenamento do dado aguardando o tempo a prescrição jurídica dos direitos do titular bem como para fins de garantias etc. ";615617": ""Toda decisão tomada de forma tempestiva por um sistema, de software ou hardware, sem interferência humana (human in the loop). Por exemplo: um radar decide tirar uma foto automaticamente ao detectar um carro que percorreu uma distância acima do limite máximo estabelecido; um motor de decisão, rodando dentro de um app bancário, que decide negar empréstimo para uma pessoa com base em suas informações bancárias. Já uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais se refere a uma decisão tomada com base em processos automatizados nos quais dados pessoais foram tratados. Isto não inclui processos nos quais o ser humano lance mão de resultados de processos automatizados somados ao seu julgamento humano (sejam tais julgamentos subjetivos ou objetivos) para uma tomada de decisão. Por exemplo: um processo de onboarding em aplicativo no qual um ser humano submeta sua foto segurando um documento pessoal, onde uma IA de reconhecimento facial gerou um score de alta probabilidade de fraude e este processo foi direcionado a um atendente humano que, ao observar com seus próprios olhos a imagem constatou que esta se tratar de uma tentativa de cadastro fraudulento. Este processo não conta como um caso de decisão baseada unicamente em tratamento automatizado de dados pois houve interferência humana (human in the loop) e esta interferência era capaz de acatar ou negar a decisão da IA de acordo com julgamento próprio. ";615618": ""O interesse é efetivamente afetado quando a decisão automática tem impactos de cunho: Econômico - afetando de forma direto o indivíduo monetariamente ou de forma indireta, afetando o acesso a produtos financeiros que o indivíduo possa ter; e Social - afetando publicamente a imagem do indivíduo, seu acesso a diferentes camadas sociais." ";615619": ""A revisão das decisões pode gerar aumentos exacerbados de custos Pode-se criar um mecanismo de incentivo para pessoas mal intencionadas pedirem revisões de decisões automatizadas repetidamente, de modo a inviabilizar o processo As revisões podem ser impossíveis devido à tempestividade do contexto no qual a decisão é tomada (carros auto-dirigidos, por exemplo) Canais pelos quais requisitar as revisões pode ser difíceis de implementar em algum contexto O própria escolha do algoritmo de inteligência artificial a ser utilizado e as variáveis empregadas durante o processo de aprendizado do algoritmo podem dificultar a revisão e explicação de resultados" ";615620": ""Toda decisão automatizada é tomada por um sistema parametrizado, com o uso de IA ou não. O controlador deveria cuidar para que, uma vez empregada IA no processo, esta seja construída de tal forma que seus resultados sejam explicáveis e auditáveis. Porém, existem casos nos quais a

negativa de revisão/explicação pode ser procedente: Situações nas quais a revisão da decisão é impraticável devido à imutabilidade das variáveis utilizadas no processo automatizado e no processo de aprendizado do algoritmo de IA. Tornando a revisão inócua, pois o modelo/processo retornaria o mesmo resultado. Situações nas quais a própria explicação da tomada de decisão revele segredos industriais que prejudiquem o controlador do sistema, causando problemas concorrenciais." "

{ "615450": "[Mattos Filho pela BigDataCorp] O prazo de 20 dias prorrogáveis por mais 10 dias do art. 11 da LAI seria razoável para o atendimento, pelos agentes privados, dos direitos dos titulares previstos na LGPD, com exceção do que diz respeito a eventuais requisições relacionadas especificamente à confirmação de existência e acesso aos dados (art. 18, I e II). O art. 19 da LGPD prevê que a confirmação de existência ou o acesso aos dados pessoais serão providenciados, mediante requisição do titular, (i) em formato simplificado, imediatamente; ou (ii) por meio de declaração clara e completa, com a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comerciais, fornecida no prazo de até 15 dias, contado da data do requerimento do titular. Considerando a complexidade do atendimento desses direitos, é razoável que a possibilidade de prorrogação por mais 10 dias do prazo legal de 15 dias seja prevista pela ANPD. Sugere-se, ainda, que a ANPD preveja mecanismo que, com razões justificadas e previsão de data para conclusão do atendimento dos direitos, os prazos totais de 25 dias para o atendimento dos direitos do art. 18, I e II da LGPD e 30 dias para o atendimento dos demais direitos possam ser excedidos. Nesse cenário, a adoção das medidas para atender os direitos dos titulares deve ser iniciada dentro do prazo total previsto, com possibilidade de prazo adicional para conclusão do atendimento, diante de eventuais particularidades e/ou das especificidades da solicitação (e.g. em caso de eventuais solicitações de exercício do direito de portabilidade, que possam atrair complexidades técnicas e a necessidade de atuação de terceiros). Por fim, qualquer orientação sobre o tema deve estabelecer que, para cada nova solicitação de exercício de direito formulada, inicia-se a contagem de um novo prazo, ainda que, no decorrer de uma comunicação com o agente de tratamento relacionada a uma solicitação inicial, o titular exerça outro direito. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "N/A", "615484": "[Mattos Filho pela BigDataCorp] A escolha sobre as características do canal de atendimento deve ser feita pelo agente de tratamento. Os elementos do binômio “características-efetividade” tendem a variar de acordo com o modelo de negócio e a organização das atividades do agente. Para um agente que lida com titulares de forma presencial, é mais eficiente o formulário impresso, ao passo que para um agente que não possua presença física (no Brasil ou não) e se relacione virtualmente com os titulares, é mais eficiente a disponibilização online do canal em que ocorrem as interações. A ANPD deve evitar regular ou dar orientações sobre os canais de comunicação que tragam ônus excessivo ou desmensurado, principalmente considerando o princípio da liberdade dos modelos de negócios promovidos na internet, prevista no art. 3º do MCI. A ANPD deve focar em orientar os agentes sobre a necessidade de que, observadas a pluralidade e as especificidades dos modelos de negócios, os direitos dos titulares sejam atendidos. Com o objetivo de garantir a efetividade da comunicação e a segurança do atendimento dos direitos dos titulares, a ANPD deve orientar os agentes sobre as medidas a serem implementadas para verificar a identidade do titular. Não parece necessário que o agente sempre requeira apresentação de documentos adicionais do titular, especialmente nos casos em que a solicitação ocorrer no âmbito de uma relação contínua entre o agente e o titular. No entanto, a ANPD deve esclarecer quando a solicitação dos documentos é recomendável e quando pode ser dispensada. Essa possibilidade é reconhecida por outras autoridades de proteção de dados (e.g. ICO no UK e CNIL na França). Além disso, a ANPD deve orientar os agentes sobre como proceder em solicitações de exercícios de direitos formuladas por terceiros. Parece razoável que

seja admitido o exercício de direitos dos titulares por terceiros nas hipóteses já previstas no ordenamento jurídico vigente, especialmente no Código Civil (tutela, curatela e representação), mediante documentos que comprovem os poderes do terceiro ao agente. "615485": "[Mattos Filho pela BigDataCorp] As obrigações de atendimento aos direitos dos titulares previstas no Capítulo III da LGPD aplicam-se especificamente ao controlador de dados pessoais. Nesse sentido, entende-se que a solicitação de exercício de direito do titular deve ser feita ao controlador, no âmbito da relação controlador-titular. Não obstante, deve ser facultada aos agentes de tratamento a possibilidade de regularem entre si quem será responsável, sob a ótica operacional, por atender (todas ou determinadas) solicitações de exercício de direitos de titulares. Em certas circunstâncias, o operador poderá ser o único agente capaz de operacionalizar a solicitação do titular (por exemplo, quando fizer a gestão do canal de solicitações ou do servidor onde estão hospedadas as informações do controlador). No entanto, entende-se que o atendimento do direito do titular pelo operador somente deverá ser feito mediante instruções do controlador (que poderá se dar de maneira mais genérica pela via contratual ou pontualmente, à medida em que solicitações sejam recebidas). Em qualquer caso, o operador não deve se antecipar e tomar a decisão de atender à solicitação do titular por iniciativa própria, sob pena de atuar fora das instruções do controlador e ser equiparado a um controlador (art. 42, §1º, I). Por fim, é importante que a ANPD deixe clara a possibilidade de que, sempre que procurado por um titular de dados que deseje exercer algum dos direitos previstos pela LGPD e desde que a identificação seja possível, o operador indique ao titular os dados de contato do controlador. Essa possibilidade está alinhada com a previsão do art. 18, §4º, II da LGPD e garantirá maior efetividade ao atendimento da solicitação do titular. "615486": "[Mattos Filho pela BigDataCorp] O Decreto nº 11.034/2022, que regulamenta o Serviço de Atendimento ao Consumidor ("Decreto" e "SAC"), é destinado aos fornecedores dos serviços regulados pelo Poder Executivo Federal. Dessa forma, a adoção do referido ato normativo como parâmetro pela ANPD pode impor aos agentes de tratamento a obrigação genérica de implementarem medidas desproporcionais para cumprir com os requisitos previstos no Decreto, o que representaria ônus excessivo ao exercício de diversas atividades econômicas. As especificidades dos canais de comunicação com os titulares irão variar de acordo com diversos elementos, que podem sim considerar a eventual atuação dos agentes de tratamento em setores regulados, mas que também deverão ser consistentes com os diferentes portes, recursos disponíveis e modelos de negócio desses agentes. Nesse sentido, importante reiterar que a LGPD é uma lei de aplicação horizontal, que impacta quase todo tipo de negócio no Brasil. Assim, orientar a forma de atendimento aos titulares com base em um único parâmetro pode representar baixa efetividade do cumprimento de direitos previstos na LGPD. Dentre os requisitos previstos no Decreto que podem ser desproporcionais a depender da estruturação do agente de tratamento, destaque-se: (i) acesso ao SAC de modo ininterrupto, durante vinte e quatro horas por dia, sete dias por semana; e (ii) atendimento telefônico obrigatório com horário de atendimento não inferior a oito horas diárias, com atendimento humano. Enfatizando a resposta à pergunta "c" deste Bloco I, entende-se que a ANPD deve evitar regular ou dar orientações sobre as diretrizes e procedimentos a serem implementados para o atendimento dos direitos de titulares que possam ser demasiadamente específicos ou restritivos. A ANPD deveria focar seus esforços em orientar os agentes de tratamento sobre a necessidade de que, observadas a pluralidade e as especificidades dos modelos de negócios existentes no mercado, os direitos dos titulares sejam atendidos eficazmente. "615487": "N/A"; "615491": "N/A"; "615492": "N/A"; "615489": "[Mattos Filho pela BigDataCorp] A eventual falta de clareza na identificação do controlador,

especialmente em casos envolvendo diversos agentes de tratamento, pode representar um desafio para o exercício dos direitos dos titulares. Na prática, o titular, ao tentar exercer seus direitos, pode encontrar dificuldades de identificar o responsável final pelo tratamento dos seus dados. Para solucionar essa dificuldade, é importante que a ANPD esclareça que os operadores, ainda que não devam tomar decisões em relação ao atendimento dos direitos dos titulares sem instruções prévias dos controladores, devem atuar de forma transparente na comunicação com os titulares. Isso está em linha com o art. 9 da LGPD, que não limita expressamente o cumprimento da obrigação de divulgação de informações sobre o tratamento ao controlador. Nesse sentido, na medida da sua participação e considerando a dinâmica específica da respectiva atividade de tratamento, o operador deveria ter a prerrogativa de fornecer informações ao titular acerca do tratamento dos seus dados. A prerrogativa do operador de indicar ao titular dos dados quem é o agente de tratamento responsável por atender às solicitações de exercício de titulares não deve depender de acordo entre controlador-operador, já que é essa premissa que garantirá ao titular acesso a outras informações ou possibilidade de exercício dos direitos previstos na LGPD. Por outro lado, a forma e o conteúdo das informações que serão divulgadas pelo operador ao titular de dados poderá ser objeto de deliberação entre os agentes de tratamento (pela via contratual, por exemplo), desde que essa deliberação não represente empecilhos para que o titular consiga ter acesso efetivo às informações que deseja.

","615490": "N/A","615494": "N/A","615493": "[Mattos Filho pela BigDataCorp] Entende-se que sim, o direito de acesso pode ser considerado satisfeito quando o agente de tratamento disponibilizar os dados pessoais ao titular em ambos os formatos, eletrônico ou impresso. No entanto, ainda que a LGPD preveja, no §2º do art. 19, que a escolha sobre o formato é do titular, acredita-se que a ANPD deve relativizar essa possibilidade de escolha diante da diversidade dos modelos de negócio no mercado e a variação dos recursos disponíveis a depender do porte do agente de tratamento. Nesse sentido, tem-se como exemplo entidades que tratam dados coletados a partir de fontes públicas legítimas e que possuem um volume considerável de informações sobre determinado titular. A solicitação de acesso às informações na via impressa pode representar custos altos à empresa, diante do volume de dados (e, logo, no material necessário à impressão), principalmente considerando que essa mesma solicitação pode ser feita por uma multiplicidade de titulares. Ainda nesse exemplo, a entrega dos dados em formato impresso dificultaria ao próprio titular a sua interpretação. Diante desse cenário, desde que garantido o acesso gratuito às informações (em linha com ao art. 6º, IV da LGPD), ainda que não no formato de preferência do titular, entende-se que deve ser considerado satisfeito o direito de acesso do titular.

","615502": "N/A","615501": "[Mattos Filho pela BigDataCorp] A ANPD deve ser cautelosa na regulamentação desse direito e não impor obrigações financeiras excessivas e impraticáveis pelas entidades sujeitas à LGPD. Os desafios tecnológicos para implementação de um padrão de interoperabilidade derivam da multiplicidade de perfis de agentes de tratamento. Deve-se buscar um equilíbrio entre a efetividade do direito à portabilidade e a viabilidade da implementação de medidas técnicas pelos agentes de tratamento, à luz de aspectos econômicos e estruturais. Isso deve considerar os diferentes modelos de negócio e a diferença em relação aos recursos disponíveis para implementar mecanismos técnicos que possibilitem a portabilidade, respeitada a diversidade dos agentes. A discrepância entre a forma de organização e o porte dos agentes demonstra que, no âmbito da regulação do direito à portabilidade, não há uma solução tecnológica “one size fits all”. É importante que a ANPD esteja atenta a esse aspecto para evitar criar obrigações que representem entraves aos agentes e que sejam implementáveis apenas por uma parcela desses,

resultando em exclusão da outra parcela. É fundamental considerar o aspecto tecnológico da interoperabilidade de dados, em particular a rápida evolução da tecnologia. Formatos de dados que eram considerados como “padrão de mercado” há poucos anos hoje são vistos como limitados em sua capacidade de representação das estruturas de informação utilizadas na maioria das bases de dados. A definição rígida de um padrão pode levar ao engessamento do setor e ao atraso tecnológico do país, por obrigar o mercado ao uso de formatos de dados ultrapassados. A ANPD deve buscar contribuições do mercado sobre aspectos tecnológicos para viabilização do atendimento desse direito. Através de consultas públicas e diálogos abertos com setores da sociedade, a ANPD poderá regular e propor orientações eficientes, equitativas e sustentáveis para todos os atores envolvidos. A criação de um sandbox regulatório, bem como um foro de autorregulação envolvendo agentes de tratamento, podem ser medidas efetivas. ”615505”:[Mattos Filho pela BigDataCorp] O art. 20 do General Data Protection Regulation, estipula que os titulares de dados têm o direito de receber os dados pessoais que forneceram a um controlador em formato que permita que os dados sejam facilmente transferidos para outro controlador e estabelece os seguintes requisitos a serem considerados: (i) Formato estruturado e de uso comum: os dados devem ser disponibilizados em um formato que seja organizado de forma estruturada e que seja amplamente reconhecido e utilizado no mercado (e.g. CSV, XML e JSON), mas sem a obrigação de um formato específico; (ii) Leitura automática: o formato dos dados deve ser legível por máquina, processados automaticamente por computadores e sistemas de TI em programas e/ou bibliotecas de código-fonte disponíveis gratuitamente no mercado, não havendo necessidade de intervenção humana; e (iii) Facilidade de transferência: o formato dos dados deve ser projetado de maneira que facilite a transferência dos dados para outro controlador, caso o titular dos dados solicite, e a adoção de padrões comuns de interoperabilidade e disponibilização de ferramentas para facilitar a transferência. O Considerando nº 68 do GDPR determina que o direito do titular de transmitir ou receber dados pessoais que lhe digam respeito não deve criar a obrigação dos controladores adotarem sistemas de tratamento tecnicamente compatíveis. Diante dos diferentes perfis de agentes de tratamento e de modelos de negócios, essa regra também deve ser considerada pela ANPD ao regular o direito à portabilidade. Some-se um quarto requisito: (iv) Leitura humana: o formato dos dados, além de legível por máquina, deve ser legível por uma pessoa em qualquer programa de leitura/edição de texto disponibilizado junto com os principais sistemas operacionais de computador, ou através de um navegador de internet padrão do mercado. Isso garante que os agentes não criem um padrão esotérico de informações que dificulte a entrada de novos participantes e não se exclua a possibilidade do titular avaliar os seus dados pessoais de maneira facilitada.”615503”:[Mattos Filho pela BigDataCorp] Sim. E essa possibilidade é importante para garantir que todos os agentes de tratamento consigam viabilizar, financeira e tecnologicamente, o atendimento desse direito. De modo a subsidiar esse posicionamento, destaque-se o art. 20 do General Data Protection Regulation (GDPR), no qual é estipulado que os titulares de dados têm o direito de receber os dados pessoais que forneceram a um controlador em um formato que permita que os dados sejam facilmente transferidos para outro controlador de dados e que estabelece os seguintes requisitos objetivos a serem considerados pelo controlador: (i) Formato estruturado e de uso comum: os dados devem ser disponibilizados em um formato que seja organizado de forma estruturada e que seja amplamente reconhecido e utilizado no mercado, o que facilitaria a interoperabilidade e a utilização dos dados por diferentes sistemas e plataformas (por exemplo, CSV, XML e JSON); (ii) Leitura automática: o formato dos dados deve ser legível por máquina, o que significa que os dados devem ser apresentados de uma

maneira que possa ser processada automaticamente por computadores e sistemas de TI, não havendo, portanto, necessidade de intervenção humana; e (iii) Facilidade de transferência: o formato dos dados deve ser projetado de maneira que facilite a transferência dos dados para outro controlador de dados, caso o titular dos dados solicite, o que envolve a adoção de padrões comuns de interoperabilidade e a disponibilização de ferramentas ou APIs para facilitar a transferência de dados. O Considerando nº 68 do GDPR determina ainda que o direito do titular dos dados de transmitir ou receber dados pessoais que lhe digam respeito não deve criar a obrigação dos controladores adotarem ou manterem sistemas de tratamento tecnicamente compatíveis. Considerando a discrepância entre os diferentes perfis de agentes de tratamento e de modelos de negócios, essa regra também deveria ser considerada pela ANPD ao regular o direito à portabilidade.

","615504": "N/A","615511": "N/A","615514": "N/A","615513": "[Mattos Filho pela BigDataCorp]

De maneira não exaustiva, destaque-se, por exemplo, controladores que possuam modelo de negócio legitimamente baseado na coleta de dados pessoais disponíveis publicamente e que, na eventual viabilidade do atendimento de uma solicitação de correção/eliminação/anonimização/bloqueio de dados do titular, não deverão ser obrigados a comunicar ao(s) controlador(es) da base de dados pessoais pública, especialmente em casos em que não tiver vínculos contratuais com esse controlador.

","615512": "[Mattos Filho pela BigDataCorp]

Sim. As práticas de mercado que envolvem o tratamento de dados pessoais são diversas, assim como os modelos de negócios dos agentes de tratamento. Nesse sentido, a depender de como as atividades do controlador se estruturam, pode não ser possível atender a uma solicitação de correção do titular do dado. São os casos, por exemplo, de empresas que tratam dados obtidos de outras fontes legítimas, como bases públicas ou dados tornados manifestamente públicos pelo titular. Nessas situações, em que a base de dados do controlador derivará de uma outra fonte, a correção do dado pode não ser possível ou, ainda que o seja, pode não ser efetiva (uma vez que, ao extrair novamente informações da base de dados original, o dado continuará incorreto). A ANPD deve estar ciente dessas nuances específicas de determinados modelos de negócios legítimos e admitir a possibilidade de que o agente de tratamento não atenda à solicitação do titular nesses cenários. Isso, no entanto, não deve eximir o agente de tratamento da obrigação de informar ao titular sobre a origem dos dados e, quando possível, sobre os mecanismos disponíveis para solicitar sua correção na fonte original. O mesmo racional deve ser aplicado a solicitações de anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e §2º da LGPD).

","615517": "[Mattos Filho pela BigDataCorp]

Sim. O titular, ao solicitar a exclusão de seus dados, deverá fornecer uma fundamentação clara para tal. Essa medida deve ter como objetivo garantir que a solicitação seja legítima e que o titular esteja ciente das implicações da exclusão. Em alguns casos, a despeito da fundamentação, entende-se que a exclusão de dados pelo agente de tratamento pode não ser viável à luz de eventuais obrigações legais ou regulatórias ou, ainda, na subsistência de um legítimo interesse do agente de tratamento (por exemplo, caso os dados venham a ser necessários para defesa de direitos no futuro). Nesses casos, acredita-se ser possível que o agente de tratamento informe o titular sobre as razões da impossibilidade de exclusão, desde que forneça justificativa razoável e fundamentada para tanto. É importante destacar ainda que a exclusão de dados do sistema do agente de tratamento nem sempre garantirá a sua completa remoção de todas as mídias ou backups. O titular deve estar ciente de que, mesmo após a exclusão da base de dados ativa do agente de tratamento, os dados poderão ainda ser mantidos em backups ou em outros sistemas por motivos de segurança ou recuperação de desastres. Por fim, especificamente nos casos de agentes de tratamento que

tratem dados pessoais advindos de fontes públicas ou que foram manifestamente tornados públicos pelo titular, não se pode exigir desses agentes que (i) excluam os dados pessoais das fontes originais; e (ii) que não voltem a tratar esses dados pessoais, especialmente quando seu modelo de negócio for baseado em sistemas automatizados de extração de dados, caso os dados pessoais não sejam excluídos das fontes originais. Em situações nas quais os dados não são coletados diretamente do titular, como em modelos de negócios que os obtêm de fontes públicas ou de terceiros, o exercício do direito à exclusão pode ser limitado. A exclusão, nesses casos, deverá ocorrer de acordo com a viabilidade técnica e operacional e observando-se as especificidades do modelo de negócio do agente de tratamento.

","615516": "N/A","615518": "N/A","615523": "N/A","615521": "N/A","615617": "N/A","615618": "N/A","615619": "[Mattos Filho pela BigDataCorp] Há vários desafios na implementação do direito de revisão do art. 20. O primeiro diz respeito ao condicionamento do direito de revisão às decisões tomadas “unicamente” de forma automatizada. O termo “unicamente” é subjetivo. Se uma decisão é tomada por um sistema, mas o agente é responsável por comunicá-la ao titular, o fator humano na “comunicação da decisão” já seria suficiente para concluir que a decisão não foi tomada “unicamente” de forma automatizada? Ou o conceito demanda uma intervenção humana mais substancial na decisão, como por exemplo, a interpretação de uma conclusão automatizada a partir de critérios considerados manualmente pelo agente de tratamento? Superada a dificuldade de definir que uma decisão é automatizada, parte-se para os desafios práticos para revisá-la. Quando o agente de tratamento fizer uso de sistemas complexos (e.g. deep learning), pode ser difícil identificar qual fator específico levou à decisão para a qual busca-se revisão (especialmente quando os sistemas possuírem algoritmos “black box”). Além disso, a documentação do processo decisório pode ser incompleta ou inexistente nesses casos. A ANPD deve orientar os agentes de tratamento a como viabilizar o direito de revisão, sem que as orientações representem barreiras ou desincentivo à inovação. É importante que a ANPD oriente os agentes de tratamento sobre (i) quando uma decisão será considerada tomada “unicamente” de forma automatizada, e (ii) em que consiste a revisão da decisão em cenários em que essa revisão se demonstrar impossível considerando a tecnologia empregada. Com as nuances técnicas da revisão de decisões automatizadas e das discussões legislativas e regulatórias envolvendo accountability e IA, a ANPD deve propor iniciativas de participação pública direcionadas para esse tema (incluindo consultas públicas e diálogos abertos com os diversos atores da sociedade), antes de regulamentar esse dispositivo da LGPD. Os resultados do sandbox regulatório de IA e proteção de dados da ANPD poderão contribuir para esse processo de regulamentação."","615620": "N/A"

{ "615450": "Seria possível utilizar o prazo da LAI (20 dias, conforme art. 11) para os demais direitos que não o de confirmação e acesso (cujo prazo de 15 dias já está definido em Lei específica). Contudo, considerando que a LGPD é uma Lei que se aplica a uma gama de setores da economia, e que a LAI é específica para o setor público (com estruturas de bancos de dados razoavelmente já definidas), entendemos que o Regulamento que irá prever os prazos deverá possibilitar a prorrogação, sem prazo definido, mas razoável, mediante justificativa do controlador. Nesse caso, o §2º do art. 11 da LAI não seria aplicável. Para evitar abusos, sugere-se a possibilidade do Titular, se discordar de tal prazo, peticionar junto à ANPD. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?": "Considerando a resposta anterior, no sentido de aplicar a LAI possibilitando a dilatação sem prazo definido em Regulamento, mas mediante justificativa, não haveria necessidade do Regulamento dispor taxativamente sobre prazos. O prazo será único, de 20 dias, com a diferenciação sendo definida pelo controlador, mediante justificativa. ", "615484": "Para maior efetividade, um canal de atendimento deve ter: (i) a indicação dos direitos que o titular poderá exercer; (ii) o prazo que o agente de tratamento possui para poder responder a requisição; (iii) informações sobre os meios de contato do Encarregado; e a (iv) disponibilização do link do Aviso de Proteção de Dados, caso o canal de atendimento seja em local diverso do próprio Aviso. ", "615485": "Sim, pois é possível que o operador descumpra com a LGPD ao atuar diante dos direitos de titulares, bem como não cumpra com uma instrução lícita do controlador, momento em que ele se equipara ao controlador e atrai para si a responsabilidade (art. 42, § 1º, I, da LGPD). Logo, o operador deverá cooperar nos limites das instruções lícitas fornecidas pelo controlador. ", "615486": "Preliminarmente, cabe destacar que o titular de dados pessoais nem sempre será considerado um consumidor. Portanto, nem sempre a aplicação da LGPD ocorre no âmbito de uma cadeia de consumo, a exemplo de titulares de dados pessoais que são funcionários. Levando isso em consideração, conclui-se que é inviável adotar as diretrizes e procedimentos análogos àqueles previstos no Decreto nº 11.034, de 5 de abril de 2022, uma vez que existem medidas que podem ser consideradas onerosas aos agentes de tratamento, a exemplo, da obrigatoriedade de acesso ao SAC por meio de atendimento telefônico (art. 4º, §2º) e a consequente disponibilidade dos canais 24h por dia, 7 dias por semana (art. 4º, caput). De todo modo, seria interessante indicar que o atendimento às requisições de titulares observem as garantias (tempestividade, segurança, privacidade e resolutividade da demanda) e os princípios (dignidade, boa-fé, transparência, eficiência, eficácia, celeridade e cordialidade) estabelecidos no art. 8º do Decreto em questão. ", "615487": "Os modelos de atendimento adotados por algumas empresas, como Nubank e Amazon, podem ser bons paradigmas para a ANPD por possuírem chatbots em suas plataformas, por meio do qual é possível filtrar a solicitação do titular e atender de forma célere algumas dúvidas. Também são disponibilizados outros canais de atendimento, como telefone, e-mail e WhatsApp, cuja escolha fica a critério do titular. ", "615491": "Sim. Caso a confirmação da existência conflite com o segredos comerciais e industriais dos controladores (ex.: alguma informação de novos negócios seja exposta em momento inoportuno) e se certos dados estiverem sendo tratados no âmbito de demandas que envolverão segredo de justiça (por exemplo, confirmar o tratamento de dados referentes a uma ação judicial que está em vias de ser ajuizada). ", "615492": "Os dados da(s) controladora(s) responsável(is) que constam no respectivo cartão CNPJ. ", "615489": "A responsabilidade do operador é a de cumprir com as

instruções lícitas do controlador, bem como o estabelecido na LGPD. ","615490": "A confirmação do tratamento e, se houver tratamento confirmado, quais são os dados tratados. ","615494": "A transparência exigida pela LGPD pode ser assegurada a priori (aviso de proteção de dados, por exemplo) ou a posteriori (após requisição). No que toca às informações fornecidas a priori, sugere-se uma exigência de transparência mínima, que incluiria os dados de identificação do controlador, dados de contato do controlador e do Encarregado, bem como um panorama de qual é a relevância dada pelo controlador para o tema proteção de dados. Como boa prática, recomenda-se a informação a priori apenas dos principais fluxos de dados tratados pela organização (dados vinculados às principais atividades), mas sem uma obrigação de um rol taxativo. Para essa informação macro, bastaria apresentar os principais dados tratados por categoria de titulares, as finalidades e bases legais, bem como uma informação acerca dos direitos do titular e como exercê-los. Sugere-se, também, o versionamento das informações apresentadas. ","615493": "O acesso simplificado estaria satisfeito. Para o acesso completo, além de disponibilizar os dados, é preciso atender o art. 19, II da LGPD. ","615502": "No que diz respeito à portabilidade dos dados, entende-se que alguns setores possuem potencial de maior maturidade: (i) o setor de telefonia, tendo em vista que a portabilidade de números de telefone já é realidade desde 2008; (ii) o setor bancário, considerando a realidade da portabilidade de salários, bem como sobre a portabilidade das operações de crédito, cujo procedimentos estão estabelecidos na Resolução 4.292, de 20 de dezembro de 2013, do BACEN; (iii) as operadoras de saúde que lidam diariamente com a portabilidade dos planos de saúde, envolvendo, inclusive, o tratamento de dados pessoais sensíveis; e (vi) setor hospitalar, que lida com a portabilidade de prontuários médicos. ","615501": "N/A"; "615505": "N/A"; "615503": "De acordo com a previsão do art. 18, V, da LGPD, o direito à portabilidade consiste na “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa (...)”. Dessa forma, entende-se que, caso o titular indique de forma expressa que seus dados devem ser transferidos para outro fornecedor, o direito à portabilidade só estará satisfeito após o cumprimento dessa transferência pelo agente de tratamento. Lado outro, caso não haja a requisição expressa, a disponibilização dos dados em formato interoperável ao titular seria suficiente para satisfazer o direito postulado. ","615504": "Sim. Além disso, a autorregulação regulada funciona bem para a definição desses padrões específicos. Sugere-se que os prazos sejam definidos em conjunto com as respectivas agências setoriais. ","615511": "Entende-se que o único critério objetivo que pode ser estabelecido é a manifestação do próprio titular sinalizando que seus dados estão incompletos, inexatos e/ou desatualizados. Demais critérios objetivos dependerão do contexto do tratamento e do dado pessoal. ","615514": "Nas situações em que: (i) o titular não comprove sua identidade; (ii) não foi identificado erro anterior, caso em que o titular deverá apresentar uma justificativa razoável para o exercício do direito de correção. ","615513": "N/A"; "615512": "Nas situações em que: (i) o titular não comprove sua identidade; (ii) não comprove que o dado estava errado, inexato ou desatualizado/não apresente motivos razoáveis para a correção; e (iii) quando a manutenção de um histórico acerca dos dados seja necessário para o controlador (nesse caso, a atualização pode ser feita, mas deve ser franqueado ao controlador a possibilidade de manter os registros antigos, para fins de histórico e produção de prova, além dos logs das correções).","615517": "O Controlador é quem possui todas as informações necessárias para definir a necessidade, a adequação e a conformidade com a LGPD. Restringir o direito à exclusão, bloqueio ou anonimização por uma obrigação formal de fundamentação seria inadequado. Contudo, é recomendável que o titular fundamente seu pedido, para que o Controlador possa exercer, quando necessário, um contraditório com o Titular.

;"615516": "Quando o requerimento de eliminação for realizado após o término de tratamento lícito (arts. 15 e 16 da LGPD), o controlador poderá, alternativamente, anonimizar os dados (art. 16, IV da LGPD). A base legal aqui seria o cumprimento da obrigação legal (art. 7º, II da LGPD), considerando que o controlador precisa encerrar o tratamento, mas lhe é franqueado pela LGPD a possibilidade de anonimizar para seu uso exclusivo, vedado seu acesso por terceiro (salvo se o terceiro for justamente um player para apoiar no processo de anonimização). ";

;"615518": "O §2º do art. 18 parece advir de erro do Legislador. Durante a tramitação legislativa da LGPD, o consentimento foi abordado como a base legal “prioritária”, inclusive prevista no caput do atual art. 7º. Contudo, considerando o texto aprovado e a redação vigente da LGPD, a menção à “hipóteses de dispensa de consentimento” não faz sentido, pois a adoção de outras bases legais, que não o consentimento, não configuram uma “dispensa de consentimento”. Veja-se que os §§4º, 5º e 6º do art. 7º, por exemplo, incorrem no mesmo erro (inclusive, é falado de “exigência do consentimento previsto no caput deste artigo”, o que não é a realidade do art. 7º). O que será necessário avaliar, naturalmente, é se a base legal adotada está adequada, assegurando-se ao titular o direito de opt out em certos casos (como em situações em que o legítimo interesse fundamenta o tratamento, mas o titular, ao exercer o opt out, deixa de ter a legítima expectativa de ter os dados tratados).";

;"615523": "Não, uma vez que até o momento da revogação do consentimento, o tratamento dos dados pessoais era lícito. Caso o titular queira que os dados pessoais tratados anteriormente sejam eliminados, ele deverá formular a requisição específica do direito à eliminação (art. 18, VI, da LGPD) e o agente de tratamento fará a análise específica dessa solicitação. Vale recordar que, conforme o art. 16, é autorizada a conservação de dados após o término do tratamento para “uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados”. ";

;"615521": "Caso o titular exerça o direito previsto no art. 18, VI, da LGPD (eliminação dos dados tratados com o consentimento), o agente de tratamento deverá cumprir com a requisição, ressalvadas as situações que autorizam a manutenção dos dados e que estão previstas no art. 16, a saber: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. ";

;"615617": "A principal diferença entre essas questões é a participação ou não de humanos no processo de tomada de decisões. Dessa forma, no caso de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, não há qualquer envolvimento de humanos no processo e é o caso, por exemplo, de um algoritmo que avalia um perfil e toma a decisão. Lado outro, seria um processo em que há uma avaliação por meio de um algoritmo, mas, após a avaliação, a orientação trazida pelo algoritmo é avaliada por um humano, que decide aprovar a recomendação ou fazer eventuais ajustes. ";

;"615618": "Não há como definir, a priori, os critérios, devendo ser avaliado no caso concreto. ";

;"615619": "Custos. Para muitas empresas, em especial do middle market, ter uma estrutura de equipe apta a endereçar manualmente um número significativo de pedidos de titulares é financeiramente inviável. Impor uma estrutura robusta para players que não possuem capital suficiente para priorizar essa obrigação poderia violar os princípios do art. 2º, em especial os fundamentos de “desenvolvimento econômico e tecnológico e a inovação” e de “a livre iniciativa, a livre concorrência e a defesa do consumidor”. Na prática, obrigações excessivas podem ser verdade barreira de entrada para novos players, prejudicando a concorrência e o mercado. ";

;"615620": "O art. 20, da LGPD, prevê o direito de o titular solicitar a revisão de decisões tomadas unicamente com base em

tratamento automatizado de dados pessoais e que afetem seus interesses. Dessa forma, caso se trate de decisão automatizada e que tenha participação de humanos, o direito não estará no escopo do art. 20 e, portanto, o controlador poderá negar o direito. Além disso, caso fique comprovado que o interesse do titular não foi afetado (ou seja, que não há fundamento para o pedido do titular), o direito também poderá ser negado. "

{ "615450": "Não. O ideal seria a indicação de prazo direcionada por requerimento e individualizada para cada direito disposto no Art. 18, respeitando a possibilidade de prorrogação mediante justificativa.", "615451": "b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "Importante definição do conceito de imediatamente e incluir critérios considerando a complexidade individualizada para cada direito disposto no Art. 18.", "615484": "Registo de data e horário da solicitação, bem como o histórico das movimentações posteriores. Número de protocolo para referência futura. Indicação do encarregado. Transparência ao titular quanto ao prazo de atendimento.", "615485": "Não. Conforme disposto no Art. 18 o direito do titular é obtido diretamente do controlador, sendo a função do operador de cooperar.", "615486": "Não, considerando que nem todas as solicitações serão consideradas relação de consumo e a inviabilidade de serviço ininterrupto.", "615487": "Desconhecemos.", "615491": "Sim, por exemplo confirmação da identidade do titular; poderes de confirmação de representatividade; quando não é agente de tratamento.", "615492": "Razão social, CNPJ e canal de atendimento.", "615489": "Cooperação prevista em contrato.", "615490": "Considerando que trata-se de declaração em formato simplificado, apenas os dados tratados, demais informações seriam apuradas na declaração completa.", "615494": "Informações do Art. 9 da LGPD, descrição do Aviso de Privacidade e Proteção de Dados; os dados pessoais dos fluxos das atividades de tratamento e os direitos dos titulares.", "615493": "Sim, formato digital ou papel (forma impressa), conforme 19, § 2º.", "615502": "Setor de Telefonia, tendo em vista a obrigatoriedade já existente de portabilidade dos números de contatos; serviço médico; setor imobiliário; bancário e rede social.", "615501": "Estruturação do banco de dados.", "615505": "Ferramentas capazes de estruturar a integração dos banco de dados entre controladores.", "615503": "Não, pois o titular não possui a capacidade técnica de validar os dados recebidos para portabilidade e somaria ao ônus de repassar para o fornecedor desejando, sendo essa responsabilidade do controlador, no sentido literal do Art. 18, V.", "615504": "Sim, é razoável a interoperabilidade por setor em conjunto com as agências reguladoras.", "615511": "A correção do dado precisa atingir a realidade atual para atendimento inclusive do princípio da qualidade do dado. Na maioria das situações caberia ao titular informar ao controlador o que precisa ser corrigido.", "615514": "Nos mesmos critérios da coleta de dado, sendo necessário o envio de evidência para situações específicas, por exemplo: alteração de endereço, mudança de estado civil, etc.", "615513": "Comprovadamente impossível: a não utilização da base compartilhada, com o devido descarte. Esforço desproporcional: quando não for possível realizar a comunicação de imediato.", "615512": "Quando não for possível comprovar a alteração do dado ou a manutenção do histórico do registro das informações ou quando não houver a comprovação da identidade do titular.", "615517": "Considerando que cabe ao controlador fundamentar, seria irrazoável a comprovação inicial pelo titular.", "615516": "Depende, considerando a situação prática. Pois ao final do tratamento os dados serão eliminados e caso não tenham hipótese legal para continuidade do tratamento, devem ser anonimizados. Por outro lado, se a anonimização for a pedido do titular não seria possível o controlador realizar a anonimização.", "615518": "O efeito seria a eliminação do dado, uma vez que a oposição foi considerada legítima.", "615523": "Não. Segue o Art. 8, § 5º da LGPD, pois a eliminação é decorrente de requerimento. O tratamento também poderá ser continuado se houver outra hipótese legal de tratamento, inclusive para eventual prova durante o prazo prescricional.", "615521": "Poderá resultar em cerceamento de defesa durante o prazo

prescricional. ";615617": "Decisão automatizada é aquela realizada exclusivamente por uma tecnologia e a decisão tomada unicamente com base em tratamento automatizado diz respeito das decisões do agente de tratamento mediante análise dos dados produzidos pela tecnologia.";615618": "Quando resultar em prejuízo comprovado ao titular ou quando os princípios da LGPD forem violados ou os direitos fundamentais desrespeitados.";615619": "A transparência aplicada à tecnologia que realizou as decisões automatizadas.";615620": "Quando comprovadamente e razoavelmente justificável for algo inviável, impossível ou oneroso."

{ "615450": "A ANPD deverá avaliar a criticidade da solicitação em comparação com o prazo previsto para seu atendimento, bem como, a especificidade da natureza do tratamento do dado pessoal em questão, i.e. compartilhamento com terceiros; relação operador-controlador, que podem gerar dependências de outros agentes; bem como, a complexidade do atendimento, como, por exemplo, num caso de anonimização.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "Sim, os prazos podem ser atendidos em até 20 dias, com prorrogação de mais 10, mediante justificativa expressa, como nos casos de algum incidente que resulte em alta demanda ou quando os dados são compartilhados em situações de controladoria conjunta e quando é necessário a identificação de operadores e suboperadores. Formato Simplificado: a resposta poderá ser feita através de templates simples ou corpo do e-mail/mensagem, sendo preferencialmente identificado dados cadastrais, sendo exclusivamente a caráter de direito da pessoa que realiza o tratamento, neste caso após a confirmação da identidade deverá ser realizado o atendimento em D+1, ou seja, em até 24 horas após a validação da identidade do titular. Declaração clara e Completa: deverá ocorrer em até 20 dias após a validação da identidade do titular, sendo em que ambos os casos a primeira resposta ao titular deverão ocorrer em até 2 dias uteis.", "615484": "O canal de atendimento deverá ser simplificado cujo direcione o titular a pontos específicos de atendimento da lei de proteção de dados, dando inclusive instruções para que o titular valide sua identidade nesse momento. Não deverá conter termos complexos e trazer uma breve explicação sobre o canal, além de uma breve explicação da lei para que o titular entenda a finalidade de sua requisição, tornando as solicitações ágeis para ambos os lados. De modo que a solicitação poderá ser feita através de formulários específicos indicados no site ou canal de comunicação. Além disso, deverá contar com processos para validação da identidade do titular ou operar por via de canal logado.", "615485": "Sim, entretanto, para essa definição deve ser levada em consideração a capacidade técnica do operador em efetivar a solicitação, visto que pode não possuir a ingerência necessária sobre os dados pessoais para que possa concretizar o pedido do titular, situação em que deverá se responsabilizar pela devida comunicação ao controlador correspondente, para que esse empenhe os esforços necessários para sua realização. Além disso, tal comunicação deverá ser acompanhada de previsão legal no regulamento a ser criado, bem como, deve ser definido prazo prévio para tal.", "615486": "A adoção de diretrizes e procedimentos análogos ao SAC para o exercício dos direitos do titular de dados pessoais é uma boa prática que pode contribuir para a efetividade da LGPD, bem como, para contribuir para a segurança jurídica tanto do ponto de vista dos titulares, quanto dos agentes de tratamento de dados, a fim de estabelecer procedimentos documentados e assegurar o cumprimento das expectativas de ambas as partes. Entretanto, tal proceduralização deve acompanhar as particularidades e complexidades inerentes ao tratamento de dados pessoais.", "615487": "O modelo utilizado é a solicitação via formulário, onde o titular é induzido as respostas de acordo com o atendimento da LGPD, onde não demanda ônus ao agente de tratamento, ocorre que em casos excepcionais devido ao grande volume, sugere-se uma ordem de prioridades de acordo com a demanda apresentada levando em consideração a solicitação do titular, devendo ser priorizada os casos de eliminação, correção, anonimização e posteriormente confirmação. O formulário é dividido em 3 partes: I – Titular fornece os dados cadastrais para identificação e de contato (e-mail e/ou telefone). II – O titular é induzido a responder dentro dos parâmetros da LGPD, ou seja,

através de um checklist, vai responder qual(is) direito(s) ele está requerendo. III – Validação da identidade do titular, nesse momento o titular encaminha 3 fotos ao agente de tratamento que ele está solicitando seus direitos. (i) foto do documento, (ii) foto do rosto (selfie), (iii) foto segurando o documento. Há outros meios de validação, por contato via SMS, WhatsApp e ou confirmação via e-mail. ","615491": "Como princípio, todo pedido de titular deve ser acompanhado com a confirmação da identidade do solicitante, a fim de resguardar os dados pessoais tratados pelo agente, bem como, assegurar a existência de nexo entre o solicitante e o dado pessoal tratado.", "615492": "Não temos contribuições.", "615489": "O operador, na capacidade de agente que atua mediante instruções prévias e documentadas do controlador, deve ser penalizado pela não efetivação do cumprimento de uma solicitação do titular quando há necessidade de sua contribuição e o agente falhar em fornecer as informações necessárias ou não disponibilizou justificativa no caso de incapacidade do fornecimento. O operador, deve, em sua capacidade, contribuir com o controlador quando necessário para que possa responder a uma solicitação de informação sobre o tratamento de dados pessoais, empregando os esforços necessários a fim de efetivar a solicitação. Nesse mesmo sentido, a ANPD, ao regulamentar o papel do operador na efetivação de solicitações dos titulares, deverá considerar situações em que o agente operador é incapaz de responder a um pedido, dada a uma possível incapacidade técnica ou operacional à vista de não possuir a devida ingerência sobre o dado pessoal, a impossibilidade de individualizar o titular, etc. Ademais, deverá ser levada em consideração os limites de responsabilidade da atuação sobre a gestão do processo de tratamento de dados pessoais por cada agente de tratamento. Por fim, a resposta do operador deve ser realizada mediante requisição em formato detalhada ou simplificado.", "615490": "- Categoria do dado pessoal tratado (i.e. "Nome"); e - O próprio dado pessoal tratado (i.e. "Paulo Silva").", "615494": "Confirmação de tratamento de dados pessoais e dados públicos ou que não gerem danos ao titular, como nome e idade. ", "615493": "O formato digital deverá ser o mais aceitável, apenas em casos específicos deverá ser tratado o dado em papel, muitas vezes o dado em papel poderá ser enviado por meio de carta, visto que nem sempre o titular ou o agente de tratamento é encontrado com fácil acesso, forçando o uso dos correios, sendo assim, a entrega da carta com os dados passa a ser mais um tratamento de riscos com um específico operador que independe do titular para realizar suas funções, além do mais os dados físicos são considerados um grande risco a incidente, tendo em vista a sua facilidade de destruição acidental ou não. ", "615502": "Não temos contribuições.", "615501": "Não temos contribuições.", "615505": "Não temos contribuições.", "615503": "Não temos contribuições.", "615504": "Não temos contribuições.", "615511": "Erros de digitação, erros crassos e critérios formais. Dados desatualizados estão de acordo com a atualização do titular, por exemplo, no caso de alteração de residência é necessário primeiro o informe do autor, posteriormente a atualização em tempo hábil. ", "615514": "Situações em que a solicitação do titular seja feita frente a um agente operador ou; situações em que o dado pessoal tenha sido recepcionado por outro agente controlador (controladoria conjunta), ocasião em que o titular deve ser orientado a postular sua solicitação frente ao controlador original e possuidor da fonte do dado pessoal questionado.", "615513": "Não temos contribuições.", "615512": "Sim, quando ocorre necessidade de apresentação de documento oficial, ou seja, quando a correção pende de decisão judicial ou alteração formal em cartório, respeitando todos os trâmites formais. ", "615517": "Não há necessidade, uma vez que após a solicitação do titular, é o controlador que irá determinar e fundamentar se a solicitação poderá ser acatada ou não. ", "615516": "Sim. A anonimização pode ser uma alternativa a eliminação de dados pessoais, garantida a irreversibilidade da identificação do

titular.;"615518": "Não temos contribuições.;"615523": "Não. Deverá ser levado em consideração a obrigatoriedade do agente de tratamento em reter os dados, à vista da necessidade de cumprir com uma determinação legal; seu legítimo interesse na retenção dos dados; e seu direito em reter os dados, como, por exemplo, para fins de defesa em procedimentos judiciais e não judiciais. Ademais, a revogação do consentimento deverá impactar tão somente tratamentos futuros, não atingindo tratamentos retroativos, a não ser que assim solicitado pelo titular. Nesse sentido, devem ser levadas em consideração as demais bases legais que possam legitimar a manutenção desses dados na base de dados do agente de tratamento.;"615521": "A revogação do consentimento deverá impactar tão somente tratamentos futuros, não atingindo tratamentos retroativos, a não ser que assim solicitado pelo titular. A eliminação dos dados não poderá ser feita por completo e imediato uma vez que existiu algum vínculo entre controlador ou titular, a determinação da eliminação dos dados dos titulares é algo pouco provável a jurisdição brasileira, podendo os dados serem armazenados em uma "base fria" onde há apenas o armazenamento do dado aguardando o tempo a prescrição jurídica dos direitos do titular bem como para fins de garantias etc. ";"615617": "Toda decisão tomada de forma tempestiva por um sistema, de software ou hardware, sem interferência humana (human in the loop). Por exemplo: um radar decide tirar uma foto automaticamente ao detectar um carro que percorreu uma distância acima do limite máximo estabelecido; um motor de decisão, rodando dentro de um app bancário, que decide negar empréstimo para uma pessoa com base em suas informações bancárias. Já uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais se refere a uma decisão tomada com base em processos automatizados nos quais dados pessoais foram tratados. Isto não inclui processos nos quais o ser humano lance mão de resultados de processos automatizados somados ao seu julgamento humano (sejam tais julgamentos subjetivos ou objetivos) para uma tomada de decisão. Por exemplo: um processo de onboarding em aplicativo no qual um ser humano submeta sua foto segurando um documento pessoal, onde uma IA de reconhecimento facial gerou um score de alta probabilidade de fraude e este processo foi direcionado a um atendente humano que, ao observar com seus próprios olhos a imagem constatou que esta se tratar de uma tentativa de cadastro fraudulento. Este processo não conta como um caso de decisão baseada unicamente em tratamento automatizado de dados pois houve interferência humana (human in the loop) e esta interferência era capaz de acatar ou negar a decisão da IA de acordo com julgamento próprio. ";"615618": "O interesse é efetivamente afetado quando a decisão automática tem impactos de cunho: Econômico - afetando de forma direto o indivíduo monetariamente ou de forma indireta, afetando o acesso a produtos financeiros que o indivíduo possa ter; e Social - afetando publicamente a imagem do indivíduo, seu acesso a diferentes camadas sociais.;"615619": "A revisão das decisões pode gerar aumentos exacerbados de custos. Pode-se criar um mecanismo de incentivo para pessoas mal intencionadas pedirem revisões de decisões automatizadas repetidamente, de modo a inviabilizar o processo. As revisões podem ser impossíveis devido à tempestividade do contexto no qual a decisão é tomada (carros auto-dirigidos, por exemplo). Canais pelos quais requisitar as revisões pode ser difíceis de implementar em algum contexto. A própria escolha do algoritmo de inteligência artificial a ser utilizado e as variáveis empregadas durante o processo de aprendizado do algoritmo podem dificultar a revisão e explicação de resultados.;"615620": "Toda decisão automatizada é tomada por um sistema parametrizado, com o uso de IA ou não. O controlador deveria cuidar para que, uma vez empregada IA no processo, esta seja construída de tal forma que seus resultados sejam explicáveis e auditáveis. Porém, existem casos nos quais a negativa de revisão/explicação pode ser

procedente: Situações nas quais a revisão da decisão é impraticável devido à imutabilidade das variáveis utilizadas no processo automatizado e no processo de aprendizado do algoritmo de IA. Tornando a revisão inócua, pois o modelo/processo retornaria o mesmo resultado. Situações nas quais a própria explicação da tomada de decisão revele segredos industriais que prejudiquem o controlador do sistema, causando problemas concorrenciais."

{ "615450": "A FecomercioSP, vem por meio desta, apresentar seu posicionamento aos quesitos levantados pela ANPD. Em relação ao primeiro questionamento: Ao nosso entender, não. De forma geral, os prazos previstos na Lei em questão variam entre 5-20 dias. Embora esses prazos possam ser exequíveis em sistemas centralizados (que tende a ser o caso da maioria dos órgãos da administração pública, que detêm atividades específicas e concentradas em alguns sistemas), tendem a ser inadequados para entes privados, que, inclusive pela necessidade de inovação para se manterem no mercado, têm sistemas e bases de dados diversos, em produção ou em teste, desempenhando atividades relevantes ao negócio, nos quais os dados pessoais do titular podem circular e, por isso mesmo, precisam ser verificados para o atendimento às solicitações dos titulares. Diante disso, para que as companhias tenham segurança nas respostas, é fundamental que prazo adequado seja concedido, sob pena de tornar inviável o atendimento com assertividade, especialmente para pequenas e médias empresas, que têm maior dificuldade para automatizar os processos de atendimento de direitos. Justamente por isso, o legislador europeu estabeleceu o prazo de 1 mês, prorrogável por até 3 meses, nos termos do art. 12(3), do GDPR, o que recomendamos seja seguido como referência por esta Autoridade. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Entendemos que os seguintes critérios relevantes podem ser razoavelmente tomados em consideração: • O grau de abstração do pedido: pedidos com escopo mais concreto tendem a ser mais facilmente (e mais rapidamente) atendidos do que pedidos com escopo demasiadamente abrangentes e abstratos. Quanto mais específica e limitada a solicitação, menor tende a ser o prazo necessário a atendê-la. • O termo inicial deveria ser contado a partir da validação da identidade do titular: em atenção ao princípio da segurança (art. 6º, VI, da LGPD), o atendimento de solicitações de direito deve ser precedido de prévia validação da identidade do titular, por intermédio de processo de autenticação razoável (ex. solicitação de cópia de documento, validação biométrica...). Deste modo, é recomendável que o termo inicial do prazo se opere após a comprovação, pelo titular, de sua identidade – nesse sentido já se posicionam alguns códigos de conduta setoriais, como a SARB 25, da FEBRABAN. • Tipo de Direito: Dependendo do tipo de direito, tempo maior pode ser necessário para atendê-lo. Assim, direitos como “acesso simplificado” (19, I), anonimização ou retificação, devem ter prazo menor, do que o de “acesso completo” (19, II), portabilidade ou exclusão por exemplo. • Complexidade da Solicitação: Solicitações complexas e que envolvam diversos pedidos em um só devem ter prazo sequenciais e individualizados – por exemplo, direito de acesso, retificação e exclusão simultâneos devem ter prazo individuais e sucessivos para atendimento. • Natureza do Dado: Quanto mais sensíveis os dados, maior a tendência de segurança no seu tratamento, logo, maior a complexidade para atender a pedidos dos titulares – como acesso e exclusão, por exemplo. ", "615484": "Entendemos que para canal de atendimento ser suficientemente efetivo, ele deve atender aos seguintes requisitos: • Acessível para a pessoa-média: Isto é, deve ser facilmente acessível pela maioria das pessoas, como: endereço de correio eletrônico, número de telefone ou formulário em um website; • Gratuito (como regra): Inexistência cobrança por parte do Controlador e os eventuais custos necessários para alcançar o canal de comunicação não apresentem óbice considerável para o exercício de direitos à pessoa-média – ex: embora acesso à internet ou a uma linha telefônica envolva custos, ele são razoáveis e, em regra, não serão óbice ao exercício de direitos – por outro lado, demandar que o titular envie solicitação por

correspondência física, com cópia de documentos autenticados, pode representar custo proibitivo. É importante apenas deixar claro que em situações de abuso do exercício regular de direitos pelo titular (exemplo: titular que reiteradamente exerce seus direitos de acesso) o agente de tratamento poderá cobrar do titular de dados os valores exatos despendidos para tal atendimento. • Permitir a Fundamentação: O titular deve ser capaz de fundamentar o seu pedido, explicar os seus motivos e/ou ofertar mais detalhes a respeito de sua solicitação, inclusive o resultado que deseja alcançar. • Seguro: considerando a tecnologia utilizada, o agente de tratamento deve adotar cuidados razoáveis para garantir a segurança do canal de comunicação escolhido (ex. criptografia dos dados em trânsito).

;"615485": "Apesar de não existir obrigação legal expressa a respeito do dever de cooperação por parte dos Operadores, é razoável deduzir que esse dever está diretamente relacionado à necessidade de serem observadas as instruções lícitas do Controlador. Adicionalmente, em atenção às boas-práticas, é recomendável que isso seja incluído (e tipicamente o é) no contrato entre o controlador e o operador. Dito isso, o dever de cooperação por parte do operador deve ser entendido como a obrigação de empregar esforços razoáveis para que o controlador consiga atender à solicitação apresentada ao titular, observado o escopo do contrato entre as Partes. Desde que relacionado ao objeto da relação entre as partes, podemos delimitar essa obrigação de duas formas, em linha com o item 8.3.1 da NBR ISO/IEC 27701: (i) fornecer as informações que sejam razoavelmente necessárias para atender às solicitações de determinado titular (ex. fornecer cópia dos dados pessoais ou lista de suboperadores que porventura tenham tido acesso aos dados do titular); (ii) implementar as medidas técnicas que sejam razoavelmente necessárias para o atendimento da solicitação (ex. executar script para descartar ou alterar determinado dado).

;"615486": "Entendemos que não, pelos seguintes motivos: • Considerando que a LGPD não determinou nenhum modelo mandatário de canal de atendimento, pelo que, qualquer canal de atendimento razoável, deve ser encarado como perfeito cumprimento das obrigações legais por parte do controlador, posição, inclusive, adotada na União Europeia, conforme se extrai da Guideline 01/2022/EDPB, não nos parecem adequadas as seguintes diretrizes constantes na norma legal em análise: (i) operar por diversos canais de atendimento integrados (Art. 2º); (ii) Atendimento telefônico obrigatório (art. 5º); (iii) Necessidade de registro numérico ou outro tipo de procedimento eletrônico (art. 12º), pois: • É impossível também garantir a disponibilidade ininterrupta (art. 4º, caput), pois: (i) garantir a disponibilidade absoluta dos canais de comunicação é impossível, sendo a interrupção ou a redução de disponibilidade, consequência, inclusive, da necessidade de manutenção dos sistemas; (ii) o atendimento de solicitações de titulares em regra depende da prévia análise de profissionais de privacidade especializados, inclusive, para verificar a adequação da solicitação apresentada – profissionais especializados e que cuja manutenção requer o dispêndio de valores significativos. • Considerando que a validação prévia da identidade do titular é uma boa-prática decorrente da necessidade de se atender ao princípio da segurança e encontra previsão tanto em códigos de conduta setoriais nacionais (SARB nº 25/FEBRABAN), quanto na Guideline 01/2022/EDPB, não entendemos adequadas as diretrizes relativas à (ao) (i) não-vinculação do contato inicial ao fornecimento de dados pessoais (art. 4º, §4º); e (ii) termo inicial do prazo contado a partir do registro da demanda (Art. 13º). • Necessidade de inclusão do canal de atendimento em todo documento na contratação do serviço (art. 7º): entendemos, com base na redação do art. 9º da LGPD, que é suficiente que o canal para o exercício de direitos dos titulares seja incluído no Aviso de Privacidade.

;"615487": "Existem modelos de atendimento já adotados, que permitem o tratamento de grande volume de solicitações, por meio de ferramentas tecnológicas (ex. OneTrust,

Securiti.ai...) que tornam o processo de resposta às solicitações de direitos, no mínimo, parcialmente automatizado. Essas soluções geralmente são conectadas às bases de dados, e, quando diante de solicitação do titular, podem, dentre outros: (i) realizar varreduras, identificando, por meio de certos identificadores (ex. CPF), se dados do titular são armazenados, quais dados e em quais bases; (ii) fornecer ao titular a possibilidade de baixar os dados ao seu respeito; e (iii) gerar (e até mesmo executar) scripts destinados à eliminação e modificação de dados. A problemática é: muitas dessas soluções tecnológicas possuem custo para a sua implantação, especialmente no atual momento de considerável desvalorização do real em relação ao dólar, pelo que, mesmo as soluções nacionais, muitas vezes não são acessíveis para as organizações em geral, não devendo, portanto, ser tornados obrigatórios, mas como recomendações de boas práticas. ";615491": "Sim. Existem situações em que é razoável que seja negado o direito de confirmação da existência do tratamento: • Quando a confirmação puder causar prejuízos significativos ao agente de tratamento ou à sociedade. Podemos trazer alguns exemplos típicos, em que é razoável manter o tratamento em sigilo: (i) dados relacionados a suspeitas e investigações de fraude, em âmbito privado; (ii) dados relativos a suspeitas e investigações de financiamento ao terrorismo ou lavagem de dinheiro; (iii) investigações de incidentes; (iv) dados relacionados a operações de tratamento resguardadas por segredos comerciais. • Quando o titular não tenha comprovado a sua identidade, em atenção a requisição razoável de prova por parte do controlador; ou • Quando o titular atue de má-fé, por exemplo, apresenta solicitações repetitivas ao controlador sem justificativa aparente. ";615492": "A avaliação precisará ser sempre casuística e atentar aos requisitos concretos. Entendemos que, na maior parte dos casos, o nome empresarial será suficiente para a identificação dos controladores, permitindo que os titulares identifiquem facilmente o controlador em questão. Em algumas situações, desde que inexistam significativo prejuízo aos titulares, o fornecimento de informações mais genéricas (isto é, categorias de controladores) deve ser entendida como adequada – por exemplo, se determinada empresa compartilha dados com os grandes bancos de crédito, entendemos que fornecer essa informação de forma ampla será suficiente para que o titular compreenda razoavelmente com quem seus dados estão sendo compartilhados. ";615489": "Conforme informado na resposta ao questionamento do item 1.d, a responsabilidade dos operadores deve ser de apresentar o suporte necessário aos respectivos controladores. Assim, caso lhes seja apresentada alguma solicitação de direito, eles devem direcionar os titulares para o controlador, jamais devendo atender a solicitação sem prévia autorização do controlador. ";615490": "Considerando que o formato simplificado requer que os dados sejam fornecidos imediatamente (prazo que entendemos deva ser entendido como em até 2 dias úteis), tal pedido deve poder contemplar apenas os dados cadastrais (nos termos do artigo 11, § 2º do Decreto 8.771/2016), no formato em que se encontram, isto é, aqueles constantes no cadastro do titular junto à organização, se existentes, visto que tendem a ser os dados prontamente disponíveis para a organização fornecer aos respectivos titulares. ";615494": "A LGPD já determina, em seu art. 9º, quais informações devem ser proativamente fornecidas pelo controlador. Os quesitos presentes no artigo devem ser interpretados à luz das normas técnicas aplicáveis, especialmente a ABNT NBR ISO/IEC 29184 e em posicionamentos da ANPD (ex. Nota Técnica nº 49/2022/CGF/ANPD), do seguinte modo: • Finalidade específica do tratamento: descrição suficiente a permitir ao titular entender de forma clara e imediata o propósito para o qual os seus dados serão utilizados, esclarecendo-se quais categorias de dados serão utilizadas para quais propósitos. • Forma do tratamento: indicando o método, momento e a localização da coleta dos dados pessoais, o método de seu uso (inclusive se envolverá tomada

de decisão automatizada) e a jurisdição legal em que os dados ficarão armazenados (isto é, se haverá transferência internacional). • Duração do tratamento: isto é, o prazo identificado, ou identificável, em que os dados serão retidos. • Identificação do controlador: seu nome empresarial, podendo incluir o seu CNPJ. • Informações de contato do controlador: entendemos tratar-se do contato do Encarregado ou, para os agentes de tratamento de pequeno porte, o canal para o exercício de direitos que fala o art. 11, §1º, do Regulamento de Agentes de Tratamento de Pequeno Porte. • Informações acerca do uso compartilhado de dados pelo controlador e a finalidade: com quais agentes de tratamento (ou categorias de agentes de tratamento) poderão ser compartilhados dados, quais dados e com quais finalidades. • Responsabilidades dos agentes que realizarão o tratamento: Complemento ao item anterior, identificando a função/papel dos agentes de tratamento (ou categoria de agentes de tratamento) no processo. • Direitos do titular: Fornecer aos titulares uma listagem com seus direitos conferidos pelo art. 18º, da LGPD. Embora a legislação não obrigue, o fornecimento de informações a respeito de direitos previstos em outros artigos, como àqueles constantes no art. 20º, deve ser visto como uma boa prática. ";615493": "Ressalvado se o titular solicitar informação adicional sobre o tratamento, entendemos como razoável que o fornecimento de cópia digital dos dados pessoais seja adequado a satisfazer os direitos de acesso. No entanto, caso o titular requeira que as informações sejam fornecidas em formato impresso, entendemos por razoável que o agente de tratamento possa requerer que o titular arque com os custos razoáveis do fornecimento das informações nesse formato (ex. custos de impressão e envio). ";615502": "Atualmente, entendemos que apenas os setores regulados, com iniciativas em vigor ou desenvolvimento para se permitir a portabilidade de dados (como o setor financeiro e o setor securitário) se encontram parcialmente aptos a implementar o direito de portabilidade de forma suficientemente madura. ";615501": "Implementar padrão de interoperabilidade global, aplicável a todos os agentes de tratamento, tende a enfrentar problemáticas técnicas, dentre as quais: • Padrões setoriais: a existência de múltiplos padrões já bem estabelecidos e pacificados nos diferentes setores – o que, se não for problema intrassetorial, pode tornar o compartilhamento de dados com controlador que não integre o setor do agente de tratamento de origem consideravelmente dificultado. • Obsolescência acelerada: o rápido desenvolvimento tecnológico faz com que padrões rapidamente sejam substituídos, pelo que padrão adequado, na atualidade, para manter a interoperabilidade, pode não o ser dentro de alguns anos. • Variedade tecnológica: as organizações tendem a utilizar diferentes aplicações e sistemas, inclusive operacionais, que podem se utilizar de diferentes linguagens e protocolos de comunicação, o que pode dificultar significativamente a interoperabilidade. ";615505": "Considerando que o direito de portabilidade afeta a todos os agentes de tratamento, inclusive os de pequeno porte, entendemos que o processo de padronização deve: (i) ser residual, isto é, apenas aplicável quando inexistir regulação (ou autorregulação) setorial sobre o tema; (ii) ser suficientemente preciso para tornar a portabilidade exequível; e (iii) ser suficientemente amplo, de modo a permitir que todos os agentes de tratamento, inclusive os de pequeno porte, possam atendê-lo. Tendo isso em consideração, em nosso entendimento a ANPD deve priorizar 3 itens: • O formato em que os dados devem ser fornecidos: sendo recomendável que os dados sejam fornecidos de forma estruturada e, preferencialmente, em formatos tipicamente utilizados para exportar dados para sistemas e aplicações de internet ou facilmente exportáveis para bancos de dados, como o XLSX. • O caminho da transferência: na inexistência de ferramentas setoriais específicas, entendemos que os dados devem poder ser transferidos por quaisquer meios razoavelmente seguros e acessíveis. • O processo de transferência: entendemos que devem ser definidos: (i) o

dever do titular de assegurar, e fornecer ao agente de tratamento de origem, as informações necessárias para permitir com que o agente de tratamento de origem execute seu processo de transferência, conforme orientações deste; (ii) os papéis e responsabilidades individuais dos agentes de tratamento; e (iii) o prazo mínimo com que o agente de tratamento de origem deve manter os dados e as informações disponibilizados ao agente de tratamento de destino. ";615503": "Considerando que, nessas hipóteses, o titular pode, por si só, compartilhar seus dados com os demais controladores, conforme acerto direto com estes, entendemos que o fornecimento aos titulares dos dados ao seu respeito será suficiente para o atendimento do direito à portabilidade. ";615504": "Sim. Além de razoável, é também desejável, tendo em vista que permite que as organizações do setor privado, em suas associações setoriais, adotem os mecanismos mais adequados para cada setor. Quanto ao prazo de definição e implantação deste padrão, utilizando o Open Finance como parâmetro, cujo marco inicial se deu no início de 2020 (Resolução Conjunta nº 01/2020) e atualmente se encontra em sua última etapa de implantação, iniciada em meados de 2023, sugerimos o prazo de, pelo menos, 05 (cinco) anos. ";615511": "- Como regra geral, um dado só deve ser considerado impreciso, incompleto ou desatualizado se estiver (ou puder ser) sujeito a verificação objetiva, indicando a falta de qualidade na informação. Em outras palavras, a informação deve poder ser objetivamente comprovada como inacurada, seja por ser historicamente imprecisa ou por ter se tornado imprecisa ao longo do tempo. Nesse sentido, dados que sejam previsões probabilísticas, derivados de análises estatísticas, meramente opinativos (representando inferência sobre alguém), resultantes de testes e questionários preenchidos pelo titular (como testes comportamentais) ou de qualquer outra forma que não possam ser objetivamente comprovados como imprecisos de maneira razoável, não devem ser considerados inverídicos, mesmo que o titular desses dados deles discorde. Essa regra tem exceções apenas nos casos em que for demonstrado que os dados objetivamente verificáveis que, porventura, fundamentam as informações não-verificáveis não são precisos, completos ou atualizados. Nessas situações, é possível solicitar a correção desses dados objetivamente verificáveis e, uma vez corrigidos, a atualização das informações que dependem deles, mesmo que não possam ser objetivamente verificadas por outros meios. Exemplificamos: embora o titular não possa solicitar a correção de sua pontuação de crédito em dada instituição, por entender que ele é melhor pagador do que a pontuação aponta, caso alguma informação utilizada no cálculo da pontuação se encontre inacurada ou desatualizada, poderá pedir a sua correção e, feita a correção, que a pontuação seja atualizada. ";615514": "Entendemos que existem situações em que é possível pressupor a possibilidade de a organização condicionar a retificação a algum processo de validação: • O dado não se enquadra na regra de verificabilidade objetiva proposta no questionamento 4.a; • Existe razoável probabilidade de dano ao titular. Por exemplo, se o titular recebe documentação financeira (ou confidencial) em seu endereço, como cartão de crédito, por exemplo, é razoável que a organização valide o endereço, antes de retificá-lo; • Existe razoável probabilidade de dano ao agente de tratamento. Por exemplo: o titular participa de programa de fidelidade de um varejista e afirma identificou erro em seu histórico de compras, que faz com que ele detenha menos pontos do que deveria (Ex. compra de alto valor não foi registrada). Retificar o histórico de compras sem que o titular comprove a realização da compra implicaria em possível prejuízo ao varejista. • Existe razoável probabilidade de dano a sociedade. Por exemplo: o titular requer a um banco de dados de crédito que remova a negativação de seu nome, alegando o pagamento da dívida. Caso em que, a aprovação da atualização sem o fornecimento de comprovante, poderá levar grande insegurança ao mercado de crédito. • Existe obrigação legal de validar a informação, como

aquelas requeridas às instituições financeiras de validar os dados cadastrais de seus clientes (art. 16, da Circular BCB nº 3.978/2020). Essa validação não necessariamente implicará na necessidade de coleta de informação adicional junto ao titular, podendo se operar por outros meios, especialmente pela comparação com informações detidas por birôs de dados. ";615513": "Igualmente, a avaliação do esforço desproporcionado deve ser uma avaliação casuística. No entanto, entendemos que alguns requisitos objetivos devem ser considerados em sua elaboração: • O volume de pessoas a serem notificadas, tendo em vista que influencia no volume de recursos que deve ser alocado para se proceder a comunicação; • Capacidade econômica do agente de tratamento, tendo em vista que influencia no volume de recursos que o agente de tratamento consegue alocar para realizar a comunicação; • O momento em que se operou o compartilhamento, tendo em vista que influencia a utilidade da comunicação – quanto mais tempo decorreu entre o momento do compartilhamento e o momento da retificação, menor a sua utilidade; • Os efeitos que a comunicação (ou ausência dela) podem previsivelmente surtir no titular, inclusive, considerando eventuais salvaguardas adotadas para resguardar o titular de eventuais danos decorrentes da inexactidão das informações. ";615512": "Entendemos que o direito de correção poderá ser negado em quaisquer das seguintes hipóteses: • A informação que se busca retificar não é objetivamente verificável, conforme descrito na resposta ao questionamento 4.a; • É razoável, ou mesmo legalmente mandatário, validar a informação fornecida pelo titular, nos termos do questionamento 4.b, e essa validação não é possível – por exemplo, o titular se recusou a fornecer o comprovante de residência para alterar o seu endereço; • Os dados, ainda que equivocados, precisam ser mantidos para fins históricos, inclusive em razão de obrigação regulatória; • O titular atua de má-fé, exercendo seu direito de retificação de forma abusiva, com objetivos outros, que não o de garantir a qualidade dos dados ao seu respeito; e • O atendimento seja excessivo, notadamente quando da apresentação de pedidos repetitivos, sobrepostos ou em volume excessivo. ";615517": "Sim. As obrigações e os encargos das organizações que tratam dados já são demasiadamente pesadas, tendo em vista a LGPD, outras leis e regulamentações setoriais, e os custos com segurança, de forma geral. O cumprimento do princípio da necessidade, da obrigação de não tratar dados excessivos (art. 6º, III), e a conformidade com a legislação e normas aplicáveis, são obrigações dos agentes de tratamento de dados pessoais. Portanto, é de se pressupor que, sendo obrigações, já haverá o seu natural cumprimento, sob pena de denúncias aos órgãos competentes, como a ANPD (além de órgãos setoriais), e respectivas fiscalizações. Há que se impor regras para os requerimentos dos titulares, sob pena de inviabilizar a conformidade. A título de exemplo, suponha que um titular solicite a exclusão de seus dados pessoais do banco de dados de marketing de uma empresa. No entanto, ele não fornece fundamentação para sua solicitação e não demonstra que os dados são desnecessários para os fins do tratamento ou que a empresa está tratando os dados de forma excessiva. Além disso, o titular não aponta nenhuma desconformidade ou descumprimento legal por parte da empresa em relação ao tratamento de seus dados. Sem a fundamentação clara, prova da desnecessidade dos dados ou da excessividade do tratamento, a empresa pode não ter o embasamento necessário para justificar a eliminação dos dados. A empresa não poderia simplesmente excluir os dados sem justificativa, e ainda estaria sujeita a reclamações do titular ou ações judiciais por não atender à sua solicitação. ";615516": "Sim. A anonimização pode ser considerada a melhor alternativa, a depender da situação específica, como no caso em que os dados são tratados para fins estatísticos. A anonimização pode ser opção mais adequada, pois permite a utilização dos dados de forma agregada, sem identificar os titulares. Entretanto, se os dados já não forem mais necessários para nenhuma finalidade

legítima e sua retenção representar risco para os titulares e ao agente de tratamento, a eliminação é a medida cabível. Portanto, a anonimização e a eliminação podem ser adotadas alternativamente, dependendo das circunstâncias específicas e das necessidades do tratamento. Ainda, tendo em vista que dados anonimizados deixam de ser considerados dados pessoais, para fins da LGPD (art. 12), deve ser considerada cumprida a obrigação do agente de eliminar os dados pessoais ao término do tratamento (art. 16, caput).

","615518": "O efeito prático da alegação do titular resultaria na cessação imediata do tratamento contestado, protegendo assim os seus direitos. O controlador deve tomar todas as medidas técnicas e administrativas para garantir que a interrupção seja efetiva, tais como a suspensão de compartilhamentos de dados com terceiros e a eliminação dos dados de seus sistemas. ","615523": "O § 5º do art. 8º da LGPD legitima os tratamentos de dados pessoais realizados antes da revogação do consentimento, ou seja, sob a égide do consentimento anteriormente concedido, e ressalta: “enquanto não houver requerimento de eliminação”. Portanto, a revogação não implica na obrigação de eliminação automática, mas somente se houver o requerimento expresso por parte do titular. ","615521": "Caso haja o requerimento de eliminação de dados sob a égide do consentimento anteriormente concedido, os dados deverão ser efetivamente eliminados pelo controlador, salvo exceções previstas no art. 16 da LGPD. ","615617": "A diferença entre decisão automatizada e decisão tomada unicamente com base em tratamento automatizado de dados está no nível da intervenção humana e do controle exercido sobre a referida decisão. Por exemplo, sistema automatizado que recebe os dados financeiros do cliente, como histórico de crédito, renda e dívidas. Com base nessas informações, em conjunto aos critérios definidos pela instituição financeira, o sistema gera automaticamente decisão sobre se o cliente é aprovado ou rejeitado para o empréstimo. Neste caso, o processo é automatizado, mas pode haver alguma intervenção humana para configurar os parâmetros do sistema, ajustar os critérios de aprovação, ou revisar exceções. Essa intervenção humana pode adicionar certo grau de supervisão e controle à decisão final. No caso da decisão tomada unicamente com base em tratamento automatizado de dados, o sistema automatizado toma a decisão sem intervenção humana significativa. Ou seja, o sistema é programado para analisar os dados do cliente e, com base em algoritmos pré-definidos, determinar se o empréstimo é aprovado ou rejeitado. Não há revisão humana dos critérios de aprovação ou consideração de circunstâncias especiais do cliente. A decisão é totalmente determinada pelo tratamento automatizado dos dados, sem influência humana direta. ","615618": "Em alinhamento com o Regulamento Europeu, entendemos que um interesse deve ser considerado como “relevantemente afetado”, quando, a decisão possui efeito jurídico relevante ou a este assemelhado. Entendemos que essas situações se concretizam quando pelo menos um dos seguintes critérios for satisfeito: • A decisão, de qualquer modo, afeta a esfera jurídica de uma pessoa, isto é: o conjunto de seus direitos e suas obrigações jurídicas. Por exemplo: decisão que determina o acesso a um produto/serviço por um titular, ou os termos com os quais esse acesso se procederá. • A decisão impede ou dificulta a produção de efeito jurídico desejado pelo titular, por exemplo, denegando acesso a determinado produto/serviço. • A decisão afeta substancialmente processo decisório que modifica (ou impede a modificação) da esfera jurídica de uma pessoa – ou seja, ainda que a decisão, por si só, não afete a esfera jurídica do titular, é esperado que ela influencie substancialmente decisões que o façam (ex. pontuações de crédito). • Embora a decisão não necessariamente afete a esfera jurídica do titular, pode surtir efeitos significativos nos objetos resguardados por seus direitos fundamentais. Por exemplo, decisão que, se equivocada, pode levar ao falecimento do titular. ","615619": "O maior desafio que se impõe na revisão de decisões automatizadas se

refere à complexidade técnica sobre a explicação dessa decisão. Para que o direito à revisão exista, é necessário que o titular tenha possibilidade de apresentar sua percepção sobre como os dados devem ser tratados, de onde possam decorrer erros, discriminações ou mesmo porque um determinado dado ou fator não se aplica ao tratamento. Assim, o direito à explicação pode ser considerado um pressuposto para o exercício de outros direitos. Há correntes doutrinárias que discutem se esse direito à explicação estaria ou não contemplado no ordenamento jurídico brasileiro, ou até mesmo se seria exequível, tendo em vista possíveis opacidades, que consistem em resultados ininteligíveis nas decisões automatizadas. Isso porque o cérebro humano pode não conseguir identificar o que efetivamente determina o resultado de um modelo algorítmico muito complexo. Além disso, é necessário preservar os segredos comercial e industrial, que por vezes podem ter direta relação com as formas pelas quais o resultado foi atingido. Outro desafio consiste em assegurar que os processos de revisão sejam transparentes, justos e imparciais, sem comprometer a eficiência e a agilidade das operações automatizadas. Esses desafios demandam não apenas esforços técnicos e operacionais, mas também abordagem cuidadosa e colaborativa entre os setores público e privado, de modo que não haja regulamentação excessiva, com a imposição de obrigações que barrem o desenvolvimento econômico, tecnológico e a inovação (fundamentos da proteção de dados, nos termos do art. 2º, V). "615620": "Entendemos que podem subsistir algumas situações em que seja razoável que o Controlador denegue o direito de revisão da decisão automatizada. Muito embora entendamos a necessidade de análise casuística, sendo impossível esgotar todas as hipóteses em uma única lista, destacamos as seguintes situações: • A decisão envolveu participação humana relevante: existindo intervenção humana relevante (isto é, apta a alterar o resultado), tendo em vista que o direito previsto no art. 20, caput, da LGPD, é limitado às decisões tomadas unicamente por meios automatizados; • O titular não forneceu nenhum fundamento apto a modificar a decisão: o exercício de revisão possui como pressuposto o fornecimento, pelo titular, de argumentos capazes de modificar o entendimento sobre o assunto. Se estes não são apresentados, é impossível proceder a revisão da decisão; • Caso, por questões de segredo comercial, o controlador não possa fornecer as informações a que se referem o art. 20, §1º, da LGPD: sem o fornecimento de informações a respeito do processo decisório, não é possível, em regra, o fornecimento de argumentos pelo titular aptos a modificar a decisão, pelo que inviável o atendimento do direito de revisão; • A revisão da decisão não apresenta qualquer utilidade ao titular: são aquelas situações em que a decisão já produziu e esgotou os seus efeitos, pelo que sua revisão não trará qualquer benefício real ao titular; • O titular atua de má-fé: exercendo seu direito de revisão de forma abusiva, com objetivos outros, que não o de garantir a qualidade dos dados ao seu respeito; • O atendimento seja excessivo: notadamente quando da apresentação de pedidos repetitivos, sobrepostos ou em volume excessivo. "

{ "615450": "De acordo com o artigo 11, parágrafo 1º, da Lei de Acesso à Informação (LAI), solicitações de acesso a informação pública devem ser atendidas prontamente, quando viável. Se isso não for possível, deve-se fornecer uma resposta no prazo de até 20 dias, prorrogável por mais 10 dias. Sob a Lei Geral de Proteção de Dados Pessoais (LGPD), especificamente no artigo 19, o direito à confirmação da existência ou ao acesso a dados pessoais deve ser atendido de imediato, em um formato simplificado, ou através de uma declaração completa, no prazo de até 15 dias. Assim, os prazos definidos tanto na LGPD quanto na LAI referem-se a contextos distintos e não geram conflitos entre si: a LAI aplica-se a pedidos de acesso a informações que não necessariamente configuram dados pessoais; e apenas às entidades listadas no parágrafo único de seu artigo 1º, notadamente a órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo e Judiciário, e do Ministério Público, e a entidades controladas pela União, Estados, Distrito Federal e Municípios. A LGPD, por sua vez, conforme seu artigo 1º, abrange tanto o setor público quanto o privado; mas se limita ao acesso a dados pessoais do titular. A complexidade da solicitação feita pelo titular ao agente de tratamento deve ser o critério principal para definir os prazos de resposta. Portanto, considerando a natureza das solicitações de dados pessoais e as exigências para a elaboração de um relatório completo sobre o tratamento desses dados, estabelecer um prazo maior que os 15 dias previstos na LGPD para o fornecimento completo das informações pode não ter justificativa factual.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Para definir prazos de cumprimento relacionados aos direitos dos titulares de dados, é essencial primeiro entender a complexidade envolvida na resposta adequada às solicitações. Isso inclui avaliar quão fácil ou difícil é atender ao pedido e se é necessário organizar os dados de alguma forma. Essa análise deve levar em conta características específicas dos agentes de tratamento responsáveis por atender a essas solicitações, especialmente a previsibilidade de tais pedidos. Se um agente já espera receber solicitações de acesso a dados, deve organizar seus processos para cumprir com essas obrigações de maneira eficiente. Existem agentes de tratamento que talvez não antecipem uma grande frequência desses pedidos. Para esses casos, o desafio de fornecer as informações solicitadas pode ser consideravelmente maior. A Autoridade Nacional de Proteção de Dados (ANPD) reconhece essa dificuldade e, conforme o artigo 14 da Resolução CD/ANPD nº 2/2022, estabelece prazos estendidos para agentes de tratamento de pequeno porte. Isso se aplica tanto ao atendimento das solicitações quanto ao cumprimento das obrigações relacionadas aos direitos dos titulares de dados. Além disso, é importante considerar o risco de danos que podem ser causados pela demora no fornecimento dos dados. Esse risco deve ser um critério adicional para determinar os prazos adequados para cada caso.", "615484": "Para assegurar uma comunicação eficaz entre o titular dos dados e o agente responsável pelo tratamento, é crucial que os canais de atendimento não se limitem apenas a sistemas automatizados. A Lei Geral de Proteção de Dados (LGPD) destaca, especialmente em seu artigo 20, as restrições impostas à automação no processamento de dados pessoais. Os titulares têm o direito de pedir revisões, obter informações sobre os critérios e procedimentos adotados nesse processo, e podem requerer à Autoridade Nacional de Proteção de Dados (ANPD) que inspecione possíveis práticas discriminatórias na automação desses tratamentos.", "615485": "Dentro do escopo das responsabilidades dos operadores no tratamento de dados, se destaca a necessidade de que suas ações sejam congruentes com

suas obrigações. Por exemplo, se um operador é responsável pela organização de uma base de dados, ele deve ser capaz de fornecer relatórios detalhados sobre essa atividade. Assim, é fundamental assegurar que haja alinhamento entre o nível de envolvimento dos operadores nas atividades de tratamento de dados e a responsabilidade atribuída a eles por essas operações."

"615486": "O Decreto nº 11.034/2022 define diretrizes essenciais para o funcionamento do Serviço de Atendimento ao Consumidor (SAC), incluindo a obrigatoriedade de oferecer o serviço gratuitamente, garantir sua disponibilidade contínua, e proibir a inclusão de mensagens publicitárias durante o tempo de espera. O Decreto promove regulamentação sobre o Código de Defesa do Consumidor (CDC) e, naturalmente, aplica-se àquelas entidades sujeitas ao CDC. Considerando que muitas interações que envolvem dados pessoais se enquadram em relações de consumo, tornando pertinente a aplicação das normas do SAC a essas situações, sempre que apropriado; no entanto, tal circunstância não se confunde com aquelas verificadas em relações com serventias extrajudiciais. Cabe notar, contudo, que, conforme amplamente reconhecido na jurisprudência de tribunais superiores, tanto pelo Supremo Tribunal Federal quanto pelo Superior Tribunal de Justiça, a relação jurídica entre o titular de serventias notariais tem natureza não consumerista. Logo, não havendo aplicabilidade do Código de Defesa do Consumidor aos prestadores de serviços cartorários extrajudiciais, tampouco incide sobre as serventias o Decreto que institui o Serviço de Atendimento ao Consumidor. Assim, os canais de atendimento aos titulares no caso das serventias extrajudiciais serão, naturalmente, distintos."

"615487": "A organização adequada de dados pessoais, especialmente aqueles sujeitos a pedidos com base nos direitos dos titulares, é crucial para aumentar a eficiência na resposta a tais solicitações. Em situações de alto volume de pedidos de acesso, a prática de manter os dados devidamente estruturados facilita a execução rápida desses pedidos, eliminando a necessidade de prazos extensos para atendimento. Considerando a variabilidade e previsão de exercício de direitos pelos titulares, uma gestão interna organizada é essencial para promover respostas ágeis às suas demandas. Ainda que exemplos de sucesso na gestão de informações possam ser usados como parâmetro, o formato de organização e o modelo a ser adotado dependerão diretamente das atividades exercidas pelo agente de tratamento, pois cada agente terá particularidades em relação à melhor forma de realizar essa gestão."

"615491": "A negativa de confirmação da existência de tratamento de dados pode ser necessária em casos excepcionais para proteger informações sensíveis ou a integridade de investigações privadas ou de interesse público. Tal resposta se limitaria a um simples "sim" ou "não" para perguntas diretas sobre o processamento de dados por um agente específico. Situações que podem justificar essa recusa incluem a proteção de investigações de compliance, ou questões já previstas como exceções pela LGPD. Além disso, a confirmação do processamento de dados que revele informações sensíveis pode ser negada para a garantia de privacidade do titular dos dados correspondentes."

"615492": "Devem ser fornecidas informações corriqueiras que permitam a individualização do agente que exerce função de controlador, tais quais seu CNPJ, nome empresarial, endereço da sede, endereço eletrônico e afins."

"615489": "As obrigações dos operadores em fornecer informações sobre o tratamento de dados aos titulares devem estar alinhadas com as funções desempenhadas pelo agente de tratamento. Se um operador é responsável por gerenciar um banco de dados, ele deve ser capaz de prestar esclarecimentos sobre esse tratamento específico. No entanto, não se espera que o operador vá além de suas responsabilidades para atender ou facilitar pedidos de titulares que não estejam relacionados à sua área de atuação."

"615490": "O art. 19 da LGPD estabelece que sua aplicação abrange não apenas o acesso aos dados, mas também a confirmação da realização de

seu tratamento. Em casos estritamente relacionados à confirmação da existência de tratamento, a resposta deve limitar-se a simples "sim" ou "não". O direito de acesso a dados, porém, prevê o efetivo fornecimento de informações tratadas, em atenção a pedido de titular. Em relação ao fornecimento rápido de dados, mesmo que de modo resumido, deve-se considerar aqueles que já estão prontamente organizados para serem acessados externamente ou que possam ser imediatamente disponibilizados para exportação. O exercício do Direito de Acesso no âmbito da LGPD, contudo, diz respeito exclusivamente à cognição de informações por parte do requerente do acesso. Por isso, tal direito não se confunde com o Direito de Certidão – garantia estipulada no artigo 5º, inciso XXXIV, da CF/88. As atividades de serventias têm como desígnio a manutenção de registros de informações socialmente relevantes, para sua disponibilização à sociedade civil ou a agentes governamentais. Assim, as certidões têm o condão não somente de dar conhecimento do teor de determinadas informações, mas precipuamente o de atestar a existência de fatos social e juridicamente relevantes; noutras palavras, para além de dar-se ciência, certidões atestam a existência e garantem a fidedignidade dos dados a si correspondentes ao serem dotados de fé-pública. Nesse sentido dispõe o artigo 98 do Provimento CNJ 149/2023, o qual confirma a gratuidade do direito de acesso aos titulares de dados nos termos da LGPD, mas explicita a diferenciação entre direito de acesso e de certidão, prevendo-se explicitamente no §1º que os documentos e direitos não se confundem.", "615494": "Se o termo "informações mínimas sobre tratamentos a serem divulgadas sem solicitação prévia" referir-se aos Avisos de Privacidade, estes devem contemplar elementos essenciais como: a identificação dos responsáveis pelo tratamento de dados, as categorias de dados pessoais processados, os propósitos específicos do tratamento, os indivíduos impactados, e a fundamentação legal para o processamento de cada categoria de dados pessoais. Além disso, é preciso esclarecer os métodos de coleta e armazenamento dos dados pessoais, bem como os possíveis destinatários com quem esses dados podem ser compartilhados. É crucial também detalhar as medidas adotadas para a proteção dos dados pessoais tratados e os procedimentos para sua eliminação após o alcance dos objetivos de coleta. Adicionalmente, o Aviso de Privacidade deve abordar os critérios aplicados nas decisões automatizadas, alinhados aos propósitos de tratamento de dados explicitados. É importante destacar que as decisões automatizadas variam conforme o contexto, como no setor da saúde em comparação com o direcionamento de conteúdo, implicando em diferentes critérios e procedimentos para cada tipo de decisão automatizada. Portanto, os detalhes e especificidades a serem comunicados ao titular dos dados por meio do aviso de privacidade devem refletir essas variações.", "615493": "O cumprimento do direito de acesso a dados pessoais, quando solicitado por um titular, está relacionado ao conteúdo fornecido ao solicitante, tendo o titular a liberdade de escolher entre as alternativas disponíveis, seja em formato digital ou impresso. A escolha do formato pelo titular não afeta a satisfação do direito de acesso, contanto que os dados solicitados sejam devidamente disponibilizados para seu conhecimento. Destaque-se vez mais, contudo, que a satisfação desse direito de acesso não se confunde com as atividades, notariais e registrais, de emissão de certidões. Conforme acima detalhado e nos termos do Provimento CNJ 149/2023, para além do fornecimento de informações (produto do exercício do direito de acesso), a emissão de Certidões por parte de serventias tem o condão de atestar a existência e garantir a fidedignidade dos dados em si constantes, em decorrência de serem dotados de fé-pública.", "615502": "A avaliação da capacidade dos agentes de tratamento para implementar o direito à portabilidade dos dados deve ser realizada em colaboração com os respectivos agentes, considerando seus processos e a natureza de seus negócios. Há casos, contudo, em que fatores

externos limitam a portabilidade de dados. Por exemplo, sobre serventias judiciais de cartórios de registro incide o Princípio da Territorialidade. Em síntese, tal característica implica que cada a cartório haja atribuição da circunscrição de sua competência; em outras palavras, cartórios de registro têm competência e base territorial delimitada. A segmentação territorial, assim, é fator que implica restrições à possibilidade de exercício da portabilidade entre agentes de tratamento. Há, naturalmente, informações uniformes e de utilização múltipla que podem, eventualmente, ser utilizadas em ocasiões diversas, tais quais, por exemplo, informações de registro civil ou a emissão de procurações. Além disso, a interconexão entre as serventias por meio de interoperabilidade pode auxiliar na utilização eficiente de dados pessoais sem que isso implique portabilidade da dados em sentido estrito. ","615501": "N/A","615505": "A realização efetiva do direito à portabilidade dos dados exige a interoperabilidade, permitindo que os dados tratados em uma aplicação possam ser utilizados de maneira equivalente em outra. Essa necessidade implica em uma certa uniformização das práticas entre agentes de um mesmo setor ou mercado, especialmente em relação ao formato dos arquivos usados para a transferência de dados. No âmbito das serventias extrajudiciais, existe uniformidade no registro e fluxo de suas informações que é garantida a partir dos sistemas eletrônicos envolvidos em suas atividades. O Sistema de Registro Eletrônico de Imóveis (SREI) garante a interconexão entre as serventias a partir da interoperabilidade da base de dados de cada Serventia. O SREI permite que haja o fluxo de documentos, títulos e certidões em formato eletrônico entre as unidades de registro de imóveis para atendimento aos usuários, garantindo o compartilhamento uniforme e eficiente dos registros em âmbito nacional. A prestação do serviço é apoiada pelo Serviço de Atendimento Eletrônico Compartilhado (SAEC) que garante o atendimento remoto dos usuários para qualquer serventia extrajudicial a partir do recebimento de solicitações e distribuição às serventias correspondentes. Por seu turno, as próprias serventias extrajudiciais garantem a atualização do registro imobiliário eletrônico por meio de anotação em matrícula eletrônica da situação jurídica do imóvel após cada registro e averbação, além de existir o registro de eventos de suas operações internas. A matrícula eletrônica é estruturada de modo que seus dados podem ser extraídos de forma automatizada contendo seções relativas aos controles, atos e situações jurídica do imóvel. Essas informações são armazenadas e atualizadas a partir de especificações técnicas editas pelas Corregedoria Nacional de Justiça e pelas Corregedorias-Gerais de Justiça dos Estados. Portanto, nota-se que as serventias extrajudiciais possuem um regime próprio de operação e de guarda das informações contidas em seus registros e relativas ao desempenho de suas atividades. ","615503": "Independentemente da forma como os dados são fornecidos aos titulares, desde que o formato escolhido atenda aos requisitos mínimos necessários para permitir a portabilidade e a utilização eficaz dos dados pelo terceiro receptor, considera-se que o direito à portabilidade dos dados foi devidamente respeitado. ","615504": "Considerando as peculiaridades de cada setor em termos de práticas e padrões, existe a necessidade de esforços para alcançar a uniformização que facilitará a interoperabilidade efetiva. Portanto, é apropriado permitir que o setor privado estabeleça padrões que se alinhem às particularidades de suas atividades. No caso das serventias extrajudiciais de Registro de Imóveis, o Sistema Eletrônico de Registro (SREI) de imóveis possui um padrão próprio de interoperabilidade de acordo com a sistemática legal prevista no Provimento nº 89/2019 do CNJ. O Operador Nacional do SREI (ONR), entidade responsável por sua implementação e operação, apresenta instruções técnicas de normalização para propiciar a operação segura do sistema, a interoperabilidade de dados e documentos e a longevidade de arquivos eletrônicos – considerando os requisitos jurídicos-formais e a garantia de autenticidade e

segurança nas operações realizadas em seus serviços. Posteriormente, essas instruções técnicas são homologadas pelo CNJ adquirindo força vinculante perante as serventias extrajudiciais na utilização do sistema. Nesse sentido, o estabelecimento de padrões de interoperabilidade no âmbito de registro de imóveis possui uma disciplina própria que já incorpora as particularidades vinculadas ao setor com homologação técnico-normativa do órgão regulador. No esquema previsto, dentre outras competências, o ONR - entidade privada sem fins lucrativos – estabelece os padrões próprios para sua atividade. Neste sentido, estabeleceu o Next Cloud SAS – Serventia Avançada Segregada em conjunto com o Google Cloud Platform, por meio do qual cada serventia tem à disposição um ambiente dedicado, isolado e exclusivo para sincronizar e acomodar seus dados de forma a não concentrar quaisquer dados no ONR. Por meio do Next Cloud SAS, as serventias podem gerenciar e monitorar de maneira autônoma o acesso aos dados que controla, ficando a cargo de cada Oficial conceder, alterar ou revogar o acesso àqueles dados, inclusive em relação ao SAEC/ONR.";

"615511": "A avaliação de dados pessoais quanto à sua incompletude, inexatidão ou desatualização baseia-se na comparação com a realidade atual. Isso significa verificar se os dados refletem a situação concreta: se estão completos, acurados e atualizados. Para corrigir informações que apresentem esses problemas, o titular pode ser solicitado a fornecer provas. Enquanto informações básicas como nome, endereço e telefone são mais diretas e baseiam-se em fatos concretos, dados derivados de inferências exigem uma análise mais detalhada para identificar e corrigir possíveis imprecisões. Há, no entanto, hipóteses de alteração de dados no âmbito de serviços notariais que contam com procedimento e burocracia próprios para a sua efetivação. A alteração de nome é direito assegurado e de efetivação extrajudicial e imotivada àqueles que o queiram, nos termos do artigo 515-A e seguintes do Provimento 149/2023. As hipóteses de alteração de prenome ou sobrenome, contudo, a depender do procedimento específico, podem estar sujeitas a comprovação, consentimento, assinatura de termos ou outras formalidades, no sentido de mitigação de riscos potenciais derivados da alteração desse registro. O artigo 518, §6º do Provimento, por exemplo, prevê para os casos de retificação de prenome e gênero a apresentação de variados documentos por parte do requerente da alteração ou retificação, tais quais certidão de nascimento atualizada, cópia de documentos de identidade (como RG, CPF, passaporte e título de eleitor), comprovante de endereço e certidões de justiça. Logo, há a instituição de procedimento próprio que conta com burocracia que não é suprida por intermédio dos canais de comunicação derivados da legislação protetiva de dados, os quais devem ser observados para além da mera solicitação ou declaração de incompletude, inexatidão ou desatualização.";

"615514": "É comum que a correção de dados pessoais exija que o titular forneça evidências da imprecisão. Contudo, a exigência de provas não deve ser aplicada em situações em que isso resulte em desproporcionalidade ou inviabilidade, como nos casos em que o documento necessário para comprovar a incorreção esteja retido pelo responsável pelo tratamento dos dados. Deve, ademais, ser feita consideração a regulações que digam respeito a retificações atípicas de dados e que, por sua especificidade, contam com normatização específica, em procedimento distinto que não se esgota na mera declaração do titular ou processos instituídos no âmbito da normatização protetiva de dados.";

"615513": "Em situações com um grande número de solicitações de correção, pode-se avaliar a transferência de informações atualizadas de forma periódica de um agente para outro que compartilhe os dados, ou fazê-lo por meio de um sistema compartilhado, sob demanda. Contudo, é importante notar que a responsabilidade de um agente se limita à notificação de correções a outros envolvidos; não se estende à verificação da execução efetiva dessas correções pelo terceiro. No âmbito do Registro de Imóveis,

o Sistema de Registro Eletrônico de Imóveis (SREI) é caracterizado pela interconexão descentralizada de todas as unidades do serviço de registro de imóveis. Isso significa que a base de dados de cada serventia permanece sob a guarda e conservação dos respectivos oficiais, mas que o sistema é integrado de modo que existe um fluxo facilitado de informações entre as serventias de registro de imóvel em âmbito nacional onde cada serventia mantém a autonomia sobre seus registros e informações. É neste sentido que funciona o Next Cloud SAS – Serventia Avançada Segregada, desenvolvida pelo ONR em conjunto com o Google Cloud Platform e hospedado em território nacional. Com o Next Cloud SAS, cada serventia tem à disposição um ambiente dedicado, isolado e exclusivo para sincronizar e acomodar seus dados de forma a não concentrar quaisquer dados no ONR. Por meio do Next Cloud SAS, as serventias podem gerenciar e monitorar de maneira autônoma o acesso aos dados que controla, ficando a cargo de cada Oficial conceder, alterar ou revogar o acesso àqueles dados, inclusive em relação ao SAEC/ONR. De aproximadamente 3600 serventias, cerca de 2400 já adotam atualmente este sistema de nuvem.

615512: "Sim, existem situações em que, se o titular dos dados não consegue fornecer provas suficientes para demonstrar a incorreção dos dados, sua solicitação de correção pode não ser atendida. Há, ainda, casos em que a correção dos dados é efetuada, mas nas quais os registros anteriores são preservados para manutenção de histórico de alterações, fenômeno que, dentre os tipos de correção, tende a ser mais frequentemente observado em relação àqueles dados desatualizados – relativamente aos quais há maior chance de justificar-se a manutenção do histórico. Destaque-se, no entanto, que a manutenção de histórico não é sinônimo de sua divulgação. A alteração de prenome e gênero de pessoas trans é, nos termos do artigo 519 do Provimento CNJ 149/2023, procedimento de natureza sigilosa, cujo teor não pode constar em certidões. Exceção à publicização dessa informação é estabelecida no âmbito desse mesmo artigo 519, de acordo com o qual a alteração relevante poderá fazer-se constar em certidões mediante solicitação da pessoa requerente ou por determinação judicial nesse sentido. Em inferência lógica, portanto, a manutenção de registros de histórico de informações que foram objeto de alteração é obrigação regulatória ao considerar-se a possibilidade de exigir-se que o teor de certidões disponha sobre todo o conteúdo registral, mas não implica sua divulgação ou acessibilidade, exceto em hipóteses muito restritas. Em assim sendo, a manutenção de históricos não implica, necessariamente, na divulgação dessas informações. A disponibilidade da informação corrigida dependerá do procedimento particular aplicado àquele caso.

615517: "Considerado o tipo de tratamento de dados realizado em uma serventia extrajudicial, é improvável que o tratamento de dados pessoais esteja baseado em outra justificativa que não o cumprimento de obrigação legal ou regulatória. Ainda assim, caso o titular deseje questionar a forma como este tratamento é realizado, é possível endereçá-lo à serventia ou à Autoridade Nacional, nos termos da Lei. Nas atividades de tratamento de dados executadas pelas serventias extrajudiciais, a retenção de registros é uma exigência legal ligada ao desempenho e à execução de suas funções específicas, cujo objetivo é aquele de documentar atividades realizadas na sociedade. Portanto, os dados mantidos por esses agentes são processados com base no cumprimento de obrigações legais. No mesmo sentido, também em estrito cumprimento de obrigações regulatórias pode haver o impedimento da eliminação de dados, como a imperatividade de preservação de informações, ainda que desatualizadas. Ainda que em consideração à condução das atividades corriqueiras em serventias, a própria razão de ser de agentes registrais e notariais implica obstrução lógica à possibilidade de eliminação das informações que estão sujeitas a seu tratamento. Logo, apesar da possibilidade de requerimento de eliminação de dados, no âmbito de serviços notariais e registrais,

em consideração ao cumprimento de obrigações legais nesse sentido e devido à própria natureza de serventias, geralmente não poderá haver a deleção de informações. ";615516": "A eliminação de dados refere-se ao processo de desvinculação de uma pessoa das suas informações pessoais. Esse procedimento assegura que o titular deixa de estar associado a quaisquer dados que possam identificá-lo direta ou indiretamente. Isso pode ser alcançado, por exemplo, removendo informações identificadoras específicas do indivíduo, como nome, endereço, fotografia, documentos, entre outros, além de separar do titular quaisquer dados que, embora não identificadores por si só, estavam ligados a ele. Contudo, em regra, conforme anteriormente aludido (vide itens 4.d e 5.a acima), em regra não é possível que serventias extrajudiciais atendam a este tipo de pedido. Tanto por sua natureza, quanto em razão da base legal que justifica o tratamento de dados pessoais implicar a necessidade de manutenção dos dados tratados, há usualmente a imperatividade de manutenção de registros sobre dados tratados por parte de agentes notariais. ";615518": "Ao interagir diretamente com o agente responsável pelo tratamento, se uma objeção ao processamento dos dados for considerada legítima, o procedimento deve ser ajustado para estar em conformidade com a LGPD. No entanto, deve-se levar em conta que essa contestação pode também ser apresentada à Autoridade Nacional de Proteção de Dados (ANPD). Nesse caso, as medidas a serem tomadas serão estabelecidas pela ANPD, de acordo com sua própria regulamentação. Especificamente no tocante às atividades notariais e registrais, porquanto a base legal de seu tratamento é majoritariamente o cumprimento de obrigações legais e regulatórias, tais operações de tratamento preponderantemente não poderão ser legítimo objeto de objeção por parte do titular de dados pessoais (vide, nesse sentido, itens 4.d, 5.a e 5.b acima).";615523": "A eliminação de dados processados com base no consentimento, após sua revogação, está sujeita a eventuais obrigações legais de retenção de dados. Se existirem normas setoriais que exijam a conservação de registros, ou se houver razões válidas para manter um histórico de dados, a retirada do consentimento pode não resultar na eliminação dos dados. Portanto, é importante considerar qualquer obrigação legal ou regulatória que exija a preservação de registros históricos, o que pode servir de justificativa para não apagar os dados coletados com base no consentimento. Em contextos como o cartorial e registral, a retenção de registros é uma exigência legal ligada ao desempenho e à execução de suas funções específicas. O objetivo desses registros é documentar atividades realizadas na sociedade, abrangendo áreas como a civil, a imobiliária e a comercial. Assim, os dados mantidos por esses agentes são processados com base no cumprimento de obrigações legais, conforme estabelecido no artigo 7, inciso II, da LGPD (ou, no caso de dados sensíveis, no artigo 11, inciso II, 'a'). Em outras palavras, a base legal que permite a condução de operações de tratamento por parte de agentes notariais é preponderantemente vinculada ao cumprimento de obrigações regulatórias, não havendo, em regra, o tratamento vinculado ao consentimento. O consentimento, por sua vez, se refere a uma base legal diferente para o processamento de dados, conforme o inciso I do mesmo artigo (ou artigo 11, inciso I). Portanto, o direito dos titulares de revogar o consentimento não se aplica a dados tratados em estrita observância a uma obrigação legal a qual o agente de tratamento está submetido. Em outras palavras, a obrigação de eliminar dados não se estende a situações que envolvem o cumprimento de deveres legais.";615521": "A revogação do consentimento torna-se efetiva imediatamente após ser manifestada, não afetando os tratamentos de dados já realizados, mas limitando qualquer processamento futuro dessas informações. Portanto, ações que foram concluídas anteriormente – como regra geral – não necessitam ser reconsideradas, sendo suficiente para o agente de tratamento assegurar a não continuação do uso das informações. Consequentemente, os

efeitos da revogação de consentimento incidem apenas sobre os dados processados após essa revogação, não exercendo efeito retroativo. A revogação de consentimento e o pedido de exclusão de dados são direitos independentes, permitindo que o titular dos dados possa revogar o consentimento sem necessariamente solicitar a exclusão dos dados. No entanto, um pedido de exclusão geralmente implica a cessação do tratamento dos dados, o que muitas vezes leva a que ambos os pedidos sejam feitos em conjunto. Quanto às atividades de serventias, conforme mencionado, sua essência reside na conservação de registros de informações de interesse social para a disponibilização ao público e a órgãos governamentais. Isso exige a preservação de um acervo que reúna esses dados, responsabilidade que recai sobre agentes notariais e registrais em conformidade com obrigações legais específicas. Levando em conta o papel público exercido por parte desses agentes, a solicitação de exclusão de dados por eles processados não somente se mostra logicamente incompatível com suas funções essenciais, mas também pode contrariar explicitamente disposições legais que determinam a manutenção, e não a eliminação, dessas informações."

615617": "Para distinguir entre "decisão automatizada" e "decisão com base em tratamento automatizado", é essencial entender a aplicação do termo 'automatizado'. Decisões automatizadas referem-se ao processo decisório em si sendo automatizado, como por exemplo, decisões tomadas por algoritmos sem intervenção humana. Por outro lado, decisões baseadas em tratamento automatizado implicam que a automação ocorre no processo de coleta e análise de dados que suportam a decisão, mas a decisão final pode ou não ser automatizada. Esses conceitos não são mutuamente excludentes e podem co-existir, destacando que a automação pode afetar tanto o processo de tomada de decisão quanto o tratamento de dados que o fundamenta."

615618": "Quando uma decisão automatizada resulta na limitação de direitos, teoricamente, há uma influência sobre interesses decorrente dessa decisão. A Lei Geral de Proteção de Dados (LGPD), especificamente em seu artigo 20, aponta que tal influência deve ser relacionada ao perfil pessoal, profissional, de consumo, de crédito do titular, ou a características da sua personalidade. Isso indica que essas áreas, embora não sejam as únicas possíveis, orientam quais interesses impactados podem ser protegidos sob as disposições desse artigo."

615619": "Potenciais dificuldades na divulgação de critérios para revisão de decisões automatizadas incluem a complexidade crescente de sistemas algorítmicos, tornando o entendimento completo desses sistemas um desafio tanto para técnicos quanto para os titulares dos dados. A complexidade aumenta com o tamanho e a abrangência da operação, dificultando a compreensão plena do processo decisório automatizado. Adicionalmente, o valor comercial dos sistemas algorítmicos representa outro obstáculo à implementação do direito de revisão. O artigo 20 da LGPD menciona decisões automatizadas com o objetivo de definir perfis pessoais, profissionais, de consumo, crédito ou traços de personalidade, elementos fundamentais para a direção de conteúdo publicitário e otimização de conversão, por exemplo em plataformas digitais. Essas plataformas, cujo lucro está intimamente ligado à publicidade, atribuem um valor comercial significativo aos sistemas algorítmicos. As informações sobre esses sistemas, incluindo seu funcionamento, são consideradas segredos comerciais, valorizados pela confidencialidade e protegidos para manter a vantagem competitiva."

615620": "A importância de tratar os algoritmos decisórios como segredos comerciais está mais relacionada à capacidade de explicar os procedimentos utilizados do que à revisão de decisões decorrentes desses procedimentos. Teoricamente, é possível revisar decisões sem revelar informações confidenciais, indicando que a recusa em detalhar o funcionamento dos mecanismos não impede necessariamente o direito à revisão das decisões."

{ "615450": "CONEXIS BRASIL DIGITAL: O artigo 11 da Lei nº 12.527/2011 prevê que o acesso às informações solicitadas deve ser atendido de forma imediata, e, caso não seja possível atender ao prazo, o órgão ou entidade que receber o pedido deverá, em até 20 dias, conduzir a resposta (§1º). Ainda, o prazo pode ser prorrogado por mais 10 dias, mediante justificativa expressa, da qual será cientificado o requerente (§2º). Nesse viés, pode haver uma variação do conceito de prazo razoável para atendimento, de acordo com o tipo de direito requerido pelo titular. O acesso “imediato” traz uma subjetividade de entendimento, podendo ser interpretado de diferentes formas pelos agentes de tratamento e, sobretudo, pelos titulares, causando insegurança jurídica e desconfortos desnecessários para ambos. Ademais, a solicitação deve ser realizada através dos canais/ferramentas oficiais disponibilizados pela organização. No contexto do setor privado, em que os direitos dos titulares de dados pessoais serão predominantemente solicitados por meio de plataformas online, é essencial considerar o volume de solicitações que as organizações podem receber, bem como suas capacidades e estruturas para gerenciar essas solicitações. Nesse sentido, entendemos que seria possível o atendimento dos direitos de acesso e confirmação sobre tratamento de dados pessoais em prazo razoável, mas não imediato, que desde logo sugerimos 30 dias úteis. Para quando a requisição apresentar um grau de complexibilidade maior, o prazo de até dois meses poderá ser o mais adequado, em consonância com o que dispõe o Art. 12, itens 1 e 3 do GDPR. Por fim, o prazo para atendimento às solicitações ainda deverá começar a contar após confirmação de identidade do titular, com a finalidade de assegurar que as informações serão enviadas ao detentor dos dados pessoais, ou seja, ao próprio titular. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "CONEXIS BRASIL DIGITAL: Considerando o nível de complexidade sistêmica, o investimento de recursos pelo Controlador, o tipo de solicitação, o volume de dados envolvidos, a necessidade de comunicação com terceiros, os pedidos múltiplos, bem como as etapas operacionais para a) validação da identidade de titulares de dados; b) formatação da resposta à solicitação de acesso pelo titular, é preciso cautela na interpretação do inciso I do art. 19 da LGPD. Em primeiro lugar é importante recordar que o caput do art. 19 menciona dois direitos distintos, são eles: 1) confirmação da existência e 2) acesso aos dados pessoais. Muito embora a redação do artigo seja um tanto confusa, não nos parece distante da realidade interpretar que o art. 19, I se refira ao direito de “confirmação de existência do tratamento de dados pessoais” e o inciso II; ao direito de acesso. E isso se deve muito à expressão “imediatamente”, a qual, pelos pontos trazidos nessa manifestação, é praticamente impossível de se operacionalizar. Nessa senda, boa prática seria entender que a disponibilização imediata do direito à confirmação de existência seria suprida desde a publicação de “avisos de Privacidade” íntegros e aderentes aos ditames do art. 9º da LGPD, ao passo que ao disponibilizar informações como dados pessoais tratados, finalidades e categorias de titulares de dados já se tornaria possível inferir pela confirmação (ou não) do tratamento de dados de determinado titular (de maneira imediata, como preconiza o art. 19, II) Por outro lado, caso seja a intenção o recebimento da cópia dos dados pessoais que eventualmente sejam tratados pelo agente de tratamento, agora sim, estaríamos à luz do art. 19, II, prevendo-se tempo hábil para resposta segura (vide o encargo de autenticação da identidade do titular) e completa (vide as questões prático-operacionais para localização de dados, formatação de resposta e retorno efetivo ao titular de dados). ", "615484": "CONEXIS BRASIL DIGITAL: sem contribuições.", "615485": "CONEXIS BRASIL

DIGITAL: Primeiramente, é preciso destacar que todos os operadores, pelo menos no que se refere ao seu quadro de colaboradores, serão controladores em algum tratamento de dados realizado. Nesse sentido, entende-se que todos os agentes de tratamento devem possuir canal de atendimento de direitos operante. Adicionalmente, ressalta-se que o operador, enquanto agente de tratamento subordinado aos comandos do controlador, pode vir a auxiliá-lo no cumprimento de suas obrigações, inclusive no atendimento aos direitos dos titulares. A maneira como essa cooperação ocorrerá, no entanto, depende de fatores como (i) o contexto do tratamento, (ii) o tipo de atividade exercida pelo operador e (iii) dos protocolos definidos entre as Partes. Nesse âmbito, a principal responsabilidade que destacamos se refere aos casos em que os titulares realizem a requisição de direitos ao operador, nos quais deverá competir ao mesmo a responsabilidade de informar ao controlador a solicitação que foi realizada, sendo vedada qualquer atendimento das solicitações sem qualquer autorização prévia do controlador. Ademais, de forma geral, para viabilizar o efetivo atendimento dos direitos dos titulares, entendemos ser possível atribuir ao operador as responsabilidades de fornecer as informações solicitadas pelo controlador, informar o controlador sobre suspeita e/ou ocorrência de incidente de segurança e atualizar, corrigir, anonimizar e eliminar dados pessoais, caso haja instrução expressa do controlador nesse sentido. Entretanto, considerando a existência de diferentes cenários, é necessário que não haja restrição a condutas específicas, de modo que a via contratual e os demais protocolos entre as partes sejam capazes endereçar, não apenas as particularidades de cada contexto, mas também as próprias decisões do Controlador a fim de melhor atender aos direitos dos titulares. ""615486"":CONEXIS BRASIL DIGITAL: Por tratar de tema específico, o canal de atendimento aos direitos dos titulares demanda a tratativa por profissionais especializados no tema, o que não ocorre no atendimento feito pelo SAC. Apesar do SAC possuir procedimentos e diretrizes familiares para os consumidores e organizações, não entendemos que esses sejam adequados para o exercício de direitos dos titulares. Ao contrário do pretendido pela Autoridade, o efeito de tal medida pode esvaziar o atendimento aos titulares, a medida em que, na tentativa de massificar os atendimentos, esses não serão mais realizados por equipe especializadas, mas sim por operadores generalistas. O decreto estabelece normas sobre o serviço de atendimento ao consumidor (SAC) e traz uma série de determinações que exigiriam a implantação de um atendimento com características de uma célula de atendimento especializada (demandando estrutura e custos), como: a) Art. 3º. § 2º: O atendimento por telefone trará ônus demasiado aos agentes de tratamento e fortalecerá a confusão que já ocorre hoje, entre o atendimento do SAC e aos direitos dos titulares; b) Art.3º, § 4º: Na grande maioria dos atendimentos aos direitos dos titulares, é imprescindível o fornecimento de dados pessoais pelo titular para que seja possível identificá-lo e, assim, prosseguir com a internalização; c) Art. 4º e Art. 5º: a exigência de múltiplos canais e atendimento contínuo pode ser impraticável devido à complexidade e custos de segurança para proteção de dados; d) Art. 12: Pela sua especificidade, o acompanhamento acerca dos direitos dos titulares deve ser feito única e exclusivamente no canal próprio sobre o tema, sob o risco de não atender as possíveis dúvidas; e) Art. 13: Os prazos estabelecidos pela legislação de SAC são exíguos e não são adequados para lidar com as requisições previstas pela LGPD, que são mais complexas e, em diversas situações, exigem mais tempo para serem atendidas; f) Art. 14: art. 14: Os direitos garantidos pela LGPD dizem respeito aos dados pessoais dos titulares e não são o foco dos serviços prestados.""615487"":CONEXIS BRASIL DIGITAL: Não. Como forma de otimizar o atendimento aos direitos dos titulares, especialmente o direito de acesso, alguns agentes de tratamento podem desenvolver um ambiente em que o titular, por meio de login e senha,

consegue acessar os dados pessoais tratados pelo controlador de forma imediata. Contudo, nem todos os direitos previstos na LGPD podem ser atendidos de maneira automatizada, bem como nem todos os agentes podem usufruir desse meio, motivo pelo qual, o controlador pode optar por atendê-los de outra forma. Assim, é necessário que a ANPD, com o intuito de verificar as práticas comumente adotadas, não priorize uma forma em detrimento de outras, mas realize estudo com o objetivo de apresentar uma gama de possibilidades de atendimento, considerando o que já é feito no mercado e, principalmente, fatores como volume de dados, tipo de tratamento e porte dos agentes. Ademais, é importante que haja autonomia para as organizações definirem o formato mais adequado às suas necessidades e realidade para atendimento dos titulares, considerando a diversidade de características relacionadas à estrutura e aos processos de cada empresa.

;"615491": "CONEXIS BRASIL DIGITAL: A fim de que seja dada maior segurança jurídica a determinadas operações e de reduzir eventuais atritos junto aos titulares de dados pessoais, as limitações a serem estipuladas não importam em afronta aos direitos e liberdades fundamentais dos titulares, mas sim evitará o não atendimento por parte dos agentes de maneira desarrazoada. Nesse sentido, a confirmação da existência do tratamento pode ser negada em algumas situações excepcionais, como: a) Confirmação de identidade: quando não restar comprovado, por meio de documentos válidos, a identidade do titular; b) Sigilo profissional: Quando a confirmação da existência do tratamento de dados pessoais revelar algum segredo de negócio da empresa; c) Atividades de Supervisão: em atividades como auditorias e investigações, é possível que a confirmação do tratamento possa prejudicar o êxito dos trabalhos. d) Sigilo profissional: profissionais como médicos e advogados, possuem o dever de sigilo profissional e, nesse sentido, podem não conseguir atender ao direito de confirmação, sob o risco de infração de outras determinações legais. e) Proteção de direitos e liberdades de outros titulares de dados pessoais: há hipóteses de solicitação que podem afetar dados de outros titulares e, por conseguinte, o atendimento a esse direito pode ser limitado. Como exemplo, uma limitação no atendimento para defender os direitos e as liberdades de terceiro através de um inquérito administrativo e/ou processo disciplinar ou investigação de alegações de assédio no local de trabalho. f) Solicitação irrazoável: é razoável que seja considerado a definição de limites, como aqueles previstos no Art 12, item 5, do GDPR, que dispõe sobre quando os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos. Assim, o responsável pelo tratamento pode: i) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou ii) Recusar-se a dar seguimento ao pedido.

;"615492": "CONEXIS BRASIL DIGITAL: Considerando que as informações a serem disponibilizadas pelos agentes de tratamento visam oportunizar ao titular o exercício de seus direitos e o acesso a informações sobre eventual tratamento de dados pessoais realizado, a disponibilização desse tipo de conteúdo nos sites institucionais pode ser adequada, na medida em que esses apresentam a empresa, seus propósitos e metas. No entanto, a informação direta dos controladores, um a um, torna-se inviável, uma vez que representa um esforço desproporcional e possível violação ao segredo industrial e comercial da organização. Nesse sentido, é informação relevante a ser fornecida aos titulares: Compartilhamento de dados: a indicação do setor empresarial em que o compartilhamento é realizado, com a respectiva finalidade e as categorias de terceiros com quem realizou o compartilhamento do dado pessoa, deve ser considerada suficiente para que o princípio da transparência seja cumprido. Isso se justifica pois o excesso de detalhamento em relação as informações prestadas podem gerar efeito contrário ao esperado, além da exposição de dados comercialmente estratégicos, tutelados pelos

segredos comercial e industrial. À vista do exposto, conclui-se ser possível atender ao direito previsto e, ao mesmo tempo, resguardar os demais pontos críticos por meio da indicação das categorias de empresas que podem receber dados e as respectivas finalidades. Por fim, a fim de dirimir quaisquer dúvidas, o atendimento a esse direito a partir da divulgação das categorias das empresas não importa em falta de controle sobre quais são os agentes com os quais o controlador compartilha dados, isso porque essa governança pode ser realizada a partir de outros instrumentos, como o ROPA. ","615489": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615490": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615494": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615493": "CONEXIS BRASIL DIGITAL: Sim. É preciso destacar que, especificamente no direito de acesso, não há qualquer obrigação legal de fornecimento de dados de maneira que esses sejam interoperáveis. É preciso levar em consideração, ainda, que o atendimento ao referido direito de forma diversa que não em formato digital pode implicar custos desproporcionais aos agentes de tratamento, a depender do volume de solicitações recebidas. Assim, a fim de garantir proporcionalidade, entende-se que o formato de atendimento ao direito deve ser correspondente à sua coleta, ou seja, apenas deveria ser recomendado a disponibilização em papel, por exemplo, caso a coleta dos dados seja feita de mesmo modo. ","615502": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615501": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615505": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615503": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615504": "CONEXIS BRASIL DIGITAL: sem contribuições."; "615511": "CONEXIS BRASIL DIGITAL: Os critérios objetivos que podem ser considerados são: 1) Dados incompletos: - ausência de informações essenciais; - falta de elementos de identificação; - informações parciais ou fragmentadas; - inconsistência dos dados pessoais. Exemplo: dado de endereço sem a informação de CEP. Ou, ainda, número de telefone sem os quatro últimos dígitos. Cabe ressaltar que quando olhamos para dados incompletos, é fundamental termos atenção quanto ao cumprimento do princípio da minimização. Por exemplo: Em determinados casos, para aquela finalidade de tratamento, o controlador não necessitará do número da residência, apenas do nome da rua ou da cidade. Isso não significa que os dados pessoais estão incompletos, mas apenas que essas informações são irrelevantes para a finalidade de tratamento, sendo, portanto, dispensáveis. Agora um número de CPF ou RG que esteja faltando algum número, poderá ser considerado um dado pessoal incompleto, bem como quando é solicitado o nome completo e apenas consta no cadastro o primeiro nome. 2) Dados inexatos: Quando o dado pessoal constante no banco de dados do agente de tratamento não corresponde ao dado pessoal do titular, conforme documentos comprobatório - fontes de dados não confiáveis; - erros de processamento de dados. Exemplo: números invertidos ou letras trocadas. 3) Dados desatualizados: - informações antigas que já não correspondem mais à realidade; - obsoletos para a finalidade tratada. Exemplo: alterações de endereço, atualização de sobrenome. ","615514": "CONEXIS BRASIL DIGITAL: Como qualquer outro direito, aqueles exercidos pelo titular também não são absolutos. Assim, é preciso considerar os efeitos que a alteração indevida de um dado pessoal pode gerar tanto para o próprio titular ou para a prestação dos serviços. Dentre eles, podemos citar: a) Ausência de envio de documentação comprobatória de identidade ou negativa de participação de quaisquer etapas de verificação de identidade, bem como apresentação de evidência que comprove a veracidade do "novo" dado pessoal corrigido. Nesse caso, esses procedimentos visam garantir a segurança dos dados pessoais e autodeterminação do titular e, por esse motivo, não seria factível atender o direito sem, antes, confirmar a titularidade do solicitante. Ademais, tendo em vista o cenário brasileiro de fraudes, a correção de dados sem comprovação da veracidade daquela

informação, pode ocasionar prejuízos não só aos agentes de tratamento, mas aos titulares e a sociedade no geral; e b) Impossibilidade de alteração de determinados dados, os quais costumeiramente são utilizados como chave de identificação única dos titulares, como código de cliente ou número de contrato, por exemplo. ";615513": "CONEXIS BRASIL DIGITAL: A "impossibilidade ou esforço desproporcional" se refere a situações em que seria excessivamente difícil, oneroso ou impraticável, informar aos agentes de tratamento sobre a correção, eliminação, anonimização ou bloqueio dos dados compartilhados. Temos então que a aplicação desse conceito é flexível, de modo que o rol a ser definido precisa ter caráter exemplificativo, ou seja, é possível que o controlador entenda como desproporcional determinado atendimento fora dos critérios trazidos, desde que realize a devida fundamentação. Entendemos que os critérios abaixo podem ser considerados para avaliar a impossibilidade ou o esforço desproporcional: a) Custos técnicos e financeiros necessários para atender à solicitação são significativamente altos em relação ao tamanho e aos recursos da organização; b) Volume e complexidade da solicitação: se estivermos diante de uma solicitação que envolva vários agentes de tratamento, o atendimento à solicitação impactaria de forma significativa as operações cotidianas da organização; c) Impacto nas operações do controlador: tendo em vista o potencial de solicitações de direitos dos titulares e a multiplicidade de agentes com os quais os dados podem ser compartilhados na atual economia data driven, o atendimento à solicitação impactaria de forma significativa as operações cotidianas da organização; d) Solicitações repetidas pelo mesmo titular ou solicitações em massa que impõem uma carga administrativa desproporcional. Adicionalmente, é imperioso destacar que todos os critérios acima ficam ainda mais pungentes quando verificamos que a determinação prevista no art. 18, § 6º requer cumprimento imediato o que, além de extremamente difícil na prática, ainda traz a insegurança jurídica no que tange a sua aferição. Por fim, deve-se lembrar que a grande maioria dos tratamentos realizados pelos agentes de tratamento atualmente (muitas vezes o core do negócio) tiveram a sua concepção muito antes do advento da LGPD. Assim, estruturar um fluxo comunicacional nesses casos pode gerar impacto demasiado aos controladores. ";615512": "CONEXIS BRASIL DIGITAL: Assim como pontuado na questão IV.b, como qualquer outro direito, aqueles exercidos pelo titular também não são absolutos. Assim, a princípio é preciso ter como premissa a impossibilidade nos casos em que a correção pode implicar em feitos significativos, como para o próprio titular ou para a prestação dos serviços. Dentre eles, podemos citar: a) Ausência de envio de documentação comprobatória de identidade ou negativa de participação de quaisquer etapas de verificação de identidade. Nesse caso, esses procedimentos visam garantir a segurança dos dados pessoais e autodeterminação do titular e, por esse motivo, não seria factível atender o direito sem, antes, confirmar a titularidade do solicitante; b) Impossibilidade de alteração de determinados dados, os quais costumeiramente são utilizados como chave de identificação única dos titulares, como código de cliente ou número de contrato, por exemplo; c) Se a empresa considerar os dados tratados como "precisos/adequados", ou seja, se entender que não há necessidade de correção, pois as informações presentes nas bases do agente são as mesmas solicitados pelo titular; d) Em caso de necessidades de manutenção para fins de histórico; e) Se a solicitação for considerada manifestamente infundada ou excessiva; f) Nas solicitações em nome de terceiro, se verificada a ausência de comprovação dos poderes de representação. ";615517": "CONEXIS BRASIL DIGITAL: Sim, o titular deve fornecer contexto ou justificativa que fundamente seu pedido no momento da requisição, demonstrando a falta de necessidade de retenção dos seus dados, visando evitar pedidos frívolos, repetitivos ou injustificados, garantindo que os direitos dos titulares sejam exercidos de forma legítima e

em conformidade com a lei. Ao contrário do que se possa afirmar, a necessidade de fundamentação por parte do titular não significa qualquer tipo de barreira ao exercício de seus direitos, mas sim uma etapa fundamental, a qual auxiliará o agente de tratamento: i. No entendimento da percepção do titular; ii. Na elaboração do retorno mais claro e adequado, a depender do contexto relatado pelo solicitante; iii. Na avaliação da pertinência da solicitação. Em sendo o caso de ser pertinente, a fundamentação auxiliará o agente adotar as medidas técnicas adequadas para a remediação. iv. a evitar excessiva onerosidade ao controlador, ao atender solicitações de titulares que atuam de forma desconexa, excessiva e, por vezes, com possível má-fé. Assim, é extremamente relevante que seja comprovada a alegação de que os dados pessoais estão sendo tratados de forma desnecessária, excessiva ou em desconformidade com a Lei, assegurando ao agente de tratamento o direito de resposta quanto ao alegado. Entendemos, ainda, que em pedidos manuais repetitivos do titular em que o controlador já apresentou resposta fundamentada, os controladores estejam dispensados de nova resposta. Vale fazer a ressalva de que essa fundamentação não se traduz, necessariamente, na comprovação da ilegalidade, mas sim em sua demonstração/indicação, para que, desse modo, o Controlador possa responder a contento e a própria ANPD compreenda melhor a demanda, caso venha a ser notificada. É importante que a avaliação seja exclusiva do controlador, na medida em que ele é quem define o contexto do tratamento de dados em uma operação interna. ","615516": "CONEXIS BRASIL DIGITAL: Sim. Os dados anonimizados estão fora do escopo de incidência da LGPD, de acordo com seu art.16. Desse modo, a anonimização e a eliminação surtiriam os mesmos efeitos, na medida em que em ambas as operações perde-se a possibilidade de identificação dos titulares. A depender das finalidades de tratamento dos dados pessoais, em determinados casos poderá o controlador optar pela anonimização ao invés da eliminação, quando ainda que não seja mais passível a identificação daquele titular, a organização consiga ainda utilizar aqueles dados (que não mais considerados pessoais após a anonimização) para prosseguimento dos negócios, fomentando, por exemplo, a inovação. ","615518": "CONEXIS BRASIL DIGITAL: O artigo 18, § 2º, da LGPD estabelece o direito de oposição do titular dos dados contra o tratamento realizado em descumprimento às disposições da própria lei. Se a alegação do titular for considerada legítima, ou seja, se ficar comprovado que o tratamento dos dados pessoais violou as disposições da LGPD, o efeito da oposição é que o controlador deve cessar o tratamento dos dados pessoais em questão. Essa cessação do tratamento pode incluir a interrupção da atividade de processamento de dados pessoais que esteja sendo realizada de forma contrária à LGPD, ou mesmo o tratamento do dado de forma anonimizada. Assim, nos cenários em que o titular conseguir expor os motivos pelo os quais entenda acerca da legalidade do tratamento e essa alegação for considerada legítima pelo agente de tratamento, ou seja, se o tratamento, de fato, vier de encontro ao disposto no Aviso de Privacidade ou em sua Política de Privacidade, deverá o agente cessar tratamento de dados em foco e avaliar acerca da possibilidade de exclusão do dado caso esse não seja utilizado para nenhuma outra finalidade que justifique a sua manutenção. No entanto, mesmo diante da possibilidade de que a oposição legítima estaria fundada em tratamento de dados em descumprimento da LGPD, isso não deveria, por si só, configurar infração para fins de aplicação de sanções administrativas perante a ANPD. Isso porque o nível de exigência, comprovação e apuração deve ser mais elevado, devendo ser respeitado o trâmite de apuração da ocorrência garantindo a ampla defesa do agente de tratamento. ","615523": "CONEXIS BRASIL DIGITAL: Não necessariamente. Cada situação é única pois, embora os controladores tenham a obrigação de excluir os dados tratados com base no consentimento, a própria LGPD traz o direito de exclusão separado do direito de revogação.

A revogação do consentimento não implica na exclusão dos dados e não deverá prejudicar o tratamento executado com suporte em outras bases legais. Essa obrigação apenas ocorrerá nas hipóteses em que os dados forem utilizados exclusivamente para o contexto em que foram tratados via consentimento. É preciso destacar, todavia, que caso haja outros tratamentos, fundamentados em outras bases legais e em que essas informações estejam relacionadas, não há que se falar em obrigação de exclusão. Assim, conclui-se que, ao contrário do exposto pela ANPD no texto introdutório aos questionamentos, os dados podem ser mantidos pelo controlador, não apenas em caso de existência de outra hipótese legal, mas também nos casos em que haja outros tratamentos de dados pessoais. Esse ponto é de extrema relevância pois, na realidade prática dos agentes, há comum que um dado seja tratado para as mais diversas finalidades, tendo cada uma delas sua respectiva base legal. Vamos ao exemplo: se adotada a teoria de que um dado precisa ser apagado tão logo seja verificada a impossibilidade de aplicação de outra base legal, sem analisar se há outros tratamentos que utilizam a mesma informação, um titular, cliente de uma empresa prestadora de serviços de internet deseja retirar seu consentimento para o recebimento de newsletter, todos seus dados deveriam ser excluídos? Como se daria a continuidade da prestação de serviços? Portanto, para que os dados pessoais sejam eliminados após a revogação do consentimento, o titular dos dados deve fazer uma solicitação específica para a eliminação, conforme o art. 18, VI, da LGPD. "615521": "CONEXIS BRASIL DIGITAL: sem contribuições." "615617": "CONEXIS BRASIL DIGITAL: sem contribuições." "615618": "CONEXIS BRASIL DIGITAL: sem contribuições." "615619": "CONEXIS BRASIL DIGITAL: a) Opacidade algorítmica: há casos em que nem mesmo quem desenvolveu a inteligência é capaz de compreender, com amplitude, como determinados algoritmos operam. b) Explicabilidade: em razão de ser um tema extremamente técnico, os agentes de tratamento possuem o desafio de serem transparentes de maneira inteligível ao titular de dados. c) Segredo comercial e industrial: é imprescindível ponderar acerca do desafio de garantir a transparência e informações aos titulares sem que esse retorno afete o segredo de negócio e, até mesmo, a segurança dos dados dos próprios titulares; d) Complexa cadeia de atores de IA: o desenvolvimento de uma IA costumeiramente envolve uma intrincada cadeia de agentes, cada um responsável por etapas específicas de formação da tecnologia. Assim, a tarefa do Controlador em atender a solicitações do gênero envolverá todas as entreves expostas acima, multiplicadas pela variedade desses agentes; e) Acesso aos dados: para revisar uma decisão automatizada, pode ser necessário ter acesso aos dados utilizados no processo decisório. No entanto, o acesso a esses dados pode ser dificultado, especialmente se forem protegidos por medidas de segurança implementadas pelo controlador, em consonância com a própria LGPD e legislações correlatas; f) Recursos técnicos e financeiros: capacitar colaboradores competentes para a revisão de decisões automatizadas pode exigir investimentos significativos em recursos técnicos e financeiros desproporcionais à finalidade e efeitos da revisão; g) Prazos e procedimentos: estabelecer prazos e procedimentos claros para o exercício do direito de revisão pode ser um desafio, especialmente considerando que a complexidade do tratamento automatizado pode variar a depender do caso concreto; h) Segurança e integridade dos dados: garantir a segurança e a integridade dos dados durante o processo de revisão é fundamental para proteger a privacidade e os direitos dos titulares dos dados, o que pode exigir medidas adicionais de segurança e controle desproporcionais à finalidade e efeitos da revisão. "615620": "CONEXIS BRASIL DIGITAL: Sim, o controlador pode negar o direito de revisão sobre decisões automatizadas nas seguintes hipóteses: i. a revisão da decisão automatizada implica no comprometimento de segredo comercial e/ou industrial do controlador; ii. quando a revisão manual de decisões

automatizadas seja tecnicamente ou praticamente inviável devido à complexidade ou ao volume dos processos de decisão. iii. as decisões automatizadas não impactam de forma significativa os direitos do titular. Ainda, existe a possibilidade de fundamentação, pelo controlador, de que as decisões que foram tomadas com base em tratamento automatizado com intervenção humana determinante para o resultado não se enquadrariam estritamente na definição de decisões automatizadas. É imperioso ressaltar que a revisão não tem, por si só, o condão de alterar as decisões tomadas de maneira automatizadas, mas apenas de revisá-las a partir da indagação do titular. Tendo em vista que a grande maioria dos titulares não possui conhecimento técnico na área é necessário que a ANPD faça esse esclarecimento nos materiais e posicionamentos a respeito do tema. "

{“615450”: “A adoção do prazo previsto na LAI (concessão imediata à informação disponível ou, não sendo possível, que seja concedida no prazo de 20 dias, prorrogável por 10 dias, mediante justificativa expressa), pelo setor privado, para atendimento aos direitos do titular de dados pessoais na forma prevista pela Lei 13.709/18 (LGPD), mostra-se inviável. As disposições da LGPD impõem prazos e obrigações a entes privados com atuações e capacidades operacionais distintas – o que influencia na quantidade de solicitações a que poderão ser submetidos e no potencial de atendimento. Assim, a fixação de prazos deve considerar a heterogeneidade do setor privado, vez que, a depender do tipo de serviço que prestam, há atores que poderão ser submetidos a milhares – senão milhões – de requisições. Trata-se, portanto, de cenário distinto ao da LAI. Ademais, a imposição de um prazo imediato como o da LAI poderá ocasionar impactos financeiro-operacionais, inviabilizando a atividade de entes privados, além de dificultar o ingresso de novos atores no mercado, prejudicando a concorrência. Por tais razões, mostra-se mais adequada a adoção de prazo semelhante ao previsto no art. 14 do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, que confere prazo de pelo menos 30 dias para atendimento de solicitações de informações por titulares de dados, podendo ser prorrogado por dois meses, a depender da complexidade e quantidade de pedidos. Conforme entendimento do Information Commissioner’s Office, os prazos podem ser prorrogados nos casos de pedidos complexos ou nos casos em que haja múltiplos pedidos do titular de dados. Em qualquer situação, o titular deverá ser avisado da necessidade de extensão do prazo com as respectivas justificativas, dentro do prazo inicial. A situação em cada caso concreto definirá a existência de um pedido complexo. Como por exemplo: dificuldades técnicas na recuperação da informação, se os dados foram arquivados em fitas de backup; grandes volumes de dados sensíveis, que exijam um tratamento mais cuidadoso; dentre outros.”,b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: “O ramo de atuação do controlador e o volume de dados pessoais coletados são critérios relevantes para a fixação de prazos, pois, a depender da área em que desenvolve a sua atividade, o controlador poderá: (a) ser obrigado a armazenar dados específicos, por força de lei e/ou de regulamentações específicas do setor; e (b) estar suscetível a um grande volume de solicitações de titulares de dados pessoais, vez que há serviços que contam com uma quantidade elevada de contratantes e são fornecidos por um número reduzido de entes públicos ou privados. Tais situações estão presentes, por exemplo, no contexto de controladores que são entes privados atuantes nos ramos de fornecimento de serviços bancários, de telefonia, conexão e aplicações de internet a milhões de titulares de dados pessoais. Dessa forma, para definição de prazos específicos e superiores àqueles constantes nos incisos I e II do caput do art. 19 da LGPD, como autoriza o § 4º do mesmo dispositivo, os seguintes critérios devem ser considerados, quais sejam: (i) o ramo de atuação do controlador; e (ii) o volume de dados pessoais coletados e suscetíveis às decisões do controlador – nos termos do art. 5º, VI, da Lei Geral de Proteção de Dados. Para o formato simplificado e resposta imediata (inciso I), entendemos que será obrigatório apenas para situações (i) que não exijam o trabalho de autenticação do titular (e.g. titular já se encontra na área logada de um aplicativo); e (ii) tratem apenas de respostas confirmatórias (e.g., “sim, armazenamos seus dados pessoais durante nossa relação contratual” ou “não, não possuímos em nossos arquivos quaisquer dados pessoais sobre você”). Para todos os outros casos, prevalecerá o inciso II.”,615484”: “Um canal de atendimento efetivo, em conformidade com a

LGPD, deve ter os seguintes componentes: • **Transparência** (Art. 6º, I, LGPD): envolve fornecer informações claras sobre o tratamento. • **Acessibilidade**: requisito crucial, seguindo o princípio da boa-fé, tornando o canal de fácil acesso e utilização. • **Segurança** (Art. 46, LGPD): garantida com medidas robustas para proteger os dados. • **Privacy by Design** (Art. 46º, § 2º, LGPD) é incorporado desde o início, e canais diversificados são oferecidos para atender às preferências dos titulares. • **Rapidez e Eficiência**: O canal de atendimento deve oferecer respostas rápidas e eficientes às solicitações e dúvidas do titular, garantindo um fluxo de comunicação ágil. • **Personalização** (Princípio da Finalidade, LGPD): para atender às necessidades individuais de cada titular. • **Registro Detalhado** (Art. 16 da LGPD) das interações. • **Capacitação contínua dos agentes** (Art. 39, LGPD). Ainda: fácil identificação no site do controlador (ou por qualquer outro canal escolhido para viabilizar o exercício de direitos dos titulares), linguagem clara, acessível e em português. O canal de atendimento deve ser estruturado de maneira simples e intuitiva, sem redirecionamentos desnecessários e, se automatizado ou amparado por ferramentas de acesso automático aos dados, organizado de forma intuitiva e que vise a transparência e não o ofuscamento dos usuários. Um canal de atendimento efetivo, com as características acima descritas, facilita, a adequada efetivação dos direitos dos titulares de dados pessoais na forma prevista pela LGPD e até a efetivação de comunicação transparente em casos de incidentes, na forma prevista no art. 48, caput e § 1º, da LGPD. "615485": "A responsabilidade pela concretização dos direitos dos titulares deverá ser sempre do controlador. Será obrigação do controlador firmar contratos com seus operadores que contenham cláusulas de cooperação para as respostas aos titulares. Nesse caso, a responsabilidade do operador será limitada ao escopo contratual e perante o controlador, e não perante o titular de dados." "615486": "É importante que haja uma diferenciação entre o SAC da empresa e o meio pelo qual o titular de dados pessoais poderá exercer os seus direitos previstos no art. 18 da LGPD. Isso porque as solicitações relacionadas à LGPD devem ser direcionadas ao Encarregado de Proteção de Dados de uma empresa (tal como previsto no art. 5, VIII da LGPD) e não ao SAC, que tratará de questões mais relacionadas ao produto/serviço prestado. Entre as principais diretrizes do SAC que podem ser aplicadas no escopo da LGPD estão: acessibilidade; gratuidade; horário de atendimento não inferior a 8 horas diárias; opções mínimas constantes do primeiro menu. Por outro lado, há algumas diretrizes que não devem ser aplicadas. Por exemplo, sugere-se que o atendimento seja limitado aos dias úteis e horário comercial (período de trabalho do Encarregado em uma empresa), e não a 7 dias por semana e por 24 horas, como estabelece o Decreto, já que o atendimento é essencialmente humano e não robotizado, bem como limitado ao uso de meios eletrônicos, como e-mail ou formulários no site da empresa, e, por isso, sem a obrigação de haver atendimento por telefone. O uso do meio telefônico inviabilizaria o trabalho de um Encarregado, que deve cuidar de todos os assuntos relacionados à LGPD em uma empresa, e não somente ao atendimento de titulares de dados. Além disso, o prazo de resposta para o atendimento ao exercício de direitos pelo titular de dados deve ser aquele previsto especificamente pela LGPD e não no Decreto do SAC – isso porque há previsão expressa na lei mais específica. Quanto à disposição do Decreto do SAC sobre o acesso inicial ao atendente não ser condicionado ao fornecimento prévio de dados pelo titular de dados, isso também não poderia ser aplicável. Para que o Encarregado possa atender a um titular é necessário que haja, primeiro, o fornecimento de um mínimo necessário de dados pessoais para que seja possível identificar aquele titular e atender especificamente à sua demanda. De outro modo, haveria o risco de excluir ou fornecer dados de titular diverso daquele que fez a solicitação." "615487": "Um modelo de atendimento eficiente, adotado tanto por entidades privadas quanto pelo setor

público, que poderia servir como paradigma é a implementação de plataformas de contato e formulários padronizados, além do uso de chatbots. A utilização de tecnologias como chatbots e assistentes virtuais visaria agilizar o suporte ao cliente e personalizar as interações, mantendo altos padrões de satisfação. No entanto, eventual utilização de chatbots e assistentes virtuais, na hipótese de atendimento ao direito de exercício de direitos do titular de dados, deve ser avaliada com cautela, uma vez que se estará lidando com dados pessoais de forma automatizada. Assim, cabe ao controlador de dados realizar uma análise de risco e de adequação à LGPD sobre a viabilidade de se adotar esses mecanismos. Por outro lado, alguns agentes públicos têm como modelo o atendimento via plataformas de contato e formulários padronizados. A plataforma Consumidor.gov.br, no Brasil, é um exemplo adicional de como o setor público pode oferecer atendimento eficiente e econômico para grandes volumes de demandas. A plataforma fornece um meio seguro para os consumidores registrarem reclamações contra empresas participantes, permitindo o acompanhamento do status da reclamação e a interação entre consumidor e empresa. Um aspecto crucial é o formulário específico para o consumidor preencher ao registrar uma reclamação, o qual evita pedidos técnicos complexos, simplificando a comunicação e reduzindo o risco de interpretações incorretas. Ao estruturar as informações de maneira clara e padronizada, a plataforma Consumidor.gov.br facilita o processamento das demandas pelas empresas e pelos órgãos de defesa do consumidor, promovendo assim uma resolução mais rápida e eficaz dos problemas.”;

“615491”: “A confirmação de existência do tratamento pode ser negada nos casos em que (i) a mera confirmação prejudique, reduza ou obstrua investigações internas, o exercício de direitos de terceiros, ou procedimentos preliminares a ações judiciais, administrativas ou arbitrais; e (ii) a confirmação for solicitada em nome de terceiros sem autorização prévia e mediante recusa ao processo de autenticação.”;

“615492”: “Razão social, meio de contato e justificativa do compartilhamento.”;

“615489”: “Os operadores não deverão ser responsáveis perante o titular de dados, sendo a sua responsabilidade limitada ao escopo de seu contrato com o controlador. Como boa prática, o operador prontamente deverá, se contatado diretamente pelo titular, comunicar o controlador da solicitação e aguardar instruções. O operador não deve ser responsabilizado pela omissão do controlador, sob o risco de estar agindo fora do seu escopo de atuação e, portanto, extrapolando sua função.”;

“615490”: “-”; “615494”: “O controlador deve divulgar, quais dados são tratados, as finalidades do tratamento, a base legal do tratamento, a duração do armazenamento dos dados, os procedimentos de segurança adotados para proteger os dados, e a possibilidade de compartilhamento com terceiros. Os dados apenas poderão ser abertos mediante solicitação específica do titular e novo processo de autenticação. A respeito dos critérios e dos procedimentos utilizados para a decisão automatizadas, Bruno Feigelson e Daniel Becker em sua obra “Comentários à Lei Geral de Proteção de Dados”, aduzem que o titular de dados: “Não deseja receber códigos-fonte, mas entender os critérios que foram utilizados, pois, para ele, como leigo, é irrelevante o número de linhas de programação utilizadas (...). Para o titular dos dados, é fundamental receber informações consistentes e compreensíveis para que ele, querendo, possa contestar a decisão automatizada”. Ou seja, os titulares devem ter acesso e compreender a lógica normativa, e não a técnica envolvida na decisão, possibilitando assim o exercício de outros direitos. Nesse sentido, Rafael Zanatta afirma que o art. 20 da LGPD estipula uma obrigação dialógica entre o controlador e o titular com relação às decisões automatizadas: (...). “a ação de “encaixar uma pessoa”, a partir de seus dados pessoais e dados anonimizados, em um perfil social e inferir algo sobre ela implica em obrigações de três naturezas: (...). (iii) dialógica, relacionada à obrigação de se engajar em um “processo dialógico” com

as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e como decisões são tomadas”. Ainda mais, será bastante importante a ANPD limitar o que de fato deverá ser disponibilizado ao titular de dados. Como exemplo, materiais produzidos a partir dos dados pessoais compartilhados pelo titular de dados, por meio da inteligência do agente de tratamento, não deveriam ser a ele disponibilizados (ex: perfilização com base em histórico de navegação em aplicativo).

,"615493": "Deverá ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital OU em papel, de acordo com as formas de comunicação costumeiramente mantidas entre o controlador e aquele titular de dados. Não seria adequado considerar satisfeito o direito de acesso com a disponibilização dos dados pessoais apenas em formato papel, pois isso limitaria o acesso à informação e representaria uma limitação injustificada, especialmente considerando a predominância de empresas que operam exclusivamente online. Ao possibilitar a forma de disponibilização no formato em papel, estaríamos ignorando a natureza predominantemente digital das operações e dos dados atualmente. Além disso, a LGPD enfatiza a importância da modernização e da adaptação às tecnologias digitais, promovendo a eficiência e a acessibilidade na gestão dos dados pessoais. Portanto, a disponibilização ao formato em papel poderia prejudicar a eficácia e a praticidade do processo de acesso aos dados, principalmente para as empresas de tecnologia, como provedores de aplicativos, que operam primariamente no ambiente digital e cujos produtos e serviços são inteiramente digitais, além de ser contraproducente em um contexto cada vez mais digitalizado. Além disso, para evitar incidentes de segurança da informação, será muito importante a ANPD determinar os critérios para a proteção do material disponibilizado ao titular de dados. Como exemplo, a necessidade de alguma forma de autenticação do indivíduo que for abrir o documento (e.g., senha para abertura do documento)."

,"615502": "Hoje apenas entendemos o setor bancário como maduro o suficiente no Brasil para implementar o direito à portabilidade no Brasil."

,"615501": "Os maiores desafios são (i) a compatibilidade de comunicação entre os sistemas e integração de informações necessárias; (ii) a segurança da informação no tráfego dos dados; (iii) a possibilidade de violação de direitos de propriedade intelectual da parte que está transferindo os dados; e (iv) a responsabilização dos agentes em casos de falhas na portabilidade."

,"615505": "Com base nas diretrizes fornecidas pelo ICO, os formatos para permitir a interoperabilidade deverão ser estruturados (a relação estrutural entre os elementos é explícita na forma como os dados são armazenados no disco do computador); comumente usados (o formato escolhido deve ser amplamente utilizado e bem estabelecido); e legíveis por máquina (dados em um formato que pode ser lido e processado automaticamente por um computador). Quando nenhum formato específico for de uso comum em determinada indústria ou setor, o controlador deverá fornecer dados pessoais usando formatos abertos, como CSV, XML e JSON."

,"615503": "Não. O direito à portabilidade apenas poderá ser considerado satisfeito quando comprovado que o agente de tratamento recebendo os dados conseguiu devidamente tratá-los."

,"615504": "Sim. Com base no Considerando 68 do GDPR, agentes de tratamento devem ser incentivados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. O prazo para fazê-lo variará de acordo com cada indústria e complexidade para a sua conclusão, sendo que, até que esteja pronto, outros formatos deverão ser adotados para possibilitar a portabilidade."

,"615511": "Para qualificar um dado como incompleto, inexato ou desatualizado, deverá ser necessária a manifestação do titular com o mesmo grau de autenticidade da submissão original. Como exemplo, se um cadastro dependia de comprovante de residência para a validação de um endereço, será necessário

que o titular submeta comprovante de residência atualizado para demonstrar a mudança. Se, por outro lado, o dado foi inserido originalmente mediante simples manifestação do titular (informando o celular, por exemplo), a mera declaração deve ser suficiente para atualizá-lo. ","615514":"Situações que exijam comprovação documental, ou determinado grau de autenticidade (cópia de documento oficial, por exemplo).","615513":"Os critérios deverão ser (i) o agente de tratamento não trata mais aqueles dados pessoais por qualquer motivo (e.g., eliminou os dados, encerrou suas atividades); (ii) o agente de tratamento não pode mais ser localizado; ou (iii) pela quantidade e relevância dos dados tratados pelo agente de tratamento, o esforço não é válido por conta de (a) dificuldades técnicas na recuperação da informação – por exemplo, se os dados foram arquivados em fitas de backup; (b) necessidade de trabalho especializado que envolva a obtenção da informação ou a sua comunicação de forma inteligível; e (c) necessidade de pesquisa de grandes volumes de registros manuais e/ou não estruturados.","615512":"Sim. O direito de correção pode ser negado pelo controlador caso seja (i) manifestamente infundado; (ii) excessivo; (iii) prejudique, reduza ou obstrua investigações internas, o exercício de direitos de terceiros, ou procedimentos preliminares a ações judiciais, administrativas ou arbitrais; e/ou (iv) solicitado em nome de terceiros sem autorização prévia e recusa ao processo de autenticação. De qualquer modo, o controlador deverá ser capaz de demonstrar ao titular de dados e à ANPD o motivo pelo qual o pedido de correção foi recusado.","615517":"Sim. O titular deve fundamentar o pedido, sendo ônus do controlador demonstrar que o tratamento é necessário, não excessivo e que não viola a LGPD. O direito à anonimização, bloqueio e eliminação está condicionado ao tratamento desnecessário, excessivo ou em desconformidade com a LGPD, de forma que qualquer solicitação infundada não cumpriria os requisitos mínimos previstos na lei para o exercício desse direito. Afinal, a lei não fala em eliminação desmotivada dos dados, exceto se tratados com base no consentimento. ","615516":"Sim. Considerando que ambos os casos gerarão a inaplicabilidade da LGPD para as atividades do agente de tratamento e não há prejuízo ao titular de dados, o próprio agente deverá ter a chance de optar pela eliminação ou anonimização dos dados, conforme suas práticas internas. Os dados anonimizados poderão ser úteis para processos internos. Caso não sirvam para quaisquer fins, o agente poderá simplesmente eliminá-los.","615518":"O controlador será então obrigado a cessar as atividades de tratamento desses dados pessoais ou buscar uma base legal legítima para tratá-los, incluindo a própria obtenção do consentimento desse titular de dados.","615523":"Não, trata-se de dois pedidos diferentes, ainda que relacionados. Da mesma maneira que a revogação do consentimento não invalida os tratamentos realizados enquanto o consentimento era válido, tal revogação não pressupõe eliminação, salvo mediante pedido do titular. ","615521":"De forma geral, as atividades de tratamento de dados com base no consentimento desse titular deverão ser imediatamente cessadas. Com relação aos materiais produzidos como frutos do consentimento anterior, deverá ser feita uma análise acerca da viabilidade da completa ou parcial eliminação. Como exemplo, é impraticável garantir que determinado material promocional contendo a imagem de um titular de dados veiculado em um amplo território seja totalmente retirado de circulação. Assim como no 1º do art. 12 da LGPD acerca da reversão do processo de anonimização, o processo de eliminação também deve contar com razoabilidade, levando em consideração fatores objetivos, tais como custo e tempo necessários para eliminar determinado material, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. De qualquer forma, o controlador deverá ser absolutamente claro com os titulares sobre o que acontecerá com seus dados quando sua solicitação de eliminação for atendida, inclusive no que diz respeito aos sistemas de backup e materiais

circulados amplamente. Ainda, deverá ser deixado claro pela ANPD que não necessariamente todo pedido de eliminação deverá ser atendido, podendo o controlador recusar-se a cumpri-lo caso haja outra base legal que justifique a sua manutenção.”;”615617”:"A decisão tomada unicamente com base em tratamento automatizado de dados pessoais é uma decisão tomada por meios automatizados, sem qualquer envolvimento humano. A decisão automatizada necessariamente leva em conta meios automatizados, mas poderá ter intervenção humana. Conforme entendimento amplamente aceito na União Europeia, uma atividade pode ser considerada exclusivamente automatizada se um ser humano inserir os dados a serem tratados e, então, a tomada de decisão for realizada por um sistema automatizado. De qualquer forma, é razoável que o titular de dados tenha o direito de revisão em ambos os casos.”;”615618”:"É bastante razoável que o padrão internacional (GDPR) seja aplicado também sob o escopo da LGPD. Assim, para determinar quando um interesse está sendo efetivamente afetado, deverá ser argumentado que a decisão automatizada produz efeitos na esfera jurídica ou afeta o titular de dados significativamente de forma similar. Conforme esclarecimentos do ICO (disponíveis em <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/#id2>), uma decisão que produz efeitos na esfera jurídica afeta os direitos do titular de dados. Por exemplo quando uma pessoa, tendo em conta o seu perfil, tem direito a determinado benefício social conferido por lei. Uma decisão afeta o titular de dados significativamente de forma similar gera um impacto equivalente nas circunstâncias, no comportamento ou nas escolhas de um indivíduo. Como exemplos estão a tomada de crédito e o recrutamento para determinada vaga de emprego. Em casos extremos, a decisão pode gerar a discriminação de indivíduos. ”;”615619”:"O principal desafio é de ordem prática, qual seja, se os agentes de tratamento deverão ter seres humanos revendo a decisão automatizada, ou designar outra ação não humana para proceder com a revisão. No primeiro caso, a revisão poderá ser extremamente onerosa ao agente de tratamento e, no segundo caso, poderá ser sempre argumentada a injustiça de existir uma máquina revendo o trabalho de uma máquina semelhante. Ainda, deverá ser exigido dos controladores que: (i) Forneçam informações sobre a lógica envolvida no processo de tomada de decisão, bem como o significado e as consequências previstas para o titular; (ii) Utilizem procedimentos matemáticos ou estatísticos apropriados; (iii) Implementem medidas técnicas e organizacionais adequadas, para que possam corrigir imprecisões e minimizar o risco de erros; e (iv) Protejam os dados pessoais de uma forma que seja proporcional ao risco para os interesses e direitos do titular e que evite efeitos discriminatórios. Ainda, entre os desafios práticos para implementar o direito de revisão de decisões podemos citar as empresas multinacionais nas quais o tratamento dos dados é realizado no exterior deixando que as empresas dependam de informações internacionais – que podem demorar para ser produzidas. No mesmo sentido, há o risco de incompatibilidade legislativas entre o Brasil e outros países.”;”615620”:"Sim. De acordo com o art. 20 da LGPD “o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais”. Desta forma, nas seguintes situações poderá o controlador negar direito: (i) quando a decisão envolver outros elementos e não for exclusivamente automatizada, o controlador poderá negar o direito de revisão apresentando o justo motivo. (ii) direito à informação deve ser limitado pela observância dos segredos industrial e comercial. (iii) as decisões automatizadas adotadas não gerem efeitos jurídicos ou similares; (iv) as decisões automatizadas já contarem com um ser humano avaliando e interpretando o seu resultado antes de aplicá-la ao titular de dados.”

{ "615450": "(Contribuições - Telefônica Brasil S.A) O prazo existente no Art.11 da Lei 12.527 de 2011, especificamente a informação contida no caput (O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível), consideramos não ser razoável. O acesso “imediato” traz uma subjetividade de entendimento, podendo ser interpretado de diferentes formas pelos agentes de tratamento e, sobretudo, pelos titulares. Assim, além de apresentar insegurança jurídica, poderá causar desconfortos desnecessários tanto para quem é detentor do direito quanto para quem deverá cumpri-lo. Ademais, o prazo de 20 dias, a depender da quantidade de informações e do direito a ser requisitado pelo titular, levando em consideração ainda os produtos e/ou serviços adquiridos, poderá ser insuficiente para cumprimento dentro do prazo legal. Um prazo considerável razoável é o de 30 dias úteis. Quando a requisição apresentar um grau de complexibilidade maior, o prazo de até dois meses poderá ser o mais adequado, em consonância com o que dispõe o Art. 12 item 3 do GDPR. O prazo para atendimento às solicitações ainda deverá começar a contar após confirmação de identidade do titular, com a finalidade de assegurar que as informações serão enviadas ao detentor dos dados pessoais, ou seja, ao próprio titular.”; b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?;

(Contribuições - Telefônica Brasil S.A) Para uma maior segurança jurídica e cumprimento quanto às solicitações, as definições de alguns critérios são extremamente relevantes. Entre eles, o tipo de solicitação deverá ser um fator determinante, devendo avaliar se o requerimento se trata apenas de concessão de informação ou de exclusão/anonimização e revogação de consentimento. A volumetria dos dados pessoais também é outro fator a ser considerado. Quanto maior a quantidade de dados pessoais necessários utilizados para aquele determinado tratamento, conseqüentemente maior será o tempo para atendimento da solicitação realizada. O prazo em que os dados pessoais permaneceram sob tratamento é extremamente relevante como critério de diferenciação para cumprimento da solicitação, uma vez que quanto mais antigo o dado pessoal estiver no banco de dados, maior o dispense de tempo para atendimento da solicitação, como o caso dos dados pessoais de bases legadas. Ademais a complexidade de sistemas também é um fator fundamental que pode influenciar na busca dos dados. Os pedidos múltiplos também deverão ser considerado um critério, tendo em vista o dispense de tempo no cumprimento de todas as solicitações.”;

“615484”: (Contribuições - Telefônica Brasil S.A) Para que o atendimento seja efetivo, o mesmo deverá ser direcionado para o canal exclusivo de atendimento às solicitações. Atualmente, a maioria das organizações têm um departamento responsável para adequação e manutenção do programa de conformidade com a LGPD, sendo por lá realizado os atendimentos às solicitações dos titulares dos dados pessoais. A centralização em um único canal é primordial para garantia de cumprimento às requisições realizadas pelos titulares, evitando solicitações direcionadas para outros canais não oficiais. Assim, é importante destacar e retirar qualquer entendimento de vinculação obrigatória no atendimento das solicitações direcionadas para outros canais que não o canal oficial.”;

“615485”: (Contribuições - Telefônica Brasil S.A) Sim. Para os casos em que os titulares realizem a requisição de direitos ao operador, deverá competir ao mesmo a responsabilidade de informar ao controlador a solicitação que foi realizada, sendo vedada qualquer atendimento das solicitações sem qualquer autorização prévia do controlador.”;

“615486”: (Contribuições - Telefônica Brasil S.A) Não. O decreto estabelece normas sobre o serviço de atendimento ao consumidor (SAC) e traz uma série de determinações

que exigiriam a implantação de um atendimento com características de uma célula de atendimento especializada (demandando estrutura e custos). Os artigos 4, 5 6, 11 12, 13 15 e 16 dispõe de providências não seriam passíveis de cumprimento, como por exemplo atendimento ininterrupto por 24 horas e prazo de 7 dias para atendimento de demandas. Essas especificações vão de encontro com diversas previsões contidas na LGPD, não refletindo uma realidade quando falamos sobre governança em privacidade e proteção de dados pessoais."

"615487": "(Contribuições - Telefônica Brasil S.A) Como forma de otimizar o atendimento aos direitos dos titulares, especialmente o direito de acesso, alguns agentes de tratamento desenvolvem um ambiente em que o titular, por meio de login e senha, consegue acessar os dados pessoais tratados pelo controlador de forma imediata. Quando tratamos sobre revogação do consentimento, alguns agentes de tratamento desenvolvem um ambiente em que é possível que o titular faça a gestão dos consentimentos concedidos de forma simples. Contudo, nem todos os direitos previstos na LGPD podem ser atendidos de maneira automatizada, motivo pelo qual, o controlador pode optar por atendê-los de outra forma."

"615491": "(Contribuições - Telefônica Brasil S.A) Sim. Nas situações onde o titular aciona insistentemente o controlador, mesmo após diversos retornos, incluindo esclarecimentos às notificações recebidas através da ANPD e não se mostra suficientemente satisfeito, realizando repetidamente os mesmos questionamentos de forma recorrente. Assim, é razoável que seja considerado a definição de limites, como aqueles previstos no Art 12, item 5, do GDPR, que dispõe sobre quando os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode: a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou b) Recusar-se a dar seguimento ao pedido."

"615492": "As informações sobre os controladores a serem disponibilizadas aos titulares são os setores das indústrias em que há o compartilhamento dos dados pessoais. (Contribuições - Telefônica Brasil S.A) A informação direta dos controladores, um a um, torna-se inviável, uma vez que representa um esforço desproporcional e possível violação ao segredo industrial e comercial da organização."

"615489": "(Contribuições - Telefônica Brasil S.A) A responsabilidade dos operadores é a de direcionar o titular para local correto de exercício dos seus respectivos direitos, ou seja, o contato do controlador dos dados pessoais. "

"615490": "(Contribuições - Telefônica Brasil S.A) As informações mínimas a constar na declaração em formato simplificado, são: Nome completo / CPF / Data de Nascimento / E-mail / Nome da mãe / Endereços / telefones (fixo e móvel), bem como informações mínimas de como os seus dados pessoais estão sendo tratados."

"615494": "(Contribuições - Telefônica Brasil S.A) A política de privacidade ou aviso de privacidade mostra-se instrumento suficiente para garantir a transparência ao titular dos dados pessoais quanto aos tratamentos realizados. Assim, a finalidade de tratamento; quais dados são tratados; categoria sobre o compartilhamento dos dados pessoais; informações sobre transferência internacional de dados; informações sobre possibilidade de anonimização dos dados; como exercer os direitos e o canal de comunicação."

"615493": "(Contribuições - Telefônica Brasil S.A) O direito de acesso compreende na disponibilização dos dados pessoais objeto de tratamento, seja essa disponibilização via digital ou impressa."

"615502": "Sem comentários."

"615501": "Sem comentários."

"615505": "Sem comentários."

"615503": "Sem comentários."

"615504": "Sem comentários."

"615511": "Sem comentários."

"615514": "(Contribuições - Telefônica Brasil S.A) Situações em que a correção do dado sem a devida comprovação possa gerar prejuízos, como a declaração de renda sem sua comprovação, para fins de concessão de crédito. Ademais, tendo em vista o cenário brasileiro de fraudes, a correção

de dados sem comprovação da veracidade daquela informação, pode ocasionar prejuízos não só aos agentes de tratamento, mas aos titulares e a sociedade no geral. Dessa maneira, em quase todos os cenários, a comprovação da veracidade da informação pelo titular quando do exercício do direito à correção se mostra razoável e proporcional."615513": "Sem comentários."615512": "Sem comentários."615517": "(Contribuições - Telefônica Brasil S.A) Sim. A mera alegação por parte do titular não é suficiente para que seja realizado o bloqueio, anonimização ou eliminação dos dados pessoais objeto daquele determinado tratamento. O que pode ser considerado desnecessário para o titular ou excessivo não representa a realidade do tratamento realizado pelo agente de tratamento, onde os dados utilizados podem refletir em caráter essencial para a finalidade pretendida. Assim, é extremamente relevante que seja comprovada a alegação de que os dados pessoais estão sendo tratados de forma desnecessária, excessiva ou em desconformidade com a Lei, assegurando ao agente de tratamento o direito de resposta quanto ao alegado."615516": "(Contribuições - Telefônica Brasil S.A) Sim. A depender das finalidades de tratamento dos dados pessoais, em determinados casos poderá o controlador optar pela anonimização ao invés da eliminação, quando ainda que não seja mais passível a identificação daquele titular, a organização consiga ainda utilizar aqueles dados (que não mais considerados pessoais após a anonimização) para prosseguimento dos negócios, fomentando, por exemplo, a inovação."615518": "Sem comentários."615523": "(Contribuições - Telefônica Brasil S.A) Não. A revogação do consentimento não implica na exclusão dos dados e não deverá prejudicar o tratamento executado com suporte em outras bases legais. Assim, em determinadas situações a exclusão não poderá ocorrer por cumprimento de obrigação legal ou regulatória, por exemplo. Ademais, são direitos que não se comunicam diretamente. A revogação do consentimento é um poder de exercício de direito, enquanto o de exclusão é outro, não gerando, portanto, obrigações vinculativas."615521": "Sem comentários."615617": "Sem comentários."615618": "Sem comentários."615619": "Sem comentários."615620": "Sem comentários."

{"615450": "Entende-se que a adoção de prazos semelhantes ao previsto na Lei de Acesso à Informação não parece a mais adequada quando se trata de atendimento a direitos previstos na Lei 13.709/2018 (LGPD). A primeira lei versa exclusivamente sobre conceder acesso a informações solicitadas por pessoa natural, sendo que os prazos ali estabelecidos levam em consideração um tempo razoável à concessão dessas informações. De outro modo, a LGPD prevê diversos direitos que se estendem muito além de um simples acesso, como por exemplo, exclusão de dados pessoais, atualização, revisão de decisão automatizada, os quais demandam uma análise jurídica e técnica para verificar a viabilidade da sua concretização. Ainda, a depender da quantidade de agentes de tratamentos envolvidos, o fluxo da informação entre os agentes pode interferir no prazo efetivo para a garantia do direito. Após pesquisas e consultas às legislações de proteção de dados pessoais de outros países, entende-se que o prazo mais adequado deve ser semelhante àquele estabelecido no General Data Protection Regulation (GDPR), inspiração para a elaboração da LGPD, especificamente em seu artigo 12, parágrafo (3). Assim, tendo-se em vista a necessidade de análise técnica e jurídica, bem como a possibilidade de mais de um agente de tratamento envolvido no fluxo de dados, recomenda-se que o prazo de atendimento seja estabelecido em 30 (trinta) dias corridos, prorrogável por mais 60 (sessenta) dias a depender da complexidade da demanda, salvo os direitos de acesso e confirmação de tratamento que já possuem previsão legal – art. 19, I e II da LGPD. Por fim, entende-se que os Agentes de Tratamento não devem ser obrigados a dar andamento e concluir o atendimento a direitos fora dos dias úteis, por ausência de previsão legal nesse sentido. Caso o titular abra solicitação em dia não útil (sábado/domingo/feriado), o Agente de Tratamento Controlador deverá analisar, dar andamento e/ou concluir a solicitação somente no primeiro dia útil subsequente. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Os critérios para definição de prazo diferenciado daqueles previstos no art. 19 da LGPD devem ser (i) jurídicos e (ii) técnicos. Entende-se que a viabilidade jurídica deverá ser averiguada a partir da análise das legislações aplicáveis ao caso concreto e que venham a reger a relação entre o titular e a Instituição Agente de Tratamento. A mero título exemplificativo, citam-se as normas do Ministério da Educação – MEC; na eventualidade de o titular abrir solicitação de direito de exclusão dos seus dados pessoais junto à Universidade de curso, a Universidade precisará observar os regulamentos do MEC acerca da temporalidade e manutenção de dados pessoais de estudantes. No que diz respeito à viabilidade técnica, será analisada casuisticamente de acordo com o ambiente físico ou digital em que os dados pessoais são tratados. Por exemplo, na análise do direito de revisão de decisões tomadas unicamente com base em tratamento automatizado é necessário que o Agente de Tratamento faça análises técnicas do sistema/ambiente digital que tomou a decisão e escolha por qual método de revisão utilizará, se será necessária alteração de alguma parte do sistema, entre outras especificidades eventualmente necessárias. Como visto acima, diferentemente da análise e atendimento dos direitos de acesso e confirmação, que apenas dependem, via de regra, da consulta a sistemas estruturados da respectiva Entidade (para verificar se há tratamento de dados e em caso positivo quais seriam os dados tratados), os demais direitos dependem de uma análise mais aprofundada sobre a viabilidade de deferimento do direito que vão além do mero acesso e preenchimento de declaração com as informações obtidas. ","615484": "O canal de atendimento a direitos dos titulares deve ser: (i) de fácil acesso, (ii) gratuito, (iii) ter uma linguagem

simplificada para o melhor entendimento do titular (que pode não deter conhecimento técnico/legal), e (iv) possuir meio para autenticar a identidade do titular ou do seu representante legal, se for o caso. Destaca-se que é imprescindível que a norma não se abstenha de determinar padrões para a correta autenticação do usuário, de modo a evitar fraudes mediante o uso de dados vazados previamente na internet. Por fim, entende-se que o Agente de Tratamento Controlador deve ter a liberdade de escolher por qual meio irá atender os direitos dos titulares, como por exemplo, por canais/sistemas próprios, e-mail, ou outro de sua escolha, desde que não violados os 4 pressupostos acima. Assim, (i) não deve haver qualquer tipo de vedação aos Agentes de Tratamento Controladores em optar por criar portais específicos para atendimento dos direitos previstos na LGPD e (ii) não haver a obrigatoriedade de atendimento por um canal específico determinado por esta Autoridade.

","615485": "O art. 18, caput, da LGPD prevê expressamente que a competência para atendimento de direitos dos titulares é do controlador. Assim sendo, a única forma que o operador poderá atender aos direitos dos titulares se houver algum instrumento jurídico (ex.: contrato) que determine expressamente o contrário e transfira essa competência para o operador. Esse ajuste, contudo, não poderá implicar, em nenhuma hipótese, na transferência de responsabilidades do controlador para o operador, uma vez que as obrigações legalmente estipuladas ao primeiro não podem ser derogadas por acordo privado. Salvo disposição em contrário prevista em instrumentos contratuais entre o controlador e o operador, caberá exclusivamente ao primeiro receber, analisar e atender os direitos dos titulares, cabendo ao segundo auxiliar, se solicitado e, dentro dos limites da sua atuação enquanto operador. Portanto, caso uma Entidade, que atue como operadora, receba demanda de titular, entende-se que a ela somente caberá a responsabilidade de encaminhar o titular ao canal correto do controlador para exercer o direito previsto na LGPD.

","615486": "Não, pois nem todo titular de dado pessoal será considerado necessariamente um consumidor nos termos da Lei 8.078/1990, o Código de Defesa do Consumidor (CDC). A adoção de procedimentos análogos a de legislações consumeristas de forma indiscriminada para a concretização de direitos dos titulares poderá ensejar uma interpretação incorreta de que todo titular é consumidor. O referido decreto, que estabeleceu o Serviço de Atendimento ao Consumidor, visa regular o CDC (rege as relações entre consumidores e fornecedores) e foi elaborado levando-se em consideração as nuances dessa legislação e as características específicas da relação entre fornecedores e consumidores. Portanto, o decreto supramencionado não se atenta para as especificidades e complexidades que o tratamento de dados e o atendimento de direitos previstos na LGPD envolvem, bem como não faz uma análise da relação entre o agente de tratamento e o titular de dados pessoais. Os prazos previstos no decreto não são exequíveis e vão, inclusive, de encontro aos já estabelecidos na própria LGPD. Ainda, o atendimento por meio telefônico aos direitos dos titulares é inviável, uma vez que, a depender do direito, é necessária a análise jurídica e técnica. Além disso, na hipótese de ser essencial uma declaração, a LGPD já determinou que essa deverá ser no formato eletrônico ou impresso (art. 19, §2º da LGPD). Por fim, reitera-se: todo consumidor pessoa natural será necessariamente um titular de dados pessoais, mas nem todo titular de dados será consumidor.

","615487": "Sim, o modelo de atendimento adotado pela Fundação Getúlio Vargas – FGV é gratuito e de fácil acesso. A FGV utiliza um portal próprio destinado exclusivamente ao recebimento e análise dos direitos previstos no Capítulo III da LGPD, disponível em clicando em “Conheça o Portal dos Direitos dos Titulares de Dados Pessoais FGV”. O cadastro é simples (e-mail, confirmação do e-mail e senha) e, após criado, basta o titular abrir o direito que deseja exercer e preencher as informações básicas (se está abrindo em nome próprio, CPF, vínculo e outras informações que o titular queira

incluir). Aberta a solicitação, a FGV receberá a demanda em sistema único e próprio destinado ao exercício de direitos dos titulares, onde um(a) analista da Equipe DPO será responsável por fazer a análise com o auxílio da unidade/área que se faça necessária. ";615491": "Não há contribuição.";615492": "Para a correta identificação dos controladores de dados pessoais é necessário que o Agente de Tratamento informe: (i) nome da instituição/pessoa física, (ii) o canal destinado à proteção de dados pessoais ou, no mínimo, o canal para exercício dos direitos dos titulares, (iii) a finalidade para qual o Agente trata os dados pessoais e (iv) a base legal que ampare o referido tratamento. ";615489": "Como mencionado em comentário anterior desta contribuição, salvo disposição em contrário prevista em instrumentos contratuais, caberá ao operador auxiliar ao controlador mediante solicitação deste e dentro dos limites da sua competência/atuação. Assim, caso uma Entidade, que atue como operadora, receba demanda de titular, entende-se que a ela somente caberá a responsabilidade de encaminhar o titular ao canal correto do controlador para exercer o direito previsto na LGPD. ";615490": "Tendo-se em vista o prazo legal previsto para o atendimento do acesso/confirmação de tratamento em formato simples, entende-se que as informações mínimas que devem ser fornecidas pelo controlador são: (i) Direito de confirmação de tratamento (simples): a confirmação ao titular se a entidade solicitada trata ou não os seus dados pessoais, o nome do controlador, finalidade do tratamento e as possíveis bases legais que o amparam; e (ii) Direito de acesso: deverão ser fornecidos os dados básicos de cadastro/registo (que poderão variar de acordo com a entidade e tipo de vínculo com o titular), o nome do controlador, finalidade do tratamento e as possíveis bases legais que o amparam. ";615494": "Não há contribuição.";615493": "Depende se o titular deseja exercer o modelo simples ou declaração. Em se tratando de direito de acesso simples, art. 19, I da LGPD, como não há exigência legal de requisitos mínimos, entende-se que a partir da disponibilização dos dados no formato escolhido pelo titular o direito poderá ser considerado satisfeito. Em se tratando do exercício de direito de acesso declaração, art. 19, II da LGPD, para além da disponibilização de todos os dados pessoais ao titular, é necessário observar os demais requisitos constantes do dispositivo ora mencionado, sendo preciso, ainda, informar para se considerar o direito satisfeito: (i) a origem dos dados, (ii) a inexistência de registro (se for o caso), (iii) os critérios utilizados e a (iv) finalidade do tratamento, observados os segredos comercial e industrial. De forma adicional, com intuito de contribuir com esta Autoridade, entende-se que a interpretação da parte final do art. 19, §2º da LGPD ("a critério do titular") deve ser lida de forma razoável e levando-se sempre em consideração a natureza do tratamento efetuado pelo Controlador. Exemplifica-se: caso uma rede social com escritório sediado em determinada capital da Norte brasileiro seja solicitada a fornecer os dados no formato impresso, por um titular situado no Sul do país, o meio mais acessível disponível para atender a essa requisição seria o envio por postagem via Correios. Contudo, tal prática seria desarrazoável e geraria uma exposição dos dados do titular que estariam sujeitos a extravio. Logo, como a rede social apenas efetua tratamento em formato digital, o razoável é que essa disponibilização se dê da mesma forma de tratamento acordado entre ela e o titular, qual seja, digital. ";615502": "Os setores de telecomunicações e bancários possuem maturidade nos processos de negócio e tecnologia capazes de auxiliar na implementação do direito de portabilidade previsto na LGPD. No que diz respeito ao setor de telecomunicações, pode ser mencionada a portabilidade do código de acesso (número de telefone celular) de uma operadora telefônica para outra, a qual dispõe de normas próprias para como deve ser operada essa transação, disponíveis no ANEXO AO REGULAMENTO DOS SERVIÇOS DE TELECOMUNICAÇÕES, APROVADO PELA RESOLUÇÃO Nº 73, DE 25 DE NOVEMBRO DE 1998 . Já no

setor bancário tem-se a Resolução CMN nº 5.057, de 15 de dezembro de 2022, disponível em < <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=5057>>, que dispõe sobre a portabilidade de operações de crédito e de arrendamento mercantil financeiro, tratando em seu Capítulo IV dos procedimentos específicos para a realização da portabilidade. Contudo, independentemente dos setores no ordenamento jurídico brasileiro, com intuito de auxiliar esta Autoridade no desenvolvimento do regulamento mais apropriado para o exercício e efetivação do direito de portabilidade estabelecido pela LGPD, recomenda-se utilizar como parâmetro as regras estabelecidas pela Autoridade de Proteção de Dados do Reino Unido, Information Commiissioner's Office, disponíveis em . Dentre as especificações, podem ser citadas, mas não limitada, as formas em que os dados devem ser fornecidos. "615501": "Existem diversos desafios, contudo, destaca-se para fins de regulamentação os seguintes: (a) Documentos físicos: a portabilidade de dados pessoais contidos em documentos que estão armazenados exclusivamente no formato físico é um desafio, pois estes dados não se encontram em sistemas estruturados que viabilizam uma portabilidade em um tempo razoável. Eventual exigência de portabilidade de dados que constam somente em documentos físicos pode tornar o processo excessivamente demorado ao titular e altamente custoso aos Agentes de Tratamento. Assim, é necessário que esta Autoridade se atente para a peculiaridade dos documentos em formato impresso, sendo que eventual regulação deve se ater aos dados em formato nato-digital. Destaca-se que a regulamentação de autoridades europeias, como o ICO, também se limita à documentos em formato nato-digital, sendo excluídos documentos físicos. (b) Formato: é necessária a definição de formatos padrões para a portabilidade dos dados entre agentes de tratamento, que esteja de acordo com aqueles atualmente já disponibilizados em mercado e amplamente divulgado/utilizado pelas instituições. Caso não sejam preestabelecidos padrões de formatos específicos para realizar a portabilidade, a concretização desse direito poderá ser um problema, pois cada agente de tratamento poderá dispor de um formato diferente tornando-se um desafio a transferência, seja pela demora, complexidade de diferentes formatos ou até mesmo pela impossibilidade de portabilidade. A título colaborativo, os formatos mais utilizados em mercado e que não são extremamente onerosos ao Agente de Tratamento, viabilizando o atendimento do direito em tempo razoável, são CSV, XML e JSON, adotados pelo ICO e recomendados pelo European Data Protection Board (EDPB) . "615505": "O primeiro objeto de padronização deve ser o formato em que os dados pessoais devem ser disponibilizados. Seguindo a linha de raciocínio exposta no comentário anterior, entende-se que deverá ser estabelecido como padrão mais de 1 formato, observados aqueles já disponíveis em mercado e amplamente utilizados pelas instituições. Os mais comuns são CSV, XML e JSON, que também são adotados pelo ICO e recomendados pelo European Data Protection Board (EDPB) . Outro ponto que deverá ser padronizado por esta Autoridade refere-se a quais documentos e dados pessoais podem ser objeto de portabilidade. Conforme pontuado anteriormente, a regulamentação deve se ater a documentos e dados pessoais disponibilizados em formato nato-digital e armazenados em sistemas estruturados. "615503": "Não há contribuição."615504": "Sim, é razoável. O direito à portabilidade de dados pessoais, informações, documentos, entre outros, não é uma inovação da LGPD, já existindo no ordenamento jurídico brasileiro legislações que garantem o direito à portabilidade de certos dados/informações e/ou documentos específicos. A depender da atividade desenvolvida pelo Agente de Tratamento e da finalidade/objetivo para a qual a pessoa deseja a portabilidade, poderá existir legislação setorial específica regulando essa operação. A título exemplificativo, citam-se, novamente, as regulamentações da portabilidade previstas nos

setores bancário e de telecomunicações, incluindo-se, ainda, eventuais normas provenientes do Ministério da Educação sobre a portabilidade no âmbito de prestação de serviços educacionais. Portanto, ante a existência de regulamentações específicas de outros setores, é razoável permitir ao setor privado a definição de padrões de interoperabilidade específicos. No que diz respeito ao prazo, caso a portabilidade se atenha especificamente ao direito previsto na LGPD (não sendo aplicável outras leis setoriais), recomenda-se que seja estabelecido em 30 (trinta) dias corridos, prorrogável por mais 60 (sessenta) dias a depender da complexidade da demanda. "615511": "O primeiro critério objetivo para que um dado seja qualificado como incompleto, inexato ou desatualizado é a devida comprovação pelo titular, por meio de documento, foto/print ou qualquer outro meio apto a provar, que o dado armazenado não corresponde com a realidade. Ainda, outro critério para o atendimento é que o tratamento de dados pessoais seja atual, gerando efeitos para o titular no tempo corrente. Qualquer tratamento pretérito ou já encerrado não deve ser objeto desse direito. "615514": "Não há contribuição." "615513": "Vislumbra-se dois critérios objetivos: (a) quando a finalidade para qual o dado desatualizado/ incorreto já foi devidamente alcançada, observadas as possibilidades de manutenção do dado pessoal conforme art. 16 da LGPD, e (b) quando existe lei ou regulamento que impeçam a referida atualização/modificação do dado pessoal. Por exemplo, supõe-se que durante a realização de uma pesquisa por um Órgão de Pesquisa foram aplicados questionários a um determinado grupo de pessoas que moravam no bairro XY, ponto de estudo da referida pesquisa. No questionário foram coletados dados pessoais de nome completo, e-mail, endereço residencial e as respectivas respostas. A pesquisa foi finalizada em 2021. Em 2022, um dos respondentes do questionário aplicado no âmbito da pesquisa, Fulano da Silva, entrou em contato com o Órgão de Pesquisa solicitando o direito de atualização do seu endereço residencial, pois não residia mais no bairro XY, havia se mudado para o bairro AAW. O referido pedido de atualização pode ser indeferido, vez que a manutenção do dado de endereço é necessária para comprovar que à época o titular residia no bairro objeto da pesquisa, bem como é um esforço desarrazoável à instituição de pesquisa incluir/atualizar suas bases com uma informação que não se faz relevante/importante para o fim para o qual foi coletada, qual seja, realização da pesquisa. "615512": "Não há contribuição." "615517": "Não, ao titular cabe somente solicitar o direito e indicar quais dados pessoais exatamente ele se opõe ao tratamento ou deseja que seja excluído ou anonimizado. Exigir do titular a fundamentação pela qual ele se opõe ao tratamento pode dificultar ou até mesmo impossibilitar o exercício do direito, uma vez que eventual falta de conhecimento sobre a lei impossibilitará a sua fundamentação. Ainda, não há qualquer exigência de fundamentação ao titular prevista no art. 18 da LGPD. Conforme depreende da leitura do mencionado dispositivo, o titular tem o direito de solicitar ao controlador quaisquer dos direitos previstos na LGPD, independente de fundamentação da sua parte. Caberá ao controlador, na análise da solicitação e das circunstâncias concretas da operação, verificar a viabilidade do pedido e, caso seja indeferido, fundamentar a decisão de forma clara e compreensível ao titular. "615516": "Sim, tendo-se em vista que o efeito prático em ambas as situações (anonimização ou exclusão) é aquele desejado pelo titular, qual seja, não ter mais determinado dado pessoal no formato identificado ou identificável na base de dados. Conforme determina o art. 12 da LGPD, a informação anonimizada não será considerada dado pessoal, logo, ao anonimizar o dado que o titular deseja excluir, ele perderá a característica “pessoal”, não sendo possível vinculá-lo a uma pessoa natural. Ainda, a exclusão definitiva de um dado em determinado sistema/base pode gerar repercussões/implicações em diferentes bancos eletrônicos ou, até mesmo, pode ser inviável tecnicamente eliminar somente o(s) dado(s)

pessoal(ais) apontado(s) sem afetar todo o sistema. Por exemplo, alguns sistemas possuem bancos de dados relacionais em que o CPF figura como dado-chave para o registro do titular. Logo, nessa situação, a exclusão do dado CPF geraria impacto em todos os outros dados relacionados, sendo a anonimização (substituição do CPF verdadeiros por um código aleatório devidamente sinalizado) o caminho tecnicamente mais confiável. Assim, ao anonimizar o dado, conforme já dito anteriormente, o controlador atenderá o desejo do titular, qual seja, de não ter determinado dado pessoal tratado. Ademais, entende-se que a anonimização do dado pessoal deve ser considerada uma alternativa à eliminação, cabendo ao próprio controlador optar por anonimizar o dado pessoal ou eliminá-lo.

","615518": "O seu efeito deve ser semelhante àqueles produzidos quando da revogação do consentimento, constantes do art. 8º, §5º da LGPD, que determina que os tratamentos ocorridos anteriormente a oposição serão ratificados e novas atividades de tratamento serão interrompidas após analisado e deferido o direito de oposição. Por conseguinte, a única diferença prática entre o direito de oposição e o de revogação do consentimento é a determinação da base legal originalmente aplicável. A determinação da base legal caberá ao controlador, sendo inclusive priorizada a aplicação análoga do princípio da instrumentalidade das formas do direito processual, para que uma requisição erroneamente sinalizada pelo titular possa ser convertida no exercício do direito correto. "

","615523": "Não, a revogação do consentimento implica na interrupção do tratamento a partir da solicitação desse direito pelo titular no canal adequado do controlador. Os demais tratamentos realizados anteriormente à solicitação serão ratificados até a solicitação expressa da exclusão desses dados pessoais, conforme determina o art. 8º, §5º da LGPD. Portanto, da leitura do referido dispositivo e da análise dos demais artigos da LGPD aplicáveis ao direito de revogação do consentimento, entende-se que a exclusão dos dados pessoais deve ser expressamente solicitada pelo titular de forma independente, isto é, solicitando-se expressamente o direito de exclusão. "

","615521": "O requerimento de eliminação dos dados pessoais não invalida as operações realizadas anteriormente pelo controlador que, à época, tinha o consentimento do titular para tratar seus dados pessoais. Ou seja, ainda que o titular revogue o consentimento, as operações realizadas até a data da revogação são válidas e devem ser ratificadas, conforme se depreende da leitura do art. 8º, §5º da LGPD. A solicitação de eliminação dos dados pessoais, se requisitada adicionalmente após o pedido de revogação de consentimento, apenas faz com que o controlador analise a situação apresentada e veja se é possível ou não excluir os dados pessoais. Uma vez deferido o direito e eliminadas as informações do titular, tem-se todas as operações anteriormente realizadas não serão invalidadas, sendo que os dados pessoais não estarão mais sob o controle do respectivo Agente de Tratamento por terem sido deletados. "

","615617": "Para os fins da LGPD, conforme o parágrafo único do artigo 20, a decisão automatizada é aquela passível do direito à informação, ou seja, da obtenção pelo titular de esclarecimentos sobre como a saída (output) de um algoritmo ponderou os dados pessoais do titular utilizados como entrada (inputs), respeitados os direitos de propriedade intelectual. Já conforme o caput do artigo 20, a decisão tomada unicamente com base em tratamento automatizado de dados pessoais é aquela passível de solicitação de revisão por parte do titular, sendo que existem dois requisitos: (i) o tratamento automatizado conforme o conceito acima e (ii) a tomada de decisão que é baseada unicamente a partir desse tratamento automatizado. Portanto, para resumir: a decisão automatizada é o processo/fórmula de ponderação de variáveis feito a partir de uma engenharia algorítmica onde dados de input são processados para gerar o output ou resultado, estando sujeita ao direito de informação ao titular sobre os critérios utilizados nesse tratamento. Já a decisão tomada unicamente com base em tratamentos

automatizados aproveita esse output e o torna o veredicto final do agente de tratamento, sem qualquer filtro humano capaz de ponderar por um resultado diverso, estando sujeita ao direito de revisão acerca desta tomada de ação (devido às alterações legislativas na LGPD, essa revisão não está condicionada a um ser humano, podendo ser feita por outra forma de tratamento automatizado devidamente balanceada para evitar distorções no processamento dos dados pessoais, por exemplo). ";615618": "Não há contribuição.";615619": "Não há contribuição.";615620": "Em situações em que a decisão não tenha sido tomada de forma automatizada. É comum que titulares, em decorrência de sua falta de conhecimento técnico, pensem que uma decisão foi tomada de forma automatizada, isto é, sem a interferência, supervisão ou qualquer tipo de participação humana. Por crer que se trata de uma decisão automatizada, o titular solicita o direito de revisão. Contudo, quando da análise do caso concreto e do processo decisório específico feito, percebe-se que a decisão foi tomada com o auxílio de pessoa natural. Logo, tendo-se em vista que a decisão não foi automatizada devido à participação de humano, é possível indeferir o pedido de direito de revisão da decisão. Assim, ainda que o Agente de Tratamento tenha se utilizado de alguma ferramenta ou programa de computador para auxiliar na tomada de decisão, se ele supervisionar ou interferir de qualquer forma nessas ferramentas, não se trata de decisão automatizada, sendo possível indeferir a solicitação do direito. "

{ "615450": "[CLARO BRASIL] A Lei nº 12.527/2011 foi criada para regular o acesso a informações no âmbito do setor público. O artigo 11, § 1º da Lei de Acesso à Informação estabelece que o órgão público deve resolver o atendimento dentro de um prazo não superior a 20 dias, prorrogável por mais 10 dias (art. 16, caput). Embora a solicitação por meio de sites oficiais esteja contemplada em tal Lei, na prática, muitas vezes exige-se que o titular se desloque a um local específico e especializado para fazer requisições aos órgãos públicos. No contexto do setor privado, em que os direitos dos titulares de dados pessoais serão predominantemente solicitados por meio de plataformas online, é essencial considerar o volume de solicitações que as organizações podem receber, bem como considerar suas capacidades e estruturas para gerenciar essas solicitações. Neste sentido, o General Data Protection Regulation ("GDPR") estabelece, em seu artigo 12.1, que os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Assim, especificamente com relação à sugestão de seguir os prazos previstos pela Lei de Acesso à Informação ("LAI"), entendemos que tal proposta é inadequada e, de modo a abranger a realidade de diferentes setores e portes de agentes de tratamento, bem como garantir que o atendimento de direitos dos titulares seja efetivo, recomendamos que sejam seguidos os prazos propostos no GDPR. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?": "[CLARO BRASIL] Ao definir prazos para atendimento às requisições feitas pelos titulares, seja em formato simplificado (conforme o artigo 19, I) ou por meio de declaração clara e completa (de acordo com o artigo 19, II), o principal critério a ser observado se refere às informações que serão prestadas, conforme demonstrado a seguir: - Declaração simplificada (art. 19, I): Deve abranger os dados de cadastro; - Declaração clara e completa (art. 19, II): a declaração deve abranger os dados tratados e suas respectivas finalidades, com especial atenção à manutenção do segredo comercial e de negócio. Ademais, necessário que seja verificado o nível de complexidade sistêmica e o investimento de recursos pelo Controlador, antes de tornar obrigatória a indicação de demais informações. Portanto, os prazos estabelecidos para atender a essas demandas devem considerar essas variáveis, a fim de garantir um atendimento eficaz e em conformidade com as expectativas dos titulares. Como exemplo, para setores que necessitam de tempo adicional para atender aos direitos previstos nos incisos I e II do artigo 19 da LGPD, uma alternativa seria seguir o prazo previsto pelo GDPR, em seu artigo 12.1: os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. ", "615484": "[CLARO BRASIL] - Divulgação: Assegurar que o acesso ao Portal de Privacidade e/ou Aviso de Privacidade seja facilmente visível na experiência do usuário, com o Canal de Atendimento claramente identificado e acompanhado de instruções claras sobre como utilizá-lo. - Informação: Informar o titular sobre seus direitos conforme previstos no art. 18 da LGPD, para que possa exercer a autodeterminação informativa. - Linguagem e Formato: Utilizar linguagem clara e acessível para garantir que as informações sejam compreendidas facilmente pelo titular e prestar informações em formato inteligível, que não demande conhecimento prévio para acessar a resposta. - Autenticação da identidade: Garantir que a pessoa que solicita acesso aos dados seja de fato o titular destes, evitando assim violações dos direitos de terceiros, como o compartilhamento indevido de dados. ", "615485": "[CLARO BRASIL]

Sim, as obrigações dos operadores no que tange ao atendimento dos direitos dos titulares, bem como sua colaboração com os controladores, são pilares essenciais da relação entre as partes. Nesse sentido, destacam-se o dever de manter registros de operações de tratamento de dados pessoais (artigo 37) e realizar o tratamento segundo as instruções fornecidas pelo controlador (artigo 39). Entretanto, a maneira como essa cooperação se dará irá depender de alguns fatores, como os protocolos estabelecidos entre as partes e o contexto do tratamento. Assim, necessário que seja considerada a existência de diferentes cenários, de forma a não restringir a condutas específicas, como também que o estabelecimento de instrumentos contratuais e demais acordos entre as partes sejam suficientes para atender as necessidades e obrigações entre as partes. ";615486": "[CLARO BRASIL] Não é apropriado equiparar as diretrizes estabelecidas para o atendimento de SAC, conforme previsto no Decreto nº 11.034/2022, ao atendimento dos direitos dos titulares, conforme estabelecido na LGPD, isso porque: a) art. 4º e Art. 5º: Embora o canal online de atendimento deva estar disponível para envio de requisições a qualquer hora e todos os dias, a exigência de múltiplos canais e atendimento contínuo pode ser impraticável devido à complexidade e custos de segurança para proteção de dados. Além disso, o atendimento telefônico para os direitos dos titulares previstos na LGPD não se equipara às tratativas no âmbito da legislação consumerista, já que as demandas demandam análise, compreensão e avaliação, conforme exigido pela legislação. b) art. 13: Os prazos estabelecidos pela legislação de SAC são exíguos e não são adequados para lidar com as requisições previstas pela LGPD, que são mais complexas e, em diversas situações, exigem mais tempo para serem atendidas. c) art. 14: Os direitos garantidos pela LGPD dizem respeito aos dados pessoais dos titulares e não são o foco dos serviços prestados. ";615487": "[CLARO BRASIL] Não entendemos que exista um modelo ideal. É importante que exista autonomia para as organizações definirem o formato mais adequado às suas necessidades e realidade para atendimento dos titulares. Essa abordagem é justificada pela diversidade de características relacionadas à estrutura e aos processos de cada empresa; à importância de garantir a liberdade para a inovação; a autonomia para implementar recursos personalizados e às variações de recursos financeiros disponíveis. ";615491": "[CLARO BRASIL] A confirmação da existência do tratamento pode ser negada em algumas situações excepcionais, como: a) Confirmação de identidade: quando não for possível a confirmação da identidade do titular do dado. b) Segredo de negócio: Quando a confirmação da existência do tratamento de dados pessoais revelar algum segredo de negócio da empresa; c) Investigação e Auditoria: durante o curso de investigações e auditorias; d) Sigilo: quando o controlador estiver submetido a norma de sigilo; e) Solicitação excessiva ou irrazoável: se uma solicitação for claramente irrazoável; Para determinar se uma solicitação é manifestamente excessiva, é necessário avaliar se ela é claramente irrazoável. Isso deve ser baseado na proporcionalidade da solicitação em relação ao ônus ou custos envolvidos no tratamento da solicitação. ";615492": "[CLARO BRASIL] As informações relevantes a serem fornecidas aos titulares são: (i) Na identificação do controlador: informações básicas, claras e precisas sobre a identidade do controlador responsável pelo tratamento dos dados pessoais do titular; (ii) Compartilhamento de dados: a indicação do setor empresarial em que o compartilhamento é realizado, com a respectiva finalidade, deve ser considerada suficiente para que o princípio da transparência seja cumprido. Isso se justifica pois o excesso de detalhamento em relação as informações prestadas podem gerar efeito contrário ao esperado, além da exposição de dados comercialmente estratégicos, tutelados pelos segredos comercial e industrial. ";615489": "[CLARO BRASIL] Os operadores têm a responsabilidade de cooperar com os controladores para garantir que os titulares dos dados possam exercer seu direito

de obter informações sobre o tratamento de dados pessoais seja por eventual: (i) cooperação e suporte no recebimento da solicitação e encaminhamento ao controlador, ou ao menos no redirecionamento do titular para o canal de atendimento do controlador que é responsável pela atividade; (ii) fornecimento de informações ao controlador que possam auxiliar na identificação da relação jurídica e do escopo do tratamento, como também na elaboração de resposta ao titular de dados; (iii) facilitação na localização e recuperação dos dados para atender solicitações dos titulares; (iv) documentação das atividades de tratamento e visibilidade para o controlador acerca de qualquer alteração ou intercorrência no tratamento. ";615490": "[CLARO BRASIL] O controlador deve fornecer informações que permitam aos titulares entenderem como seus dados estão sendo tratados, o que inclui a forma do tratamento, bem como o livre acesso aos seus dados pessoais. Além disso, como institui o artigo 19 da LGPD, a confirmação de existência ou o acesso a dados pessoais podem ser disponibilizados em formato simplificado ou por meio de declaração clara e completa. ";615494": "[CLARO BRASIL] Para garantir a transparência e o direito à informação no âmbito de decisões automatizadas, as informações mínimas sobre o tratamento consistem na indicação do produto ou serviço a que se refere à tomada de decisão automatizada e quais as possíveis informações que poderão ser utilizadas para a obtenção do resultado. A partir dessas informações, o titular tem plenas condições de exercer sua autodeterminação informativa para, caso queira, solicitar informações mais detalhadas sobre o tratamento, nos termos do que prevê o artigo 20 e § 1º da LGPD. ";615493": "[CLARO BRASIL] Sim, poderia ser considerado satisfeito. Segundo diretrizes internacionais, como as da EDPB, os agentes de tratamento responsáveis pelo atendimento ao direito não são obrigados a fornecer as informações de outra forma além daquela solicitada pelo titular. No entanto, os formatos podem variar dependendo dos próprios dados pessoais a serem fornecidos e da forma de contato normalmente mantida entre titular e controlador. ";615502": "[CLARO BRASIL] No Brasil não enxergamos algum setor que possua maturidade para implementar a portabilidade dos dados pessoais, dado que é um tema complexo que deve ser melhor discutido antes do desenvolvimento de regras e orientações de implementação. A título de exemplo, citamos abaixo alguns tópicos que requerem análise prévia pela ANPD, dada a sua complexidade: i) definição do conceito de portabilidade e interoperabilidade; ii) definição de quais dados devem ser objeto da portabilidade; iii) limites técnicos e legais aplicáveis, visando a proteção de terceiros; iv) consentimento de terceiros para portabilidade; v) transferência direta de dados ou através do titular; vi) equilíbrio entre portabilidade e privacidade; vii) limites ao tratamento dos dados pelos destinatários; viii) responsabilidade dos agentes de tratamento; ";615501": "[CLARO BRASIL] Os desafios tecnológicos para implementação de um padrão de interoperabilidade para o direito de portabilidade são diversos e abrangentes. Eles envolvem a complexidade das operações, a diversidade de formatos de dados e metadados, bem como as ferramentas e protocolos de comunicação adotados pelo mercado de cada setor e indústria. ";615505": "- ";615503": "- ";615504": "- ";615511": "[CLARO BRASIL] Os critérios objetivos que podem ser considerados são: 1) Dados incompletos: - ausência de informações essenciais; - falta de elementos de identificação; - informações parciais ou fragmentadas; - inconsistência dos dados pessoais. 2) Dados inexatos: - fontes de dados não confiáveis; - erros de processamento de dados. 3) Dados desatualizados: - informações antigas que já não correspondem mais à realidade; - obsoletos para a finalidade tratada. ";615514": "[CLARO BRASIL] A simples declaração do titular pode não ser suficiente para o exercício do direito à correção em situações em que haja dúvidas sobre a veracidade dos dados, ausência de documentação comprobatória; eventual alteração em bases públicas; impossibilidade de confirmação de

tratamento de dados do titular ou de confirmação da sua identidade.";"615513": "[CLARO BRASIL] Os critérios que podem ser considerados como esforço desproporcional são: a. Custos: custos técnicos e financeiros necessários para atender à solicitação são significativamente altos em relação ao tamanho e aos recursos da organização. b. Impacto nas operações: atendimento à solicitação impactaria de forma significativa as operações cotidianas da organização; c. Complexidade da solicitação: volume ou complexidade dos dados solicitados é tal que tornaria o processo de recuperação e fornecimento impraticável dentro de um período razoável. d. Volume das solicitações: solicitações repetidas pelo mesmo titular ou solicitações em massa que impõem uma carga administrativa desproporcional. ";"615512": "[CLARO BRASIL] A solicitação de correção pode ser recusada se a empresa considerar os dados tratados como "precisos/adequados", ou seja, se entender que não há necessidade de correção. Também em situações de alteração ou em caso de necessidades de manutenção para fins de histórico. Além disso, o direito à correção pode ser negado se a solicitação for considerada manifestamente infundada ou excessiva; em caso de ausência de envio de documentação comprobatória da identidade do solicitante ou em casos de impossibilidade de alteração de determinados dados, como código de cliente ou número de contrato, os quais servem como chave de identificação única dos titulares, ";"615517": "[CLARO BRASIL] Sim. O titular deve fornecer contexto ou justificativa que fundamente seu pedido no momento da requisição, demonstrando a falta de necessidade de retenção dos seus dados. Nesse sentido, a exigência de justificativa por parte do titular não representa uma barreira ao exercício de seus direitos, mas sim uma etapa essencial que auxiliará o responsável pelo tratamento dos dados a formular uma resposta clara e apropriada, de acordo com o contexto apresentado pelo requerente. ";"615516": "[CLARO BRASIL] Sim, ambas podem ser adotadas pelas empresas, a depender das circunstâncias aplicáveis, e são reconhecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD). Embora as implicações das operações sejam diferentes para as empresas, a eliminação implica na exclusão total dos dados pessoais tratados, sem retenção de qualquer informação relacionada, enquanto a anonimização preserva dados que podem ser usados para outros propósitos, mas sem vínculo com o titular original. A alternativa da anonimização está em consonância com o artigo 16 da LGPD, além de satisfazer os objetivos do titular. Ainda, a anonimização pode ser adotada alternativamente nos casos em que houver dificuldades operacionais de eliminação dos dados pessoais tratados. ";"615518": "[CLARO BRASIL] Caso o titular se oponha ao tratamento de dados realizado com base em uma das hipóteses de dispensa de consentimento, e essa oposição seja considerada legítima, o controlador deverá interromper a operação de tratamento, a menos que consiga justificá-la com base em outra fundamentação legal. No entanto, mesmo diante da possibilidade de que a oposição legítima estaria fundada em tratamento de dados em descumprimento da LGPD, isso não deveria, por si só, configurar infração para fins de aplicação de sanções administrativas perante a ANPD. Isso porque o nível de exigência, comprovação e apuração deve ser mais elevado, devendo ser respeitado o trâmite de apuração da ocorrência garantindo a ampla defesa do agente de tratamento. ";"615523": "[CLARO BRASIL] Não necessariamente. Cada situação é única pois, embora os controladores tenham a obrigação de excluir os dados tratados com base no consentimento, a própria LGPD traz o direito de exclusão separado do direito de revogação. Em certos casos, portanto, o controlador poderá continuar tratando os mesmos dados pessoais com base em outra hipótese legal, especialmente quando se tratar de conjunto de dados que são tratados para diferentes finalidades legítimas e amparadas pela lei. Nesse sentido, para que os dados pessoais sejam eliminados após a revogação do consentimento, o titular dos dados deve fazer uma solicitação

específica para a eliminação, conforme o art. 18, VI, da LGPD. ","615521":"[CLARO BRASIL] Como regra geral, se o consentimento for revogado, todas as operações de tratamento de dados que eram baseadas nele e ocorreram antes de sua retirada permanecem legais; no entanto, o controlador deve interromper as ações de tratamento futuras. Se não houver outra base legal que justifique o tratamento (para outras finalidades ou que justifiquem o armazenamento), eles devem ser excluídos ou anonimizados pelo controlador. - ","615617":"[CLARO BRASIL] A decisão automatizada abrange diversos processos operados automaticamente, nos quais não há envolvimento humano no processo de tomada de decisão. ","615618":"- ","615619":"[CLARO BRASIL] A transparência pode ser desafiadora na revisão de decisões que afetam os titulares dos dados, especialmente quando essas decisões são baseadas em algoritmos complexos. Explicar esses algoritmos de maneira compreensível para os titulares dos dados, sem comprometer informações sigilosas e segredos de negócio são um desafio, e manter a transparência requer esforço contínuo à medida que os algoritmos evoluem e são atualizados. Nesse sentido, temos a opacidade algorítmica e a dificuldade de explicabilidade como desafios enfrentados pelos agentes de tratamento. Para empresas que tratam um grande volume de dados e possuem processos complexos de tomada de decisão automatizada, como também a participação de diferentes agentes, torna difícil identificar e explicar como uma decisão foi tomada e quais dados foram considerados. Garantir que os pedidos de revisão sejam tratados dentro de prazo razoável, conforme estabelecido pela LGPD, pode ser outro grande desafio, especialmente para empresas que recebem um grande volume de solicitações. ","615620":"[CLARO BRASIL] Sim, o controlador pode negar o direito de revisão sobre decisões automatizadas nas seguintes hipóteses: i. a revisão da decisão automatizada implica no comprometimento de segredo comercial e/ou industrial do controlador; ii. quando a revisão manual de decisões automatizadas seja tecnicamente ou praticamente inviável devido à complexidade ou ao volume dos processos de decisão. iii. as decisões automatizadas não impactam de forma significativa os direitos do titular Ainda, existe a possibilidade de fundamentação, pelo controlador, de que as decisões que foram tomadas com base em tratamento automatizado com intervenção humana determinante para o resultado não se enquadrariam estritamente na definição de decisões automatizadas. "

{ "615450": "Contribuição Zetta (CNPJ 37.253.906/0001-28): A Lei nº 12.527/2011 (LAI) prevê que o pedido de acesso à informação deve ser atendido imediatamente ou, sendo impossível atendê-lo nesse prazo, em até 20 dias da solicitação, prorrogáveis por mais 10 dias mediante justificativa (art.11). Contudo, os prazos da LAI são elaborados tendo em vista apenas direitos informacionais. Na LGPD, seriam direitos informacionais a confirmação da existência de tratamento (art.18,I), acesso aos dados (art.18,II) ou o direito de acesso facilitado a informações do tratamento de dados (art.9º). Ocorre que a LGPD prevê uma gama muito maior de direitos, muitos dos quais demandam a análise de uma equipe especializada para serem atendidos de acordo com os princípios da lei. Por exemplo: na necessidade de verificar a identidade do titular antes de proceder com o atendimento da solicitação; na análise de pedidos de bloqueio, anonimização ou deleção de dados, as empresas deverão analisar todas as obrigações legais e regulatórias de retenção de dados e fazer uma busca por todos os locais de armazenamento antes de executar ações. É uma atividade que envolve também vários esforços técnicos para viabilizar o efetivo atendimento dos direitos (e.g. realizar uma deleção segura dos dados pessoais indicados pelo titular). Além disso, é comum que empresas de pequeno ou médio porte recebam dezenas de pedidos de titulares de direitos todas as semanas, que demandam a mobilização de diferentes equipes internas para sua execução. Dada a complexidade particular apresentada pelas demandas previstas na LGPD, acreditamos que o prazo de 30 dias úteis para resposta, com prorrogação de 30 dias úteis mediante justificativa, é adequado para o atendimento aos direitos de titulares, no geral. Há ainda o caso de direitos mais complexos de serem implementados na prática, como a revisão de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais. A depender da estrutura do controlador, esse tipo de providência exige implementações de ordem técnica mais complexas, sendo impossível sua execução imediata.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "Contribuição Zetta (CNPJ 37.253.906/0001-28): No caso de solicitações de deleção, anonimização ou bloqueio de dados: (i) para dados tratados em interesse legítimo da empresa, quando oportuno, ou consentimento do titular, em até 15 dias; (ii) para os demais, em até 30 dias. Estes prazos auxiliam as equipes a conduzir a análise de quais dados deverão ser mantidos devido a obrigação legal e regulatória da empresa, e a empreender os esforços técnicos necessários para efetivar de maneira adequada a solicitação feita pelo titular. Os prazos propostos também contemplam a possibilidade de o titular se arrepender e cancelar a solicitação de exclusão dos dados antes que ela ocorra. Ademais, ainda que se trate de dados pessoais tratados com base no interesse legítimo do controlador ou de terceiro, é importante destacar que nem sempre as informações podem ou devem ser deletadas após a oposição do titular, podendo o agente de tratamento adotar medidas como controle de acessos ou outras técnicas menos onerosas. É importante destacar que as entidades reguladas pelos órgãos supervisores do Sistema Financeiro Nacional possuem um conjunto especializado de regras de retenção de dados pessoais com o objetivo de garantir a segurança e higidez do sistema financeiro. Citamos, por exemplo, regras de prevenção e combate à fraudes, à lavagem de dinheiro e ao financiamento de atividades terroristas.", "615484": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Entendemos que tanto sistemas de gestão de privacidade, padrões de mercado quanto o e-mail (cabendo ao controlador a escolha do canal mais adequado, de acordo com as suas características) são canais de atendimento efetivos para a

comunicação com o titular de dados e facilitam o registro e controle das demandas pelos controladores, considerando a necessidade de validação de identidade, registro das datas de recebimento e mecanismos de controle de prazos de resposta.";"615485": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim. Ainda que atuando de acordo com as instruções do controlador em relação ao tratamento de dados pessoais, os operadores de dados frequentemente são incumbidos com diversas decisões relacionadas ao tratamento, tais como: (i) os procedimentos de manuseio interno dos dados; (ii) a infraestrutura de segurança cibernética que protegerá os dados; (iii) os métodos de armazenamento; (iv) o compartilhamento de responsabilidades para a resposta a incidentes de segurança com os dados pessoais etc. Grande parte dessas decisões não são especificamente escolhidas pelo controlador no momento de assinatura do contrato, mas fazem parte do padrão de serviço oferecido por determinado prestador que atuará como operador de dados. Em muitos casos, o controlador está submetido às regras definidas por operadores em nível global, com padrões inflexíveis que impedem uma ingerência efetiva nas práticas de tratamento de dados de operadores. Nesse sentido, o operador deverá responder não somente por violações às instruções do controlador mas, como determina a lei, por violações à própria LGPD ocasionando dano aos titulares. Além disso, não se trata de responsabilidade solidária, na qual o operador poderia exercer direito de regresso contra o controlador de dados, mas cabe em uma hipótese regular de responsabilidade civil, respondendo o operador por danos que ele próprio ocasionou. Os operadores também precisam agir de maneira proativa e prestativa para auxiliar o controlador no atendimento dos direitos dos titulares direcionando o titular para o canal de comunicação adequado quando aplicável, prestando todas as informações necessárias dentro do prazo acordado em contrato e mantendo registros das atividades de tratamento de dados pessoais.";"615486": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Entendemos que é inviável e prejudicial implementar diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor. Inicialmente, pelo fato de que, para atender aos direitos dos titulares, é necessário validar a identidade do titular, manter o registro dos atendimentos, dentre outras medidas mais onerosas e que não se mostram compatíveis com a exigência de atendimento telefônico previstos na Lei do SAC. Além disso, titulares de dados pessoais que pleiteiam os seus direitos junto aos controladores não necessariamente são consumidores, o que, portanto, afasta a necessidade de reconhecimento da vulnerabilidade do consumidor no mercado de consumo. Assim, entendemos que o e-mail e/ou sistemas de gestão de privacidade padrões de mercado são as formas mais adequadas para atendimento dos direitos dos titulares.";"615487": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Não. Entendemos que e-mail e/ou sistemas de gestão de privacidade padrões de mercado são os canais mais adequados. Tratam-se de modelos adotados em jurisdições nas quais a regulamentação do tratamento de dados pessoais se encontra em estágios mais maduros, e que demonstram eficácia e permanência (a exemplo dos países europeus). Sublinhamos a importância de que o agente de tratamento escolha a forma como se dará o atendimento, especialmente face à realidade de empresas totalmente digitais que não possuem atendimento físico. Portanto, deve-se garantir segurança jurídica na regulação para que o uso de canais inteiramente digitais seja autorizado como prática garantida.";"615491": "Contribuição Zetta (CNPJ 37.253.906/0001-28): 1. No caso de crianças e adolescentes, é necessário que a ANPD estabeleça critérios específicos e objetivos para o compartilhamento de dados e atendimento de direitos por meio dos responsáveis legais. Entendemos que a obtenção do consentimento dos pais para o tratamento de dados se aplica exclusivamente às crianças (menor de 12 anos), tornando razoável que o controlador atenda às solicitações do responsável

legal em relação aos direitos de uma criança titular dos dados. Já para os adolescentes (entre 18 e 13 anos), qualquer solicitação de titularidade feita por um responsável legal deve ser rejeitada, visando preservar a privacidade do titular. Assim, a confirmação da existência de tratamento de dados também deve ser negada quando solicitada pelo responsável legal buscando agir em nome do adolescente titular dos dados. Deve ser considerada pela ANPD, a existência de legislações e normas de sigilo bancário (LC 105/01), que impedem a exposição de dados pessoais financeiros a terceiros e que submetem em obrigações as entidades do setor financeiro.

2. No caso de recebimento de informações sobre suspeita de fraude (Resolução Conjunta CMN BCB nº 6/23) e de outros atos ilícitos, principalmente em setores regulados (como informações sobre listas restritivas nacionais e internacionais), entendemos que não é adequado que as instituições receptoras das informações tenham a obrigação de confirmar a existência de tratamento deste tipo de dado para os titulares.

3. No caso em que o direito de acesso é solicitado por terceiros (ex: autoridade policial; advogado), sem outorga de poderes específicos para agir em nome do titular, seria importante a definição dos requisitos formais que os controladores devem observar nos casos de pedidos feitos por terceiros em nome do titular.

4. No caso em que o atendimento ao direito de confirmação da existência do tratamento envolve uma comunicação que seja comprovadamente impossível ou implique esforço desproporcional, a ANPD pode estabelecer parâmetros exemplificativos para delimitar essas situações.

"615492": "Contribuição Zetta (CNPJ 37.253.906/0001-28): CNPJ, razão social, nome fantasia, endereço e contato do encarregado. Esperamos esclarecimento da ANPD sobre o termo “uso compartilhado de dados”, especificando se aplicado a qualquer comunicação de dados (ex.: com operadores de dados, parceiros comerciais, provedores de software de comunicação interna nas empresas, etc). Sugerimos que o regulamento considere categorias diferenciadas de co-controladores de dados para estabelecer os tipos de informação a serem obrigatoriamente divulgados aos titulares. A disponibilização de dados gerais sobre a existência e função dos co-controladores na Política de Privacidade é adequada como medida de conformidade geral, tendo o titular o direito de solicitar informações específicas sobre cada co-controlador ao Encarregado. Antes de serem atendidos, esses pedidos deverão ser analisados pela equipe jurídica de cada empresa para averiguar se o compartilhamento de informações sobre parceiros configura violação de segredo comercial. Também no caso de operadores, o excesso de informações a respeito de provedores de softwares, serviços de computação em nuvem, infraestrutura e sistemas de TI em geral poderá comprometer a segurança cibernética do controlador. Sem contar o fato de que um compartilhamento excessivo de dados de terceiros com os quais os dados são compartilhados podem prejudicar o controlador em aspectos concorrenciais. Nesses casos, recomendamos a disponibilização de informações genéricas e, se houver pedidos de informação específicos, estes poderão ser analisados pelas equipes de Segurança Cibernética e Proteção de Dados Pessoais de cada empresa. Divulgar nominalmente os outros agentes envolvidos no uso compartilhado de dados gera riscos ao segredo comercial, à concorrência e a obrigações de sigilo/confidencialidade que os controladores têm em determinadas parcerias. A alternativa para suprir essa eventual lacuna de informação mais específica para o titular é considerar a divulgação nominal apenas em casos excepcionais, como incidentes que resultem em risco ou dano relevante."

"615489": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Os operadores precisam agir de maneira prestativa para auxiliar o controlador no atendimento dos direitos dos titulares, direcionando o titular para o canal de comunicação adequado quando aplicável, prestando todas as informações necessárias dentro do prazo acordado em contrato e mantendo registros das atividades de tratamento de dados pessoais. O operador de

dados, que administra diretamente os dados dos titulares no dia-a-dia, deve comprometer-se com a prestação de todas as informações solicitadas pelos controladores em prazo adequado e que torne possível ao controlador observar os prazos legais definidos, de forma a viabilizar a análise das informações a serem comunicadas pelo controlador em prazo razoável. A possibilidade de resposta direta pelos operadores e os parâmetros para tal resposta devem constar de disposições contratuais entre as partes.";"615490": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Confirmação de existência de tratamento de dados do titular, e dados básicos de registro ou de cadastro que possam ser buscados de forma rápida, permitindo que a declaração seja entregue imediatamente. Informações detalhadas, que exijam consultas a diferentes fontes e ambientes de dados, devem ser entregues no relatório do Art. 19, II.";"615494": "Contribuição Zetta (CNPJ 37.253.906/0001-28): As informações mínimas que constam das políticas de privacidade dos controladores e que evidenciam, de maneira ampla, quais são os dados básicos tratados pela instituição, e todas as informações contidas no artigo 9º da LGPD, de maneira genérica (ex.: indicação dos tipos de agentes envolvidos no tratamento, sem mencioná-los nominalmente, tais como “fornecedores de software”, “bureaus de crédito”, etc.).";"615493": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim. O direito de acesso deve ser atendido por meio de disponibilização de cópia digital ou física de listagem dos dados tratados, para evitar qualquer comprometimento dos sistemas de tratamento de dados empregados pelo controlador e seus operadores. O controlador deve ter a liberdade de decidir o formato ideal para atender o direito de acesso, considerando o meio e forma em que os dados pessoais do titular foram coletados. Isto é, se os dados foram obtidos via meios digitais, entende-se que o controlador poderá atender o direito de acesso fornecendo cópia digital dos dados do titular, dispensando-se a necessidade de cópia física. Além disso, o formato digital consta como mais alinhado à realidade da maior parte dos controladores.";"615502": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Setor financeiro, a exemplo da estrutura do Open Finance.";"615501": "Contribuição Zetta (CNPJ 37.253.906/0001-28): A padronização da estrutura e a utilização dos mesmos protocolos de transferência entre os agentes seria o maior desafio. Eventual padrão de interoperabilidade deverá respeitar arranjos já estabelecidos nos setores regulados, como Open Finance, portabilidade de investimentos, entre outros, para evitar esforços extras de adequação para algo que já existe.";"615505": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Padronização de APIs entre sistemas, quais tipos de dados pessoais a nível de atributo devem ser objeto de portabilidade, prazos para envio e recebimento, nível de qualidade do dado, jornada de usuário, seguindo o modelo do Open Finance, por exemplo. Entendemos, contudo, que a fixação de padrões extremamente rígidos pode ser negativa diante do rápido avanço tecnológico e do risco de obsolescência dos padrões fixados.";"615503": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim. O padrão de interoperabilidade deve ser atendido quando são comunicados dados de uma instituição à instituição apontada pelo titular de maneira estruturada, sendo os dados necessários exclusivamente aqueles tratados pela instituição original com base legal na execução de contrato com o titular (dados tratados por consentimento, legítimo interesse e demais bases legais deverão ser obtidos pelo novo controlador de dados, responsável por garantir a legitimidade da base legal para tratamento). Trata-se de medida que se faz suficiente, especialmente considerando a ausência de regulamentação específica acerca da interoperabilidade.";"615504": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim. Os prazos de interoperabilidade devem considerar o tempo de disponibilização das informações à nova instituição a partir da solicitação do titular (15 dias), um prazo para confirmação de recebimento da instituição receptora à instituição original (7 dias) e a possibilidade de

prorrogação dos mesmos prazos em caso de ausência de confirmação de recebimento.";"615511": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Entendemos que o titular deve ser o responsável por alimentar/atualizar seu cadastro a fim de que os produtos e serviços financeiros partam de premissas corretas. Em casos de retificação de identidade de gênero, deverá ser apresentado documento de identidade oficial retificado para alteração de dados de gênero e nome social (enquanto houver obrigação imposta pelo BACEN para que tal alteração seja realizada apenas mediante processo judicial de retificação concluído). A correção dos dados tampouco deverá ser atendida quando solicitada por responsável legal de menores de idade entre os 13 e 18 anos, para garantir a proteção dos dados pessoais e da privacidade dos adolescentes. "; "615514": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Nos casos em que o titular não apresente documentos válidos ou caso o controlador esteja atrelado a cumprimento de obrigação regulatória (ex: fraude que a instituição financeira precisa manter registro no sistema para obedecer disposições do Bacen). Quando o titular dos dados for uma criança (menor de 13 anos) as solicitações de direito, inclusive correção de dados, deverão ser acompanhadas de documentos comprovando (i) a identidade da criança; (ii) a identidade do responsável legal; e (iii) o vínculo jurídico entre ambos (relação de tutela). Além disso, a ANPD deverá se pronunciar sobre a possibilidade de atendimento de direitos de titular solicitados por responsável/representante legal, especialmente no caso de crianças e adolescentes. "; "615513": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Devem ser considerados critérios como o porte do controlador, o volume de solicitações recebidas, os quais variam de acordo com o caso concreto a ser observado. "; "615512": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Nos casos em que o titular não apresente documentos válidos ou que o pedido seja incompatível com o documento ou com o ordenamento jurídico, ou caso o controlador esteja atrelado a cumprimento de obrigação regulatória (ex: fraude que a instituição financeira precisa manter registro no sistema para obedecer disposições do Bacen). "; "615517": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim, tendo em vista que o controlador pode estar tratando os dados do titular com uma base legal válida e o titular não tenha uma lesão a direito e liberdade fundamental violada apta a interromper o tratamento via bloqueio ou oposição ou anonimização. "; "615516": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Sim, em situações específicas pode ser que a anonimização atinja a mesma finalidade que a eliminação sem prejudicar as atividades do controlador que utiliza os insights para promoção de suas atividades. Para efeitos de proteção dos dados e privacidade dos titulares, a anonimização feita corretamente e com baixo risco de reidentificação avaliado pela empresa equivale a uma deleção completa dos dados, sem nenhuma possibilidade de prejuízo ao titular. Entretanto, eliminar ao invés de anonimizar pode ser inviável considerando as obrigações legais/regulatórias das instituições reguladas pelo Bacen. "; "615518": "Contribuição Zetta (CNPJ 37.253.906/0001-28): O efeito deverá ser a deleção ou anonimização dos dados, conforme os parâmetros de término de tratamento dos dados do art. 16. "; "615523": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Pensando em um cenário regulado, a revogação de consentimento poderia conflitar com obrigações de manter registro de atividades para a prevenção à fraude, lavagem de dinheiro, combate à corrupção e demais imposições dos reguladores do sistema financeiro, conforme os parâmetros de término de tratamento dos dados do art. 16. "; "615521": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Pensando em um cenário regulado, a revogação de consentimento poderia conflitar com obrigações legais e/ou regulatórias aplicáveis ao controlador (e.g., manter registro de atividades para a prevenção à fraude, lavagem de dinheiro, combate à corrupção e demais imposições dos reguladores do sistema financeiro). "; "615617": "Contribuição Zetta (CNPJ 37.253.906/0001-

28): Uma decisão tomada unicamente com base em tratamento automatizado é aquela na qual não há participação humana no processo de tomada de decisão. Isso implica que a decisão é completamente gerada por meio de processamento automatizado, sem qualquer intervenção ou influência direta de indivíduos ou normas de reguladores. Assim, uma decisão de crédito realizada por uma instituição financeira ou assemelhadas (SCFI, IPs etc.), baseada em um modelo de risco de inadimplemento de obrigações financeiras, não deve ser considerada uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais, eis que o modelo apenas executa uma política de crédito definida em comitês especializados das organizações. Essas políticas de crédito estão em seus fundamentos vinculadas a princípios e regras de natureza prudencial definidas pelos órgãos normatizadores e supervisores do sistema financeiro. Portanto, além da existência de uma política, debatida e aprovada em instâncias humanas, há também controle social por meio de regras de direito público e financeiro. Portanto, modelos de gestão de risco de crédito de instituições financeiras e assemelhadas não devem ser compreendidos como decisões tomadas unicamente com base em tratamento automatizado de dados pessoais."

615618": "Contribuição Zetta (CNPJ 37.253.906/0001-28): Os interesses dos titulares devem ser considerados como afetados quando (i) uma interação com o titular é gerada a partir da decisão automatizada; ou (ii) uma faculdade do titular é afetada (criada ou excluída) devido à sua categorização por sistema automatizado. Exemplos do resultado (ii) incluem: aprovação de cadastro, aprovação de crédito, publicidade direcionada, precificação dinâmica, comunicações a autoridades sobre suspeita de fraude, monitoramento de cibersegurança, etc., em que a categorização do titular por meio de decisão automatizada resulta em uma ação com potencial de afetar as escolhas, oportunidades e proibições apresentadas ao titular. Os meios de organização da informação, para o controlador, que não geram nenhuma dessas duas hipóteses não devem ser considerados como uma decisão automatizada que afeta os interesses do titular (ex.: redirecionamento de conteúdo dos chats de atendimento ao cliente para diferentes canais de comunicação internos da empresa, para viabilizar os processos de atendimento ao cliente, contanto que garantidos os padrões mínimos de segurança explicitados pelo controlador em sua Política de Privacidade). Ademais, importante ressaltar que decisões sobre risco de crédito realizadas por intermediadores de recursos financeiros são decisões semi-automatizadas, haja vista que o modelo de score apenas executa uma política de crédito que, por sua vez, está lastreada em princípios e regras de natureza prudencial do Sistema Financeiro. Portanto, modelos de gestão de risco de crédito de instituições financeiras e assemelhadas não devem ser compreendidos como decisões tomadas unicamente com base em tratamento automatizado de dados pessoais."

615619": "Contribuição Zetta (CNPJ 37.253.906/0001-28): A ANPD deve especificar em que consiste a revisão assegurada pelo art. 20. Caso seja necessário implementar revisão humana sobre a decisão, como assegurado pelo GDPR, isso deve ser explicitamente definido em regulação. Caso contrário, os parâmetros para uma "decisão revisada" devem ser delineados (por exemplo, com apontamento de que o sistema para revisão deve ser diferente daquele utilizado para a primeira tomada de decisão). Ademais, importante ressaltar que decisões sobre risco de crédito realizadas por intermediadores de recursos financeiros são decisões semi-automatizadas, haja vista que o modelo de score apenas executa uma política de crédito que, por sua vez, está lastreada em princípios e regras de natureza prudencial do Sistema Financeiro. Portanto, modelos de gestão de risco de crédito de instituições financeiras e assemelhadas não devem ser compreendidos como decisões tomadas unicamente com base em tratamento automatizado de dados pessoais."

615620": "Contribuição Zetta (CNPJ 37.253.906/0001-28): O controlador poderá

negar o direito à revisão quando: (i) a decisão não tiver efeito relevante sobre os interesses dos titulares (conforme parâmetro acima); ou (ii) a revisão exigir esforços desproporcionais do controlador, sendo facultada ao titular a solicitação de eliminação dos dados. Ademais, importante ressaltar que decisões sobre risco de crédito realizadas por intermediadores de recursos financeiros são decisões semi-automatizadas, haja vista que o modelo de score apenas executa uma política de crédito que, por sua vez, está lastreada em princípios e regras de natureza prudencial do Sistema Financeiro. Portanto, modelos de gestão de risco de crédito de instituições financeiras e assemelhadas não devem ser compreendidos como decisões tomadas unicamente com base em tratamento automatizado de dados pessoais."

{"615450": "A Lei 12.527/11 dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, não sendo abordado na norma em comento acerca dos demais direitos que temos assegurados pela LGPD, portanto, não se vislumbrando assertiva adoção deste prazo em situação que não se limita ao acesso de informações, vez que o Controlador deverá atender também requisições por exemplo com pedido de retificação de dados na base da companhia, exclusão e revogação de consentimento, podendo-se tornar-se inviável a operacionalização de todos direitos com prazo de 20 dias apenas e trazer impacto em vários setores da economia, diante de custos para implementação de ferramentas que proporcionem automação de processos internos. Desta forma, tem-se que seria prudente seguir como parâmetro os prazos estabelecidos no GDPR e o GPDR da UK, sendo 30 (trinta) dias corridos para cumprimento do atendimento aos direitos dos titulares, podendo ser prorrogado de forma justificada por até dois meses, dependendo da complexidade, sendo a contagem nos termos do GDPR da UK a partir da confirmação da identidade do solicitante (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/>), considerando que o Controlador tem o dever de adotar medidas técnicas e administrativas de governança corporativa e assegurar a proteção de dados (Art. 50 da LGPD).", "b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?": "Pode-se ter como critério de consideração para impor uma resposta imediata ao Controlador a identificação se este possui viabilidade de automação para verificação de dados na base, se o Controlador possui mais de uma base de dados ou bases descentralizadas, bem como se possui mais de um setor ou segmento de atuação e se os dados estão todos em formato digital, sopesando que a localização de dados de forma manual em locais físicos demanda maior esforço e não seria possível levar uma devolutiva de imediato ao Titular nesta hipótese. Deve ser levado em consideração a razoabilidade do esforço para atendimento às solicitações dos titulares. O atendimento às solicitações envolve um trabalho interno pelo controlador que não é nada simples. São levantamentos internos e busca pelos dados inseridos em diversos locais (físicos e lógicos), que demandam verificação e análise para somente então ser possível responder o titular. Reforço que no GDPR há prazo de um mês, prorrogável por até dois meses a depender da complexidade (art. 12º, 3.). Caso a ANPD venha a considerar como prazo geral 15 dias para resposta, que este prazo seja contado em dias úteis, com início apenas a partir da identificação do solicitante.", "615484": "Identifica-se no dia a dia que o canal de atendimento se torna mais efetivo se estiver publicado em local de fácil visualização ao titular, bem como se for centralizado, ou seja, um único canal para tanto. Em várias situações, disponibilizar um canal de atendimento e depois direcionar para outra ferramenta ou outra central de atendimento poderia dificultar acesso ao titular, mormente, prudente que haja características de acessibilidade, pensando igualmente em políticas de inclusão e centralização do canal a ser disponibilizado ao Titular. Com isso, não é razoável exigir de todos os agentes de tratamento, em especial os de pequeno porte, que não possuam recursos ou que mantenham um padrão de atendimento presencial de seus titulares, por exemplo, a existência de um canal de atendimento a nível de uma grande empresa, que inclusive faça uso de soluções que automatizem o atendimento e que haja integração entre sistemas. Assim, deve haver, no mínimo, um canal de recebimento de solicitações devidamente publicizado e de

fácil acesso aos titulares, tal qual a indicação de e-mail ou disponibilização, no site institucional do controlador, de portal ou formulário para preenchimento pelo titular solicitante. Poderá também haver o recebimento de solicitações de titulares em via física, em estabelecimento próprio ou recebido por correios. Outro ponto relevante a ser estabelecido é a necessidade de confirmação da identidade do solicitante, seja o titular ou seu representante legalmente constituído, sob risco de acesso indevido a dados pessoais por terceiros não autorizados. ","615485": "Veamos que o Art. 18, caput, da LGPD, dispõe acerca de direitos do titular perante o Controlador, que possui por sua vez a responsabilidade de observar o efetivo cumprimento destes direitos, não se vislumbrando que o Operador possui responsabilidade direta perante os titulares, contudo, tem-se uma responsabilidade solidária nos termos do Art. 42 da LGPD, devendo cooperar sob o princípio pacta sunt servanda, ou seja, nos limites estabelecidos contratualmente entre as partes (operador e controlador). Assim, por exemplo, caso um operador receba uma solicitação de titular, deverá ele indicar ao titular o canal correto e, ao mesmo tempo, informar ao controlador da solicitação. Por parte da ANPD, entendo que isso deveria vir como uma orientação/sugestão de boa prática aos agentes regulados, mas não por meio da criação de nova obrigação legal. ","615486": "Veamos que o Decreto nº 11.034 de 2022, regulamenta a Lei nº 8.078/1990 - Código de Defesa do Consumidor, para estabelecer diretrizes e normas sobre o Serviço de Atendimento ao Consumidor - SAC, no âmbito dos fornecedores dos serviços regulados pelo Poder Executivo federal, diferentemente do escopo da LGPD que se aplica para todas as instituições com e sem fins lucrativos que tratam dados pessoais, não sendo razoável, portanto, que seja exigida as mesmas diretrizes de forma análoga. Por outro lado, plausível considerar como diretrizes a acessibilidade para todos cidadãos e disponibilidade de forma facilitada do canal de atendimento aos titulares, com fim que a efetividade do exercício dos direitos dos titulares não impacte de forma desproporcional para economia frente as imposições legais. Em relação a maioria de agentes de tratamento de pequeno porte, o que inclusive motivou a existência de um regime jurídico diferenciado na Resolução CD/ANPD nº 2, tornaria inviável, por questões de complexidade técnica, operacional e de investimento, a adoção do Decreto como parâmetro geral. Assim, vindouras diretrizes e procedimentos a serem estabelecidos pela ANPD devem considerar a situação concreta do país e dos agentes regulados. Como exemplos de inviabilidade do Decreto aos agentes regulados em geral, cite-se, a obrigatoriedade de atendimento telefônico e suas exigências (arts. 4º, §2º, 5º e 11), prazo exíguo (art. 13) e acompanhamento por regulador (art. 15). ","615487": "Algumas empresas instituem um Portal de Privacidade que deixa claro ao titular o seu canal de atendimento, bem como fica visível um formulário para realização da solicitação e a Autoridade da França CNIL (Commission nationale de l'informatique et des libertés), possui um canal de atendimento centralizado no mesmo sentido (<https://cnil.fr/fr/webform/contactez-le-delegue-la-protection-des-donnees-dpo>), contudo, não há um padrão de atendimento que poderia ser adotado por todos setores privados ou pelo setor público de forma igualitária, recomendado manter a liberdade de operacionalização do canal de atendimento pelo Controlador, observando o setor de atuação e peculiaridades das categorias de titulares que possuem como público alvo do negócio. ","615491": "O GPDR no Art. 12, possibilita ao Controlador recusar-se a atender a requisição do titular na hipótese dos pedidos do titular dos dados forem manifestamente infundados ou excessivos, com caráter repetitivo. Assim, poderia ser possível ao Controlador a negativa caso o direito esteja sendo exercido de forma abusiva pelo titular, a exemplo da mesma solicitação reiterada em curto período. Entendo, contudo, que este deveria ser um critério para os demais direitos também, não restrito apenas ao direito de confirmação da

existência do tratamento. Ainda, o ICO atualizou seu “Subject Access Code of Practice” para demonstrar que o Controlador poderá recusar-se a atender a requisição se esta for manifestamente infundada ou excessiva. Em contrapartida, a impossibilidade de atendimento está prevista no texto legal da própria LGPD em seu art. 18, § 4º, nos cenários em que o requerido não é o agente de tratamento na operação suscitada ou haja a indicação de razões de fato ou de direito que impedem a adoção imediata das providências (incisos I e II do art. 18, § 4º da LGPD). Igualmente, é relevante mencionar que a Lei nº 10.406/2002 (“Código Civil”) em seu art. 187 dispõe que “também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes”. Desta forma, há de se suscitar que este critério também deve ser aplicável aos demais direitos. “615492”: “Os artigos 9º, II; 18º, V; 19º II; §3º; e 20º, §1º, todos da LGPD, possuem disposição expressa de salvaguarda aos segredos comerciais diante do exercício dos direitos dos Titulares de Dados, permitindo-se por interpretação literal da norma, que o legislador se preocupou com a proteção desses direitos, conferindo aplicação dos princípios contemplados no art. 6º, contudo, em harmonia com o direito da empresa/controlador ter preservado as informações essenciais e vinculadas ao próprio negócio, vez que se expostas permitiriam até mesmo a concorrência desleal no setor em que a empresa eventualmente se insere. Neste sentido, devem ser fornecidos aos titulares informações apenas quanto a nomenclatura dos controladores envolvidos na operação que não afronte o segredo comercial e industrial. “615489”: “Conforme exposto no bloco anterior, temos que o Art. 18, caput, da LGPD, dispõe acerca de direitos do titular perante o Controlador, que possui por sua vez a responsabilidade de observar o efetivo cumprimento destes direitos, não se conjecturando responsabilidade diretamente em prima face perante os titulares por parte do Operador, contudo, tem-se uma responsabilidade solidária nos termos do Art. 42 da LGPD, devendo cooperar sob o princípio pacta sunt servanda, ou seja, nos limites estabelecidos contratualmente entre as partes (operador e controlador). Outrossim, em virtude do princípio de cooperação, o operador deve informar ao titular acerca do canal de atendimento das requisições do controlador responsável pelo tratamento para que possa ser direcionado a solicitação pelo próprio titular. “615490”: “Considerando o caput do artigo 19, que se refere aos direitos de confirmação da existência de tratamento ou acesso a dados pessoais, entendendo-se que a declaração em formato simplificado deva se limitar apenas à confirmação do tratamento, afirmando-se se há ou não, após confirmação da identidade pelo titular Ainda assim, deve ser considerada a proporcionalidade e razoabilidade no atendimento a este direito pelo controlador, considerando seus efeitos práticos, tal como o esforço que é exigido do controlador para realizar o levantamento das informações necessárias para a resposta. Em não sendo um controlador que conte com meios automatizados de verificação dos dados do titular solicitante, tal como nos casos em que o controlador preste serviços de modo online e que consiga permitir este acesso imediato, a exemplo de aplicativos que disponham de perfis do titular que já é cliente, não é razoável e proporcional tal exigência. Na prática pode ser impossível que o controlador consiga responder ao titular de forma imediata. Diante disto, entende-se necessário que a ANPD estabeleça limites a esta exigência, devendo haver a previsão das situações em que não será exigida a resposta imediata.” 615494”: “A transparência e o direito à informação pressupõem a existência de conhecimento prévio das finalidades do tratamento, motivo pelo qual o controlador nos termos do Art. 6º da LGPD, deve dar ciência se utiliza procedimentos para tomadas de decisões automatizadas, com informações claras se solicitado pelo titular sobre os critérios utilizados para tanto, podendo ser evidenciado e apresentado pelo controlador quando solicitado pela ANPD,

em razão de accountability, os procedimentos matemáticos ou estatísticos utilizados, implementação de medidas técnicas e organizacionais para garantir que os fatores que eventualmente resultem em imprecisões nos dados pessoais sejam corrigidos e medidas de mitigação de riscos implementadas, conforme disposto no Considerando 71 do GDPR, observados os segredos de negócio do Controlador.";"615493": "Sopesando que a LAI (Lei 12.527/11) no Art. 7º, II, menciona que o acesso à informação compreende informação contida em registros ou documentos, pode-se ter por satisfeito o direito de acesso ao Titular quando lhe for disponibilizado dados pessoais para conhecimento, seja em formato digital ou físico.";"615502": "Considerando que tal termo é usualmente já aplicado pelo setor de telecomunicações e o setor financeiro permite igualmente portabilidade de operações financeiras e a existência do openbank, nestes setores poderia haver implementação ao direito a portabilidade, bem como o setor securitário demonstra igualmente maturidade para implementação inicial do direito a portabilidade. ";"615501": "Haja vista que interoperabilidade se refere a possibilidade de interação de diversos sistemas para compartilhamento de informações o Decreto 10.046/19 disciplinou o processo de compartilhamento de dados necessários à execução de políticas públicas, o que demandou criação de Comitê Central de Dados e processos de categorização. Desta forma, o esforço empregado no âmbito público possibilita visualizar desafios de padronizar regras de interoperabilidade para diversos setores na economia. Contudo, podemos utilizar como parâmetro do cenário do GDPR que possibilitou a transmissão de dados em formato estruturado, que sejam legíveis por diferentes linguagens de programação como JSON ou XML, possibilitando combinar esses dados com conjunto de metadados que facilita a reutilização do conjunto de dados transmitido (<https://cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite>). ";"615505": "Utilizando como parâmetro os critérios aplicados na UE, conforme o GDPR, para portabilidade de dados, o controlador poderá fornecer uma funcionalidade que permite ao titular baixar seus dados por meio de ambiente autenticado e obter em formato padrão legível por computador (JSON, CSV, XML, ODS, etc.) ou disponibilizar por API (Application Programming Interface) segura para que um agente de tratamento que se destina a portabilidade possa ter acesso automaticamente aos dados (<https://cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite>).";"615503": "Pode-se ter por satisfeito o direito à portabilidade quando houver a disponibilização dos dados pelo agente de tratamento em formato que permita a interação e compartilhamento destes para outro agente de tratamento destinatário, na ocasião de requisição do titular. Desta forma, a satisfação do direito à portabilidade independe da obrigatoriedade ou não de o controlador recipiente receber os dados pessoais.";"615504": "Seria razoável e democrático permitir que o setor privado defina os padrões de interoperabilidade específico para suas atividades, visto que as companhias precisarão observar medidas direcionadas para atender suas peculiaridades setoriais, como por exemplo em relação a saúde, educação etc.";"615511": "Tendo em vista que, o Código de Defesa do Consumidor (CDC) no Art. 43, §3º, dispõe que o consumidor pode exigir a correção de dados sempre que encontrar inexatidão nos seus dados, pode-se interpretar como critério objetivo para qualificar a inexatidão ou desatualização dos dados pessoais a ciência ou notificação acompanhado de evidência por parte do titular. Neste sentido, vejamos ainda que o mesmo dispositivo legal o Art. 61, atribui a consumação de crime de menor potencial ofensivo se depois de recebida a solicitação do consumidor ou percebida a inexatidão, não for atualizado ou corrigido o dado no prazo estabelecido no CDC. No que tange à correção em si dos dados tratados, considerando a natureza objetiva, há de se compreender possível erro material no dado pessoal, do qual sua incorreção poderá trazer prejuízos ao titular de dados

pessoais. Para atender o direito suscitado, é suficiente que o titular demonstre de maneira concreta a incorreção do dado pessoal. Por exemplo, um número de CPF incorreto pode ser retificado mediante apresentação de documento de identidade. "615514": "Vejam os que o controlador precisa observar os princípios do Art. 6º da LGPD e dentre estes da accountability, segurança e da prevenção com adoção de medidas que evitem a ocorrência de danos ao titular, mormente, apenas proceder com alteração de dados na base por simples declaração sem a apresentação de evidência comprobatória da identidade do solicitante poderia ocasionar exposição à incidente de segurança. Outrossim, em situações por exemplo de alteração cadastral em contratos bancários que a alteração do dado pessoal tido por incompleto, inexato ou desatualizado pudesse gerar risco ao negócio, a depender do caso, a simples declaração deveria ser evidenciada. Alteração de dados relacionadas à execução de contrato como no caso de um titular solicitar a alteração de endereço de cobrança ou indicar que o número do seu documento está errado. Tal ocorrência merece apresentação de evidências para evitar quaisquer transtornos contratuais ou danos materiais ao próprio titular." 615513: "Definir um critério objetivo a ser considerado para identificar a impossibilidade ou esforço desproporcional para que o responsável informe de forma imediata os agentes de tratamento com quem tenha compartilhado o dado, para que procedam com correção, eliminação, anonimização ou bloqueio de dados, pode não refletir aplicabilidade em todos os setores da iniciativa privada, sendo prudente que haja margem de justificação e comprovação deste pelo próprio agente de tratamento. Considerando ainda que, o termo “esforço desproporcional”, deixa margem interpretativa de ausência de equilíbrio com a situação que lhe fora imposto, bem como uma ação excessiva ou inadequada em relação ao contexto vivenciado. "615512": "Conforme disposto no Guide to the General Data Protection Regulation (GDPR) disponibilizado pela ICO (<https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> p. 150), poderia ser negado o direito de correção pelo Controlador se este for manifestamente excessivo ou infundado, ou seja, se reiteradamente repetitivo o conteúdo de solicitações pedidos já realizadas com intenção de ocasionar esforço desnecessário do Controlador e demais agentes de tratamento envolvidos na operação, bem como não havendo clara intenção de exercício do direito pelo titular ou demonstrado que a solicitação está sendo usada para maliciosamente obter vantagem ilícita do Controlador, sem outro objetivo real. Podendo ser considerado inclusive negativa na hipótese de não haver comprovação da identidade do titular." 615517: "O Código de Defesa do Consumidor permite a inversão do ônus da prova para proteção do consumidor, por ser a parte hipossuficiente em relação a empresa contratada, não sendo plausível atribuir que o titular apresente a comprovação da desnecessidade de seus dados ou existência de excessividade e que são tratados em desconformidade com a legislação, o que demandaria inclusive contraditório em virtude da ampla defesa assegurada na Carta Magna. Todavia, o titular poderia fundamentar sua solicitação apontando as razões que o levam a identificar eventual desconformidade para viabilizar atendimento e resolução adequada ao pedido. Até por isso muitos “portais de privacidade” disponibilizam, além da seleção do direito que o titular pretende exercer, um espaço para que ele descreva a solicitação. Porém, não seria propriamente um ônus do titular, mas poderia ser uma boa prática que o controlador estimulasse a apresentação da fundamentação. Um exemplo prático seria no próprio formulário de solicitação haver um espaço específico destinado à justificativa do titular. Em todo caso, caberá ao controlador verificar se a solicitação procede ou não e justificá-la ao titular. Deste modo, sobretudo por falta de estipulação legal presente no artigo em comento e considerando o fato de que o dado é propriedade estritamente vinculada à

figura do titular, recomendável ao exercer direitos incisivos quanto os elencados não sejam exigidos maiores esforços além da mera solicitação direta, podendo o titular fundamentar sua solicitação apontando as razões que o levam a identificar eventual desconformidade para viabilizar atendimento e resolução adequada ao pedido. "615516": "Enquanto a anonimização e a eliminação são “soluções” definitivas para os dados, pois não haverá mais tratamento de dados pessoais a partir dessas situações, no bloqueio há apenas uma suspensão temporária. No bloqueio, ainda deverá haver alguma definição quanto aos dados pessoais, se eles poderão ainda ser tratados pelo controlador ou não. Entendo que o pedido de bloqueio deverá ser processado pelo controlador até verificar se, de fato, a atividade de tratamento está irregular. Em estando o tratamento em conformidade com a lei, o bloqueio deverá ser levantado e os dados voltariam a serem tratados normalmente pelo controlador. Do contrário, os dados pessoais deverão ser eliminados ou anonimizados. Com isso, outro ponto relevante é se o controlador terá o benefício de escolher se prefere eliminar os dados pessoais ou anonimizá-los. Digo “benefício”, pois na eliminação os dados pessoais simplesmente deixarão de existir para o controlador, de forma definitiva, enquanto na anonimização ele ainda poderá beneficiar-se da inteligência a partir dos dados anonimizados, o que pode ser relevante como subsídio para tomadas de decisão de negócio. Não se verifica benefício direto ao titular ao optar pela anonimização em vez da eliminação. Ao titular, interessa apenas que seus dados deixem de ser tratados, pois até então o estavam sendo em desconformidade com a lei. Por isso, a opção por uma via ou outra faz mais sentido se for atribuída ao controlador. Em optando o controlador pela anonimização dos dados pessoais, contudo, deverá ele garantir que seja efetiva, conforme exige a LGPD, sob pena de infração e não atendimento ao titular. De outro lado, poderá o controlador preferir a eliminação dos dados, seja porque não o interessa realizar o processo de anonimização ou se esta revelar-se inviável ou exigir esforço desproporcional. Isto porque a anonimização requer meios técnicos suficientes para que seja efetiva, o que, considerando o elevado grau de dificuldades técnicas e operacionais, pode ser inviável ou desproporcional ao controlador. "615518": "O Art. 63 da LGPD dispõe que a ANPD estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor da norma, considerando ainda para tanto a complexidade das operações de tratamento e a natureza dos dados. Desta forma, eventuais disposições de efeitos do Art. 18, §2º, da LGPD devem convergir com a regulamentação acerca da adequação progressiva de base legada. Uma solicitação do direito à oposição considerada procedente deverá implicar, na prática, na interrupção do tratamento dos dados pelo controlador em relação à finalidade específica que sofreu a oposição, a exemplo do caso de oposição ao tratamento de dados para recebimento de comunicações de marketing. A consequência prática é que as comunicações de marketing ao titular sejam cessadas. Importa destacar, contudo, que a oposição do titular não afetará as atividades de tratamento dos dados pessoais que tenham outras finalidades, desde que estejam em conformidade com os requisitos legais, tal como a existência de hipótese de tratamento (base legal), conforme artigos 7º ou 11. "615523": "Não, pois a revogação do consentimento e a eliminação dos dados são direitos distintos expressamente previstos na LGPD e suas consequências práticas também são distintas. Além disso, a revogação do consentimento não deverá implicar, necessariamente, na eliminação dos dados pessoais, pois pode haver outra(s) finalidade(s) do tratamento que esteja(m) fundamentada(s) em outra(s) hipótese(s) legal(ais), a exemplo da execução de um contrato ou do cumprimento de obrigação legal ou regulatória. Assim, por exemplo, um controlador pode tratar dados pessoais de um consumidor para a finalidade de execução do contrato mantido com ele e em algum momento houve a obtenção do seu

consentimento para uma nova finalidade, que vai além da execução do contrato. Nesta hipótese, a revogação do consentimento irá atingir apenas o tratamento que tenha a finalidade baseada no próprio consentimento, e não afetará aquele(s) relacionado(s) à execução do contrato e tampouco eventuais obrigações legais e regulatórias decorrentes. O Art. 8, §5º da LGPD dispõe que o consentimento revogado não invalida o tratamento realizado sob amparo do consentimento anteriormente manifestado de forma livre e inequívoca, não havendo disposição legal no sentido de impor ao controlador a eliminação após a revogação do consentimento. Outrossim, o Art. 16 da LGPD permite o armazenamento dos dados para finalidades delimitadas, como cumprimento de obrigação legal por exemplo, em atenção a harmonia das demais legislações incidentes a depender da relação estabelecida com o titular. ","615521": "Os efeitos não devem invalidar o tratamento realizado sob amparo do consentimento manifestado anteriormente, sem efeito retroativo e devem ser restritos a finalidade que teve fundamentada a hipótese legal no consentimento, vez que pode haver finalidades distintas com justificação por exemplo no cumprimento de obrigação legal ou execução de contrato. Devendo ser observado, conforme mencionado na questão anterior, que o Art. 16 da LGPD permite o armazenamento dos dados para finalidades delimitadas, como cumprimento de obrigação legal por exemplo, em atenção a harmonia das demais legislações incidentes a depender da relação estabelecida com o titular. ","615617": "Uma decisão tomada com base em tratamento automatizado caracteriza-se conforme ICO, por excluir qualquer decisão humana do resultado ([https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/)). Enquanto, a decisão automatizada, um ser humano pode inserir dados e a decisão ser realizada por sistema automatizado, gerando um resultado com o emprego de mecanismos de automação para processar informações. Desta forma, um processo não será considerado exclusivamente automatizado se alguém avaliar e interpretar o resultado de uma decisão automatizada antes de aplicá-la ao titular por exemplo, ou seja, com característica da interferência humana de alguma forma ao longo do processo. A grande preocupação reside em como revisar as decisões tomadas com base unicamente no tratamento automatizado se a IA generativa tem a capacidade de gerar novas informações das contidas em base de dados já existentes. ","615618": "O direito à revisão de decisão automatizada previsto no art. 20 da LGPD pode ser considerado amplo quando comparado ao previsto no art. 22 da GDPR. A expressão "interesse" do art. 20 da LGPD não se restringe a decisões automatizadas que produzam efeitos legais ou análogos, conforme o texto europeu. Deste modo, caso a decisão afete os interesses do titular de dados pessoais. Pode ser entendimento como uma decisão de impacto dos direitos e liberdades individuais dos titulares. Ainda, o Glossário de Proteção de Dados Pessoais publicado pela ANPD define o tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares como "Aquele em que a atividade de tratamento possa impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade", de modo que o direito de revisão poderá ser invocado, independentemente de já caracterizado eventual dano efetivo. ","615619": "Os desafios práticos residem em como revisar efetivamente as decisões tomadas unicamente com base no tratamento automatizado, equalizando esforços a serem empregados em relação a natureza, porte da companhia ou o volume de operações de tratamento de dados. Sendo que, a demonstração pelo agente de tratamento dos meios empregados de governança e análise de riscos frente ao emprego da tecnologia no

processo contribui para que o resultado da decisão não impacte de forma prejudicial o titular. Os dados de treinamento da decisão tomada com base no tratamento automatizado devem ser éticos, respeitando direitos autorais e a dignidade das pessoas, evitando marginalização de grupos com correção de vieses, promovendo o respeito a privacidade e a proteção de dados. Importante citar, sobretudo a dificuldade sistemática e também operacional de leitura e interpretação do provedor da aplicação ou do desenvolvedor do software de mapear de maneira precisa o *modus operandi* pela qual a decisão automatizada culminou, principalmente pelo falo da caixa preta existente em sistemas que utilizam Inteligência Artificial já que os algoritmos e as árvores de decisão são obscuros o suficiente para que seres humanos possam concluir os caminhos que foram diretamente tomados até que se chegasse a decisão final. Cabe, portanto, o ânimo da empresa Controladora de estabelecer uma sistemática tanto operacional quanto procedimental para que fique claro que as informações prestadas sempre terão limite na fronteira entre o que se entende do software e o que é gerado pelo processamento massivo de dados. ",615620": "Conforme mencionado anteriormente, o disposto no Guide to the General Data Protection Regulation (GDPR) disponibilizado pela ICO (<https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf> p. 150), poderia ser negado o direito de revisão sobre decisões automatizadas pelo Controlador se este for manifestamente excessivo ou infundado, ou seja, se reiteradamente repetitivo o conteúdo de solicitações pedidos já realizadas com intenção de ocasionar esforço desnecessário do Controlador e demais agentes de tratamento envolvidos na operação, bem como não havendo clara intenção de exercício do direito pelo titular ou demonstrado que a solicitação está sendo usada para maliciosamente obter vantagem ilícita do Controlador, sem outro objetivo real, outrossim, se revelar segredos de negócios devendo haver a complementação legislativa em âmbito nacional com a lei do cadastro positivo lei nº 12.414, de 9 de junho de 2011 que já previa tal direito, e, em âmbito internacional a Diretiva 95/46/CE que também estabelece os critérios para esta temática."

{"615450": "Embora os prazos indicados no art. 11 da Lei 12.527/2011 sejam razoáveis, entendemos que é importante levar em conta as complexidades operacionais envolvidas no atendimento de alguns direitos de titular, dado que estas podem trazer implicações em outras frentes de atividade do controlador, a exemplo de situações de encerramento de conta, alinhamentos de sistemas e bancos de dados, entre outros aspectos operacionais. Nesse sentido, a fim de garantir o máximo de eficiência e precisão no atendimento às demandas do titular, sem gerar a este último insatisfação ou frustração de expectativa, sugerimos a aplicação do prazo de 20 dias úteis, prorrogáveis por mais 10 dias úteis mediante justificativa da prorrogação ao titular. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Embora no seu art. 19 LGPD tenha se atentado à necessidade de oferecer uma confirmação da existência de tratamento de dados pessoais em prazo menor do que o definido para a emissão de um relatório completo, entendemos que para oferecer a transparência necessária ao titular quanto à existência de tratamento, bem como de forma a gerar a menor incidência de custos operacionais aos controladores, seria importante utilizar o prazo de 15 dias como um parâmetro mínimo para que o controlador possa atender à solicitação de acesso à informação do titular de forma completa e consistente, sem que haja a necessidade de reiteração das solicitações por parte do titular, bem como permitindo um fluxo fluido e eficiente tanto na perspectiva do controlador, quanto do titular que terá um retorno efetivo e completo. Além disso, cabe destacar que embora o prazo de 15 dias deva ser utilizado para o acesso do titular à confirmação de existência de tratamento e à informação quanto aos seus dados pessoais tratados, tal prazo não deve ser confundido com os prazos a serem aplicados no atendimento dos demais direitos previstos na forma do art. 18 da LGPD, considerando todos os desafios operacionais existentes em relação ao controlador, conforme já mencionado nesta contribuição. ","615484": "A fim de garantir um atendimento seguro e adequado ao titular, sugerimos que a ANPD estabeleça quais são as informações mínimas que o titular deve fornecer ao controlador para confirmar sua identificação ao entrar em contato com o controlador via canais de atendimento disponíveis. Tal medida é necessária dado que a insuficiência de concessão de informações pelo titular, além de dificultar a sua identificação e até mesmo a sua autenticação, podem trazer riscos quanto ao tratamento dos dados pelo controlador no atendimento das solicitações, já que podem implicar em ineficiências de atendimento, e até mesmo situações de insegurança, como ocorrência de fraudes por terceiros mal-intencionados. Assim, tendo em vista a centralidade da privacidade nas tratativas com o titular, sugerimos que a Autoridade disponha sobre a necessidade de fornecimento pelos titulares de informações base de identificação, de forma a garantir a correta comparação dos dados cadastrais/identificados indicados no momento inicial do contato com as bases internas do controlador, garantindo ao titular um atendimento mais célere e seguro. Isso é ainda mais importante quando considerados os controladores de dados vinculados ao Sistema Financeiro Nacional, além de demais prestadores de serviço que tratam bases amplas de dados. Para além disso, é importante que o canal de atendimento seja condizente com a estrutura operacional do controlador e com os canais que são por este disponibilizados para atendimento ao consumidor. Nesse sentido, é preciso considerar que as empresas que prestam serviços por meio de plataformas e sistemas digitais já estruturam seus canais de atendimento através desses mesmos mecanismos, de forma que não faria sentido exigir o uso de um canal de atendimento que seja incompatível com a prática usual e a

legítima expectativa, tanto do agente de tratamento, quanto do próprio titular. ";615485": "Sim. É preciso que qualquer norma referente ao atendimento dos direitos do titular tenha previsão expressa da responsabilidade dos operadores quanto à cooperação e garantia de atendimento rápido e eficiente de solicitações relativas ao tratamento de dados pessoais de titulares cujos dados sejam tratados por eles em nome do controlador. A própria LGPD, na forma de seu art. 42, §1º, I, prevê a responsabilidade solidária do operador em razão do não atendimento às instruções lícitas do controlador. É importante que a regulamentação respalde tal responsabilidade, e também leve em consideração a diversidade de situações que implicam em cenários de tratamento de dados entre partes controladoras-operadores, a exemplo do processamento massivo de dados em nuvem, relações de representação comercial ou de atuação do operador como intermediador ou preposto de uma parte controlador, atividades relacionadas à segmentação de dados, dentre inúmeras outras. Em razão dessa diversidade, entendemos que qualquer regulamentação deverá também se pautar por normas principiológicas, que respaldem a liberdade contratual das partes envolvidas (controlador-operador), de maneira a garantir uma estruturação eficiente do relacionamento entre as partes, considerando sensibilidades de atividade econômica e também complexidades regulatórias existentes. ";615486": "Sim. É preciso que qualquer norma referente ao atendimento dos direitos do titular tenha previsão expressa da responsabilidade dos operadores quanto à cooperação e garantia de atendimento rápido e eficiente de solicitações relativas ao tratamento de dados pessoais de titulares cujos dados sejam tratados por eles em nome do controlador. A própria LGPD, na forma de seu art. 42, §1º, I, prevê a responsabilidade solidária do operador em razão do não atendimento às instruções lícitas do controlador. É importante que a regulamentação respalde tal responsabilidade, e também leve em consideração a diversidade de situações que implicam em cenários de tratamento de dados entre partes controladoras-operadores, a exemplo do processamento massivo de dados em nuvem, relações de representação comercial ou de atuação do operador como intermediador ou preposto de uma parte controlador, atividades relacionadas à segmentação de dados, dentre inúmeras outras. Em razão dessa diversidade, entendemos que qualquer regulamentação deverá também se pautar por normas principiológicas, que respaldem a liberdade contratual das partes envolvidas (controlador-operador), de maneira a garantir uma estruturação eficiente do relacionamento entre as partes, considerando sensibilidades de atividade econômica e também complexidades regulatórias existentes. ";615487": "Têm sido visíveis no mercado modelos de atendimento às solicitações de titulares a partir de canais digitais especializados para o endereçamento de demandas, dúvidas e questionamentos. Entendemos que o canal digital é o mecanismo mais eficiente e com maior escalabilidade e economicidade para controladores de dados pessoais, dado que através de tais canais é possível disponibilizar ao titular informações base a respeito do tratamento de dados de forma prática e rápida (através de FAQs, referências à Política de Privacidade, dentre outras). Além disso, tal modelo também favorece o encaminhamento de demandas já solicitando informações pertinentes para possibilitar o atendimento aos direitos do titular dentro dos prazos legais e em conformidade com os princípios da LGPD (o que pode ser feito através de formulário na plataforma digital, por exemplo). ";615491": "Sim. Para a negativa do direito de confirmação da existência do tratamento, é importante pautar-se em premissas básicas para o atendimento do titular, como o fornecimento de informações básicas que permitam a sua identificação e autenticação nos sistemas do controlador. Essas premissas são relevantes, pois permitem que não seja gerado um ônus operacional ao controlador, além de permitir o respaldo à segurança do titular quanto ao tratamento e o acesso aos seus dados pessoais. É

importante considerar situações em que terceiros mal-intencionados podem utilizar de fragilidades em sistemas de autenticação para solicitar informações quanto aos dados pessoais de possíveis vítimas de fraude, o que é ainda mais relevante para os controladores que tratam de informações sujeitas a sigilo legal, ou dados pessoais sensíveis. Além do citado acima, é importante considerar também a negativa ao direito de confirmação da existência do tratamento em situações em que o tratamento de dados pessoais é respaldado por obrigação legal, regulatória, ou por interesse do controlador no exercício regular de seus direitos em processos judiciais, administrativos e arbitrais, no qual a divulgação ou confirmação da existência de tratamento pode comprometer procedimentos sigilosos e gerar perdas e danos ao controlador dos dados, dependendo da solicitação que foi realizada. ";615492": "É importante ter em mente que o controle de dados pessoais pode ser exercido por uma entidade única ou por um Grupo Econômico, sendo crucial uma identificação transparente do controlador para que os titulares possam contatar e exercer seus direitos. Quanto ao uso compartilhado, essa é uma prática comum, abrangendo diversos tipos de serviços e relacionamentos entre controladores, que precisam ser apresentados ao titular de forma transparente, mas que detêm complexidades inerentes que, se apresentadas de forma inadequada, podem causar prejuízos à relação titular-controlador. Sendo assim, embora a LGPD respalde o direito de acesso a essa informação, é importante que a regulação não torne o que é um mecanismo de transparência útil em um instrumento excessivamente oneroso ao titular e ao controlador, destacando-se o papel da relevância como um elemento das informações prestadas para o efetivo exercício e satisfação do direito do titular nesses casos. Por esse aspecto, elementos descrevendo os tipos de prestadores ou parceiros que podem acessar os dados e os motivos para tal, já são adotados no mercado, apresentando a informação de forma transparente e não excessiva, respeitando os princípios da LGPD, e evitando desconfortos e questionamentos do titular quanto a processos que para ele podem notoriamente parecer excessivamente complexos e até mesmo intimidadores, mas que são essenciais no exercício de atividades do controlador, sem gerar qualquer prejuízo ou risco às liberdades e direitos fundamentais do titular. Mesmo assim, em respeito à autodeterminação informativa, deve-se respaldar o acesso do titular a informações sobre o uso de seus dados por um controlador, quando for razoável e justificável o acesso de forma detalhada. Para tanto, a atuação da ANPD é essencial para garantir um equilíbrio adequado entre o direito do titular à informação e os fundamentos da LGPD orientando sobre as informações que devem ser disponibilizadas de forma a satisfazer os pleitos dos titulares sem comprometer as atividades legítimas do controlador. ";615489": "O papel do operador dos dados deve estar intimamente conectado ao atendimento das diretrizes legítimas de tratamento dadas pelo controlador. Dessa forma, sua responsabilidade reside em assegurar que o titular, quando solicitar informações a respeito de seus dados pessoais, seja devidamente encaminhado para os canais e mecanismos disponíveis do controlador para permitir o exercício de seus direitos. Cabe destacar que o operador não pode ser um canal próprio para o atendimento do titular, salvo se atue dessa forma em nome do próprio controlador, por conta da própria natureza de sua relação quanto aos dados pessoais tratados, de forma que seu papel se limita à cooperação com o controlador, e a responsabilidade de garantir que não será, ele mesmo, um obstáculo para que o titular possa acessar informações e exercer direitos na forma da Lei. Nesse sentido, ressalta-se o já mencionado anteriormente na presente contribuição quanto à necessidade de que a norma referente aos direitos do titular reforce as disposições de responsabilidade da LGPD quanto ao operador, assegurando a sua obrigação em cooperar de maneira eficiente e adequada junto ao controlador, tanto no encaminhamento devido do

titular dos dados aos canais próprios para o exercício de seus direitos e acesso a suas informações, quanto na cooperação junto ao controlador para atender às demandas relacionadas ao exercício de tais direitos e acesso às informações que precisem ser disponibilizadas. ","615490": "Embora a LGPD tenha se atentado à necessidade de o controlador oferecer ao titular uma confirmação da existência de tratamento de dados de forma imediata, entendemos que para oferecer a transparência necessária ao titular quanto à existência de tratamento de dados pessoais seria necessário um trabalho operacional por parte do controlador de forma a entender quais dados são tratados e a respectiva forma de tratamento, o que traria a necessidade de levantamento interno dessas informações. Dessa forma, a simples confirmação de existência de tratamento seria uma das poucas informações disponíveis em caráter imediato dentro do teor do inciso I da LGPD, mas vale destacar, conforme já mencionado em outros pontos desta contribuição, que tal confirmação pode resultar em confusão ou dúvidas do titular, dada a incapacidade operacional do controlador de ofertar de imediato maiores informações relevantes sobre o tratamento dos dados, gerando ao titular a necessidade de solicitar ao controlador a elaboração de uma declaração completa, a qual deverá ser enviada no prazo estipulado em lei. ","615494": "Em atenção ao cumprimento da norma e concessão imediata de informações mínimas sobre o tratamento de dados pessoais aos titulares, os controladores disponibilizam em suas páginas na internet a Política de Privacidade, cujo teor possui informações mínimas necessárias para entendimento pelo titular, de forma transparente e relevante, sobre as práticas relacionadas ao uso do dado pessoal, o que normalmente inclui: (i) forma de coleta; (ii) finalidades e possíveis bases legais do tratamento; (iii) possibilidades de uso compartilhado de dados; (iv) cenários de transferência internacional de dados; (v) práticas gerais de segurança sobre os dados pessoais; (vi) possibilidade de retenção e armazenamento posterior dos dados, quando aplicável; (vii) Direitos do Titular; e (viii) canais de contato para atendimento de demandas. ","615493": "Embora a LGPD tenha previsto que a disponibilização dos dados pessoais em papel seja uma possibilidade, é importante considerar que tal previsão pode ser desconexa com a prática comum e estrutura de muitos controladores do mercado, cuja atividade majoritariamente reside em meio digitais, inclusive com canais de contato junto ao titular exclusivos pelo meio digital, de forma que o papel se torna um ônus operacional ao controlador apenas para o cumprimento de previsão legal, não trazendo nenhum benefício ao titular, o que é um contraponto ao propósito da LGPD quanto à defesa da tecnologia e inovação. Nesse sentido, é importante que orientações por parte da ANPD sobre o tema permitam considerar as expectativas do controlador sobre os meios de oferta dos relatórios completos dos dados pessoais dos titulares dos quais trata dados. ","615502": "Os setores regulados são atualmente os que possuem maior maturidade para a portabilidade de dados, considerando a similaridade de atividades entre os agentes regulados, bem como a existência de mecanismos regulatórios e autorregulatórios que permitem o desenvolvimento conjunto de padrões e meios de interoperabilidade para assegurar o compartilhamento adequado de dados. Como um dos principais exemplos dessa maturidade destaca-se o Open Finance, regulamentado pelo Banco Central através da Resolução Conjunta nº 1 de 2020, cujos termos possibilitaram o desenvolvimento de um mecanismo viável e eficiente de compartilhamento de dados entre diversos agentes em tempo real, através do direito de portabilidade, formalizado pelo consentimento dos titulares. ","615501": "A diferença de estruturas entre diversas empresas no Brasil constitui um dos principais desafios tecnológicos para a interoperabilidade, dado que se tratam de inúmeras empresas atuando em setores diversificados, nos quais informações específicas são utilizadas com maior ou menor relevância, gerando dificuldades de conexão e padronização. ","615505": "Para essa

hipótese, o ideal é que seja prevista a padronização do formato dos arquivos a serem compartilhados, a definição dos dados mínimos necessários para a portabilidade/interoperabilidade e um canal único e seguro para o tráfego das informações compartilhadas, considerando a proteção dos dados pessoais. É preciso que tais objetos de padronização sejam devidamente discutidos junto aos setores e mercados afetados, considerando a complexidade de cada uma de suas atividades e suas sensibilidades.";"615503": "Para os casos em que não existirem regras setoriais definidas para a portabilidade, seria aceitável considerar que o relatório de acesso garantiria o exercício do direito. Não obstante isso, cabe destacar a preocupação quanto à segurança dos dados do titular, dado que informações compartilhadas através do relatório, se não adequadamente submetidas a normas adequadas e padronizadas de segurança, podem gerar exposição do titular a danos provocados por terceiros mal-intencionados.";"615504": "Sim. No caso do Open Finance, o regulador habilitou os agentes privados do setor financeiro a desenvolverem entre si os padrões de interoperabilidade que seriam utilizados para o compartilhamento de informações.";"615511": "Entendemos que o principal critério a ser considerado deverá partir da própria declaração do titular devidamente identificado e autenticado quanto às suas informações pessoais. Não obstante isso, cabe ressaltar que a mera declaração pode conter informações imprecisas e inexatas, sendo a utilização de outras fontes de dados, como dados de natureza pública e bureaus privados, um mecanismo importante e eficiente na correção de informações inconsistentes.";"615514": "Entendemos que existem situações em mercado nos quais a alteração ou “correção” de um dado tem potencial de gerar fragilidades à segurança do próprio titular, a exemplo de alterações de dados solicitadas por fraudadores para a realização de atividades ilícitas. Nesses casos, é importante que o exercício do direito pelo titular esteja sujeito a mecanismos apropriados de autenticação de identidade e do dado corrigido, de forma a permitir a realização da correção com segurança. A exemplo de tal situação, pode-se considerar a necessidade de comprovar uma alteração de endereço mediante o envio de um comprovante de residência, ou uma alteração de número de telefone mediante autenticação por outro meio de contato, dentre outros exemplos possíveis.";"615513": "É preciso que os critérios utilizados impliquem no correto equilíbrio entre o custo necessário quanto à correção ou exclusão dos dados, e o impacto efetivo junto ao titular no exercício de seus direitos e liberdades fundamentais. Para esse caso, pode-se exemplificar backups armazenados de forma física ou em meios de difícil acesso, no qual apesar de fazer sentido a correção dos dados, o efeito real e material da correção seria efetivamente nulo para o titular. Nesse cenário, o Controlador deve ter espaço para avaliar os custos e ônus operacionais envolvidos na correção, de forma a justificar a sua efetivação ou não, com pauta no impacto material efetivo junto ao titular de dados.";"615512": "Sim. Pode-se considerar hipóteses em que a correção implica em esforços desproporcionais, bem como situações na qual não houve a efetiva autenticação ou identificação do titular ou da informação que supostamente seria corrigida. Além disso, existem cenários em que o controlador pode necessitar manter os dados armazenados para fins regulatórios, autorregulatórios ou legais, no cumprimento de seus deveres para fins de auditoria, não sendo possível a correção dos dados no histórico retido.";"615517": "Sim. Embora o titular tenha direito à eliminação e oposição ao tratamento de dados, é importante considerar que as bases legais previstas na LGPD na forma do art. 7º e 11º não limitam o controlador à manifestação expressa da vontade do titular, sendo esse caso aplicado mais especificamente nos cenários em que há o uso do consentimento. Por tais fatores, o titular tem o direito ao acesso à informação quanto às práticas do controlador quanto aos seus dados, mas não pode opor-se a tais práticas de forma ilegítima, sem embasamento nos

princípios e diretrizes legais da LGPD, e fundamentando-se na existência de prejuízo e risco material aos seus direitos e liberdades fundamentais. Nesse sentido, é importante que a ANPD regule as diretrizes e os mecanismos disponíveis para a oposição do tratamento de dados por parte de um titular, de forma a assegurar a composição e determinação adequada quanto à legalidade ou não de determinado tratamento de dado pessoal para que, quando verificado, seja possível providenciar a interrupção da prática à qual o titular se opôs. ","615516": "Sim. Tendo em mente os efeitos práticos e materiais ao titular e suas liberdades e direitos fundamentais, o dado pessoal, uma vez anonimizado de forma adequada e irreversível, impossibilita a identificação do titular, o que implica, inclusive por disposição da própria LGPD, na inaplicabilidade da lei quanto a esse tipo de informação. ","615518": "Uma vez verificada a ilegitimidade de determinada prática de tratamento de dado pessoal, deve ser assegurada ao controlador prazo adequado para interromper o tratamento em face daquele titular, bem como demais titulares de dados cujas informações estejam sujeitas ao tratamento identificado como ilegítimo. Nessa hipótese, a interrupção do tratamento dentro de um prazo razoável é o melhor mecanismo para assegurar a proteção dos dados pessoais, em consonância com o desenvolvimento tecnológico e a proteção da inovação. ","615523": "O tratamento de dados pessoais de determinado titular somente poderá ser interrompido após o esgotamento de todas as finalidades existentes quanto ao tratamento da informação, mesmo que a base original de coleta do dado pessoal seja o consentimento. Nesse caso, destaca-se a redação da LGPD quanto ao princípio da finalidade, em que é vedado o tratamento posterior de dado pessoal somente quando incompatível à sua finalidade original. Dessa forma, em caráter exemplificativo, se um determinado controlador coleta um dado através do consentimento, e por tal consentimento, incorre em obrigação legal, ou precisa armazenar as informações para realizar atividades legitimadas na forma dos arts. 7º ou 11º da LGPD, que derivem e sejam compatíveis com a finalidade original, a simples revogação do consentimento não pode ser suficiente para implicar na obrigação de eliminação dos dados. ","615521": "Em linha com o pontuado na questão anterior, reforçamos que a eliminação dos dados pessoais apenas deve ocorrer quando não houver mais nenhuma base legal para tratamento dos respectivos dados. Assim, na hipótese de revogação do consentimento, o tratamento dos dados pessoais realizado sob o amparo de tal base legal deve ser interrompido, respaldados os tratamentos realizados anteriormente à revogação, os posteriores promovidos pelo controlador que sejam compatíveis com a finalidade original, bem como os respaldados por demais bases legais previstas na forma dos arts. 7º e 11º da LGPD. ","615617": "Entendemos por decisão automatizada a decisão tomada sem qualquer interferência manual, isto é, em que em todo o processo (desde a coleta, consulta, processamento, decisão e execução da decisão tomada), não há interferência ou avaliação crítica humana, gerando um resultado específico e determinado de forma automática. ","615618": "Caso a decisão automatizada implique em discriminação ou execução de tratamento de dado pessoal de forma negativa para o titular, ou promova decisões atreladas a uma finalidade não previamente comunicada ao titular atendendo aos princípios da LGPD, poder-se-ia considerar que há efeito sobre um interesse do titular. ","615619": "Entendemos que há desafios práticos pertinentes quanto ao direito de revisão, especialmente no que tange à leitura dos algoritmos utilizados e a interpretação das decisões tomadas de forma a entender se houve, ou não, efeitos sobre decisões que são de interesse do titular, especialmente considerando contexto, negócio e demais informações relevantes que podem ter sido utilizadas na tomada de decisão automatizada. ","615620": " "

{ "615450": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim, sobretudo para o setor da saúde, no qual as solicitações dos direitos dos titulares podem apresentar questões de alta complexidade a depender do contexto, considera-se que o prazo de 20 (vinte) dias, conforme mencionado no § 1º do art. 11, e, sobretudo, a possibilidade de prorrogação do prazo por mais 10 (dez) dias, em conformidade com o §2º do mesmo artigo, garantiria maior efetividade do cumprimento de resposta ao exercício dos direitos pelos agentes de saúde.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Os seguintes critérios devem ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD: (i) Teor da Solicitação; (ii) Urgência do pedido; (iii) Impacto ao titular; (iv) Complexidade para a solução; (v) Segmento de atividade do controlador; (vi) Porte do Controlador; (vii) Variedade de serviços prestados; (viii) volume de dados tratados. Sobre tudo no que se refere à declaração clara e completa presente no inciso II do art. 19, compreendemos que é pertinente prazo estendido, conforme critérios acima, tendo em vista a necessidade de apuração interna do agente de tratamento.", "615484": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Canal de atendimento que possua: (i) Meios de identificação do titular; (ii) Linguagem simples e acessível para compreensão do titular; (iii) Canal com boa usabilidade e direcionamento.", "615485": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim, na extensão da responsabilidade que lhe é atribuída conforme a legislação (responsável secundário em relação ao controlador), o operador possui responsabilidade na concretização dos direitos dos titulares, sobretudo em situações nas quais: (i) for diretamente acionado pelo titular, cooperando para indicação de correto canal junto ao controlador, se o caso; (ii) apoiando o controlador com subsídios para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação pelo controlador.", "615486": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Não, o tema deve ser tratado de forma diferenciada. Questões relacionadas ao atendimento ao consumidor poderão diferenciar-se em demasiado no tocante à natureza de requisições de titulares, sobretudo em determinados segmentos do mercado, como o setor da saúde. Algumas obrigações de difícil aplicação na norma requerem, por exemplo: (i) disponibilidade ininterrupta - durante vinte e quatro horas por dia, sete dias por semana; (ii) pluridade de canais; (iii) obrigatoriedade de atendimento telefônico; (iv) acesso inicial não condicionado ao fornecimento prévio de dados pelo consumidor, (v) prazo de atendimento de demandas no prazo de sete dias corridos, contado da data de seu registro; (vi) horário de atendimento não inferior a oito horas diárias dentre outras. As justificativas incluem: (i) não é necessário um serviço de atendimento ininterrupto para cumprir com a LGPD; (ii) o atendimento ao cliente pode ser feito durante o horário comercial e por diferentes canais, como e-mail; (iii) a identificação prévia do titular de dados é recomendada para direcionar o atendimento e apurar violações; (iv) o tempo mínimo de funcionamento do SAC pode variar de acordo com a natureza dos serviços oferecidos pelas empresas, e se diferencia do prazo já previsto na LGPD (15 dias); (v) o contato direto com o atendente nem sempre é necessário, e o tempo máximo de espera para atendimento da solicitação depende de análises específicas; (vi) pode ser necessário solicitar repetição da demanda para coletar informações necessárias junto ao titular; (vii) meios digitais podem ser

suficientes para atender solicitações dos titulares; (viii) o prazo de 5 dias corridos para atender solicitações pode ser curto, especialmente considerando o histórico do titular.";"615487": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Consideramos que o modelo de Ouvidoria do Gov.br é um sistema que pode ser utilizado como paradigma no tocante ao setor público. Inclusive, a indicação de métricas para a calcular a efetividade dos atendimentos realizados e a satisfação do público. No tocante ao setor privado, uma das alternativas é utilizar os indicadores e as métricas implementadas pelo IBRC - Instituto Brasileiro de Relacionamento com o Cliente.";"615491": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Eventualmente, quando o tratamento de dados pessoais estiver relacionado a procedimentos de investigação e/ou auditorias, a fim de proteger o processo, seria possível a negativa.";"615492": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Razão social, CNPJ, Nome Fantasia e/ou Marca e DPO.";"615489": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Cooperação na indicação de correto canal do controlador, se o caso ou apoio ao controlador com subsídios para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação.";"615490": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Considerando que o formato simplificado prevê que o relatório seja encaminhado imediatamente, a informação mínima que pode ser fornecida é sobre a Existência do tratamento: Sim ou não. Quaisquer informações mais detalhadas sobre os titulares de dados podem necessitar de consultas a diferentes sistemas das companhias (a depender do seu porte e tipo de serviço prestado), de modo que a liberação de um relatório imediato com todos os dados poderia necessitar de uma maior de análise, razão pela qual não poderia ser fornecido imediatamente. Em caso positivo, ficará facultado a cada controlador complementar ou não a requisição com informações adicionais, se assim entender pertinente.";"615494": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Dados pessoais tratados para a tomada de decisão e finalidades do tratamento.";"615493": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim, tanto a disponibilização digital quanto em formato de papel satisfazem os direitos do titular. No entanto, o fornecimento em papel deve considerar o volume de dados e ser oferecido apenas se o cliente não tiver acesso digital ou preferir o formato físico, com os custos de impressão repassados ao solicitante. A prioridade deve ser sempre o formato digital, dada a disponibilidade de meios tecnológicos seguros.";"615502": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Telecomunicações e Setor Financeiro. No que se refere aos atores do segmento de saúde, incluindo entes públicos e privados, compreende-se que não há maturidade em processos que permita assegurar a Portabilidade na forma de dados interoperáveis no momento, considerando, dentre outros elementos, a sensibilidade, volumetria e formato dos dados. Para maior segurança jurídica, roga-se à ANPD, ainda, que se defina o conceito de Portabilidade para fins da legislação, diferenciando-o do conceito de Compartilhamento de dados (ou histórico dos titulares de dados nas instituições).";"615501": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Com referência ao setor da saúde, é possível citar: (i) Integrações entre plataformas que operam dados; (ii) formato válido de dados; (iii) qualidade de dados; (iv) operações e estrutura de tecnologia; (v) multidisciplinariedade de sistemas; (vi) dados estruturados e não estruturados (imagem); (vii) protocolos de comunicação e protocolos de segurança; (viii) alto custo. Atualmente existem diversos mecanismos de coleta dados, cada um com sua particularidade e operação. Para que a interoperabilidade de dados fosse

realizado, deveria inicialmente existir uma padronização no formato de coleta de dados e armazenamento de metadados, bem como sanitização do conjunto para que todo ele permaneça legível. ","615505":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Prioritariamente o formato de dados, protocolos e terminologias comuns. Em seguida a padronização das ferramentas operadoras de dados e por fim a sanitização das bases. ","615503":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim. ","615504":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim, é razoável que o setor privado possa definir os padrões de interoperabilidade, por segmentos de atividade - pois cada cenário possui desafios específicos. O prazo deverá ser determinado de acordo com o mercado que o operador atua, sendo que, no tocante à área da saúde, compreende-se prazo inferior a 12 (doze) meses demasiado desafiador. ","615511":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Para que um dado seja considerado incompleto, inexato ou desatualizado, devem ser consideradas as seguintes características: Dado incompleto: Quando falta alguma informação essencial para compreensão ou utilização adequada. Isso pode incluir campos vazios, informações ausentes ou inconsistências nos dados fornecidos. Idado Inexato: Quando contém informações incorretas, imprecisas ou desatualizadas. Isso pode ocorrer devido a erros de entrada de dados, falhas de comunicação ou mudanças nas circunstâncias que tornam as informações obsoletas. Dado Desatualizado: Quando as informações que ele contém estão obsoletas ou não refletem a situação atual. Isso pode ocorrer quando os dados não são atualizados regularmente para acompanhar mudanças no tempo, como atualizações de status, alterações de contexto ou novos desenvolvimentos. No que se refere ao contexto ou consideração situacional para enquadramento do dado, deve ser considerado o último registro do dado, com evidências de data. ","615514":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] A simples declaração do titular não seria suficiente nos casos de: (i) solicitação genérica, como, por exemplo, sem indicação do dado a ser corrigido e/ou onde consta desatualizado; (ii) solicitações de correção sem comprovação da identidade do titular; (iii) situações em que é necessária a validação/cadastro por meio de comprovação documental e não é apresentado o documento para correção/atualização. De modo geral, a simples declaração do titular não seria suficiente nas situações em que houver registro documental, necessárias à comprovação do conteúdo da solicitação. ","615513":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Os critérios objetivos para avaliar a impossibilidade ou o esforço desproporcional conforme o art. 18, §6º da LGPD envolvem: (i) considerações sobre a complexidade da infraestrutura dos agentes de tratamento envolvidos; (ii) formato dos dados (iii) padrão de interoperabilidade; (iv) tipo de solicitação, (v) implicações da não recepção pelos demais da solicitação e (vi) volume de agentes a serem comunicados. Por fim, é necessário levar em conta desafios para que seja informado ao outro controlador "imediatamente", conforme menciona a legislação - devendo a ANPD fornecer critérios mais claros quanto ao prazo fornecido. ","615512":"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Em circunstâncias excepcionais, o direito de correção pode ser negado pelo controlador em situações em que o pedido de correção é feito para informações que não necessitam de alteração, como quando os dados estão corretos e precisos. Além disso, o direito de correção pode ser negado quando as correções demandam comprovação por meio de documentos, e o titular não forneceu a documentação necessária para comprovar a necessidade da correção. Nesses casos, o controlador pode negar o pedido de correção até que a documentação adequada seja fornecida pelo titular,

considerando trâmites burocráticos e administrativos, bem como possíveis consequências jurídicas da alteração."615517": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] É essencial que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado, pois isso possibilita aos agentes de tratamento a verificação de inconsistências internas, melhorando seus programas de governança ou de seus parceiros, fornecedores e demais agentes que realizam o tratamento em seu nome ou juntamente a eles. A fundamentação permite que o controlador analise as alegações do titular e ofereça esclarecimentos adicionais, se necessário, sobre o tratamento de dados considerados desnecessários, excessivos ou em desconformidade. Além disso, ao apresentar elementos que embasem suas alegações, o titular possibilita que o agente de tratamento analise os pontos abordados e apresente justificativas pertinentes para o tratamento, quando aplicável, sem burocracias excessivas, desde que comprovadas as alegações do titular, ressalvadas as hipóteses legais de exceções."615516": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Sim, considerando situações específicas, a anonimização e a eliminação podem ser adotadas alternativamente pelos agentes de tratamento. Respeitando os limites de finalidade do tratamento de dados, bem como os riscos de reidentificação e as possibilidades legais e regulatórias, essa alternativa pode ser aplicada, especialmente em setores sensíveis como o da saúde, onde essa flexibilidade pode promover a inovação em ferramentas voltadas para a saúde. Além disso, essa escolha pode atender às solicitações dos titulares quanto à cessação do tratamento de seus dados pessoais, ressalvadas as hipóteses legais de exceções. A adoção de medidas de anonimização ou eliminação pode ser considerada de forma alternativa, levando em conta que a anonimização remove as características de dados pessoais, mitigando substancialmente os riscos para os titulares de dados. Isso possibilita a utilização de dados para análises estatísticas relevantes ao aprimoramento dos negócios, sem a necessidade de eliminar os dados, desde que sejam observadas as melhores técnicas de anonimização disponíveis e seja constatada a impossibilidade de reversão da anonimização."615518": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] É necessário que o agente de tratamento, mesmo agindo de boa-fé e tendo conhecimento da possível configuração de tratamento inadequado dos dados, se comprometa proativamente com as medidas necessárias para correção do processo e as devidas comunicações, se o caso. A legitimidade do tratamento deve ser considerada sob os diversos aspectos que envolvem as atividades do Controlador. Se, após tais análises, restar confirmado que a oposição é legítima e o agente não possui previsão legal que justifique o tratamento, o pedido do titular deve ser recepcionado, cessando o tratamento. Essas ações garantem a conformidade com a LGPD e demonstram o compromisso do agente de tratamento com o respeito aos direitos dos titulares de dados."615523": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Não necessariamente. A revogação do consentimento do titular, conforme estipulado no art. 18, IX, da LGPD, não automaticamente exige a eliminação dos dados pessoais tratados com base nesse consentimento. O titular precisa expressar explicitamente o desejo de eliminar seus dados. Além disso, é importante considerar que os dados tratados até a revogação do consentimento são válidos e podem ser retidos por obrigação legal ou regulatória, como exceções previstas no art. 16 da LGPD e em normativas específicas. A revogação do consentimento deve interromper novas operações de tratamento, mas não afetar os tratamentos já realizados de maneira lícita e legítima enquanto o consentimento era válido. Os tratamentos realizados anteriormente sob o consentimento válido devem ser mantidos, a menos

que haja um pedido expresso de eliminação dos dados pelo titular, observando as disposições legais que permitem a retenção de dados em certas circunstâncias.";"615521": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Considerando o art. 8º da LGPD, é importante observar que os tratamentos realizados sob o amparo do consentimento anteriormente manifestado podem ser mantidos pelos agentes de tratamento em determinados casos, conforme previsão legal e normativas setoriais. Por exemplo, a conservação de dados em órgãos e estudos de pesquisas clínicas, conforme o art. 16, inciso II da LGPD, e o Guia Orientativo para fins de Tratamento acadêmicos e para realização de estudos e pesquisas elaborado pela ANPD. Isso se deve ao fato de que certos tratamentos, como os dados clínicos em pesquisas, não podem ser removidos sem afetar o resultado estatístico da pesquisa. Assim, o direito de revogação do consentimento deve estar em consonância com as normas do setor e respeitar os limites previstos pela LGPD.";"615617": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Uma decisão automatizada geralmente implica que, embora o processo de tomada de decisão possa ser automatizado, ainda pode haver alguma forma de intervenção humana no processo. Isso inclui a definição dos critérios ou regras que o algoritmo deve seguir, revisão periódica dos resultados gerados pelo sistema automatizado ou a possibilidade de os indivíduos afetados contestarem a decisão e obterem uma revisão humana. Por outro lado, uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais implica que não há intervenção humana significativa no processo de tomada de decisão. Isso significa que a decisão é totalmente gerada pelo sistema automatizado, sem revisão ou intervenção humana durante todo o processo.";"615618": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] De modo geral, compreendemos que demonstra uma afetação dos interesses quando os titulares de dados sofrem limitações ao exercício de direitos ou de acesso a produtos e serviços devido a decisões automatizadas. No que concerne a elementos objetivos para definição de afetação de interesses, recomendamos que os elementos abaixo sejam considerados: 1 - Natureza dos direitos afetados: Avaliar se os direitos fundamentais ou interesses legítimos dos indivíduos estão sendo comprometidos, tais como privacidade, liberdade de expressão, liberdade de associação, entre outros. 2 - Gravidade do impacto: Determinar a gravidade do impacto sobre os indivíduos afetados, considerando se a decisão automatizada pode resultar em consequências significativas, como perda de oportunidades, discriminação, prejuízos financeiros ou reputacionais. 3 - Abrangência da decisão: Analisar se a decisão automatizada tem um alcance amplo e afeta um grande número de pessoas ou se é direcionada a indivíduos específicos. 4 - Transparência e explicabilidade: Verificar se os critérios e algoritmos utilizados na tomada de decisão automatizada são transparentes e compreensíveis, permitindo que as pessoas entendam como suas informações foram usadas e como a decisão foi tomada. 5 - Possibilidade de contestação: Avaliar se as pessoas têm meios eficazes para contestar ou contestar a decisão automatizada, garantindo o direito de corrigir informações imprecisas ou contestar decisões injustas.";"615619": "[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD envolvem a complexidade dos algoritmos, a interpretação dos resultados, o acesso aos dados, o conhecimento técnico necessário, o tempo e recursos requeridos, bem como a efetividade das correções. Além disso, há o desafio de dar transparência ao titular de dados sobre os critérios utilizados no processo de decisões automatizadas, considerando que diferentes estruturas e sistemas podem envolver segredo de negócio das companhias. Além disso, importante que se defina que garantir a revisão nas decisões não garante mudança

no resultado anteriormente tomado, a menos que haja alteração nos critérios utilizados pelos controladores ou dados novos e/ou atualizados. Superar esses desafios demanda uma abordagem colaborativa entre reguladores, profissionais da área, desenvolvedores de tecnologia e usuários finais para garantir que os direitos de revisão sejam efetivos e que as decisões automatizadas sejam justas, transparentes e precisas."615620"[Contribuições em nome da Associação Brasileira de Medicina Diagnóstica – ABRAMED] Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas. Isso pode ocorrer quando não houver cabimento nas hipóteses previstas no art. 20 da LGPD, que incluem afetação aos interesses, definição de perfil pessoal, profissional, de consumo, de crédito ou aspectos da personalidade, bem como eventualmente normas setoriais relacionadas à matéria. Além disso, encontramos algumas circunstâncias em que o direito de revisão podem vir e ser negados: 1 - Obrigação legal: Se a decisão automatizada for exigida ou autorizada por lei, o controlador pode não ter a capacidade de alterá-la ou revisá-la. 2 - Risco à segurança: Se a divulgação das informações utilizadas na decisão automatizada representar um risco à segurança, integridade ou confidencialidade dos sistemas ou dados, o direito de revisão pode ser negado. 3 - Proteção de direitos de terceiros: Se a revisão da decisão automatizada violar os direitos ou interesses legítimos de terceiros, como segredos comerciais ou propriedade intelectual, o controlador pode ser impedido de realizar a revisão. 4 - Decisões manifestamente infundadas: Se a solicitação de revisão for considerada manifestamente infundada ou excessiva, o controlador pode recusar a revisão, desde que comunique claramente os motivos para tal decisão. É importante observar que, mesmo nessas circunstâncias, o controlador deve informar claramente os motivos para negar o direito de revisão e fornecer mecanismos para que os indivíduos contestem essa decisão, quando aplicável."

{“615450”:"Em relação aos prazos para resposta do controlador em relação aos direitos exercidos pelos titulares no moldes dos incisos I e II do artigo 19 da LGPD, é preciso que se considere que tais prazos estão legalmente estabelecidos. No que se refere aos demais direitos listados nos incisos III a IX, para fins de segurança jurídica, de fato é imprescindível uma orientação mais clara da ANPD não só quanto aos prazos em si, mas também em relação à sua contagem. Quanto à sugestão de adotar os prazos da LAI, há uma distinção fundamental entre os propósitos das leis, que deve ser considerada. Enquanto a LGPD visa garantir que os titulares de dados exerçam uma série de direitos em relação aos seus dados pessoais, a LAI trata do acesso a informações públicas. Portanto, encargos decorrem dessa distinção, como a necessidade de verificação da identidade do titular, entre outros procedimentos técnicos e administrativos necessários para o cumprimento da LGPD, que inevitavelmente afetam o tempo necessário para atender a esses direitos, o que não se aplica à LAI. Nesse sentido, os prazos estipulados pela LAI podem ser considerados insuficientes para o atendimento dos direitos mencionados nos incisos III a IX do artigo 18 da LGPD, ainda mais porque são contados em dias corridos, como regra. Em contraste, o General Data Protection Regulation (“GDPR”) estabelece, em seu artigo 12 (3), que os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Assim, uma saída regulatória ao tema seria adotar os prazos estabelecidos pelo GDPR como inspiração. Contudo, para serem mais compatíveis com a forma de contagem brasileira, que seja previsto em formato de dias: 30 dias a partir do dia útil seguinte ao dia em que houver o recebimento de pedido legítimo, prorrogando-se para o dia seguinte o fim do prazo que caia em feriados ou finais de semanas. ...”,b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:“Entende-se que a distinção entre os prazos estabelecidos nos incisos I e II do artigo 19 da LGPD se baseia no nível de detalhamento das informações solicitadas. Enquanto o inciso I trata da confirmação de existência ou acesso a dados pessoais em formato simplificado, o inciso II aborda uma declaração mais abrangente, incluindo a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento. No que tange ao inciso I, é necessário esclarecimento quanto ao que se entende por atendimento imediato. Organizações de variados tamanhos e setores possuem realidades distintas de tratamento de dados, bem como números diversos de titulares e sistemas envolvidos, de modo que a interpretação conferida a este termo deve levar em consideração que o cumprimento depende de tempo hábil para processamento do pedido pelos agentes de tratamento. Nesse contexto, a questão pode ser desenvolvida a partir do §4º do artigo 19, que permite à Autoridade definir prazos diferenciados dos previstos nos incisos I e II do artigo 19 da LGPD para setores específicos. Nos caso em que setores específicos necessitam de tempo adicional para cumprir com os direitos de confirmação de existência ou o acesso a dados pessoais, seria possível (i) adotar entendimento flexível quanto à margem de cumprimento “imediato” (ex.: a partir da solicitação o sistema pode levar até 48 horas para gerar os dados em formato simplificado); e (ii) seguir o previsto pelo GDPR, conforme disposto em seu artigo 12(3): os direitos dos titulares devem ser atendidos em um mês, com a opção de prorrogação por até dois meses, levando em consideração a complexidade e o volume de solicitações. ... ”;“615484”:"Para garantir uma comunicação eficaz entre o titular e o agente de tratamento, a Câmara-e.net destaca a importância de a ANPD fornecer orientações claras

sobre vários aspectos. Estes incluem: (i) A importância de a Autoridade reconhecer a necessidade de cautela na autenticação do titular e possivelmente sugerir boas práticas para o tema; (ii) A necessidade de a Autoridade afirmar explicitamente que o processo de autenticação dos titulares antes do atendimento a solicitações relacionadas aos seus direitos é legítimo, e que cabe ao controlador determinar a melhor forma de realizá-lo, inclusive indicando quais dados deve ou não coletar para o cumprimento dessa função, considerando sua realidade organizacional, situação específica e riscos envolvidos, entre outros fatores; (iii) Estabelecer que o prazo para atender aos direitos dos titulares deve começar a partir do dia subsequente à validação de um pedido como legítimo, o que implica na autenticação do titular, na clareza do pedido e no seu encaminhamento por canal adequado; (iv) Reconhecer a liberdade do controlador para definir a abordagem mais apropriada para o atendimento dos titulares, como a utilização de um canal unificado ou a disponibilização de diversos canais; (v) Deixar claro que o formato da resposta ao titular deve ser determinado pelo controlador, levando em consideração a realidade organizacional e outras circunstâncias relevantes. Ao avaliar as características dos canais de atendimento aos titulares, é fundamental que a Autoridade leve em conta a diversidade dos agentes de tratamento, considerando fatores como tamanho e estrutura organizacional. É importante destacar que as organizações lidam de maneiras diversas com os direitos dos titulares, adaptando-se à sua realidade específica e sendo as mais indicadas para determinar as características desses canais. Nesse sentido, um estudo conduzido pela International Association of Privacy Professionals (The State of Data Rights, 2020) ressalta essas variações e suas implicações. ... ";615485": "É fundamental reconhecer que a execução adequada das obrigações legais pelo operador é essencial para garantir os direitos dos titulares. Isso inclui a obrigação de manter registros das operações de tratamento de dados pessoais (conforme estabelecido no artigo 37) e de conduzir o tratamento de acordo com as instruções do controlador (conforme estipulado no artigo 39). Quanto às responsabilidades específicas que devem ser atribuídas ao operador para viabilizar o adequado atendimento dos direitos dos titulares pelo controlador, é necessário estabelecê-las por meio de contrato, após negociações entre as partes. Essas responsabilidades podem abranger aspectos como suporte técnico e operacional, notificação tempestiva do recebimento de solicitações de exercício de direitos ou de solicitações de esclarecimento provenientes da Autoridade, entre outras. ";615486": "A adoção de abordagens semelhantes às do Serviço de Atendimento ao Consumidor ("SAC") apresenta desafios significativos quando aplicada ao atendimento dos direitos dos titulares. Vários aspectos tornam essa estratégia inadequada: 1) Disponibilidade contínua: Manter um serviço disponível 24 horas por dia, 7 dias por semana, é impraticável para muitas organizações, especialmente as de menor porte. Além disso, o atendimento adequado aos direitos dos titulares muitas vezes requer análises detalhadas, cooperação entre equipes e, por vezes, consultas legais, o que torna difícil manter uma disponibilidade ininterrupta. 2) Imposição do atendimento telefônico: Tornar o atendimento telefônico obrigatório limita a flexibilidade dos controladores para escolher o melhor meio de comunicação, desconsiderando as preferências e necessidades dos titulares. Isso pode, ainda, não ser eficaz para respostas mais complexas, considerando o que foi disposto no item anterior, e prejudicar a acessibilidade e conveniência para os titulares. 3) Acesso irrestrito aos dados: Embora a autenticação seja essencial para proteger os dados dos titulares, exigir acesso irrestrito pode comprometer a privacidade e segurança dessas informações. 4) Padronização excessiva do atendimento telefônico: Estabelecer requisitos rígidos para o atendimento por telefone pode resultar em burocracia e custos adicionais para as organizações, sem necessariamente melhorar a qualidade do serviço prestado. 5) Inclusão

obrigatória de opções de contato em documentos impressos: Exigir opções de contato em todos os documentos impressos pode ser excessivo e desnecessário, especialmente considerando o ambiente digital predominante. 6) Rigidez nos parâmetros de acompanhamento das demandas: Definir parâmetros muito específicos pode ser inadequado e inflexível, não levando em conta a diversidade das organizações, as necessidades dos titulares e a complexidade para elaboração de respostas às solicitações. ...";615487": "É fundamental reconhecer que alguns elementos necessitam de esclarecimentos por parte da ANPD, conforme destacado na resposta à questão “c” da presente Seção. No entanto, é crucial que as organizações tenham liberdade para estabelecer o formato de atendimento mais adequado às suas particularidades e às necessidades dos titulares dos dados. Essa abordagem se justifica por diversos motivos: Flexibilidade: As organizações possuem estruturas, processos e sistemas diferentes, o que significa que não há uma abordagem única que sirva para todas. Possibilitar que as organizações determinem seu próprio formato de atendimento permite adaptar-se de forma mais eficiente às suas próprias realidades e às demandas dos titulares. Inovação: Ao permitir que as organizações tenham liberdade para definir seus próprios formatos de atendimento, incentiva-se a inovação e o desenvolvimento de novas soluções e tecnologias que possam melhorar a experiência do titular e a eficiência do processo. Personalização: Cada organização pode ter uma compreensão diferente das necessidades e preferências dos seus titulares. Permitir que elas determinem seu próprio formato de atendimento possibilita a personalização das soluções para melhor atender às expectativas dos usuários. Eficiência econômica: Ao dar liberdade às organizações para estabelecerem seu próprio formato de atendimento, possibilita-se a busca por soluções mais econômicas e eficientes, levando em conta as capacidades financeiras e operacionais de cada organização. Portanto, embora seja importante que a ANPD forneça orientações claras e elucidativas, é igualmente crucial que as organizações tenham autonomia para determinar como implementar essas diretrizes de forma a melhor atender às necessidades dos titulares e garantir a conformidade com a legislação de proteção de dados. ";615491": "Primeiramente, é importante destacar que, embora a questão tenha sido abordada na seção dedicada ao direito de acesso, esta reflexão se estende a todos os direitos previstos na LGPD. Sobre os limites dos direitos dos titulares, é importante que se considere que nenhum direito individual deve ser considerado absoluto. Essa mesma lógica se aplica à interpretação da LGPD em relação aos novos direitos concedidos aos titulares de dados pessoais. Dentro desse contexto, existem valores e considerações legais que limitam o exercício dos direitos de acesso e outros direitos estabelecidos pela LGPD. Esses incluem: (i) a liberdade de expressão; (ii) necessidade de cumprimento de obrigação legal; (iii) a condução de investigações e processos internos; (iv) os direitos e liberdades de terceiros; (v) informações confidenciais e dever de sigilo; (vi) a proteção da propriedade intelectual e, de maneira mais ampla, dos segredos empresariais; e (vii) a impossibilidade de verificação da titularidade do solicitante. Além disso, é necessário coibir o exercício abusivo dos direitos, comportamento expressamente condenado pela legislação nacional (conforme o artigo 187 do Código Civil). Nesse sentido, pode haver recusa em atender a um pedido quando seu exercício for abusivo, o que pode ser determinado pelo excesso do pedido ou pela má-fé na solicitação. Como exemplos de condutas de má-fé, podem-se citar: (i) a ausência de intenção genuína de exercer o direito, buscando apenas prejudicar o controlador com solicitações infundadas; (ii) solicitações maliciosas feitas com o intuito de assediar a organização sem propósito legítimo; (iii) insistência em usar um canal inadequado para o exercício dos direitos, apesar das orientações do controlador; (iv) direcionamento do pedido a um funcionário específico por motivos pessoais; ou (v) envio

sistemático de múltiplos pedidos sem aguardar o prazo de resposta. ...";615492": "Entendemos que a obrigação de fornecer informações sobre o compartilhamento de dados deve se restringir à indicação das categorias de destinatários e às finalidades para as quais os dados são tratados, o que atende ao princípio da transparência e às solicitações de acesso dos titulares dos dados. Nesse sentido, é importante considerar que a divulgação nominal das entidades públicas e privadas com as quais o controlador compartilhou dados pode acarretar uma série de problemáticas. São exemplos: Aspectos concorrenciais: Revelar as entidades com as quais o compartilhamento é realizado pode proporcionar uma vantagem competitiva a determinadas empresas, o que pode distorcer o mercado e prejudicar a concorrência. Propriedade intelectual e segredo de empresa: Em muitos casos, as informações sobre as entidades com as quais os dados são compartilhados são consideradas confidenciais e estratégicas para a empresa. Divulgá-las nominalmente pode comprometer a propriedade intelectual e o segredo empresarial, especialmente se a restrição a essas informações representar um valor econômico significativo para a empresa. Confidencialidade contratual: Em alguns casos, as organizações podem estar sujeitas a acordos de confidencialidade que as proíbem de divulgar a identidade das entidades com as quais compartilham dados. Isso pode ocorrer em contratos comerciais ou parcerias estratégicas, nos quais a confidencialidade é essencial para proteger os interesses das partes envolvidas. Sugerimos que, caso o titular não esteja satisfeito com os dados fornecidos inicialmente, seja adotada uma abordagem de repasse de informações em camadas, como recomendado pela Agência Espanhola de Proteção de Dados ("AEPD"). Isso permitiria um fornecimento mais específico de informações sobre as entidades com as quais o compartilhamento é realizado, garantindo ao mesmo tempo a proteção dos interesses comerciais e legais das organizações envolvidas. Mais detalhes sobre essa abordagem podem ser encontrados no seguinte link: . ";615489": "É fundamental reconhecer que a execução adequada das obrigações legais pelo operador é essencial para garantir os direitos dos titulares. Isso inclui a obrigação de manter registros das operações de tratamento de dados pessoais (conforme estabelecido no artigo 37) e de conduzir o tratamento de acordo com as instruções do controlador (conforme estipulado no artigo 39). Quanto às responsabilidades específicas que devem ser atribuídas ao operador para viabilizar o adequado atendimento dos direitos dos titulares pelo controlador, é necessário estabelecê-las por meio de contrato, após negociações entre as partes. Essas responsabilidades podem abranger aspectos como suporte técnico e operacional, notificação tempestiva do recebimento de solicitações de exercício de direitos, entre outras. ";615490": "Para atender ao requisito do inciso I do artigo 19 da LGPD, que estabelece a necessidade de uma declaração em formato simplificado sobre o tratamento de dados pessoais, entendemos que bastaria o fornecimento de uma cópia dos dados pessoais do solicitante, a depender da extensão daquilo que foi solicitado pelo titular. Nesse formato simplificado, deve-se evitar que nele se encaixem pedidos genéricos ou excessivos relacionados "a todos os dados em posse do controlador" ou "tudo que tenha sobre mim", mas sim atrelar a um contexto / serviço / funcionalidade determinada, que deve estar expressa no requerimento do titular (ex.: "fornecer os meus dados cadastrais em posse do controlador", "histórico de minha transação financeira", "histórico de meus pedidos" etc.). Além disso, é importante que a Autoridade esclareça que o fornecimento da declaração em formato simplificado é suficiente para fins de cumprimento do direito de acesso, salvo se o titular expressamente solicitar a declaração completa. ";615494": "As informações destinadas ao titular sobre o tratamento de seus dados, sem necessidade de solicitação específica, estão definidas no artigo 9º da LGPD e, portanto, estarão nas políticas de privacidade externas do controlador. Estas incluem a

finalidade específica do tratamento, a modalidade e o prazo do tratamento, respeitando os segredos comerciais e industriais, a identificação e os detalhes de contato do controlador, informações sobre o compartilhamento de dados pelo controlador, considerando apenas as categorias de destinatários e sua finalidade, as responsabilidades dos agentes encarregados do tratamento e os meios para exercício dos direitos do titular, com destaque para os direitos listados no artigo 18 da lei. É importante esclarecer que, devido à complexidade de algumas dessas informações, elas poderão ser fornecidas de forma mais ampla, inclusive para permitir o entendimento do titular. Em relação ao exercício dos direitos dos titulares, entende-se que a LGPD requer que o controlador oriente os titulares a respeito do meio de seu exercício, capacitando-os. Contudo, não requer informações publicamente disponibilizadas sobre os critérios e procedimentos utilizados na decisão automatizada, sendo que essas informações requerem a solicitação do titular, dentro do contexto do artigo 20 da LGPD. Além disso, no contexto das informações solicitadas pelos titulares, a Câmara-e.net gostaria de reiterar a abordagem recomendada pela Agencia Española de Protección de Datos, que propõe a disponibilização dessas informações em camadas aos titulares. Mais detalhes sobre essa metodologia podem ser consultados no seguinte link: [";615493":](#)"A questão suscita certa ambiguidade em relação ao seu propósito, porém, parece estar questionando se o direito de acesso é considerado satisfeito quando o agente de tratamento disponibiliza os dados pessoais em formato digital ou em papel, de acordo com a escolha do titular. O parágrafo 2º do artigo 19 da LGPD estipula que o controlador deve cumprir o direito de acesso conforme solicitado pelo titular. Isso implica que, caso o titular especifique sua preferência por um formato específico (digital ou papel), o controlador deve fornecer os dados nesse formato. No entanto, na ausência de especificação por parte do titular, cabe ao controlador selecionar o meio que considere mais adequado para disponibilizar os dados. Além disso, entendemos que o formato da entrega “em papel”, advinda da requisição de “forma impressa”, deve ser interpretada à luz das evoluções tecnológicas recentes. Atualmente, serviços podem ser desenvolvidos e prestados inteiramente em formato digital, de modo que se faz necessário que a Autoridade possibilite que a escolha pelo titular em receber os dados de forma impressa inclua a via do documento digital em que se permite a sua impressão pelo titular, o que inclusive é condizente com os fundamentos da LGPD nos quais, dentre outros, se incluem o desenvolvimento econômico, tecnológico e a inovação. [";615502":](#)"É fundamental destacar que, antes de determinar se um certo setor possui maturidade para atender aos pedidos de portabilidade, várias questões precisam ser esclarecidas (definição de portabilidade e interoperabilidade, limites técnicos e legais, consentimento de terceiros, responsabilidade dos agentes de tratamento, limites diante de direitos de propriedade intelectual e segredo de negócio, etc). Logo, esse tema deve ser discutido em tomadas de subsídios e consultas públicas para compreensão e esclarecimento das complexidades envolvidas no atendimento a um eventual pedido do titular para a portabilidade de seus dados. Para alguns dos associados da Câmara-e.net, a portabilidade de dados não representa um desafio significativo. Um exemplo notável é a abordagem da Google, que oferece aos seus usuários a portabilidade de dados há mais de uma década. Desde 2007, a empresa investiu em uma equipe dedicada à facilitação da exportação de dados de seus produtos, culminando no desenvolvimento do Google Takeout, que permite o download de dados de mais de 70 produtos da Google (mais informações podem ser encontradas aqui: <: <https://blog.google/outreach-initiatives/public-policy/building-data-portability-help-consumers-choose/>). Além disso, em 2018, Google, Apple, Meta, Microsoft, Twitter e SmugMug lançaram o Projeto de Transferência de Dados (DTP), uma iniciativa que visa simplificar a portabilidade de dados em nível

global. O DTP desenvolveu um framework de tecnologia de código aberto que alimenta recursos de transferência direta de dados em serviços como Google Takeout, Transferência de Informações do Facebook e Página de Dados e Privacidade da Apple (mais informações encontram-se disponíveis aqui:). Outros associados, por sua vez, cumprem o direito à portabilidade por meio de soluções próprias ou de terceiros. ...";615501": "Os desafios para a implementação do direito à portabilidade vão desde aspectos legais, por exemplo, o que realmente é a portabilidade de dados e quais dados podem estar sujeitos a ela, até técnicos, por exemplo, como permitir que indivíduos movam, copiem ou transfiram facilmente dados pessoais em diferentes plataformas de maneira segura e protegida. Entretanto, dado que a portabilidade de dados requer adoção de medidas administrativas e técnicas para desenvolvimento ou aprimoramento das tecnologias específicas para a sua implementação, poucas orientações até o momento foram fornecidas aos responsáveis pelo tratamento de dados no que diz respeito à conformidade. Levando em consideração os diversos campos de ação do setor privado e os diferentes estágios de maturidades em tecnologia de cada organização, a ANPD deve fornecer esclarecimentos e apresentar exemplos concretos, no sentido de explicar as circunstâncias nas quais este direito é aplicável, quais os limites quanto ao alcance dos pedidos e abrangência do fornecimento de dados, bem como permitir que as organizações tenham flexibilidade para entender e adotar o melhor formato de atendimento aos pedidos de portabilidade para cada uma, em respeito às melhores práticas dos seus setores, possibilitando maior eficiência na adaptação das diferentes realidades em estrutura, processos e sistemas, devendo haver especial atenção da ANPD quanto a preservação dos segredos comerciais e industriais, expressamente ressaltados no artigo 18 inciso V da LGPD. ";615505": "As organizações devem ter flexibilidade e autonomia para escolha do melhor formato para a transmissão dos dados, respeitando um formato que seja de uso corrente e garanta a interoperabilidade, o que não implica exigir que os responsáveis pelo tratamento tenham que necessariamente manter sistemas compatíveis. A ANPD deve focar, portanto, no desenvolvimento de padrões e boas práticas que permitam a comunicação de sistemas, arquivos e/ou ferramentas sem que, com isso, se dê preferência a uma delas em detrimento das demais. Isso porque, o mercado é dinâmico e a tecnologia evolui a níveis exponenciais, sendo plausível que o mercado se autorregule nas formas de interação e comunicação para a implementação da interoperabilidade. Cabe à ANPD, portanto, orientar e trazer exemplos concretos, sem limitar as vias técnicas possíveis. ";615503": "Embora a LGPD não traga essa possibilidade de forma expressa no artigo 18, inciso V, o artigo 40 permite a compreensão no sentido de que uma vez fornecidos os dados para o titular em formato interoperável, conforme futuro Regulamento da ANPD, o direito de portabilidade poderá ser considerado com atendido, nos moldes do que é previsto no GDPR. Isso porque se o próprio titular optar por solicitar os dados pessoais a certo controlador em formato interoperável, é porque entende que seu direito será melhor atendido dessa forma. Assim, entendemos ser importante que a ANPD disponha sobre padrões de modo flexível, permitindo aos agentes adequar-se segundo as práticas consolidadas e o contexto das atividades de tratamento específicas de seus nichos, levando em consideração fatores como: (i) os segredos comercial e industrial; (ii) a carga financeira ou técnica excessiva ou irrazoável para o porte da empresa; (iii) os direitos e a privacidade de terceiros; (iv) a quantidade e complexidade dos dados solicitados; (v) o volume de solicitações. É relevante observar que este aspecto do direito de portabilidade não deve: 1) Impor aos controladores a obrigação de adotar e manter sistemas de processamento tecnicamente compatíveis; 2) Responsabilizar o agente de tratamento transmissor pelo tratamento realizado pelo próprio titular dos dados ou por outro agente de tratamento receptor dos dados

peçoais; 3) Estabelecer uma obrigação específica de verificar a qualidade dos dados antes da transmissão; 4) Exigir que o controlador retenha os dados pessoais por mais tempo do que o necessário ou além de qualquer período de retenção especificado. 5) Incluir informações que revelem segredos comercial e industrial, como categorias de segmentação de titulares de dados, trazendo, em exemplos, os critérios ou as informações mínimas que poderiam ser assim consideradas. "615504": "É plausível permitir que o setor privado desempenhe um papel na definição de padrões de interoperabilidade específicos para diferentes atividades econômicas no âmbito da portabilidade de dados. Essa abordagem se justifica pela diversidade de necessidades e características que os diversos setores podem apresentar em relação à variedade de formatos de dados tratados e à transferência de dados entre sistemas e plataformas distintas. Envolvendo o setor privado nesse processo, podemos esperar soluções mais adaptadas e eficazes tanto para empresas quanto para consumidores dentro de cada setor. Embora possam servir como referências úteis ou diretrizes para as empresas, esses padrões específicos não podem ser interpretados como uma imposição, o que poderia limitar a capacidade das organizações de encontrar as soluções mais adequadas às suas necessidades individuais ou de seus setores. No que se refere ao estabelecimento de prazos, considerando que a definição pelo setor privado será apenas uma sugestão, não haveria que se falar em prazo para a implementação desses padrões. "615511": "A fim de avaliar a qualidade de um dado, considerando se está incompleto, inexato ou desatualizado, é necessário analisar a situação específica à luz dos princípios da qualidade e finalidade estabelecidos pela LGPD. Embora o princípio da qualidade demande a exatidão dos dados, é relevante entender que essa exigência pode variar conforme a finalidade do tratamento. Por exemplo, em um cadastro de e-commerce, pode ser aceitável que o titular forneça apenas um dos seus sobrenomes, enquanto em procedimentos mais formais, como o registro de uma escritura de imóvel, a precisão dos dados torna-se mais crucial. O Information Commissioner's Office ("ICO", disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/#ib5>) destaca que, ao receber um pedido de retificação, o controlador deve adotar medidas razoáveis para verificar a precisão dos dados e corrigi-los, se necessário. Essas medidas devem levar em conta a natureza dos dados pessoais e sua finalidade de uso. Quanto maior for a necessidade de precisão da informação, mais esforço será necessário para verificar e corrigir sua exatidão, especialmente se os dados forem fundamentais para decisões significativas que impactam o indivíduo ou terceiros. Adicionalmente, é essencial estabelecer claramente os limites desse direito, assegurando que ele se aplique apenas a dados genuinamente incompletos, inexatos ou desatualizados. Esse direito não deve ser utilizado para revisar eventos passados, e os controladores devem ter o direito de solicitar ao indivíduo evidências específicas que comprovem a incorreção das informações retidas. É crucial ainda que tais evidências se refiram exclusivamente a fatos, excluindo opiniões, em respeito à liberdade de expressão. A ANPD deve deixar claro que a retificação se aplica exclusivamente a dados que são factualmente incompletos, inexatos ou desatualizados, e não a dados com os quais o indivíduo simplesmente discorda. "615514": "É relevante destacar a estreita relação entre o direito de correção e o princípio da qualidade dos dados, que visa garantir aos titulares a exatidão, clareza, relevância e atualização dos dados conforme necessário para cumprir a finalidade do seu tratamento. Nesse contexto, é fundamental que o controlador tenha a possibilidade de solicitar aos titulares (i) elementos suficientes para comprovar a autenticidade do titular-requerente para evitar incidente de segurança; (ii) evidências de que os dados estão incompletos, inexatos ou desatualizados; e (iii) as informações necessárias e comprovadas para

fins de correção. Por exemplo, o Information Commissioner's Office ("ICO", para mais informações consulte: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/>) destaca que, ao receber uma solicitação de correção, o controlador deve adotar medidas razoáveis para verificar a qualidade dos dados e corrigi-los, se necessário, levando em consideração os argumentos e as evidências apresentadas pelo titular. "615513": "Para determinar a impossibilidade ou o esforço desproporcional, conforme definido no art. 18, § 6º, da LGPD, é fundamental examinar cada caso de maneira específica e individualizada. Não existe uma lista definitiva de critérios objetivos que se apliquem uniformemente a todas as situações. Em vez disso, é necessário uma análise dos detalhes específicos de cada solicitação de acesso aos dados pessoais. Essa abordagem personalizada permite considerar uma variedade de fatores contextuais que podem influenciar a capacidade de atender à solicitação. Por exemplo, o volume de solicitações, os recursos disponíveis para o controlador, o tamanho da equipe responsável pelo tratamento dos dados e os possíveis impactos nas operações do controlador são aspectos relevantes a serem ponderados. Portanto, ao lidar com solicitações de acesso aos dados pessoais, é essencial que o controlador avalie cada situação individualmente, levando em conta os diversos fatores que podem afetar a capacidade de atender à solicitação de maneira adequada e em conformidade com a LGPD. Isso garante o respeito efetivo aos direitos dos titulares de dados, ao mesmo tempo em que reconhece os desafios e limitações enfrentados pelos controladores na gestão e proteção desses dados. "615512": "Considerando os preceitos do princípio da qualidade dos dados e as disposições do inciso III do artigo 18, é facultado ao controlador recusar o atendimento ao pedido do titular caso julgue que os dados estejam completos, precisos e atualizados. Ademais, a falha na verificação da autenticidade e a ausência dos documentos necessários fornecidos pelo titular também pode fundamentar a negativa do controlador. Acrescenta-se que a ANPD deve esclarecer que o direito de correção não implica em uma revisão retroativa, visando, assim, evitar possíveis implicações legais decorrentes de mudanças passadas, e que deve ser restrito a fatos, preservando a liberdade de expressão (essas opiniões são defendidas pelos Centre for Information Policy Leadership no seguinte documento:). Além disso, reitera-se os pontos trazidos em relação aos limites do exercício abusivo de direito, o que pode ser verificado pelo excesso do pedido, e até mesmo pela má-fé na solicitação dos dados. Como condutas de má-fé podem ser consideradas as seguintes situações, entre outras: (i) o indivíduo claramente não tem intenção de exercer o seu direito, mas procura retaliar ou incomodar o controlador de seus dados com pedidos descabidos; (ii) a solicitação tem intenções maliciosas e está sendo evidentemente usada para assediar, de forma recorrente, uma organização sem nenhum propósito real a não ser causar transtorno; (iii) quando o controlador indica o canal correto para o exercício dos direitos (ex: OneTrust, e-mail específico, campo específico em seu website) e o titular insiste reiteradamente em realizar o exercício por canal diverso; (iv) o pedido é feito a um funcionário específico contra o qual fica evidente que o requerente tem algum rancor pessoal; ou (v) quando o titular envia sistematicamente pedidos de correção para o controlador sem sequer aguardar o decurso do prazo para resposta. ... "615517": "Sim, de acordo com o inciso IV do artigo 18, o titular deve apresentar justificativas e evidências que indiquem que os dados são desnecessários, excessivos ou estão sendo tratados em desconformidade com a legislação, a fim de exercer os direitos de anonimização, bloqueio ou eliminação. Assim, é fundamental que a ANPD esclareça aos titulares que forneçam recursos suficientes para os agentes de tratamento analisarem as solicitações, sobretudo em relação à identificação do possível problema que ocasionou o pedido. Em muitos casos, o titular se opõe ao tratamento com

alegação de irregularidade, mas que na verdade é uma incompreensão ou falta de conhecimento da legislação nacional e da regulamentação setorial no tema, por falta de leitura dos contratos que fazem parte (Termos de Uso, Política de Privacidade ou demais contratos de prestação de serviço), e até mesmo por desconhecimento da existência de outras bases legais para além de seu consentimento. É importante ressaltar ainda que a anonimização, bloqueio ou eliminação não devem ser realizados se o controlador estiver tratando os dados pessoais de acordo com uma base legal válida (por exemplo: cumprimento de obrigação legal ou regulatória pelo controlador, como é o caso do artigo 16 da Resolução BCB nº96/2021, para o exercício regular de direitos em processo judicial, administrativo ou arbitral e prevenção à fraude e à segurança do titular), pois nesse caso os dados continuarão sendo necessários e seu uso será legalmente justificado. Além disso, os dados também poderão ser mantidos nos casos previstos no artigo 16 da LGPD. ...";615516": "Sim, tanto a anonimização quanto à eliminação são medidas que podem ser consideradas de forma alternativa, dependendo do contexto específico, sendo ambas reconhecidas pela Lei Geral de Proteção de Dados Pessoais. O artigo 12 da LGPD estipula que os dados anonimizados deixam de ser considerados dados pessoais. Isso implica que, ao seguir os critérios definidos pela legislação para anonimização, os dados perdem sua capacidade de identificar indivíduos, oferecendo uma alternativa viável à eliminação completa dos dados. Além disso, o inciso IV do artigo 16 da LGPD permite a retenção de dados pessoais pelo controlador, desde que os dados sejam anonimizados e utilizados exclusivamente por ele. Essa disposição legal reconhece que a anonimização dos dados oferece um nível suficiente de proteção à privacidade, permitindo que o controlador mantenha os dados para usos específicos, desde que não possam ser acessados por terceiros. Portanto, a LGPD reconhece tanto a anonimização quanto à eliminação como medidas equivalentes para garantir a proteção dos dados pessoais, oferecendo às organizações a flexibilidade necessária para escolher a abordagem mais adequada às suas necessidades e à natureza dos dados envolvidos. ";615518": "Se a alegação do titular for considerada legítima de acordo com o art. 18, § 2º, da LGPD, isso implica que o controlador deve atender ao pedido formulado pelo titular. Essa obrigação de cumprimento do pedido não apenas satisfaz as demandas individuais do titular, mas também induz o controlador à conformidade legal com a LGPD. Com o atendimento de tal pedido e a consequente conformidade legal, o direito de oposição, nos termos do referido dispositivo, perde seu fundamento. ";615523": "A revogação do consentimento, conforme estipulado no art. 18, IX, da LGPD, não implica necessariamente na obrigação de eliminar os dados pessoais tratados com base nesse consentimento. Isso se deve à possibilidade de existir outra base legal que justifique o tratamento desses dados, como em casos em que são necessários para o cumprimento de um contrato entre o controlador e o titular dos dados, ou para o cumprimento de uma obrigação legal. É importante ressaltar que, frequentemente, as empresas precisam dos dados pessoais para uma variedade de propósitos, e o tratamento pode ser fundamentado em mais de uma base legal, conforme se extrai do artigo 16 da LGPD. Portanto, a revogação do consentimento não implica automaticamente na exclusão de todos os dados, tampouco afeta o tratamento de dados realizado até o momento em que a eliminação foi solicitada, sendo, em princípio, legítimo o tratamento de dados realizado até então. Esse entendimento é corroborado pelos Guidelines on consent under Regulation 2016/679 do Working Party 29, que destacam a complexidade das bases legais para o tratamento de dados (disponível em: <https://ec.europa.eu/newsroom/article29/items/623051>). Além disso, um exemplo prático é a necessidade do controlador de reter os dados para garantir o cumprimento das preferências do titular. Nesse cenário, é necessário manter certos dados para assegurar que determinado

tratamento não ocorra, o que evidencia a importância de considerar diferentes bases legais para o tratamento de dados pessoais. "615521": "Na falta de outra base legal para o tratamento, a eliminação dos dados é obrigatória. Quando os dados foram compartilhados, é crucial notificar os entes com quem foram compartilhados. No entanto, em certas situações específicas, é imprescindível que o controlador mantenha certos dados para orientar suas ações. Por exemplo, se um titular manifestar o desejo de não receber mais propagandas, é necessário manter os dados para garantir que o direcionamento não ocorra. É importante destacar, contudo, que o tratamento realizado com base no consentimento anterior à revogação continua legalmente válido. Portanto, nas situações em que os dados tenham outras finalidades a eles atreladas (por exemplo, contrato vigente, obrigação legal ou regulatória, legítimo interesse para combate à fraude, defesa judicial etc), o regime do artigo 18, IV, da LGPD é que deve ser aplicado, considerando que os dados serão mantidos não pelo consentimento já revogado, mas sim para dar cumprimento às demais situações que justificam a sua retenção, que envolvem as demais bases legais do art. 7º ou 11 da LGPD. "615617": "Uma decisão tomada unicamente com base em tratamento automatizado é aquela na qual não há participação humana no processo de tomada de decisão. Isso implica que a decisão é completamente gerada por meio de processamento automatizado, sem qualquer intervenção ou influência direta de indivíduos. Além disso, é importante observar que, ao discutir a LGPD e, mais especificamente, o artigo 20, está a se debater decisões automatizadas que envolvam o tratamento de dados pessoais e que necessariamente afetem os interesses dos titulares de dados envolvidos. "615618": "Para determinar quando um interesse está sendo efetivamente afetado, a ANPD deve levar em consideração, no cenário brasileiro, critérios ou situações em que: (i) o indivíduo é impossibilitado - ilegalmente - de exercer regularmente seus direitos previstos pelo ordenamento jurídico de modo prolongado, causando efeitos negativos que comprometam o exercício de direitos fundamentais; (ii) o indivíduo é - ilegalmente - prejudicado em seu acesso a serviços, por exemplo, relacionado a educação, saúde, transporte etc.; (iii) o indivíduo sofre com situações ilícitas, com impactos graves ou prejudiciais, como em caso de discriminação. "615619": "A aplicação do direito de revisão de decisões, conforme delineado no art. 20 da LGPD, enfrenta uma série de desafios práticos consideráveis. Um dos principais obstáculos reside na complexidade dos sistemas que empregam tecnologias de aprendizado de máquina e inteligência artificial. Estes sistemas frequentemente geram decisões automatizadas com base em algoritmos intrincados, dificultando a explicação clara aos titulares sobre os motivos subjacentes a uma decisão específica. Ademais, a possível necessidade de intervenção humana para revisar e explicar as decisões automatizadas pode acarretar custos adicionais de recursos para as organizações. Isso decorre do fato de que a participação humana pode elevar os custos operacionais e administrativos, sem que, necessariamente, ganhe-se em capacidade intelectual, eficiência ou que se potencialize seus efeitos mitigatórios, já que o humano possui acesso a menos informações ou variáveis do que os inputs fornecidos na decisão automatizada. Outro desafio está em fornecer explicações claras e acessíveis aos titulares sem comprometer os direitos de propriedade intelectual e segredos comerciais das organizações. A divulgação das informações requeridas pelos §1º do artigo 20 pode entrar em conflito com a necessidade de resguardar informações confidenciais e estratégicas da empresa, criando uma complexidade adicional na aplicação desse direito. Além disso, a manutenção de registros detalhados sobre as decisões tomadas e os processos envolvidos pode demandar investimentos significativos em sistemas de registro e armazenamento de dados. Isso pode representar um desafio para pequenas e médias empresas. Por fim, a efetiva implementação do direito de revisão de

decisões também está sujeita à definição do que seria “afetar interesses”, o que se espera seja definido pela ANPD de forma razoável. ",615620": "Sim, o controlador pode negar o direito de revisão sobre decisões automatizadas quando: (i) a decisão possuir alguma participação humana ou a decisão automatizada não impactar de forma relevante os interesses do titular, o que não se enquadra nos termos do artigo 20 da LGPD, afastando a sua incidência (em linha com os itens “a” e “b” acima); (ii) a resposta pode revelar algoritmo, informações do código fonte ou a lógica de programação, violando direitos de propriedade intelectual e segredo comercial; e (iii) quando a revisão é inviável, seja por questões técnicas ou práticas. "

{ "615450": "A LGPD estatui uma dupla possibilidade de atendimento para os direito de acesso e confirmação: (i) imediatamente por meio de um relatório em formato simplificado ou; (ii) por meio de um relatório completo, que contenha todas as informações previstas no art. 19, II no prazo de 15 dias. Nesse sentido, pontua-se que esta é a regra geral aplicável aos casos em que não houver norma específica que regule outros setores. O racional de possibilitar a prorrogação deste prazo mediante justificativa expressa previsto na LAI poderá adotado na regulamentação pela ANPD sem contrariar o disposto na LGPD, como uma forma de comportar as dificuldades em seu atendimento para diferentes realidades. Para os demais direitos da LGPD entendemos que o parâmetro de prazo previsto na LAI, aplicável somente à administração pública considera um contexto e grau de complexidade distintos dos enfrentados pelo setor privado, em resumo, pois a) o conjunto de direitos facultados aos titulares na LGPD é mais complexo do considerado para o caso da LAI, 2) A iniciativa privada, por vezes, está sujeita a procedimentos mais complexos para possibilitar o atendimento do direito 3) a obrigação de transmissão do pedido do titular a outros agentes de tratamento (que adiciona mais uma camada de processos e procedimentos), 4) a LAI permite ao solicitante acesso o atendimento do pedido formulado com a especificação da informação requerida, ao passo que os direitos conferidos pela LGPD contemplam a totalidade dos dados pessoais tratados pelo agente. O GDPR, aplicável à países com histórico e cultura de proteção de dados mais madura, impõe um prazo de 30 dias a contar da data de apresentação do pedido, podendo ser prorrogado no caso de pedidos complexos ou se tiver recebido vários pedidos da pessoa em causa. Entendemos que este deve ser o parâmetro aplicado pela ANPD. No caso de normas mais específicas, tal como CDC e LAI, deverá se aplicar a norma específica, adequada àquela realidade. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:"Considera-se que esta previsão está atrelada à capacidade/dificuldade específica imposta aos controladores para atendimento dos referidos direitos, ainda que a LGPD, no artigo 19, §4º, indique que a ANPD poderá dispor de forma diferenciada acerca dos prazos previstos para setores específicos. Em princípio, entende-se que a capacidade/dificuldade de observância de tal dever relaciona-se, sobretudo, não somente às características de determinado setor mas, sobretudo, ao porte, faturamento e capacidade dos agente. Ademais, é fundamental que o regulamento da ANPD faça um cruzamento expresso e ratifique os prazos diferenciados para atendimento dos direitos dos titulares previstos no Regulamento de Agentes de Pequeno Porte. Desta forma, aduz-se que o principal critério a ser verificado para o estabelecimento de prazos diferenciados para atendimento destes direitos seja o volume/relevância de dados tratados tradicionalmente em determinados setores, pois isso torna o processo de atendimento de dados pessoais mais ou menos oneroso (tanto por volume de requerimentos concomitantes em processamento, quanto pela diversidade e complexidade das buscas a serem feitas para o atendimento de tais direitos). Por fim, faz-se essencial que sejam feitos recortes mesmo dentro dos setores, considerando a diversidade de agentes e os diferentes elos da cadeia. Por exemplo no setor elétrico, há uma cadeia que envolve tanto transmissoras de energias quanto distribuidoras de energia, que possuem desafios e capacidades completamente distintas - denotada, por exemplo, pela maior interação com o usuário-final, o que enseja um maior tratamento de dados pessoais. "; "615484": " Em linha com a LGPD, entende-se que um canal de atendimento ideal para assegurar a comunicação entre o titular e o agente de tratamento é aquele que contenha as

seguintes características: (i) Meios de comunicação: Na medida do possível, o oferecimento de diferentes formas de contato de acordo com as capacidades dos agentes e necessidades dos titulares (como por exemplo, e-mail, canal de mensagens, telefone e entre outros); (ii) Acessibilidade e transparência: Simplicidade e clareza nas comunicações, respeitando as capacidades dos diferentes titulares; (iii) Segurança e privacidade das comunicações: garantia de que as informações tratadas nas comunicações tenham os mesmos cuidados dispensados com os demais tratamentos de dados; (iv) Disponibilidade: Disponibilidade dos diversos canais de atendimento, na medida do possível e; (v) Prazo de resposta ágil: celeridade, dentro dos limites estabelecidos pela lei. Nesse sentido, urge salientar a necessidade da ANPD definir o que entende por "imediatamente" nos termos da LGPD, quais deveriam ser os parâmetros considerados nesse tipo de comunicação simplificada."

"615485": "Sim. Embora não sejam os diretamente responsáveis perante os titulares (na forma da lei), a LGPD a eles se aplica (especialmente autodeterminação informativa dos titulares, transparência, livre acesso, qualidade), de forma que devam apoiar e contribuir (não fornecer embaraços) ao recebimento, processamento/encaminhamento e implementação dos direitos dos titulares (nos limites do que lhe for aplicável conforme o caso concreto), tendo também por base a forma e o prazo previsto na legislação, principalmente quando silente o contrato que regule esta questão. No entanto, a maneira específica, como procedimentos e limites de interação com os titulares, deve ser regulamentada em contrato contendo tais pormenores e não via regulamentação da ANPD, sob pena de interferência no relacionamento privado e processos definidos e negociados entre as partes. O tipo e o grau de assistência a ser prestado pelo operador podem variar muito tendo em vista a natureza do tratamento e as informações de que o operador dispõe."

"615486": "Entendemos que o Decreto nº 11.034, de 5 de abril de 2022 não é aplicável para o exercício dos direitos do titular de dados pessoais, uma vez que sua regulamentação se concentra nas relações de consumo e se aplica exclusivamente aos fornecedores de serviços regulados pelo Poder Executivo federal. No entanto, algumas diretrizes e procedimentos sobre o Serviço de Atendimento ao Consumidor ("SAC") podem servir como referência para orientar a regulamentação do atendimento dos titulares de dados, uma vez que a LGPD garante o direito do titular de peticionar em relação aos seus dados perante os organismos de defesa do consumidor (art. 18º, § 8º), além de ambas as regulamentações tratarem da proteção ao indivíduo e da gestão de informações pessoais. Dessa forma, algumas diretrizes estabelecidas no Decreto podem ser adotadas para o exercício dos titulares de dados, como: (i) a gratuidade do atendimento; (ii) a disponibilidade, na medida do possível, dos canais de atendimento; (ii) a tempestividade, privacidade e segurança na solução da demanda; (iii) o direito de acesso ao histórico das comunicações, quando possível e; (iv) a clareza, objetividade e abrangência da resposta à demanda. No entanto, é importante ressaltar que a LGPD tem características específicas que diferem das regulamentações relacionadas ao SAC (i.e o tratamento de dados pessoais muitas vezes envolve considerações mais sensíveis e complexas, como consentimento, finalidade da coleta etc.). Portanto, é imprescindível que estabeleçam diretrizes para atender às nuances específicas da LGPD."

"615487": "Sem comentários"

"615491": "Entendemos que existem hipóteses excepcionais para negar o direito de confirmação do tratamento, que podem, inclusive, ser endereçadas pelo agente de tratamento mediante explicação de razões de fato ou de direito - conforme previsão do artigo 18, §4º, II, da LGPD. É o caso, por exemplo, de previsão legal que impossibilite ao agente de tratamento a confirmação de existência ou não de tratamento de dados ao titular, em razão de deveres de sigilo previstos em lei. No mesmo sentido, é possível considerar a existência de decisões judiciais e/ou obrigações regulatórias que impeçam o cumprimento do

referido direito. Ademais, cabe considerar previsão da regulação europeia de dados (GDPR, art. 14) que estabelece que, quando dados utilizados não vieram diretamente por meio do titular, informações sobre o tratamento ao titular podem ser excepcionadas se (i) o titular já possuir acesso àquela informação; (ii) ser impossível providenciar a informação ou o fornecimento da informação envolver esforços desproporcionais; (iv) tornar impossível ou prejudicar gravemente a consecução dos objetivos do tratamento; (v) existirem obrigações legais impostas sobre o controlador que limitem informação sobre o tratamento, incluindo confidencialidade e sigilo. Entendemos que esses parâmetros poderiam inspirar a autoridade para excepcionar respostas a pedidos de confirmação do tratamento. Ainda sobre a experiência internacional, aponta-se que a ICO aborda a possibilidade da negativa de acesso em casos em que um órgão público que identifique um conflito entre a solicitação do titular de confirmação com base na lei de dados e alguma legislação ou procedimento vigente, deve avaliar (i) se possui as informações solicitadas e (ii) se a confirmação ou negação da existência do tratamento poderia interferir em algum procedimento ou investigação em curso confidencial. Conclui-se que esses parâmetros poderiam servir de inspiração para a regulamentação de confirmação de existência. "615492" Em relação aos dados de identificação do controlador, cabe recordar que o fundamento legal dessa exigência está, primeiro, refletido no art. 9º, IV, da LGPD, qual prevê ser necessário fornecer ao titular dos dados as informações de contato do controlador. A fim de que as informações permitam comunicação efetiva entre titular e controlador para exercício de seus direitos (seja por meio digital ou por correspondência física), é importante que sejam informados endereço, CNPJ, canais de comunicação por e-mail para contato e telefone). Já no caso de uso compartilhado de dados pessoais, as informações mínimas a serem fornecidas para os titulares tem como base legal o artigo 9º, V, da LGPD. De acordo com o referido dispositivo, é necessário o fornecimento de informações acerca do uso compartilhado de dados pelo controlador e a sua finalidade. Muito embora a especificações quanto à finalidade do compartilhamento sejam de suma importância para transparecer de forma adequada ao titular as condições do tratamento – como categorias de dados compartilhados e de agentes que receberam os dados - entendemos que o fornecimento de informações de identificação da totalidade de agentes que tem posse de dados compartilhados pode não só ser impossível de ser realizado de forma atualizada e com qualidade, como não agregar – ou mesmo, ter o condão de atrapalhar - na compreensão do titular acerca do tratamento. Nessa linha, entendemos que informações sobre agentes de tratamento terceiros com os quais dados foram compartilhados devem se limitar ao nome de empresas ou mesmo o ramo de suas atividades (esta é, inclusive, recomendação da ICO.UK - <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>). Nada impede, relembramos, que ao exercer seus direitos de titulares, titulares possam solicitar de maneira mais precisa informações sobre agentes terceiros. "615489" As decisões relacionadas ao atendimento de direitos do titular incumbem ao controlador. Nesse sentido, o operador não é a parte responsável por determinar as informações que deverão ser repassadas ao titular, uma vez que apenas realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD). Assim, caso chegue ao operador algum pedido de titular em relação aos dados em sua posse, ou mesmo, tendo ele alguma função nos mecanismos de atendimento aos pedidos de titulares, é necessário que comunique tal demanda ao controlador, que irá o instruir sobre como agir. No entanto, em cenários que, mediante contrato, são delegadas funções ao operador para garantir que informações provenientes de dados cheguem aos controladores (e.g., operador contratado para implementar mecanismos para exercício de direitos de titulares, operador que realiza

o contato direto com titulares), o operador passa a ser responsável solidário pelo fornecimento de informações, caso não atenda às instruções lícitas do controlador (art. 42, LGPD). A exemplo, caso o operador informe dados que excedem ou sejam inferiores ao que o controlador determinou que seriam passados ao titular, em linha com o art. 42 da LGPD, o operador terá responsabilidade solidária por danos causados ao titular e eventualmente sancionado por descumprimento de suas obrigações como operador (art. 39).

,"615490": "Tendo em vista que o formato simplificado mencionado no art. 19, inciso I, da LGPD se refere a uma resposta imediata, as informações fornecidas podem ser (i) a confirmação da existência e (ii) informações similares as que já estão disponíveis na Política de Privacidade externa no website (ou, ainda, a parte tecnicamente viável de ser apresentada de imediato de acordo com o modelo simplificado), com a ressalva de que em seguida outras informações poderão ser enviadas, se o formato simplificado não for o suficiente para o atendimento ao titular. Neste caso, a versão estendida conterá informações previstas no Art. 9º da LGPD."

,"615494": "As informações mínimas sobre o tratamento de dados pessoais que deveriam ser evidenciadas pelo controlador, mesmo que independentemente de requerimento, são aquelas que visam garantir, de um lado, que o titular tenha acesso de maneira transparente e clara sobre as etapas do tratamento de seus dados sem que, de outro lado, o excesso de informações possa comprometer sua compreensão do tratamento dos dados, podendo ser inclusive inexequível ao agente de tratamento fazer essa descrição. Assim, considera-se como referência o art. 9 da LGPD, além de inspiração que também pode ser retirada das informações elencadas no art. 13 da GDPR, quais sejam: identidade e contato do controlador, contato de Encarregado, finalidades do tratamento, existência de compartilhamento de dados com terceiros e que categorias de terceiros (ramo de atividade, por exemplo). O grau de especificidade dessas informações deve ser suficiente de modo a garantir o acesso efetivo às informações necessárias mas, ao mesmo tempo, não sobrecarregar a compreensão do titular. Já especificamente em relação as decisões automatizadas, o art. 20 da LGPD dispõe que o controlador deverá fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Nesse sentido, independente do requerimento do titular, entende-se que devem estar disponibilizadas informações relacionadas (i) aos dados tratados e a sua fonte, observados o segredo comercial e industrial; (ii) os critérios para a tomada de decisão, observados o segredo comercial e industrial; (iii) os mecanismos por meio dos quais a pessoa pode contestar a decisão tomada unicamente com base em tratamento automatizado de dados pessoais; e (iv) medidas de segurança, de não-discriminação e de confiabilidade adotadas, desde que não prejudiquem segredos de negócio."

,"615493": "Sim, o direito de acesso pode ser considerado satisfeito quando o agente de tratamento disponibilizar os dados pessoais para o conhecimento do titular, pelo modo escolhido pelo último, desde que garantido que as informações solicitadas foram fornecidas de forma acessível e clara ao titular. Isso porque, o direito de acesso está ligado à garantia de que o titular receba informações de maneira inteligível e por meios facilmente acessíveis, e não à garantia de acesso a uma ferramenta virtual ou cópias físicas de dados especificamente. Dito isso, importante notar que nem sempre, a depender do pedido do titular ou da natureza dos dados solicitados, estes poderão ser fornecidos pelo meio solicitado pelo titular, situação na qual, ao nosso ver, poderá o controlador atender ao direito pelo mecanismo mais adequado, resguardada justificativa ao titular pelo método escolhido. Será importante tão somente: (i) estabelecer um procedimento para autenticar a identidade do solicitante (seja ele o próprio titular ou representante legal) e (ii) estabelecer um mecanismo de se comprovar o cumprimento do atendimento à solicitação (ex: no caso

de atendimento em papel, obter um recibo). ","615502": "Inicialmente, é possível apontar que o nível geral de maturidade dos setores brasileiros no que tange à implementação e operacionalização do direito à portabilidade é consideravelmente baixo. Acresce-se o fato da indispensabilidade de uma regulamentação mais exaustiva dos elementos fundamentais do direito à portabilidade, etapa imprescindível para o estabelecimento de um quadro técnico, organizacional e tecnológico voltado à implementação de uma arquitetura que possibilita tal direito. Entre esses elementos, destacam-se: quais dados estão sujeitos à portabilidade e suas limitações, quem está sujeito ao direito à portabilidade e para quem esses dados deverão ser portados, o que é exatamente o direito à portabilidade e outros fatores basilares para a compreensão desse complexo sistema a ser implementado. Ainda, o Ibrac respeitosamente entende que a presente questão não deveria ser endereçada por meio de uma consulta que abrange genericamente todos os direitos dos titulares, uma vez que a complexidade do tema e de seus efeitos demanda de uma atenção especial. Neste cenário, constata-se que não é possível identificar, avaliar e estruturar uma resposta adequada - considerando o exíguo prazo dessa consulta e a multitudine de temas sobre quais ela versa - à pergunta sobre quais setores possuiriam maturidade e tecnologia adequadas para a portabilidade. Compreende-se que seria apropriado um procedimento mais robusto conduzido pela ANPD em conjunto com outras autoridades e com a sociedade para avaliar a referida maturidade, as peculiaridades de cada setor, as tecnologias necessárias, as questões fundamentais supramencionadas bem como os efeitos esperados por essa regulamentação, dado que o referido direito possui o potencial de remodelar integralmente um determinado setor. Por fim, é recomendável que, quando iniciado, que o procedimento de implementação seja feito nos setores regulados, especialmente nos que já possuam iniciativas semelhantes, como o Open Finance do BCB, de modo a facilitar a aplicação inicial do modelo de regulamentação para expandi-lo a outros."","615501": "Primeiramente, cumpre destacar que a portabilidade e a interoperabilidade não são sinônimos. Tratam-se de dois conceitos com implicações e complexidades distintas. Essa distinção é essencial pois a LGPD somente prevê como direito do titular a portabilidade. Ainda que se considere a menção feita no art. 40, não se reputa razoável confundir os dois conceitos nem estabelecer as regras sobre interoperabilidade (que pressupõe a portabilidade) antes de endereçar corretamente a portabilidade. Desta forma, é imprescindível amoldar a consulta aos ditames e limites estabelecidos pela LGPD. Deste modo, registra-se que o Ibrac limitará a sua resposta à portabilidade, ainda que a pergunta faça referência à interoperabilidade. Feita essa consideração inicial, entende-se que os principais desafios tecnológicos relativos ao direito à portabilidade são de ordem do desenvolvimento tecnológico: considerando que, uma vez que se definirem padrões necessários para a portabilidade, é necessário que todos os agentes sujeitos à regulamentação se adequem aos referidos padrões. Nesse sentido, destaca-se que a tecnologia necessária para alcançar um padrão uniforme, por mínimo que seja, é robusta, considerando a necessidade de mecanismos e padrões de segurança para esses dados e conjuntos de dados, mecanismos de organização e estruturação, mecanismos de verificação e validação de solicitações e entre outros. Mesmo na lógica de uma aplicação setorial, não há como ignorar as peculiaridades, capacidades e recursos (financeiros e tecnológicos) de cada organização. Além disso, existem desafios relativos à própria compreensão do direito à portabilidade, uma vez que carece de regulamentação específica. Precede à implementação e estabelecimento de padrões para agentes sujeitos a definição do próprio escopo agentes e de suas relações com outros agentes, se só haverá portabilidade horizontal ou se também haverá portabilidade para outros setores. É preciso também definir quais dados são passíveis de portabilidade, tema relevante em razão

da necessidade de tutela da PI e dos segredos de negócio."615505": "Novamente, ressalta-se que interoperabilidade e portabilidade não serão tratadas como sinônimo nessa contribuição. Dito isso, é primordial destacar a experiência internacional aponta que a estruturação e implementação de padrões pelo setor privado é mais eficaz que legislações rígidas e horizontais sobre portabilidade. Por isso, de modo a compreender as peculiaridades e necessidades de cada setor, a ANPD deve permitir que estes se organizem para definir quais padrões deverão ser adotados de modo a observar, de forma eficiente, os direitos dos titulares. Todavia, a ANPD poderá auxiliá-los ao estabelecer requisitos mínimos para o bom funcionamento desse sistema como, por exemplo: os dados deverão ser fornecidos em formato legível e compatível com sistemas do mesmo setor, de forma eletrônica, gratuita e entre outros critérios mínimos de concretização de direitos. Não há necessidade de adoção de padrões de arquivos, basta que sejam compatíveis com as ferramentas no contexto em que se inserem. Além disso, seria interessante que os padrões fossem estabelecidos conforme o tipo de dados a serem tratados, de modo a garantir a eficiência dos padrões a adequação destes aos atributos singulares dos casos concretos. Nesse ponto, evidencia-se a vantagem de se adotar uma forma de regulamentação focada em setores (e não ampla), uma vez que os tipos de dados tratados e as ferramentas utilizadas tendem a ser mais semelhantes. "615503": "Sim, entende-se como suficientemente observado o direito à portabilidade dos dados a disponibilização dos dados ao titular para que este, em posse de suas informações, possa utilizar as ferramentas do outro controlador para concretizar o seu direito. Novamente, ressalta-se que interoperabilidade e portabilidade não são sinônimos e que se faz necessário definir a portabilidade antes de regulamentar sobre padrões de interoperabilidade, uma vez que estes pressupõe aqueles."615504": "Sim, é adequado e proporcional, de acordo com a experiência internacional e com a literatura especializada permitir que setores específicos se organizem, seja por meio dos padrões de mercado ou seja por incentivo das autoridades setoriais, para definir os padrões adequados para a portabilidade ao caso concreto. Todavia, não é trivial a definição de um prazo razoável para todo e qualquer setor, visto que cada um compreende agentes de diferentes portes e capacidades, volumes e quantidade de informações tratadas distintas e entre outros fatores que podem dificultar em muito o estabelecimento destes. Nesse sentido, há vantagem em se adotar o procedimento robusto mencionado na primeira pergunta sobre portabilidade, permitindo que no processo os entes interessados possam indicar o prazo razoável para a implementação. Há de se destacar que, caso permaneça a ideia de tratar portabilidade como sinônimo de interoperabilidade, que é consideravelmente mais complexo e oneroso de ser implementado, a tendência é que o prazo de implementação seja proporcionalmente muito maior do que o da hipótese de se restringir a portabilidade."615511": "De acordo com o artigo 18, III, da LGPD, o titular do dado tem o direito de obter do controlador, a qualquer momento e mediante requisição, a correção de dados incompletos, inexatos ou desatualizados. Trata-se de uma retificação de natureza objetiva, sendo suficiente a evidência material de que o dado está incompleto, inexato ou desatualizado. Alguns critérios objetivos a serem considerados para tais qualificações: (i) tratar de erro material no dado, cuja incorreção pode prejudicar o titular, sendo necessária a retificação; (ii) demonstração/comprovação (evidência material) pelo titular quanto ao dado estar incompleto, incorreto ou desatualizado; (iii) o tratamento do dado inicialmente registrado não atende ao princípio da qualidade dos dados; e (iv) o tratamento do dado inicialmente coletado impede o cumprimento da finalidade para o tratamento."615514": "Da leitura do artigo 18, III, da LGPD, depreende-se que o direito à retificação/correção previsto na LGPD, prevê hipóteses de retificação de natureza objetiva, em razão de erro material, bastando a evidência de que

o dado tratado está incompleto, inexato ou desatualizado. Referido artigo encontra paralelo no artigo 16 da GDPR, que dispõe ao final “Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.” Esta declaração complementar leva-nos a interpretação acerca da possibilidade de retificação de natureza subjetiva. Feito esta diferenciação, podem ser mencionadas algumas situações em que a simples declaração do titular não seria suficiente para o exercício do direito à correção, fazendo-se necessária documentação complementar por parte do titular de dados: (i) o titular não demonstra ter legitimidade para a solicitação da correção; (ii) a correção tem natureza subjetiva (paralelo no art. 16 da GDPR) e a informação que se pretende corrigir não está incorreta, inexata ou desatualizada. Contudo, para a correta interpretação dos dados pessoais a favor do titular, faz-se importante acrescentar informações adicionais; (iii) a alteração/retificação solicitada não corresponde aos documentos apresentados inicialmente pelo titular do dado.”;”615513”:"O artigo 18, § 6º, da LGPD, dispõe que “O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.” Alguns critérios objetivos que devem ser considerados para avaliar a impossibilidade ou esforço desproporcional para informação aos agentes de tratamento acerca da correção dos dados são: (i) se o tratamento de dados pessoais é de acesso público ou não; (ii) custo envolvido (levando-se em conta o caráter técnico e operacional existente); (iii) o prazo decorrido entre o compartilhamento dos dados, pedido de correção do dado e o atendimento da finalidade para o qual o dado foi tratado; e (iv) conhecimento de todos os agentes de tratamento que trataram o dado antes da correção. Exemplos: Situações em que há o cocontrole dos dados e não há como assegurar/conhecer quantos e quais dados foram tratados por outros agentes de tratamento (p.ex. plataformas que disponibilizam consultas gerais de crédito) ou situação em que o tratamento de dados pessoais é de acesso público. ”;”615512”:"Sim. Há situações excepcionais em que o direito de correção poderia ser negado pelo Controlador. Cite-se, por exemplo, (i) situações em que os dados já foram eliminados pelo Controlador (exaurida a finalidade do tratamento); (ii) se após cumprida a finalidade para o qual o tratamento se deu, os dados foram anonimizados; (iii) se não há comprovação formal da alteração solicitada (p. ex: solicitação para manter apenas o nome social, excluindo o nome de registro inicial, sem a alteração nos registros oficiais); (iv) se o tratamento do dado que se pretende atualizar ocorre por obrigação legal a ser observada pelo Controlador ou exercício regular de direito em processo judicial; (v) se a retificação solicitada for caracterizada como uma ação ilícita, fraudulenta ou com base em informações falsas; (vi) hipóteses em a finalidade de tratamento já ocorreu e que seja inviável a manutenção de todo o histórico/registo dos dados inicialmente tratados e as posteriores correções solicitadas; e (vii) a atualização dos dados implicaria em criação de novos dados e impactando eventual modelo de negócio/modelo industrial.”;”615517”:"Sim. Consideramos que, para fins de exercício das prerrogativas específicas indicadas no Art. 18, seja razoável exigir que o titular no mínimo fundamente a base para o requerimento aplicável, indicando a desnecessidade, a excessividade, a desconformidade ou o descumprimento legal do tratamento executado. A fundamentação do titular será relevante para se determinarem as medidas que devam ser adotadas pelo agente de tratamento com relação à solicitação do titular, bem como para viabilizar eventual esclarecimento por parte do agente em caso de negativa legítima da solicitação apresentada.”;”615516”:"Considerando-se que a anonimização e a eliminação de

dados ensejam o afastamento da aplicação da LGPD e geram efeitos similares em termos de tutela de direitos para o titular, consideramos razoável que os procedimentos sejam tratados de forma alternativa e possam ser adotados a critério do agente de tratamento. Salienta-se que ao titular permaneceria reservado o direito de questionar a adequação do procedimento de anonimização adotado, caso, em busca de preservar alguma utilidade para o dado, o agente realize procedimento insuficiente para reduzir satisfatoriamente os riscos de reidentificação.";"615518": "Não vislumbramos necessariamente uma relação de causa e efeito. O exercício da prerrogativa estabelecida pelo art. 18, §2º pode servir tanto como fundamento para eventual adoção de medidas voltadas a sancionar e reparar danos ocasionados pelo descumprimento da LGPD (ex.: o titular identifica o descumprimento, solicita a interrupção do tratamento, e isso eventualmente desencadeia medidas previstas em lei), quanto como consequência de um descumprimento identificado (ex.: ocorre descumprimento, e com base nisso o titular exerce o direito de solicitar a interrupção do tratamento). Ainda, é importante, para evitar a criação de obstáculos ao exercício de direitos pelos titulares, que o atendimento a determinada solicitação, ainda que fundamentada em alegação de descumprimento da LGPD, não seja tomado como reconhecimento de que a LGPD foi descumprida pelo agente de tratamento. Se essa presunção for estabelecida, a tendência é de que os agentes passem a adotar postura "defensiva" em relação ao exercício de direitos pelos titulares, diante do receio da aplicação imediata de sanções administrativas e outras consequências legais.";"615523": "Conforme a leitura sistemática da LGPD, em especial do art. 8º, §5º e do art. 16, a revogação do consentimento não implicará, necessariamente, a eliminação dos dados pessoais, a qual somente deverá ser levada na hipótese de o tratamento ser baseado unicamente na base legal do consentimento e quando houver um pedido específico nesse sentido, nos termos do art. 18, VI. Com relação a revogação do consentimento, depreende-se que o legislador fixou um marco temporal com efeitos a partir do pedido de revogação, conforme depreende-se do artigo 8º §5º ("O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei). Ademais, os controladores somente serão obrigados a deletar os dados tratados específicos dos quais o consentimento foi revogados, não afetando outros tratamentos baseados em outras bases de dados.";"615521": "Da leitura do art. 8º da LGPD, entendemos que o requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestados implica tão somente na deleção de dados até o momento do requerimento, sem afetar a regularidade da base legal aplicável, de forma que dados poderão continuar sendo tratados com base no consentimento do titular. Vale a distinção aqui dos direitos de (i) revogação de consentimento e (ii) eliminação de dados que, respectivamente, dizem respeito ao (i) tratamento e (ii) aos dados. Assim, o pedido de eliminação dos dados não tem o condão de encerrar o tratamento baseado no consentimento (na prática, revogar o consentimento), mas tão somente eliminar dados solicitados pelo titular. Em um exemplo prático, dados de perfil comportamental armazenados pelo agente de tratamento gerados a partir de dados coletados do titular por meio do seu consentimento serão, então, excluídos a partir do pedido de eliminação, o que não significa que o agente não poderá realizar novos tratamentos sobre os dados coletados inicialmente, com base no consentimento do titular (salvo se o titular optar pela revogação do consentimento). Ademais, caso haja outra finalidade/tratamento ocorrendo em paralelo, a partir de outra base legal que permita ou imponha a sua manutenção, os dados atrelados a esta outra finalidade poderiam ser

preservados. ";615617": "Para o Ibrac, "Decisão automatizada" e "Decisão tomada unicamente com base em tratamento automatizado" devem ser entendidos como sinônimos. Desta forma, o Ibrac compreende que é quando a máquina faz predição e julgamento, e com base no julgamento, indica e efetua uma ação que leva a um resultado prático. Ou seja, a máquina toma a decisão com base no algoritmo pré-estabelecido. Assim, o caput do Art. 20 estabelece o direito à revisão (automatizada ou não) de decisões tomadas unicamente com base em tratamento automatizado, enquanto o §1º estabelece direito à explicação do funcionamento do tratamento automatizado de dados pessoais (medidas incrementais de transparência). ";615618": "O uso da expressão "interesse" estende a aplicação do art. 20 para além de violação de direitos propriamente ditos. Contudo, é importante considerar o critério a partir de potenciais efeitos negativos para o titular, como por exemplo efeitos discriminatórios ilícitos, restrição indevida ao crédito e a outros serviços, entre outros. Trata-se, portanto, de prejuízo a interesse legítimo que não esteja baseado em fundamentos legítimos. Como método de avaliação para aplicação do dispositivo, entende-se que devam ser considerados: (a) a existência de um interesse legítimo do titular (interesse tutelado por princípios ou normas) - não se trata, por exemplo, de simples frustração de expectativas e (b) a ausência de justificativa, fundamentada em critérios objetivos e lícitos, para que o interesse do titular seja afetado. ";615619": "Em relação à implementação do previsto no art. 20 da LGPD, considera-se a existência de uma gama de desafios que impedem e/ou retardam a correta implementação do direito previsto na LGPD, seja em razão de dificuldades técnicas ou mesmo em razão de dificuldades atinentes à própria normatização do tema. Inicialmente, considera-se que a indefinição do conceito de "revisão" é um obstáculo a ser superado por uma definição jurídica mais precisa. Isso porque não há clareza se o conceito de revisão significa a reanálise, com eventual supervisão humana ou outras formas, ou se implica necessariamente a mudança de resultado. No entendimento do Ibrac, a primeira interpretação é a mais ponderada e razoável, devendo prevalecer na normatização da ANPD. Um segundo desafio observa é o concernente à compreensão do titular de quando as decisões são tomadas unicamente com base em tratamento automatizado. Por exemplo, uma situação em que uma pessoa atue em nome do responsável pelo tratamento de dados, mas apenas comunica uma decisão previamente tomada por um algoritmo - como um atendente de banco que apenas repassa a decisão do sistema - não deve ser confundida com uma situação em que o resultado que impacta os interesses do titular é o resultado de um processo decisório em que há intervenção efetiva de seres humanos na análise de crédito. Outro desafio decorre do fato de que o artigo 20 não exige a revisão humana das decisões. Assim, mesmo que o titular solicite a revisão do resultado, ela pode ser conduzida por meio de outro tratamento automatizado. É importante determinar em que medida a revisão por meio de outros parâmetros seja suficiente para atender de forma definitiva o pedido de revisão. Por fim, o último desafio a ser destacado decorre da legítima preocupação dos agentes de tratamento com seus segredos de negócio e propriedade industrial, no caso de decisões automatizadas, sendo necessário estabelecer equilíbrio sustentável entre o direito à obtenção de informações acerca dos parâmetros utilizados para a decisão e a tutela de segredos de negócio.";615620": "Sim, entendemos que, na medida em que as decisões não afetarem interesses legítimos dos titulares, ou em que sejam justificadas com base em critérios legítimos, observados requisitos de transparência, o direito à revisão poderá ser negado. Exemplo: o titular tem direito a crédito negado e solicita revisão, mas recebe prontamente informação no sentido de que o crédito foi negado por haver situação financeira insuficiente, com base em parâmetros objetivos adotados pelo agente de tratamento em questão."

{ "615450": " ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "615484": "Deve-se ponderar a facilidade de acesso a esse canal de atendimento com meios que assegurem a identificação inequívoca do requerente, seja o titular ou seu representante legal, para evitar o envio indevido a terceiro não autorizado pela legislação. O controlador deve manter registro dos requerimentos dos titulares e respectivas respostas, assegurando a “rastreadibilidade” dos atendimentos, logo o atendimento meramente verbal, sem registros, deve ser evitado. De igual modo, é importante que o requerente tenha ciência do andamento e previsão quanto à conclusão de seu requerimento. Assim, busca-se compatibilizar os princípios do livre acesso e transparência com os princípios da segurança e prevenção. Entende-se como características essenciais a facilidade de acesso, a identificação inequívoca do requerente, ou seu representante legal e a manutenção de registros dos atendimentos para possibilitar sua “rastreadibilidade”. É característica desejável, que denota boa fé e transparência, que o controlador adote mecanismos para cientificar ao requerente da evolução das etapas de seu atendimento. Características: - Facilidade de acesso. - Meios que permitam a Identificação inequívoca do requerente. - Comunicação do andamento e previsibilidade de conclusão. - Registro dos atendimentos para rastreadibilidade. - Tempestividade. - Sem ônus ao requerente. "615485": "Pela lógica aplicada à LGPD, caberá ao operador atuar de acordo com os parâmetros delineados pelo controlador (Art. 5.º, VII; Art. 39). Os §§ 3.º e 5.º do artigo 18 seguem essa mesma lógica. Assim, embora a literalidade do § 3.º possa levar ao entendimento de que também seja competência do operador atender requisições dos titulares de forma autônoma, visto ser um dos agentes de tratamento especificados na LGPD, uma interpretação adequada seria de que, em relação ao atendimento aos direitos dos titulares, o operador pode: - Fornecer informações/insumos/meios para que o controlador proceda com a elaboração da resposta à requisição do titular, independente se este fluxo informacional ocorre de forma manual ou automatizada (Art. 18, caput). - Fornecer a resposta para que o controlador a valide e proceda com a conclusão do atendimento à requisição (Art. 18, caput) . - Atender diretamente as requisições dos titulares, desde que determinado pelo controlador e informado aos titulares, atendendo assim ao princípio da transparência (Art. 18, caput c/c § 3.º). "615486": "Para muitos controladores é inviável realizar o atendimento telefônico obrigatório, conforme artigo 3.º, § 2.º e artigo 5.º do Decreto 11.034/2022. Entretanto, o prazo corrido de sete dias corridos, conforme o artigo 13, do Decreto 11.034/2022, poderia ser utilizado por analogia como alternativa para o cumprimento do prazo especificado no artigo 19, inciso I da LGPD que apresenta o conceito jurídico indeterminado “imediatamente”. "615487": " "615491": " "615492": " "615489": " "615490": " "615494": " "615493": " "615502": " "615501": " "615505": " "615503": " "615504": " "615511": " "615514": " "615513": " "615512": " "615517": " "615516": " "615518": " "615523": " "615521": " "615617": " "615618": " "615619": " "615620": " "

{ "615450": "Idec: Em razão do §4º do art. 18 da LGPD, os direitos dos titulares devem ser cumpridos, a princípio, imediatamente. Caso o controlador não consiga atender essa regra geral, é que poderá indicar as razões de fato ou de direito que impedem a adoção imediata da providência. Nessa hipótese (art. 18, §4º inciso II), dá-se início a contagem de prazo a ser estabelecido pela ANPD. A Autoridade deve travar um diálogo com outras legislações e normas infralegais para defini-lo. Ainda que a LAI traga parâmetros relevantes para o tratamento de dados, o prazo de 20 dias (prorrogáveis por 10) para acesso aos dados é muito extenso em comparação a outras legislações (art. 11, §1º e 2º). O prazo decorre da dinâmica do poder público e do acesso a informações que não são necessariamente dados pessoais dos requerentes de LAI. Ou seja, o exercício de direitos dos titulares não se refere à mesma realidade e deve ter seu exercício facilitado. Comparando com outros instrumentos de acesso e correção de dados, a Lei nº 9.507/1997, que disciplina o rito processual do remédio constitucional habeas data (art. 5º, inciso LXXII da CRFB), define que o prazo máximo para concessão do acesso à informação e de sua retificação é de, respectivamente, 10 e 15 dias (art. 8º, incisos I e II). Já o CDC estabelece que o direito à correção de informações em bancos de dados deve ser realizado em até 5 dias úteis (art. 43, §3º). Em benefício do melhor interesse dos titulares, o regulamento da ANPD deve se orientar pelo prazo mais benéfico, portanto o do CDC (prazo de 5 dias), com exceção de bancos de dados de caráter público que devem se orientar pelo habeas data, dadas as especificidades do tratamento pelo poder público. Também deve-se manter a exceção de prazo máximo de 15 dias para o acesso completo aos dados pessoais (art. 19, inciso II, LGPD). Reitera-se que o regulamento infralegal não terá legitimidade para afastar a aplicação da regra geral de imediatidade prevista nos §§ 4º e 6º do art. 18 ou de outras legislações federais, por se tratarem de disposições mais benéficas aos titulares. ",b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:"Contribuição do Idec - Instituto de Defesa de Consumidores: As únicas exceções para a regra geral de imediatidade no cumprimento dos direitos dos titulares estão previstas no art. 18, §4º, inciso II (prazo a ser definido pela ANPD, conforme resposta anterior) e o art. 19, inciso II (prazo de 15 dias para o acesso pormenorizado e completo), cabendo a manutenção de prazos diferenciados somente nessas hipóteses. Em caso excepcional da necessidade de previsão de prazo diferenciado para setores em específico, a discussão deve entrar em consulta pública ou tomada de subsídios para participação de interessados, sempre buscando privilegiar o tratamento mais benéfico aos titulares de dados. ", "615484": "Idec: Acessibilidade e usabilidade: A assimetria informacional e a vulnerabilidade dos titulares-consumidores (art. 4º, inciso I CDC) deve ser considerada na formulação dos canais de atendimento. O e-mail do encarregado deve conter obrigatoriamente o canal unificado por se tratar da pessoa responsável pela comunicação entre controlador e titular (art. 5º, inciso VIII e art. 41). Tratando-se de serviços também relacionados à defesa do consumidor, o atendimento telefônico também deve ser obrigatório (Decreto nº 11.034/2022). Deve ser garantido o acesso às pessoas com deficiência aos canais de atendimento. Segurança: Os agentes de tratamento devem garantir a segurança dos dados tratados nos canais (art. 46 e 47). Privacidade, finalidade e transparência: Os dados tratados por meio dos canais devem (i) ser transparentes em como são realizados seus processos, (ii) resguardando a privacidade e (iii) tendo como finalidade exclusivamente o próprio atendimento aos direitos dos titulares, vedadas finalidades de publicidade ou outros fins. Efetividade: Impossibilitado o imediato

cumprimento (art. 18, § 4º), o canal de atendimento deve ter prazos máximos para o atendimento das demandas. Para a efetividade dos direitos dos titulares, a ANPD deve acompanhar a instalação dos canais e a taxa de resolução dos atendimentos. Para isso, em razão da competência fiscalizatória da ANPD, os agentes de tratamento devem enviar semestralmente relatórios e diagnósticos a partir da análise das reclamações e de outras demandas dos titulares, sem prejuízo de solicitação de informações complementares. Trata-se de um paralelo de uma obrigação imposta pela Anatel às operadoras de telecomunicações no Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (RGC, art. 88). Por fim, independente dos canais de atendimento dos agentes de tratamento, também deve ser oportunizado aos titulares os canais de reclamação e/ou solicitações diretas a autoridades públicas, como o consumidor.gov e a ANPD, incluindo direito de petição (art. 55-J, inciso V).

615485: "Contribuição do Idec - Instituto de Defesa de Consumidores: Sim. Os direitos dos titulares colocam os operadores também como protagonistas do tratamento de dados pessoais. Devida sua relevância, o descumprimento desses direito deve culminar em responsabilidade solidária entre os agentes de tratamento por falhas na prestação do serviço. Isso porque a falta de concretização dos direitos dos titulares deve ser considerada um descumprimento das obrigações impostas pela LGPD (art. 42, §1º, inciso I e art. 44), além de ser uma violação ao fundamental da autodeterminação informativa (LGPD, Art. 2º, inciso II). Ainda, quando o tratamento de dados ocorrer no âmbito de uma relação de consumo deve ser aplicado as regras de responsabilidade do Código de Defesa do Consumidor. De maneira que a responsabilidade é solidária entre todos que integram a cadeia de consumo, inclusive os operadores (art. 45 da LGPD c/c art. 12 e 18 do CDC). Reitera-se que, em ambos os casos, considerando a assimetria informacional e a vulnerabilidade dos titulares de dados, o regime de responsabilidade deve ser objetivo - independente de comprovação de culpa.

615486: "Idec Sim, o SAC deve ser um parâmetro mínimo. Entretanto, não deve ser considerado um parâmetro máximo. Caso a ANPD regule prazos mais benéficos, esses devem ser aplicados, considerando a vulnerabilidade e assimetria informacional inerente ao tratamento. O SAC é um conjunto de canais integrados para garantir o direito dos consumidores à obtenção de informações adequadas sobre os serviços contratados e para o tratamento de suas demandas. O tratamento de dados pessoais no âmbito relações de consumo também se submete a legislação de defesa do consumidor, logo o SAC também deve atender os direitos dos titulares. Além disso, o SAC deve ser considerado para que a ANPD regule os canais de atendimento voltados exclusivamente para o exercício dos direitos dos titulares. Em especial, as diretrizes sobre o acompanhamento e tratamento das demandas devem ser observadas; deve ser garantido aos titulares o acompanhamento e um prazo máximo para o atendimento de suas demandas. A ANPD também deve implementar ferramentas de acompanhamento da efetividade dos canais de atendimento. Para isso, em razão da competência fiscalizatória da ANPD, os agentes de tratamento devem enviar semestralmente relatórios e diagnósticos a partir da análise das reclamações e de outras demandas dos titulares, sem prejuízo de solicitação de informações complementares pela Autoridade. Trata-se de um paralelo de uma obrigação imposta pela Anatel às operadoras de telecomunicações no Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (RGC, art. 88). Nesses documentos deve ser informado (i) as demandas recebidas no período, apresentados em bases mensais comparadas com o mesmo período do ano anterior; (ii) análise crítica sobre possíveis causas-raízes dos problemas identificados e (iii) eventuais mudanças para o cumprimento dos dispositivos da LGPD. Considerando a quantidade de agentes de tratamento, é possível que a ANPD determine essa obrigação apenas aqueles que tratam uma grande quantidade de

dados ou aqueles que representam maiores riscos (regulamentação assimétrica).
";615487": "Sem contribuições. ";615491": "Contribuição do Idec - Instituto de Defesa de Consumidores: Não. Considerando que a LGPD não traz essas exceções, os agentes de tratamento não têm possibilidade de negar o acesso aos direitos dos titulares. O direito à confirmação da existência do tratamento é o mais relevante dos direitos dos titulares. Afinal, não haverá possibilidade do titular exercer sua autodeterminação informativa caso sequer tenha conhecimento do tratamento de seus dados. A autodeterminação fundamenta a disciplina de proteção de dados por ser a garantia ao titular que ele poderá controlar a circulação de seus dados (art. 2º, inciso II). Além disso, esse direito encontra lastro em diversos princípios que devem orientar o tratamento de dados, em especial o princípio do livre acesso, o princípio da qualidade dos dados, o princípio da transparência e da boa-fé objetiva (art. 6º, incisos IV, V, VI). Ainda que a ANPD compreendesse ser necessário criar exceções em razão da segurança da sociedade ou do Estado, de maneira similar às previsões do art. 23 da Lei 12.527/2011, é fundamental relembrar que a LGPD não se aplica ao tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e/ou atividades de investigação e repressão de infrações penais (art. 4º, inciso III).
";615492": "Contribuição do Idec - Instituto de Defesa de Consumidores: A identificação dos controladores é essencial para o exercício dos direitos dos titulares. Devem ser fornecidos dados de todos os controladores de dados responsáveis pelo tratamento. Assim como a possibilidade dos titulares excluírem o tratamento de dados com um controlador em específico. Os controladores devem manter um cadastro atualizado junto aos canais públicos de atendimento aos titulares de dados. De maneira que as autoridades públicas - como ANPD, Senacon e Procons - e os titulares-consumidores possam acessá-lo. Devem ser fornecidas informações relacionadas ao CNPJ, nome social e nome fantasia, identificação do encarregado de dados e informações de contato, como números de telefone, e-mails e canais de atendimento. Por fim, deve-se considerar que o segredo comercial, segredo industrial e o sigilo em geral não devem servir de escusa para a identificação dos controladores. Os titulares devem ter informações completas sobre os controladores que realizam a gestão de seus dados e o segredo comercial não guarda relações diretas com essas informações. Desta maneira, o segredo industrial não deve ser considerado superior ao exercício regular do direito de titulares de dados.
";615489": "Contribuição do Idec - Instituto de Defesa de Consumidores: Os direitos dos titulares os colocam como protagonistas do tratamento de seus dados pessoais. Devida sua relevância, o descumprimento desses direitos devem culminar em responsabilidade objetiva e solidária entre os agentes de tratamento por falhas na prestação do serviço, isso porque a falta de concretização dos direitos dos titulares deve ser considerada um descumprimento das obrigações impostas pela LGPD (art. 42, §1º, inciso I e art. 45 da LGPD c/c art. 12 e 18 do CDC). A obtenção de informações sobre o tratamento de dados pessoais é central para a efetivação da autodeterminação informativa, fundamento crucial para a materialização dos direitos garantidos na LGPD. O direito à informação deve ser prestado de forma ostensiva, ou seja, deve estar disponível aos titulares por diversos meios e independente de solicitação - por meio das Políticas de Privacidade, por exemplo. Em caso de falha na prestação das informações adequadas, os agentes devem ser responsabilizados. Além disso, o pedido de confirmação de existência do tratamento pressupõe o envio dos dados mínimos. Compreende-se que diante da necessidade de confirmação da existência do tratamento já há uma falha de transparência e informação, uma vez que os titulares deveriam ter conhecimento de todos os agentes que tratam seus dados. Com o objetivo de corrigir tais falhas, os dados e informações mínimas devem ser enviadas independente de novo requerimento.

","615490": "Contribuição do Idec - Instituto de Defesa de Consumidores: Na declaração simples, além dos dados previsto no art. 9º, também devem ser disponibilizada (i) a confirmação do tratamento de dados, (ii) quais dados são tratados, (iii) a fonte dos dados e (iv) os critérios utilizados em decisões automatizadas. Na hipótese art. 19, inciso II, os titulares de dados podem solicitar informações e dados adicionais de seus interesses, sem a necessidade de justificar a solicitação. Além disso, é possível, por exemplo, que dados mais complexos, como inferências, sejam disponibilizadas com o prazo expandido previsto no inciso II do art. 19. Ressaltamos que inferências são feitas a partir de dados pessoais, de forma que o tratamento continua sujeito à autodeterminação e a titularidade do indivíduo (art. 17). De modo ainda mais grave, em razão das tecnologias e algoritmos utilizados, inferências automatizadas têm grande potencial de refletir no livre desenvolvimento da personalidade dos titulares e na maneira com que eles se identificam socialmente, sendo fundamental que eles tenham acesso às informações sobre si. Por fim, deve-se considerar que o segredo comercial e industrial não deve ser uma escusa para o fornecimento das inferências. O tratamento automatizado de dados afetará a vida dos indivíduos, devendo ser garantido a eles o exercício de suas autodeterminação por meio dos direitos dos titulares. O segredo comercial poderá proteger a integridade do código, mas os controladores devem manter públicas informações quanto aos critérios básicos de decisão. Com isso, espera-se submeter os algoritmos a escrutínio público e aumentar a transparência, prestação de contas e responsabilidade. ","615494": "Idec: O direito à informação não deve ser garantido pelos operadores apenas quando solicitado por autoridades públicas ou pelos titulares. Em razão da natureza coletiva dos dados e do interesse público em seu tratamento, as informações devem ser claras, adequadas e ostensivas e a transparência deve orientar o tratamento (art. 6º, inciso VI e art. 6º, inciso III do CDC). 1. AS INFORMAÇÕES MÍNIMAS DEVEM SER DISPONIBILIZADAS NA POLÍTICA DE PRIVACIDADE A própria LGPD define em seu art. 9º os direitos de informação mínimo dos titulares. As informações mínimas e relacionadas ao coletivo devem ser públicas e disponibilizadas na Política de Privacidade e Proteção de Dados. A Política deve ser uma descrição de todas as ações tomadas no tratamento de dados, o que envolve as finalidades do tratamento, a necessidade dos dados coletados, as hipóteses legais que o justificam, medidas para mitigação de riscos e procedimentos que deverão ser adotados pelos operadores de dados. É importante que a ANPD defina critérios e informações mínimas para as Políticas, independente disso, cada controlador deve redigir sua Política considerando a adequada avaliação de risco do tratamento concreto de dados. A partir dessa avaliação poderá ser compreendido quais são as informações, riscos e medidas mitigadoras que devem ser adotadas para evitar ou atenuar riscos de dados. Espera-se, com isso, auxiliar os titulares a compreender o fluxo de seus dados e o exercício de seus direitos. 2. INFORMAÇÕES MÍNIMAS, PARA ALÉM DO ARTIGO 9º - Confirmação do tratamento (atual ou passado) de dados do titular - Especificação de quais dados pessoais são tratados - Indicação de compartilhamento de dados com terceiros - Instruções claras e acessíveis sobre como exercer direitos dos titulares e de revogação do consentimento, caso essa seja a base legal utilizada, e a consequência do seu exercício - Em relação ao tratamento automatizado, os operadores devem informar em suas políticas a finalidade do tratamento, as consequências e o grau de risco, os dados coletados e quais os critérios avaliados. ","615493": "Contribuição do Idec - Instituto de Defesa de Consumidores: Sim. Deve ser disponibilizado os dados claros e completos, bem como a correlação entre os dados e as finalidades e hipóteses legais que legitimam o tratamento de dados. Isso pode ser realizado no formato digital ou em papel. Também deve ser disponibilizado ao titular o envio das informações por e-mail ou, para os que solicitarem e aqueles sem acesso

qualificado à Internet, por correios. A disponibilização em formato alternativo dessas informações é uma maneira de garantir a acessibilidade e, portanto, a efetividade do exercício de direitos de titulares. Há de se considerar, por exemplo, eventual desafio com a alfabetização digital para a população idosa. ","615502": "Idec: O ônus da maturidade do setor deveria ser demonstrado pelo setor privado e o tema deveria ser colocado em consulta específica. Porém, é necessário destacar que o setor de saúde suplementar NÃO está maduro para a portabilidade de dados. Ainda que esse direito seja relevante, é necessário considerar os riscos de segurança e exploração econômica de dados que a portabilidade carrega. Afinal, os dados pessoais não podem ser usados de maneira a trazer desvantagens (sociais e econômicas) ao usuário-titular. No setor suplementar de saúde, por exemplo, a interoperabilidade de dados pode ampliar riscos relacionados a abusividades e discriminações ilícitas, como análises preditivas com base em dados (por exemplo, para perfilização, publicidade direcionada e healthscores) e seleção de riscos, vedada pelo art. 11, §5º da LGPD e também pela regulação sanitária. Para mitigar esses riscos é preciso um direcionamento regulatório da Agência Nacional de Saúde Suplementar (ANS) e da ANPD para mapear práticas de seleção de risco e construir melhores vedações. Uma vedação, por exemplo, seria restringir o acesso a dados aos prestadores de saúde (como hospitais e clínicas) e vedá-los às operadoras de saúde (planos de saúde), justamente pela preocupação com seleção de risco e potencial exclusão indevida de beneficiários. Não existe argumento técnico que justifique o acesso aos dados por operadoras de planos de saúde (ou, no caso de empresas verticalizadas, do seu braço administrativo), devendo ser vedado o acesso aos dados pessoais, incluindo dados clínicos, de gestão e metadados. Recomenda-se que a ANPD insira em sua agenda regulatória a regulamentação de tal setor, seguindo as recomendações de cooperação com a ANS para evitar qualquer prática maléfica ao direito fundamental à saúde. Sobre o tema, também se recomenda a leitura da publicação do Idec "Agenda de Dados e Saúde: Recomendações para uma Saúde Digital Inclusiva": <https://idec.org.br/publicacao/agenda-de-dados-e-saude-recomendacoes-para-uma-saude-digital-inclusiva>","615501": "Sem contribuições. ","615505": "Sem contribuições. ","615503": "Contribuição do Idec - Instituto de Defesa de Consumidores: O direito deve ser considerado satisfeito ao disponibilizar o documento em formato interoperável apenas quando comprovado a falta de maturidade do setor, a impossibilidade técnica dos operadores efetuarem a portabilidade dos dados e os elevados riscos aos direitos e garantias dos indivíduos. Ademais, a possibilidade de interoperabilidade pressupõe um protocolo existente entre diferentes agentes e há preocupação caso um novo agente de mercado ainda não tenha aderido ao protocolo. Desta maneira, e também considerando a assimetria informacional entre titular de dados e agentes de tratamento, a portabilidade também deve ser uma medida preferencialmente viabilizada, ainda que existente a possibilidade de interoperabilidade. ","615504": "Contribuição do Idec - Instituto de Defesa de Consumidores: Sim, desde que a definição dos padrões seja acompanhada e preferencialmente validada pela ANPD. A criação de padrões de difícil cumprimento por parte de agentes menores deve ser um dos critérios avaliados pela ANPD. A criação de barreiras de entrada a players menores por meio de padrões inatingíveis de portabilidade de dados pode diminuir a concorrência entre agentes de tratamento e impedir o desenvolvimento de uma concorrência frutífera em diversos setores - o que não deve ser admitido pela ANPD. ","615511": "Contribuição do Idec - Instituto de Defesa de Consumidores: Considerando que a boa-fé que orienta o tratamento de dados pessoais (art. 6º da LGPD), a classificação de um dado como incompleto, inexato ou desatualizado deve depender da manifestação simples do titular. Sendo fundamental para tanto que os agentes de tratamento disponibilizem de forma facilitada e acessível os dados

dos titulares, que poderão solicitar sua correção quando acharem necessário. Ademais, as inferências decorrentes do tratamento automatizado também devem ser lastreadas em dados concretos e passíveis de correção. Deve ser oportunizado aos titulares a correção de dados utilizados em inferências e a possibilidade de recorrer de decisões automatizadas. ";615514": "Contribuição do Idec - Instituto de Defesa de Consumidores: A simples declaração do titular seria insuficiente quando a correção do dado pessoal implicar na relação dos agentes de tratamento com terceiros e/ou implicar em uma informação dependente de comprovação oficial (e.g. quando é necessário o envio de comprovante de domicílio ou o RG com nome alterado após casamento para comprovar a identificação pessoal para fins de cumprimento de obrigação legal ou regulatória). Seguindo essa lógica, dados meramente cadastrais ou aqueles que não impliquem em dano ao agente de tratamento devem ser alterados imediatamente após a declaração simples do titular. Inclusive a possibilidade de utilização de nome social e de identificação de gênero diverso ao documento, ainda que não estejam oficializados perante o poder público. ";615513": "Sem contribuições. ";615512": "Contribuição do Idec - Instituto de Defesa de Consumidores: A negativa só poderá ser admitida em dois casos excepcionais. Em primeiro lugar, diante da absoluta e comprovada impossibilidade técnica de alteração dos dados. Em segundo lugar, caso o pedido de correção esteja em contradição com dado cadastral público. Para este segundo ponto, entretanto, ressalva-se a possibilidade de utilização de nome social e de identificação de gênero diverso ao documento, ainda que não estejam oficializados perante o poder público. Exceto nessas situações absolutamente excepcionais, o direito de correção não poderia ser negado pelo controlador. O direito de correção tem um fundamento no remédio constitucional habeas data (art. 5º, inciso LXXII da CRFB e Lei 9.507/97), sendo fundamental que os agentes de tratamento possibilitem a correção dos dados pessoais. Ainda que a aplicação do habeas data esteja limitada a bancos de dados de caráter público, sua relevância deve ser considerada na regulamentação deste dispositivo da LGPD. Afinal, o direito à correção está diretamente relacionado ao gozo da autodeterminação informacional dos titulares (Art. 2º, inciso II, da LGPD) e a possibilidade que eles gerenciem o fluxo de seus dados pessoais. Na sociedade informacional esse direito ganha relevância ao considerarmos que os dados pessoais e algoritmos de inteligência artificial intermedeiam os indivíduos e o acesso a serviços, oportunidades sociais e direitos, influenciando em última instância a vida dos titulares de dados. Ainda, não deve ser admitido escusas por parte dos agentes de tratamento para não cumprir um direito tão simples tecnicamente quanto a correção dos dados. Se há possibilidade de coletar dados novos, deve haver a possibilidade de corrigi-los, mesmo que para isso seja necessário eliminá-los e inseri-los novamente nas bases de dados. ";615517": "Contribuição do Idec - Instituto de Defesa de Consumidores: Não, o ônus não deve recair sobre o titular de dados. No exercício de sua autodeterminação informativa poderá o titular de dados se (1) opor ao tratamento de seus dados tratados nas hipóteses de dispensa do consentimento e (2) revogar o consentimento. O fundamento para tais solicitações é a própria autodeterminação do indivíduo, na medida que deve ser garantida aos titulares, autonomia na gestão de seu fluxo de dados. Aliás, em razão das assimetrias informacionais no tratamento de dados, deve haver a inversão do ônus da prova para que o controlador demonstre a regularidade do tratamento. Tal ônus não deve recair sobre o titular, especialmente em situações de excessividade de tratamento, que pode acabar tendo um caráter subjetivo. Além disso, caso fosse deixado à mera discricionariedade dos agentes de tratamento para que julgassem a suficiência da motivação do exercício de direitos de titulares, diante de um evidente conflito de interesses, é provável que o pedido do titular fosse negado. É necessário considerar que a oposição do titular ao

tratamento de dados nas hipóteses que dispensam o consentimento também deve gerar a eliminação dos dados pessoais, uma vez que põe fim ao tratamento de dados considerado por ele irregular. Tratando-se especificamente da hipótese do legítimo interesse, ao considerarmos sua dimensão subjetiva (legítima expectativa do titular, art. 10, inciso II da LGPD), poderá o titular de dados se opor ao tratamento independente da regularidade desse. A legítima expectativa do titular está relacionada ao que o próprio titular espera do tratamento de dados, sendo fundamental que ele goze de sua autodeterminação informacional para se opor ao tratamento quando assim julgar necessário. Além disso, no tratamento irregular que resulte em dano aos direitos à privacidade e proteção de dados, poderá o titular, além de dar fim ao tratamento por meio da oposição e da revogação, requerer a responsabilização objetiva dos agentes de tratamento (art. 42 ss. da LGPD e art. 12 e 14 do CDC).

","615516": "Idec: Somente em situações excepcionais. A regra deve ser seguir a requisição feita pelo titular, priorizando a eliminação. A eliminação é a alternativa prioritária e que mais respeita a proteção de dados pessoais (art. 16, caput). Em situações em que o tratamento de dados seja ilícito ou irregular deverá haver o término do tratamento e, consequentemente, a eliminação dos dados pessoais. Mesmo que a anonimização também signifique o fim do tratamento, ela ainda resultará em potencial lucro e/ou vantagens aos controladores de dados, o que não deve ser admitido. Apenas quando tratamento seja reconhecido como lícito pela ANPD e que o titular, exercendo sua autodeterminação, o compreenda como excessivo é que pode haver a anonimização dos dados para uso exclusivo do controlador (art. 16, IV). Nesses casos, a anonimização deve estar relacionada ao interesse público (como a vigilância em saúde) e não afetar a esfera íntima dos titulares, não sendo razoável que, mesmo após manifestação expressa de objeção do titular, seus dados continuem sendo utilizados. A anonimização pode ser uma importante alternativa para a mitigação de riscos desproporcionais no tratamento de dados (art. 7º, IV, art. 13 e art. 16, II. Entretanto, dados (pseudo-)anonimizados carregam riscos de reidentificação, ainda mais com novas tecnologias, triangulação de dados e “quase-identificadores”, não sendo admitido que riscos e violações à privacidade e proteção de dados sejam perpetuados. Por fim, o art. 18, IV reforça a primariedade da eliminação ao fim do tratamento. Se a eliminação é considerada prioritária nas situações de revogação do consentimento em que, em regra, já há maior autonomia dos titulares do fluxo de seus dados, não há razões para que nas demais hipóteses seja ofertada apenas a anonimização dos dados. Além disso, é muito provável que os titulares não compreendam a diferença entre anonimização e eliminação dos dados, de maneira que deve ser garantida informação suficiente para o titular tomar a decisão e a situação mais benéfica à proteção de seus dados deve prevalecer.”

","615518": "Contribuição do Idec - Instituto de Defesa de Consumidores: Ao identificar que o tratamento de dados está em descumprimento à Legislação, o controlador de dados deve imediatamente (1) se abster de realizar o tratamento irregular e (2) se adequar aos dispositivos da LGPD. A adequação deve ser informada ao titular, que poderá preservar seu pedido de término do tratamento de dados. Por fim, em razão da competência fiscalizatória da ANPD, os agentes de tratamento devem enviar semestralmente a ela relatórios e diagnósticos a partir da análise das reclamações e de outras demandas dos titulares, sem prejuízo de solicitação de informações complementares pela Autoridade. Trata-se de uma obrigação imposta pela Anatel às operadoras de telecomunicações no Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações (art. 88) que poderia ser incorporada e adaptada no contexto da proteção de dados pessoais. Essas informações poderiam ser utilizadas para fins de monitoramento e, se necessário, sanção de agentes de tratamento.

","615523": "Contribuição do Idec - Instituto de Defesa de Consumidores: Sim.

A revogação do consentimento (art. 18, inciso IX da LGPD) deve interromper o tratamento de dados, com isso os dados pessoais, incluindo inferências, provenientes do consentimento devem ser eliminados. Reitera-se ser muito importante que as inferências geradas a partir de dados pessoais sejam também consideradas dados pessoais, uma vez que passam a compor a esfera individual do titular. Dessa forma, elas também devem ser excluídas com o término do tratamento de dados. A partir da decisão dos titulares de dados pela revogação do consentimento não haveria mais hipótese legal que justificasse e legitimasse o tratamento de dados pessoais. Com isso, a manutenção dos dados significaria um tratamento de dados ilegal. No caso de outra hipótese justificar a manutenção dos dados pessoais, deve ser informado ao titular a (1) finalidade do tratamento de dados, (2) quais são os dados tratados e, evidentemente, (3) a hipótese legal que legitima o tratamento. No mesmo sentido, caso a revogação do consentimento se limite a determinadas finalidades do tratamento de dados, o titular deve ser devidamente informado sobre a finalidade e os dados que continuarão a ser tratados. Em resumo: se, por um lado, o consentimento dá início ao tratamento de dados; por outro, sua revogação deve significar o fim desse tratamento, devendo, com isso, os dados serem excluídos. No mesmo sentido, a oposição do titular ao tratamento de dados nas hipóteses que dispensam o consentimento também deve gerar a eliminação dos dados pessoais. ","615521": "Contribuição do Idec - Instituto de Defesa de Consumidores: O tratamento anterior ao pedido de eliminação será ratificado caso o consentimento que o justificou seja lícito - além das finalidades adequadas, tratamento seguro e demais requisitos da LGPD. No entanto, a partir da revogação do consentimento e da necessidade de eliminação dos dados, o tratamento de dados será consequentemente interrompido integralmente ou em partes, a depender do caso concreto. No caso do consentimento ilícito - aquele que não for livre, informado e inequívoco - o tratamento anteriormente realizado deve ser considerado ilícito e, portanto, os tratamentos realizados sob seu amparo devem ser desconsiderados no que for possível. Em ambos os casos, deve haver exclusão dos dados pessoais. ","615617": "Contribuição do Idec - Instituto de Defesa de Consumidores: Uma DECISÃO tomada UNICAMENTE por tratamento automatizado de dados pessoais é aquela em que uma pessoa humana não é capaz de alterar seu RESULTADO. Entretanto, uma intervenção humana prévia não afasta a faculdade de exercício desse direito. Desta maneira, o direito à revisão de decisões automatizadas deve ser interpretado de maneira abrangente, inclusive para efetivar o fundamento à autodeterminação informativa de titulares de dados. Desta maneira, para afastar o direito à revisão, os agentes de tratamento de dados devem ter o ônus de comprovar que houve intervenção humana na DECISÃO. Neste caso, deve ser garantido o direito dos titulares de outra maneira. Em qualquer caso, não é afastado o direito à explicabilidade. ","615618": "Contribuição do Idec - Instituto de Defesa de Consumidores: O termo "interesses afetados" deve ser interpretado de maneira abrangente. A diminuição da possibilidade do exercício de um direito demonstra um interesse individual e coletivo está sendo potencialmente afetado. No caso da proteção de dados, é possível compreender que este direito é afetado quando o titular de dados tem sua autodeterminação limitada pelo tratamento de seus dados pessoais ou quando são limitados outros direitos. Ainda, devemos considerar que, em muitos casos, os titulares de dados também são consumidores, devendo ser imposta a essa relação jurídica as normas de defesa do consumidor. Conforme estabelecido no art. 4º, inciso I do CDC, os consumidores são vulneráveis no mercado de consumo em razão da falta de informações adequadas e da sociedade da informação. ","615619": "Contribuição do Idec - Instituto de Defesa de Consumidores: É um desafio garantir a explicabilidade de decisões unicamente automatizadas. Justamente por este desafio, para que o direito à explicabilidade seja

efetivado, é necessário haver INTERVENÇÃO HUMANA NA REVISÃO da decisão. Presume-se que a revisão de uma decisão automatizada utilize mecanismos diferentes da inferência inicial para atender à demanda de direito do titular. Para tanto, considerando a relevância desse direito à luz da Constituição Federal e da LGPD, a ANPD deverá determinar a presença de humana no processo de revisão. O controlador deve garantir que o processo de revisão é capaz de fazer conclusões diferentes da inicial com base em mudanças concretas. Sem a intervenção humana, o direito de revisão não será substancialmente concretizado. Seria um paradoxo realizar a revisão de que a decisão automatizada por outra decisão automatizada. "615620": "Contribuição do Idec - Instituto de Defesa de Consumidores: Não. Algoritmos de inteligência artificial, que realizam as decisões automatizadas, passaram a intermediar a relação entre os indivíduos e o acesso a serviços, oportunidades sociais e direitos, influenciando em última instância a vida dos titulares de dados. São algoritmos caracterizados pela opacidade e a falta de explicação na tomada de decisão. É fundamental que eles também sejam submetidos a critérios de transparência e accountability. Para tanto, no âmbito da LGPD, o direito de revisão deve ser garantido para aumentar a transparência e a autonomia informacional dos titulares no tratamento automatizado. Afinal, para que o direito de revisão seja efetivo, os agentes de tratamento também deverão dar transparência aos dados e critérios utilizados para a tomada de decisão. Os agentes de tratamento capazes de fornecer tecnologias de tomada de decisão automatizada também devem conseguir revisá-las. A eficiência econômica e a redução de custos não podem escusar os agentes de revisar decisões automatizadas, compreende-se que se o agente disponibiliza uma IA, ele também deve garantir meios de mitigar e cumprimento dos direitos dos titulares. No mesmo sentido, o segredo comercial e industrial dos agentes de tratamento não podem ser invocados para deixar de cumprir direitos individuais e coletivos dos titulares de dados. O segredo comercial poderá projetar a integralidade do código, mas os controladores devem manter públicas informações quanto aos critérios básicos de decisão. Com isso, espera-se submeter os algoritmos a escrutínio público. "

{ "615450": "Ainda que os temas tratados na Lei nº 12.527 ("LAI") e na Lei Geral de Proteção de Dados ("LGPD") possam, à primeira leitura, ser considerados similares, não se pode deixar de ressaltar suas diferenças conceituais, pois, ao passo em que a primeira busca regulamentar o acesso dos cidadãos exclusivamente a informações públicas, objetivando a transparência do poder público, a LGPD busca estabelecer regras para o tratamento de dados pessoais dos cidadãos conferindo extensa gama de direitos a serem observados em benefício dos titulares por entidades públicas e privadas. O tratamento das informações e as tratativas no escopo da LAI são menos morosos que o tratamento de dados pessoais e outros procedimentos necessários para atendimento aos direitos dos titulares pela LGPD. Diante do exposto, recomenda-se que seja determinado o prazo para primeira resposta no período de até 1 (um) mês da solicitação, podendo ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos - a exemplo do disposto no artigo 12.1 do GDPR. Outrossim, propõe-se que a ANPD estabeleça contagem de prazos em dias úteis, excluindo o dia do começo e incluindo o dia do vencimento, em linha com o estabelecido nos Arts. 218 a 235 do CPC e pela GDPR.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? " "615484": "Em primeiro lugar, para garantir a efetividade na comunicação entre o titular e o agente de tratamento, a ABIPAG entende relevante que haja autonomia das organizações para estabelecer o formato de atendimento. Sem prejuízo, também propõe: (i) Identificação do titular solicitante a fim de permitir que o controlador atue de maneira assertiva na demanda; (ii) Possibilidade de solicitação de informações complementares pelos agentes para que possam identificar o titular requerente, desde que respeitadas as diretrizes de proteção de dados pessoais; e (iii) Disponibilidade do canal nos principais meios de comunicação e divulgação do agente de tratamento (ex.: sites e aplicativos). Modelo comum no mercado é a utilização de formulários de solicitação integrados em sistemas de atendimento e a realização de pedidos por e-mail com padrões de informações. " "615485": "A ABIPAG considera que o operador desempenha um importante papel na execução adequada das obrigações legais, o que inclui a manutenção dos registros das operações de tratamento de dados pessoais e o tratamento dos dados em acordo com as instruções do controlador. Neste sentido, entende-se que a responsabilidade deve ser estabelecida contratualmente entre as partes e haja cooperação entre controlador e operador para assegurar a proteção dos dados pessoais de forma eficaz. " "615486": "No lugar de uma abordagem padronizada, sugere-se que haja autonomia para adoção de práticas no contexto específico de cada organização e de acordo com as necessidades dos titulares. Entende-se que aplicação de medidas como SAC poderiam se mostrar proibitivas para organizações de menor porte - sobretudo diante da complexidade de implementação. " "615487": "Não. Conforme reforçado anteriormente, a ABIPAG entende que a autonomia das organizações na definição do formato de atendimento é fundamental para possibilitar a adaptação às suas especificidades e às necessidades dos titulares dos dados. " "615491": "Sim. A ABIPAG entende que tal direito não é absoluto, podendo sofrer limitação com o intuito de assegurar a proteção da liberdade de expressão, a conformidade com a lei, a realização de investigações, a proteção dos direitos de terceiros, a preservação de informações confidenciais, a defesa da propriedade intelectual e a prevenção de abusos. Para fins exemplificativos, elencam-se os casos em que a confirmação da existência do tratamento possa comprometer informações estratégicas ou sigilosas de uma instituição, ocasião em que a legislação pode permitir a

negativa desse direito com base na proteção do direito comercial.";"615492": "Para evitar desafios como vantagens competitivas indevidas, violação de segredos empresariais, dentre outros similares, a ABIPAG sugere que as informações fornecidas para identificação dos controladores, mesmo em casos de compartilhamento de dados pessoais, limitem-se a indicar as categorias de destinatários e as finalidades do tratamento dos dados.";"615489": ";"615490": "Sugere-se que a declaração simplificada sobre o tratamento de dados pessoais inclua os dados pessoais tratados e suas finalidades, observado o escopo solicitado pelo titular. Devem constar também os dados de identificação do titular solicitante e a justificativa para a manutenção dos grupos de dados identificados e encaminhados – exigência que poderá ser cumprida com simples remissão ao aviso de privacidade do controlador, por exemplo.";"615494": "A ABIPAG acredita que, para assegurar transparência e direito à informação, o controlador deve divulgar, conforme os artigos 9º e 18º da LGPD, informações como a finalidade do tratamento, modalidade, prazo, identificação do controlador, detalhes de contato, informações sobre compartilhamento de dados e suas finalidades, responsabilidades dos agentes de tratamento e direitos do titular. Adicionalmente, recomenda-se a criação e ampla divulgação de avisos de privacidade e disponibilização de informações em camadas para facilitar o entendimento dos titulares. Estas informações incluiriam aspectos relacionados à adoção de decisões automatizadas e os agrupamentos de dados pessoais necessários na avaliação, como dados de contato, biométricos, entre outros.";"615493": "Sim, entende-se que haverá satisfação do direito do acesso se o agente de tratamento disponibilizar as informações no formato escolhido pelo titular (digital ou em papel), conforme determina o parágrafo 2º do artigo 19 da LGPD. Se o titular não especificar sua preferência, o controlador tem a liberdade de escolher o formato mais adequado para disponibilizar os dados, sendo que, no caso da necessidade de encaminhamento dos dados em papel, seja considerada a possibilidade de repasse do custo para os titulares de dados";"615502": "Setor financeiro, em que o projeto de implementação do Open Finance apresenta-se como um grande sucesso, pois possibilitou o acesso a dados e históricos financeiros, beneficiando os usuários finais com a melhoria de produtos e serviços bancários que lhe eram oferecidos, bem como facilitando o acesso ao crédito. Contudo, considerando que a maturidade para lidar com a portabilidade pode variar entre os setores, a ABIPAG recomenda que ANPD promova debates e estudos aprofundados, incluindo análises internacionais e consultas públicas, antes que seja realizada uma recomendação específica.";"615501": "A ABIPAG entende que, para além dos desafios tecnológicos de implementação de um layout padrão que garanta a compatibilidade de todos os agentes, existem desafios relacionados à implementação em si, tais como atribuição de quem será o ente responsável pela base que permitirá a interoperabilidade, definição de custos, garantia de segurança cibernética dos dados e afins. Por essa razão, para que haja efetividade em eventual regulação, a ABIPAG recomenda que a ANPD promova um amplo debate com os agentes controladores antes de disciplinar o tema.";"615505": "Para assegurar a capacidade de comunicação entre sistemas, é importante avaliar a viabilidade da padronização, visando possibilitar a transferência de dados em formatos compreensíveis e facilmente acessíveis. Para além disso, a ABIPAG ressalta que entende relevante que eventual padronização não se restrinja a integrações complexas via API, mas também seja viabilizado, sempre que possível, o compartilhamento em formatos de exportação menos complexos, como planilhas e PDFs, assegurando a utilização da funcionalidade por pequenos e médios empresários.";"615503": ";"615504": "Entende-se que a participação do setor privado é indispensável para definição dos padrões obrigatórios de interoperabilidade, devendo ser definidos em comum acordo pelas principais associações representativas do setor. É

importante que essas associações também estejam envolvidas em discussões futuras acerca dos prazos de implementação, considerando que possuem conhecimento prático da complexidade das atividades exercidas por seus associados, bem como do tempo necessário para se adaptarem às novas exigências. ","615511": "Sugere-se que, para que um dado seja qualificado como incompleto, inexato ou desatualizado, é importante considerar critérios objetivos, como a verificação da fonte dos dados, a data da última atualização, a precisão das informações e a integridade dos registros.", "615514": "Entende-se que a declaração do titular não seria suficiente para exercer o direito à correção caso a alteração interfira no princípio da qualidade do dado que exige exatidão. Nestas instâncias, a correção deve ser avaliada, pois pode gerar complexidades para outros direitos regulares do controlador. ","615513": "A ABIPAG entende que não há critérios objetivos passíveis de aplicação a todas as situações. Por essa razão, a associação sugere uma abordagem individualizada para cada solicitação de acesso a dados pessoais. Para tanto, é essencial que haja análise de aspectos como o número de entidades envolvidas, a diversidade dessas entidades, a complexidade da cadeia de compartilhamento, a variação na sensibilidade dos dados e os recursos disponíveis para o controlador. Encontrar o equilíbrio adequado entre transparência e eficiência é fundamental, garantindo que a divulgação das entidades envolvidas seja proporcional às circunstâncias específicas de cada caso. Além disso, é importante considerar a proporcionalidade entre o esforço necessário para atender à solicitação de acesso e os benefícios reais para o titular dos dados. Em alguns casos, o fornecimento de acesso pode demandar um esforço desproporcional em relação aos benefícios que o titular obterá com esta informação. Nestes casos, faz-se necessária a avaliação criteriosa para garantir equilíbrio entre os direitos do titular e as limitações do controlador. Portanto, a ABIPAG destaca a importância de uma abordagem flexível e contextualizada para a avaliação da impossibilidade ou esforço desproporcional previstos no art. 18, § 6º, da LGPD. Esta abordagem busca conciliar a proteção dos dados pessoais com a viabilidade operacional das empresas, garantindo um tratamento equilibrado para todas as partes envolvidas.", "615512": "A ABIPAG acredita que o controlador pode recusar o atendimento caso entenda que os dados estejam completos, precisos e atualizados, isto é, em conformidade com o princípio da qualidade dos dados e a disposição do art. 18, III da LGPD ou quando o titular não fornece documentação adequada que comprove a inexatidão dos dados. Cabe também ressaltar que, abusos no exercício desse direito, como pedidos feitos de má-fé ou excessivos, podem fundamentar a negativa. Exemplos de má-fé incluem intenções de retaliação ou assédio ao controlador sem propósito legítimo, solicitações maliciosas ou pedidos feitos de forma repetitiva sem justificativa válida.", "615517": "Sugere-se aplicação da regra prevista no art. 18, IV da LGPD para os casos em que haja solicitação de anonimização, bloqueio ou eliminação de dados, ou seja, que o titular fundamente e comprove a desnecessidade, excessividade ou desconformidade legal dos dados, ainda que não o faça lastreado em fundamentos legais. ","615516": "Sim, pois trata-se de alternativa permitida pela LGPD levando em consideração o contexto específico do tratamento e da organização, bem como a particularidade de cada cenário. Instituições com grandes volumes de armazenamento em nuvem enfrentam desafios financeiros ao considerar a eliminação de dados, dada a necessidade de revisão e exclusão em larga escala. Em contrapartida, a anonimização emerge como uma alternativa mais viável, preservando dados para análise estatística sem comprometer a privacidade dos titulares. ","615518": "Quando um titular apresenta uma alegação legítima de oposição ao tratamento de seus dados, o controlador tem a responsabilidade de agir conforme a lei. Isto pode envolver a suspensão da atividade de tratamento ou a realização de modificações para garantir a legalidade do processo. Além

disso, é importante que os dados coletados ilegalmente sejam excluídos ou anonimizados, uma vez que caso seja, sua manutenção sem fundamento legal também poderia constituir uma violação. Nesse contexto, a transparência é outra obrigação do controlador, podendo ser necessário que este informe ao titular as medidas adotadas em resposta à sua alegação de oposição. Isto pode incluir mudanças nas práticas de tratamento ou até mesmo a suspensão do tratamento, se for o caso. ","615523": "","615521": "Conforme previsto no art. 8º da LGPD, o requerimento de eliminação de dados pessoais gera efeitos sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado. Na mesma linha, entende-se que os tratamentos realizados com base no consentimento anteriormente concedido pelo titular dos dados permaneceriam válidos, até que haja requerimento de eliminação, nos termos do inciso VI do art. 18 da referida Lei. Dessa forma, entende-se que a revogação do consentimento mediante manifestação expressa do titular não invalida os tratamentos realizados anteriormente, reforçando a importância do requerimento de eliminação para cessar tais atividades. ","615617": "Uma decisão automatizada é aquela em que o processo de tomada de decisão é realizado por meio de algoritmos ou sistemas computacionais, sem intervenção humana direta. Uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é aquela em que não há qualquer participação ou interferência humana no processo de tomada de decisão, sendo totalmente conduzida por algoritmos ou sistemas computacionais. Essas decisões são baseadas somente nos dados pessoais fornecidos e processados, sem a análise ou consideração de informações adicionais por parte de uma pessoa. ","615618": "Sugere-se que sejam considerados os seguintes critérios: (i) quando há impacto significativo na vida do titular dos dados (Ex.: decisões relacionadas a emprego, crédito ou acesso a serviços essenciais) ou quando há uso de dados sensíveis; (ii) quando não há explicações ou transparência em processos decisórios que podem gerar consequências substanciais, como negação de serviços ou restrição de direitos; e (iii) quando há violação de direitos fundamentais, como o direito à não discriminação ou à privacidade. Esses aspectos são importantes para garantir que as decisões automatizadas respeitem os princípios de equidade e transparência, protegendo os interesses dos titulares dos dados. ","615619": "A ABIPAG identifica desafios como: (i) a criação de sistemas e processos capazes de rastrear e analisar as decisões automatizadas, bem como garantir a transparência e a explicabilidade dessas decisões para os titulares dos dados; (ii) o desenvolvimento de mecanismos que permitam que os titulares contestem e solicitem a revisão de decisões automatizadas, especialmente quando essas decisões são complexas ou baseadas em algoritmos; e (iii) a falta de recursos nas organizações para lidar com as solicitações de revisão de decisões de forma oportuna e eficiente, especialmente considerando a possibilidade de um grande volume de solicitações, e a falta de documentação e regras padronizadas sobre os critérios de decisões automatizadas, o que pode dificultar ainda mais o processo de revisão. Nesse sentido, a ABIPAG recomenda o desenvolvimento de diretrizes bastante objetivas para orientar as organizações sobre como cumprir suas obrigações de revisão de decisões sob a LGPD, garantindo uma abordagem uniforme e apropriada em todos os casos. ","615620": "A negativa do direito de revisão sobre decisões automatizadas pode ocorrer quando há razões técnicas, legais ou de segurança que justifiquem a não divulgação ou revisão detalhada da decisão ao titular dos dados. A ABIPAG entende que a revisão deverá ser feita dentro do limite da tecnologia, ou seja, dentro dos casos em que seja possível executá-la."

{ "615450": "NDA", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "NDA", "615484": "De acordo com o artigo 20, § 1º da LGPD, o controlador deveria fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Entretanto, em função do estágio de aplicação da legislação ser imaturo no país, é perceptível que não há parâmetros estabelecidos sobre como essas informações devem ser fornecidas. Além disso, um indicador da efetividade na comunicação entre o titular e o controlador é a presença de um design arquitetural "user-friendly". Por fim, outro fator essencial para se aprimorar a efetividade é a existência de um padrão de confirmação de identidade que seja seguro - para identificar se é realmente o titular dos dados que está solicitando seus dados -, mas não extremamente exigente de modo a criar um grande óbice para o titular. Na análise empírica realizada, foi verificado que, em sua maioria, os mecanismos de verificação de identidade envolvem o envio de documentos oficiais com foto. Algumas plataformas exigem, também, o envio de uma selfie do titular ao lado do documento oficial. Algumas plataformas entraram em contato por meio de uma ligação. Além de desconhecido, o número foi classificado pelo telefone como "suspeita de spam", razão pela qual não foram atendidas as primeiras ligações. Em seguida, a plataforma enviou um e-mail avisando que não tinha obtido contato e solicitando a marcação de horário no dia seguinte para a realização do telefonema. Entretanto, não há motivo que justifique a necessidade de contato telefônico; na ligação, foram apenas confirmados os dados relativos ao nome e o encarregado logo tratou de informar quais dados pessoais constavam na base de dados. Dessa forma, há um grande espaço para aprimorar os meios de verificação. ", "615485": "Na nossa pesquisa empírica de 100 marketplaces, nota-se que apenas 42 empresas forneceram os dados dos titulares em respeito ao seu direito de acesso, enquanto que em 26 não se chegou ao resultado desejado - envio de dados -, e o contato não foi possível com outras 27 empresas. Durante a experiência, notou-se uma fraca preparação dos operadores, pois muitos não sabiam como proceder e das 27 empresas no qual o contato não foi possível, o e-mail constante na Política de Privacidade era inválido em 3, não havia meio para realizar o contato em outras 2 empresas, não houve qualquer tipo de resposta em 20, e outras 2 empresas apresentaram problemas, na qual uma delas o processo de verificação de identidade não foi possível por erro no reconhecimento facial. Menciona-se também que, em relação ao contato com essas empresas, em 2 o contato foi realizado por WhatsApp, e em 1 o formulário de requisição descrito na Política de Privacidade era inexistente. Além disso, em algumas requisições os operadores responderam com o link da Política de Privacidade, link de Política de Cookies, e, inclusive, em ao menos 8 casos os estudantes foram informados equivocadamente que sequer havia cadastro do titular. Por fim, o número de requisições nos quais nenhum dado foi enviado surpreendeu com um alto número (26), com 1 empresa alegando que esse direito não existia por não constar na Política de Privacidade da empresa, e dentre as 25 restantes, ocorreu um provável erro de desorganização, motivado pela falta de treinamento ou simulação do modelo de resposta aos titulares, em razão de respostas que não tinham a ver com a questão ou de negligência posterior. ", "615486": "As diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor ("SAC") poderiam ser utilizadas para o exercício dos direitos do titular de dados pessoais. Assim como previsto para o SAC, o exercício dos direitos dos titulares deve ser realizado tempestivamente, de modo que o controlador/operador forneça as respostas dentro de um prazo, via de regra, de 7 dias

(artigo 7 do Decreto 11.034/2022). Essa celeridade é possível uma vez que os padrões de identificação de ambos procedimentos são, na maioria das vezes, idênticos, já que os consumidores são identificados com base em seus dados pessoais, como CPF e número de telefone. Além disso, as normativas que regulam ambos procedimentos possuem uma ratio decidendi muito semelhante: fornecer ao consumidor uma resposta clara em relação ao atendimento de suas demandas (Art. 1º do Decreto 11.034/2022 c/c Art. 2, inciso II da LGPD). Entretanto, as companhias brasileiras possuem um tratamento diferente com demandas do SAC e do exercício dos direitos dos titulares. Conforme a análise empírica, 62% das empresas que tiveram requisições de dados pessoais não enviaram os dados solicitados de forma adequada, sendo que em sua maioria não chegaram a enviar os dados solicitados e, alguns, quando enviavam o formato do arquivo não possibilitava a visualização pelo titular. "615487": "NDA", "615491": "NDA", "615492": "NDA", "615489": "NDA", "615490": "NDA". Na nossa amostra de 100 marketplaces, em 8% dos casos, controladores alegaram não possuir registros de nossos dados pessoais, embora pudéssemos comprovar que havíamos nos cadastrado em suas plataformas e não havíamos efetuado qualquer eliminação. Essas inconsistências parecem ser especialmente comuns quando o cadastro ocorre por meio da utilização de uma conta de alguma outra plataforma (por exemplo, “entrar com Google”), embora as políticas de privacidade das plataformas em questão prevejam o registro justamente desses tipos de dados. No caso de pedidos de acesso, é evidente que se exige do controlador o fornecimento de uma cópia de todos os dados pessoais do titular solicitante mantidos em seus registros. Infelizmente, nossa pesquisa sugere que mesmo essa exigência basilar não é suficientemente atendida pelas plataformas analisadas. Em 32,2% dos casos, não foi possível entrar em contato com a plataforma; em 24%, houve o contato, mas os dados não foram fornecidos adequadamente (por exemplo, a resposta consistiu em uma transcrição de trechos da política de privacidade); em 2,1% dos casos, os dados foram enviados, mas não foi possível acessá-los. Ademais, é razoável que se exija que essa cópia seja providenciada em um formato que facilite a compreensão de um titular leigo, inclusive à luz do parágrafo 1º do art. 19. Em nossa pesquisa, constatamos que em 8,4% dos casos os controladores negaram possuir nossos registros, embora tivéssemos evidências de nosso cadastro. Quanto aos pedidos de acesso, é esperado que o controlador forneça uma cópia de todos os dados pessoais do solicitante mantidos em seus registros. No entanto, nossos resultados indicam que essa exigência básica não é consistentemente atendida pelas plataformas analisadas. Em 30,5% dos casos, não conseguimos contatar a plataforma; em 24%, os dados não foram fornecidos adequadamente (por exemplo, enviaram uma transcrição da política de privacidade); e, em 2%, embora os dados tenham sido enviados, não pudemos acessá-los. "615494": "Entre as 100 políticas de privacidade analisadas em nossa pesquisa, 44 indicam apenas o e-mail do DPO; 28, e-mail e nome; 26, nenhum dos dois; e 2, apenas o nome. Nossa pesquisa indica das 83 políticas de privacidade que citam responsabilidades apenas se referem a medidas de segurança adotadas no tratamento de dados, com diferentes graus de especificidade. Eventualmente, informações sobre a distribuição de responsabilidade entre os atores, e as respectivas atividades de tratamento encabeçadas por cada um deles, poderia facilitar a realização do endereçamento de futuras denúncias administrativas ou ações cíveis por titulares de dados com seus direitos violados. Nossos dados também indicam que nem todos os direitos dos titulares são explicitados. 87% das políticas de privacidade mencionam o direito de eliminação; também 87% mencionam o direito de correção; 84%, o direito de acesso; 80%, o direito de retirar o consentimento; 70%, o direito à confirmação da existência de tratamento; 63%, o direito de portabilidade; 50%, o direito à anonimização; e 49%, o

direito de bloqueio. Outras informações essenciais dizem respeito às finalidades específicas do tratamento. É recomendável que (i) essas finalidades indiquem usos concretos dos dados adotados pelo controlador, e não apenas referências vagas. Entre as políticas analisadas, 47% relacionam finalidades a tipos de dados, 46% fazem menções inespecíficas e 7% não abordam de qualquer forma as finalidades. É igualmente importante para o titular compreender quem são os destinatários do compartilhamento de seus dados pelo controlador — ou, ao menos, o seu setor de atuação — e para quais finalidades esse compartilhamento pode ocorrer. 16% das políticas analisadas identificam quais categorias de dados podem ser compartilhadas; 22% identificam especificamente terceiros; 77% indicam apenas as categorias desses terceiros (por exemplo, “órgãos públicos” ou “fornecedores”); 73% identificam base legal para o compartilhamento; e 77% identificam finalidades para esse compartilhamento.

;"615493": "NDA"; "615502": "NDA"; "615501": "NDA"; "615505": "NDA"; "615503": "NDA"; "615504": "NDA"; "615511": "NDA"; "615514": "NDA"; "615513": "NDA"; "615512": "NDA"; "615517": "NDA"; "615516": "NDA"; "615518": "NDA"; "615523": "NDA"; "615521": "NDA"; "615617": "NDA"; "615618": "NDA"; "615619": "NDA"; "615620": "NDA"

{ "615450": "Os prazos da LAI devem ter sua premência compreendida dentro do contexto de relevância democrática dessa norma. É dizer, se os órgãos públicos, nesse contexto, têm o dever de atender aos cidadãos em prazo não superior a 20 dias, prorrogável por mais 10 dias, com mais razão deve-se estabelecer aos entes privados prazos como este, como parâmetro mínimo, ou superiores. Além disso, recomenda-se a não utilização de termos como "imediato", que são frequente e necessariamente flexibilizados pela possibilidade técnica dos controladores e podem gerar um aumento indesejável de demandas à Autoridade. Por fim, ressalta-se que para fins de uniformização da contagem de prazos, ainda que se utilize o parâmetro mínimo dos prazos da LAI, estes devem ser contados em dias úteis.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "No acesso completo a dados deve ser considerada primordialmente a complexidade técnica para operacionalizar a solicitação, no que tange, por exemplo, a anonimização e portabilidade. Essa complexidade técnica (factual) deve ser analisada em cada caso concreto, à luz da boa-fé subjetiva no cumprimento do dever de atendimento ao titular.", "615484": "É essencial que se adote linguagem simples (plain language) evitando o uso de expressões jurídicas em excesso e, se possível criando um formulário de atendimento intuitivo. Para assegurar, de fato, o exercício de direitos pelos titulares é essencial que o canal de atendimento seja simples, de fácil acesso e fácil visualização.", "615485": "Os operadores devem ser obrigados, nos termos do contrato existente entre as partes, a fornecer todas as informações e cooperar com os controladores para garantir o exercício de direitos dos titulares de dados pessoais. Muitas vezes são eles que conseguem, factualmente, gerenciar partes profundas dos sistemas contratados pelos controladores e efetivar as requisições de titulares de dados, fornecendo dados, eliminando e, principalmente, garantindo a portabilidade de dados pessoais. Contudo, essa possibilidade técnica/fática não deve ter o condão de criar ou extinguir responsabilidades onde a lei não o fez. A figura do operador, por definição, age em nome do controlador, que é o responsável pelo atendimento ao direito dos titulares e deve articular as cooperações necessárias para efetivar esse atendimento. A responsabilidade do operador, portanto, se dá nos termos contratuais.", "615486": "Embora seja inegável o viés consumerista e a importância do âmbito de defesa do consumidor na proteção de dados pessoais no Brasil, em razão da amplitude e complexidade do atendimento aos titulares de dados, a adoção de diretrizes e procedimentos do SAC não seria o melhor parâmetro. Se por um lado, alguns pontos como a padronização de registros sobre o atendimento podem ser úteis, em geral os procedimentos do SAC serão limitados para atender às demandas da LGPD. Por exemplo, a forma de atendimento ao titular, que varia muito em razão da quantidade e qualidade da informação que é fornecida por cada controlador e deve ser sua responsabilidade adequar seus meios ao conteúdo a informar. Além disso, os prazos exíguos, válidos para um atendimento pontual de consumo, são insuficientes para uma informação de qualidade apta a garantir a autodeterminação informativa dos titulares. Por fim, o SAC prevê atendimento integrado, o que é contrário à própria disposição da LGPD que prevê a necessidade de existência de um canal próprio para isso.", "615487": ":", "615491": ":", "615492": "Nome fantasia e CNPJ atualizados do recipiente das informações (outro controlador) e a finalidade do compartilhamento.", "615489": "Os operadores devem fornecer as informações que estiverem em seu poder e que o controlador julgue necessárias para responder os titulares de dados pessoais desde que isso não implique violação à segredos de negócio. Se isso ocorrer, todavia, o operador

deve justificar o motivo pelo qual entende que há uma violação."615490": "Acreditamos que uma lista com finalidades com duas colunas, uma com uma lista de dados pessoais e outra com uma lista das finalidades de uso dos dados seja suficiente para suprir o direito."

"615494": "Em relação ao acesso às informações mínimas sobre tratamento de dados pessoais, acreditamos que o conteúdo disposto no artigo 9º, LGPD, que contém os requisitos para o livre acesso, é suficiente para cumprir esse dever de transparência. Contudo, em relação às decisões automatizadas, não se deve confundir o direito à explicação aos que podem estar sujeitos a elas, com o direito ao acesso. Embora haja na literatura quem entenda que o direito à explicação é, na verdade, um direito ao acesso - e que se esgota no direito ao acesso (ver WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. In *International Data Privacy Law*, 2017, Vol. 7, No. 2, p. 76-99. Disponível em <https://academic.oup.com/idpl/article/7/2/76/3860948>), é importante ressaltar a importância de fornecer explicações adicionais sobre a decisão automatizada, de forma que o titular possa compreender como seu âmbito de direitos é afetado por ela (e nesse sentido, temos SELBST, Andrew; POWLES, Julia. "Meaningful Information" and the Right to Explanation. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 233 – 242. Disponível em <https://academic.oup.com/idpl/article/7/4/233/4762325>). Isso implica dizer, no âmbito da LGPD, que o direito a informação sobre decisões automatizadas não se encerra no artigo 9º, LGPD. De forma ex ante (ao tratamento, independentemente de requerimento), o agente de tratamento deve indicar a existência de uso de tecnologia de decisão automatizada em que momento/etapa da prestação de serviço e, de forma geral, os critérios utilizados para que a decisão automatizada aconteça. De forma ex post, ou seja, considerando o exercício de direitos do art. 20, a informação deve focar na comprovação de que houve apuração de risco de discriminação e com os parâmetros que orientam a decisão são conformes e como eles podem ou não causar discriminação."

"615493": "Considerando a ausência de custograturidade e limitação para requerer o direito, sugerimos a criação da possibilidade de que o controlador disponha uma lista de opções (possíveis para ele) dentre as quais o titular pode escolher livremente. No mais, o direito pode se considerar satisfeito, desde que em linguagem simples, voltada para o público ao qual ele se destina."

"615502": "Os setores já regulamentados, como telecomunicações, bancário e saúde complementar."

"615501": "Incompatibilidade sistêmica, segurança jurídica do compartilhamento, construção de arquitetura específica e segura para o trânsito dos dados pessoais, especificidade dos agentes envolvidos na operação."

"615505": ""

"615503": "Não, pois a mera disponibilização dos dados para o titular de dados deve ser entendida como direito ao acesso. A interoperabilidade diz respeito ao trânsito das informações de um agente de tratamento originário para o novo agente de tratamento selecionado pelo titular."

"615504": "Sim, especialmente em setores não regulados. Após período de diálogo multissetorial (diante da necessidade de conhecimentos específicos), entendemos que cada setor poderá, de forma mais criteriosa, estabelecer prazos de acordo com as suas atividades."

"615511": "Documentação apresentada pelo titular de dados pessoais informando a mudança dos dados pessoais inicialmente fornecidos ao controlador."

"615514": "A regra geral deve ser anexar documentação ao pedido de alteração de dados pessoais. No entanto, situações nas quais a ausência de alteração pode ocasionar discriminações ou vexatórias isso deve ser revisto, a exemplo da mudança de nome social, que pode ser um processo demorado para os cidadãos."

"615513": "Podemos mencionar como critérios objetivos: - porte do controlador; - se possui infraestrutura à disposição; - número

de agentes de tratamento; - se os agentes da cadeia de tratamento ainda existem e estão ativos. ","615512": "Quando se identificar prejudicialidade da alteração para terceiros e quando os documentos não comprovarem a alteração requisitada pelo titular. ","615517": "Não, é responsabilidade do controlador fundamentar o uso dos dados pessoais adequadamente considerando todos esses pontos fazendo prova dessa conformidade. ","615516": "b. Sim, por exemplo em situações nas quais seria demasiadamente oneroso para o controlador garantir o processo de anonimização, considerando procedimentos técnico e o registro administrativo do procedimento utilizado para anonimizar, ou vice-versa, em situações em que seria onerosa a eliminação, por exemplo em casos em que os dados são relevantes para compor uma massa de dados, e em que se opta pela anonimização. ","615518": "O efeito prático deve ser a interrupção da atividade de tratamento à qual a pessoa se opôs, considerando que os dados podem ser utilizados para outras finalidades legítimas como o cumprimento de obrigação legal-regulatória. ","615523": "Não, implica a interrupção a atividade de tratamento de dados que ocorria com base no consentimento. Sendo necessário observar também eventual necessidade de armazenamento dos dados por obrigações regulatórias. ","615521": "A interrupção a atividade de tratamento de dados que ocorria com base no consentimento. ","615617": "(1) O termo decisão inclui qualquer “medida” que “produza efeitos jurídicos em relação ao titular de dados” ou “afete significativamente o titular de dados de forma semelhante”, motivo pelo qual o titular tem direito de não ser submetido a tal decisão. Por exemplo o resultado do cálculo da capacidade de uma pessoa cumprir obrigações de pagamento futuras, é uma “decisão”; (2) Essa decisão deve ser “exclusivamente com base no processamento automatizado, incluindo a criação de perfis” – por exemplo a perfilização; (3) Por fim, a decisão automatizada deve causar “efeito jurídico” ou afetá-lo “significativamente de forma semelhante” – Por exemplo o valor de probabilidade determinado por um ente sobre a possibilidade de pagamento do titular representa um papel decisivo na concessão do empréstimo, afetando significativamente o titular de dados pessoais; (4) Autonomia da pessoa responsável pelo uso de uma previsão para a tomada de decisão. : aqui, não se deve confundir a previsão (“decisão” algorítmica, que na realidade é uma projeção com base de dados imputada inicialmente) com a decisão (humana, ou seja, o uso humano que se faz da previsão, decisão algorítmica). Aqui, é importante considerar em cada caso, a autonomia que o humano posicionado no loop possui para decidir de forma diversa. ","615618": "Um interesse é afetado quando a decisão automatizada produz efeitos jurídicos no direito dos titulares de acesso a produtos ou serviços, sejam eles públicos ou privados. ","615619": "Podemos mencionar como desafios práticos situações nas quais o controlador não é o desenvolvedor da IA e não tem acesso aos critérios de decisão da IA. Nesses casos há uma assimetria informacional entre as partes que têm o dever de informar e as que poderiam ter acesso à informação devida. Além disso, é relevante mencionar a dificuldade de avaliar se a decisão foi injusta/enviesada/discriminatória em uma análise individual. Em geral, é necessária a análise de uma base amostral dos resultados algorítmicos para verificar se há uma distribuição anormal para algum grupo social que possa ser considerada ilícita ou algum outro marcador social da diferença afetado de forma ilícita. - ausência de conceituação do que é uma decisão automatizada nos termos da lei; ","615620": ""

{“615450”：“Os prazos propostos pela Lei Nº 12.527/2011 (“Lei de Acesso à Informação” ou “LAI”) foram originalmente estabelecidos pelo legislador para serem aplicáveis aos órgãos públicos integrantes da Administração Pública Direta. Ademais, os prazos previstos pela LAI contemplam somente o direito de acesso à informação, prevendo: (I) acesso imediato; e (II) na ausência de acesso imediato, prazo de 20 (vinte) dias (art. 11, §1º, LAI), prorrogável por mais 10 (dez) dias mediante justificativa do responsável pela guarda e apresentação de testemunhas que justifiquem o impedimento (art. 11, III, §2º, LAI). De início, cumpre ressaltar que a ANBC entende que os prazos em questão são razoáveis, no entanto, a aplicação de legislação ao setor privado poderá gerar insegurança jurídica já que o precedente poderia possibilitar e fortalecer entendimentos diversos sobre a aplicabilidade dessa e de outras legislações. ”,b.Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:“Nos casos em que o prazo de concretização de direitos do titular não estiver previsto em lei, é necessário ponderar o equilíbrio entre o melhor interesse do titular, e a finalidade do tratamento conduzida. O controlador deve considerar: (I) a possibilidade de atender ao exercício de direito do titular, a partir da situação concreta na qual houve solicitação; (II) o canal de atendimento correto para o recebimento e tratamento da solicitação do titular; e (III) a necessidade de implementação de processos de autenticação do usuário. Em razão das semelhanças entre a LGPD e a Regulation (EU) 2016/679 (“GDPR”), é possível colher parâmetros objetivos de autoridades estrangeiras. Nesse sentido, o Information Commissioner’s Office (ICO), DPA do Reino Unido, estabelece que as solicitações dos titulares devem ser respondidas no prazo máximo de 1 (um) mês, contados a partir do recebimento da solicitação. O prazo poderá ser alterado caso o controlador necessite de documentação específica para atender à solicitação, hipótese em que o prazo será contado a partir do recebimento dos documentos. Caso o último dia de prazo seja em um final de semana ou em um feriado nacional, o dia final deverá ser o próximo dia útil subsequente (<https://ico.org.uk/for-the-public/time-limits-for-responding-to-data-protection-rights-requests/>). O inciso I do art. 19, por sua vez, estabelece que a solicitação simplificada deve ser respondida de imediato, todavia, não apresenta formato de resposta da solicitação e/ou quais informações deverão ser disponibilizadas. Para o setor privado, a obrigação de atendimento imediato à solicitação do titular poderá ser mais onerosa, posto que a tempestividade dificulta a condução de diligências prévias para avaliar se a solicitação é viável, se compromete segredos comerciais ou se afeta obrigações de confidencialidade das quais o agente de tratamento está submetido. A ANBC sugere, nos casos em que o controlador não tenha a disponibilização de forma on-line, que o prazo seja de 2 (dois) dias úteis, contados a partir do atendimento dos requisitos de segurança”,”615484”：“A ANBC entende que o canal de atendimento deve prezar pela facilidade de comunicação. Isto é, deve fornecer aos titulares informações claras e pertinentes, em linguagem acessível e em design facilitado, prezando pelo uso intuitivo das ferramentas. Outro ponto de importância diz respeito à implementação de mecanismos de verificação, identificação e autenticação da solicitação e de seu solicitante, de modo que os agentes de tratamento devem adotar ferramentas que permitam a confirmação da identidade do solicitante. Buscase, assim, evitar potenciais fraudes e assegurar que as solicitações estão sendo efetivamente submetidas pelos titulares dos dados pessoais tratados ou por seus representantes legais. A título de exemplo, são características essenciais de um canal de atendimento: (i) garantia da identificação do titular (autenticação positiva); (ii) meio para que o titular

forneça as informações mínimas para que o controlador possa atender a solicitação; (iii) fácil acesso; e (iv) acompanhamento da solicitação. ","615485": "De acordo com o art. 18 da LGPD, "o titular tem direito de obter do controlador" o exercício de seus direitos. Nesse sentido, de forma geral, não é ônus do operador assegurar ou responsabilizar-se pela concretização dos direitos do titular. Todavia, é razoável sustentar, com base nas atribuições dos agentes de tratamento, que o operador deverá envidar seus máximos esforços na colaboração com o controlador, de modo a indicar ao titular de dados o contato do controlador (razão social/nome fantasia e canal de contato/atendimento), a fim que o direito pleiteado possa ser exercido. ","615486": "A implementação de diretrizes e procedimentos análogos aos regulamentados no Decreto nº 11.034/2022 seria excessivamente custoso aos agentes de tratamento, haja vista o alto grau de regulação do setor e a necessidade de pontos de divergências inicialmente inviáveis. Exemplificativamente, o Decreto que estabelece atendimento ininterrupto em todos os dias da semana (art. 4º, caput do Decreto), bem como atendimento telefônico obrigatório (art. 4º, §2º), cuja aplicação para fins de atendimento aos direitos dos titulares seria de difícil implementação pelo setor privado e público, em pelos custos de custos de manutenção. O atendimento humano diário pelo período de oito horas mínimas (art. 5º, I) demonstra-se, também, de difícil aplicabilidade, pois demandaria o recebimento de solicitações intermediadas diretamente por prepostos dos agentes de tratamento exclusivamente para esta função. Na prática, o recebimento e o atendimento de solicitações de exercícios de direitos dos titulares são realizados por canais digitais (i.e através do endereço eletrônico do Encarregado) ou com o auxílio de outras ferramentas para filtrar o recebimento de solicitações, tornando o processo mais dinâmico. De igual importância, vale esclarecer que a legislação é aplicável a setor regulado específico, de modo que, à época de sua criação, foi considerado a pertinência de um canal de atendimento nesse moldes, dada a atividade setorial, bem como a viabilidade financeiro de estabelecimento do fluxo. ","615487": "Para conferir celeridade e economicidade ao atendimento de demandas de titulares, é possível que o setor público venha a adotar o uso de ferramentas digitais que contribuam para o recebimento e a filtragem de solicitações, como por exemplo softwares de privacidade e segurança, prática mais usual para agentes privados. Nesse sentido, o desenvolvimento de portais de privacidade, amparados pelo uso de tais ferramentas, colaboram para a simplificação do recebimento de demandas por formatos comumente adotados, tal qual demandas submetidas diretamente ao correio eletrônico do Encarregado e/ou da área de privacidade de agentes privados ou do setor público. Recomenda-se, ainda, que os agentes de tratamento tomem medidas administrativas necessárias para fornecer instruções aos titulares para a solicitação do exercício de seus direitos de maneira clara e objetiva, através de documentos como políticas de privacidade. Nesse sentido, deve-se informar previamente ao titular: (I) os canais específicos para envio da solicitação de exercício de direitos; (II) quais direitos são conferidos ao titular pela LGPD; (III) quais documentos de identificação e/ou demais documentos aplicáveis são necessários para verificação de identidade do titular; e (IV) avisos de transparência indicando que, diante de determinadas hipóteses, o agente de tratamento poderá estar impossibilitado de atender ao direito solicitado. ","615491": "Entende-se, a partir da análise do ordenamento jurídico brasileiro, que inexistem direitos absolutos. No âmbito da LGPD, haja vista que o direito à proteção de dados possui caráter de direito fundamental, uma das hipóteses que ensejaria a negativa ao direito de confirmação de existência do tratamento está associada à colisão de direitos fundamentais. Por exemplo, para dados tratados pelo Poder Público para fins de persecução do interesse público, é possível sustentar que a sobreposição do interesse público, em face do direito individual do titular, poderá ensejar a

negativa do tratamento. Esta hipótese poderá ser aplicável aos dados pessoais tratados de maneira necessária para a execução de políticas públicas (art. 11, II, “b”). É possível sustentar semelhante tese para dados pessoais que sejam tratados para garantia da prevenção à fraude e à segurança do titular (art. 11, “g”), hipótese em que a LGPD, ao prever os direitos que deverão ser resguardados aos dados tratados sob esta base legal, não menciona o direito de confirmação da existência do tratamento. Em síntese, é possível entender como exceção ao direito de confirmação da existência do tratamento nos casos em que houver: (I) sobreposição do interesse público ao interesse particular do titular; (II) nos casos em que a concretização do direito puder comprometer a segurança do titular, bem como corroborar para fraudes, acesso indevido aos dados ou inviabilizar a finalidade legal pretendida, salvo nas hipóteses de sobreposição às liberdades e direitos fundamentais dos titulares. (iii) solicitações específicas que envolvem segredos comerciais, conforme resalta o artigo 19, inciso II da LGPD “;”615492”:

“À luz das boas práticas de proteção de dados e privacidade, recomenda-se que os documentos informacionais elaborados para prestar esclarecimentos aos titulares a respeito do tratamento de seus dados, como a política de privacidade, apresentem informações suficientes para indicar ao titular a qualificação do controlador, isto é, a razão social e/ou nome fantasia da pessoa jurídica que atue como controladora de dados pessoais e seu canal de contato. Caso haja compartilhamento de dados pessoais com terceiros que igualmente atuem como controlador, seja mediante hipótese de controladoria singular ou conjunta, é recomendável que haja previsão expressa na política de privacidade para que o titular seja satisfatoriamente informado ou possua legítima expectativa de que seus dados serão compartilhados com terceiros. Nesse caso, os demais controladores poderão ser indicados a partir de sua relação contratual com o controlador responsável pela coleta dos dados - por exemplo, indicação de que os dados serão compartilhados com “parceiros comerciais”, “fornecedores”, “prestadores de serviços” ou com “demais órgãos da administração pública”, na hipótese de cumprimento de obrigação regulatória ou em dados tratados pelo Poder Público. ”;”615489”:

“O operador possui a obrigação legal de auxiliar o controlador de dados pessoais na concretização do exercício de direitos dos titulares, a partir do fornecimento de instruções lícitas do controlador. Tal entendimento, além de advindo da LGPD, foi ratificado pela ANPD no âmbito do Guia de Agentes de Tratamento, que prevê que os direitos de titulares são exercidos, em regra, em face do controlador. Nesse sentido, o operador possui apenas a responsabilidade legal de cumprir com as determinações do controlador e, neste caso, de prestar os auxílios necessários para garantir o direito informacional dos titulares, na medida e na extensão em que os dados pessoais objeto da solicitação forem tratados pelo operador. ”;”615490”:

“Em formato simplificado pode ser confirmada a existência de tratamento, contendo, por exemplo, categorias de dados pessoais mais usualmente solicitados pelos titulares de dados e as finalidades de tratamento ou categoria de dados convencionadas por entidades representativas setoriais, na medida em que cada setor possui especificidades relevantes a respeito das atividades de tratamento realizadas.”;”615494”:

“Recomenda-se que as atividades de tratamento de dados pessoais conduzidas sejam, na medida do possível e de maneira geral, indicadas na Política de Privacidade ou em demais documentos correlatos. Neste caso, é possível sustentar como mínimo que a Política apresente: (I) as finalidades das quais os dados pessoais poderão ser submetidos a processo de tratamento, especialmente diante das bases legais apresentadas pela LGPD - por exemplo, para cumprimento de obrigações regulatórias, para execução de contratos, para atendimento dos legítimos interesses do controlador; e (II) os direitos assegurados aos titulares e seus canais e meios de exercício. ”;”615493”:

“A ANBC entende que sim. No entanto, é imprescindível analisar a

onerosidade do envio das informações em papel, bem como o risco de exposição maior do dado pessoal ali contido. ";615502": "A consolidação dos direitos dos titulares está intrinsecamente conectada aos níveis de conformidade e adequação à LGPD pelo controlador, incluindo a elaboração de documentos necessários para cumprir com as obrigações legais previstas pela lei, além da adoção e implementação de medidas técnicas, administrativas e de governança. A esse respeito, o Tribunal de Contas da União (TCU) conduziu, em 2022, uma auditoria para avaliar o grau de implementação da LGPD nos órgãos da Administração Pública Federal. À época, o TCU identificou que 58,9% das organizações estavam em níveis iniciais (225 organizações), enquanto 20,4% estavam em níveis intermediários (78 organizações), em comparação aos 2,9% (11 organizações) em níveis avançados. Demonstra-se, a partir da auditoria, que apesar do expressivo número de organizações em estágios iniciais de adequação no momento de avaliação, a existência de condução de medidas para a correta conformidade com a lei. Por fim, a garantia da portabilidade entre agentes de tratamento de maneira efetiva deve ser acompanhada por avaliação e regulação setorial, a partir de entidades de representação setorial, como forma de assegurar que eventuais normas regulatórias estarão em conformidade com a realidade e com as questões específicas de cada setor";615501": "A interoperabilidade está relacionada à capacidade de compartilhamento e leitura de informações e recursos em sistemas distintos, preservando a possibilidade de leitura e compreensão dos dados pessoais tanto pelo sistema do controlador que está realizando a transferência, quanto pelo sistema do controlador que esteja recebendo os dados. O ICO destaca, ainda, que não é esperado que sejam “tecnicamente compatíveis” com os de demais organizações, visto que a portabilidade de dados visa produzir sistemas que sejam interoperáveis entre si, não necessariamente compatíveis. Nesse sentido, ao estabelecer que os dados deverão ser transferidos em formato “estruturado, de uso corrente e legível”, existem desafios tecnológicos como: (I) assegurar que os softwares adotados pelos controladores serão capazes de extrair todos os elementos específicos dos dados; (II) estabelecer um sistema padronizado de uso comum no mercado, considerando especificações setoriais e comerciais, avaliando, ainda, se o padrão adotado assegura que os dados serão transferidos de forma legível e estruturada; (III) assegurar que os sistemas utilizados serão capazes de transferir arquivos de forma segura e em formatos diversos, além de garantir que tais formatos poderão ser lidos com precisão pelos demais agentes de tratamento, permitindo a identificação e o reconhecimento de todos os dados pessoais transferidos; (IV) proteção dos agentes econômicos de práticas concorrenciais desleais e assimetrias da informação inerente ao mercado; e (V) os elevados custos de implementação. Em suma, a definição de sistemas aptos a transferir os dados entre agentes de tratamento, conservando a qualidade dos dados e preservando segredos comerciais e industriais, são desafios tecnológicos de considerável grau de transposição. ";615505": "A padronização é desejável, especialmente, na definição dos formatos que melhor assegurem a interoperabilidade dos dados, levando em consideração a capacidade e facilidade de leitura dos dados por diferentes sistemas. A esse respeito, uma padronização setorial, como, por exemplo, considerando as práticas comuns de mercado adotadas pela área de atividade econômica, poderá satisfazer a necessidade de padronização sem que a Autoridade Nacional venha a dispor normas específicas sobre o tema, embora a manifestação expressa da ANPD, nos termos do art. 40, confira maior grau de conformidade aos agentes de tratamento. ";615503": "Sim, é adequado considerar satisfeito o direito, uma vez que a solicitação advém do próprio titular de dados, o qual entende que seu direito será melhor atendido através da indicação de dados pessoais em formato interoperável. Para a ANBC é importante que a ANPD considere, em seu futuro Regulamento sobre a matéria, nos termos

do artigo 40 da LGPD, que padrões de portabilidade considerem: (i) especificidades de cada setor; (ii) o segredo comercial e industrial; (iii) a quantidade e complexidade dos dados solicitados; (iv) eventual criação de carga financeira ou procedimental excessiva ou irrazoável; (v) em caso de portabilidade, a empresa que enviou os dados do titular tem direito de manter uma cópia dos dados por um determinado período para fins de histórico, auditoria e cumprimento de obrigação legal. ";615504": "As especificidades de certos setores e segmentos de atividades econômicas, a exemplo do setor bancário, farmacêutico, crediário e securitário, em que a satisfação ao direito de portabilidade demanda a condução de diligências técnicas e operacionais internas poderá se beneficiar de um grau razoável de autorregulação para dispor acerca os padrões e interoperabilidade específicos para as áreas de atuação. Ademais, a definição de padrões específicos poderá ser elaborada de maneira conjunta aos agentes privados, mas regulamentada por autoridade competente e formalmente constituída, como o Banco Central do Brasil e a Superintendência de Seguros Privados. No que diz respeito a definição de prazos, a complexidade envolvida no tratamento de dados pessoais por determinados agentes econômicos poderá demandar a fixação de prazos maiores para a condução de diligências técnicas e operacionais internas para fornecer aos titulares e/ou aos agentes de tratamento a portabilidade dos dados de maneira funcional e efetiva. Nesse sentido, caso os órgãos regulamentadores venham a elaborar normas setoriais específicas para o tema, é recomendável que sejam tomados subsídios dos principais agentes de cada segmento econômico para entender todas as especificidades necessárias e estipular prazos que sejam favoráveis aos agentes econômicos e aos titulares de dados pessoais. ";615511": "A partir do quality framework proposto pela OECD, ao analisar as dimensões para a qualidade dos dados, a organização propõe alguns eixos que poderão ser observados para analisar a concretude da qualidade dos dados. De maneira apartada, para verificar a incompletude e a (in)exatidão dos dados pessoais, é necessário verificar sua acurácia, isto é, avaliar o grau em que os dados pessoais são apenas parcialmente corretos ou se necessitam de complementação, ou seja, se descrevem ou endereçam corretamente todas as características, informações ou se atendem satisfatoriamente às finalidades para as quais foram coletados. Conjuntamente, é necessário avaliar a coerência dos dados pessoais coletados em face da realização de atividades de tratamento para alcançar a finalidade proposta, de modo que é necessário avaliar se os dados pessoais estão sendo utilizados de maneira lógica para o cumprimento da finalidade. Para verificar se os dados pessoais estão desatualizados, por sua vez, é necessário avaliar a atualidade ou temporalidade dos dados pessoais, quando aplicável. Nesse caso, o agente de tratamento deve conduzir diligências para determinar se o período de tempo entre a coleta dos dados pessoais e a condução da atividade de tratamento é capaz de tornar os dados desatualizados, bem como se, em razão do tempo decorrido, os dados pessoais tratados perderam sua funcionalidade e utilidade para a qual foram coletados. ";615514": "É imprescindível que, primeiramente, a declaração esteja acompanhada de documentos que validem a identidade do titular e legitimidade dele em relação ao direito pleiteado. Importante também destacar que, a declaração não poderá ser suficiente quando dependente de confirmação de uma terceira parte ou documentação correlatada. Vale indicar que, existindo procedimentos específicos para verificação da declaração, previstos em lei ou estabelecidos setorialmente, como por exemplo alteração de dados do cadastro de inadimplentes, a ANPD entende imprescindível que os mesmos sejam observados anteriormente à eventual atendimento ao pleito do titular de dados, sob o risco de gerar insegurança jurídica e financeira para a toda a sociedade. ";615513": "A análise para verificar se o atendimento à solicitação do titular demanda esforço desproporcional deve ser realizada

com base na solicitação em concreto, considerando os custos para atendimento da solicitação e sua viabilidade. Nesse sentido, é necessário que o agente de tratamento considere: (I) o volume de dados pessoais tratados; (II) a temporalidade do tratamento, isto é, se os dados pessoais coletados permanecem objeto de tratamento e/ou estão armazenados pelo agente; (III) a possibilidade de dar efetividade à solicitação; e (IV) as especificidades setoriais da área econômica em que o agente de tratamento está inserido, por exemplo, se estão sendo solicitados dados e/ou informações que não poderão ser compartilhadas. O ICO, por sua vez, elenca potenciais critérios objetivos que podem lançar luz no processo de avaliação individual da impossibilidade ou do esforço desproporcional na concretização do direito de correção dos dados. Para tanto, de acordo com a autoridade, deve-se avaliar, como por exemplo: (I) a natureza da informação e dos dados pessoais objeto da solicitação; (II) o contexto da solicitação e eventuais circunstâncias existentes na relação entre titular e controlador capazes de interferir; (III) se o controlador possui recursos disponíveis para atender à solicitação. "615512": "De maneira geral, os direitos dos titulares devem ser analisados à luz da situação concreta, não devendo ser, de antemão, considerados absolutos. Dessa forma, as liberdades e direitos individuais do titular devem ser balizadas com demais valores defendidos pelo ordenamento jurídico, em especial, caso esteja em colisão com o interesse público ou com direitos fundamentais de terceiros. Exemplificativamente, nas hipóteses em que a concretização do direito de correção puder implicar em fraude, ao prejuízo do cumprimento de obrigações legais, judiciais ou regulatórias, é possível que a solicitação de atualização não seja prontamente atendida pelo agente de tratamento. Ou, ainda, como citado supra, em hipóteses cuja concretização da solicitação demande esforço desproporcional ou se demonstre materialmente inviável de ser atendida, a exemplo de dados oriundos de órgãos institucionais, como Bacen e o CCF (Relatório de Cheques sem Fundos). Ademais, o ICO entende que o direito à correção poderá ser limitado caso a solicitação tenha como objetivo: (I) obstruir ou confundir uma investigação ou procedimento judicial; e (II) para a proteção de direitos e liberdades individuais de terceiros. Dessa forma, faz-se necessário que as solicitações de titulares sejam analisadas individualmente e considerando as especificidades e finalidades do tratamento, bem como às demais obrigações legais e/ou regulatórias do controlador. "615517": "No que diz respeito ao direito de anonimização e eliminação, especialmente, será necessário a condução de processo de avaliação do uso dos dados pessoais para verificar se a concretização do direito é possível à luz das operações realizadas pelos agentes de tratamento, uma vez que o atendimento à solicitação dos titulares poderá ter como efeito a interrupção definitiva da atividade de tratamento realizada pelo controlador. A esse respeito, é desejável que os titulares fundamentem suas solicitações indicando as razões pelas quais acreditam que: (I) existem irregularidades e/ou violações concretas ou aparentes à LGPD que ensejem o bloqueio do tratamento dos dados fornecidos pelo titular, a partir de evidências ou suspeitas razoáveis; e (II) as razões pelas quais os titulares consideram que seus dados pessoais coletados para finalidades específicas estão sendo objeto de tratamentos excessivos, ou que se demonstram desnecessários para que seja atingida a finalidade pretendida pelo controlador. Assim, a mera solicitação de bloqueio ou exclusão de dados pode não ser suficiente para assegurar a concretização do direito e efetiva ação do controlador, caso não sejam verificadas irregularidades ou razões de fato e/ou de direito para ensejar a tomada de medidas pelos agentes de tratamento. "615516": "A escolha da medida técnica a ser adotada deverá ser avaliada em face da solicitação do titular. Caso o titular solicite apenas a interrupção da atividade de tratamento e, diante do caso concreto aplicável, o controlador tenha a obrigação legal de interrompê-lo, deverá ser facultado ao controlador a

adoção de qualquer uma das medidas. Caso o controlador necessite utilizar dos dados para finalidades estatísticas ou para o desenvolvimento de índices ou métricas operacionais, os dados pessoais poderão ser submetidos ao processo de anonimização. Todavia, esvaída a necessidade de retenção dos dados pessoais anonimizados para o controlador, ou caso o armazenamento não seja necessário para o cumprimento de obrigações legais ou regulatórias, ou para as demais hipóteses previstas no art. 16 da LGPD, recomenda-se pela eliminação total dos dados pessoais nas bases de dados dos agentes de tratamento. Em síntese, a anonimização e a eliminação poderão ser adotadas alternativamente, a depender da solicitação específica do titular e das condições da situação concreta em questão. No entanto, a eliminação não é viável quando o controlador tenha o dever de manter respectivos dados para fins judiciais e regulatórios. ","615518": "O efeito inicial deverá ser a interrupção imediata da atividade de tratamento em questão, em razão da ausência de base legal aplicável legítima para fundamentar a operação. Em sequência, caberá ao controlador avaliar a atividade de tratamento contestada, a fim de verificar a possibilidade de aplicação de uma base legal alternativa prevista pela LGPD, como o armazenamento para fins de auditoria e cumprimento de obrigações legais ou regulatórias (art. 7º, II, LGPD) e para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI, LGPD). Caso não seja possível a fundamentação a partir de uma nova base legal, o controlador deverá optar pela anonimização ou pela eliminação física dos dados pessoais. Em caso de fato superveniente ou legislação nova, a ANBC entende ser necessário o estabelecimento de prazo razoável para atendimento. ","615523": "Não, a revogação do consentimento não implica em exclusão dos dados pessoais tratados em decorrência do consentimento, mas tão somente na paralização do tratamento realizado pelo controlador para a finalidade expressamente consentida – ratificados os tratamentos realizados sob amparo do consentimento anteriormente consentido enquanto não houver requerimento de eliminação - nos termos do inciso VI do caput do art. 18 desta Lei. Em sequência, caberá ao controlador avaliar a aplicação de base legal posterior, prevista pela LGPD, como o armazenamento para fins de auditoria e cumprimento de obrigações legais ou regulatórias (art. 7º, II, LGPD), por exemplo. ","615521": "O efeito do requerimento de eliminação só será existente quando assim estiver sido estabelecido entre partes. Caso o controlador tenha outra base legal para a manutenção do dado, como para cumprimento de obrigações legais, auditoria ou exercício regular de direito, o requerimento em questão limitará o uso do dado apenas para cumprimento das novas bases legais atribuídas. ","615617": "Uma decisão automatizada tem interferência humana. Já uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais não haverá interferência humana no ato da tomada de decisão. ","615618": "A correção de informação equivocada pode ou não alterar o resultado final. Nesse sentido, entendemos que restringir a isso estaria expondo os bureaus. Sugiro que coloquemos o mesmo racional do incidente - já estabelecido pela ANPD: (i) o indivíduo é impossibilitado - ilegalmente - de exercer regularmente seus direitos previstos pelo ordenamento jurídico de modo prolongado, causando efeitos negativos que comprometam o exercício de direitos fundamentais; (ii) o indivíduo é - ilegalmente - prejudicado em seu acesso a serviços, por exemplo, relacionado a educação, saúde, transporte etc.; (iii) o indivíduo sofre com situações ilícitas, com impactos graves ou prejudiciais, como em caso de discriminação ilícita ou abusiva. ","615619": "A ANBC entende que o maior desafio na revisão de decisões é realizar a atividade de modo a preservar o segredo de negócio e, conseqüentemente, gerar segurança jurídica a todo mercado. ","615620": "O direito de revisão deve ser avaliado a partir da situação concreta, identificando (I) se aplicável,

viável e possível; (II) quando advindo de solicitações recorrentes do mesmo titular de dados sem que outros direitos, como por exemplo correção, sejam também exercidos. "

{ "615450": "Consideramos razoável para o setor privado a adoção de prazos similares aos previstos na Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação. Esses prazos estabelecem um equilíbrio entre o direito do titular de dados pessoais de ter acesso às suas informações e a capacidade operacional das organizações para atender a tais solicitações. Os prazos estabelecidos na referida lei, de vinte dias para resposta inicial e possibilidade de extensão por mais dez dias mediante justificativa, fornecem um padrão claro e consistente para o processamento de solicitações de dados pessoais. No entanto, é importante destacar que, em alguns casos, o atendimento dentro desses prazos pode se tornar inviável devido à complexidade do pedido ou à multiplicidade de solicitações recebidas pela organização. Nesses casos, seria razoável permitir a extensão do prazo de resposta, desde que devidamente justificada e em conformidade com critérios objetivos, como os adotados pela Regulamentação Geral de Proteção de Dados (GDPR). Esses critérios poderiam incluir a complexidade técnica da solicitação, o volume de dados a serem processados e a necessidade de cooperação com terceiros para garantir a precisão e integridade das informações fornecidas ao titular dos dados. Portanto, sugerimos que os prazos estabelecidos para o atendimento aos direitos do titular de dados pessoais sejam alinhados com os da Lei nº 12.527/2011, com a possibilidade de extensão por critérios justificados e em conformidade com as melhores práticas internacionais de proteção de dados, nos moldes dos estabelecidos pela GDPR. Isso garantirá um equilíbrio adequado entre os direitos dos titulares de dados e as responsabilidades das organizações no tratamento dessas informações. ",b.

Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Na definição de prazos para o atendimento aos direitos do titular de dados pessoais, sugerimos que os seguintes critérios sejam levados em consideração para dispor de forma diferenciada, conforme previsto nos incisos I e II do caput do art. 19 da LGPD: 1. Complexidade do Pedido: Deve-se considerar a complexidade técnica da solicitação, como a dificuldade em recuperar informações devido a problemas técnicos, a necessidade de aplicar exceções que envolvam grandes volumes de dados sensíveis ou a exigência de trabalhos especializados para obter ou comunicar as informações de forma compreensível. 2. Multiplicidade de Pedidos: O número de solicitações recebidas pela organização deve ser levado em conta, especialmente se houver um grande volume delas simultaneamente. No entanto, é importante ressaltar que a mera quantidade de solicitações não deve ser considerada como critério único para caracterizar a complexidade do pedido. 3. Direitos do Titular: Aspectos relacionados à proteção dos direitos do titular de dados devem ser considerados, como a necessidade de esclarecer questões sobre a divulgação de informações de uma criança a um responsável legal ou a proteção da confidencialidade de informações médicas sensíveis ao compartilhá-las com terceiros autorizados. É importante observar as diretrizes estabelecidas por autoridades de proteção de dados, como o Information Commissioner's Office (ICO) do Reino Unido, que identificou elementos-chave para caracterizar solicitações complexas. Por exemplo, dificuldades técnicas na recuperação de informações, aplicação de exceções que envolvam grandes volumes de dados sensíveis e a necessidade de obter orientação legal especializada. Por outro lado, é necessário reconhecer que certos elementos, como o volume total de dados envolvidos ou a recuperação de dados de múltiplos sistemas, podem não, por si só, justificar a caracterização de um pedido como complexo. No entanto, esses fatores podem ser considerados como agravantes em casos complexos. Sugerimos que os critérios acima mencionados sejam

utilizados de forma ponderada e flexível.";"615484": "Para garantir a efetividade na comunicação entre o titular de dados e o agente de tratamento, é essencial que o canal de atendimento apresente as seguintes características: 1. Transparência: O canal de atendimento deve fornecer informações claras e transparentes sobre o processo de tratamento de dados pessoais, incluindo os propósitos do tratamento, as categorias de dados coletados, os direitos do titular e como exercê-los, além de quaisquer transferências de dados para terceiros, quando aplicável. 2. Linguagem Simplificada: As informações fornecidas pelo canal de atendimento devem ser apresentadas em linguagem clara e acessível, evitando jargões técnicos ou jurídicos que possam dificultar a compreensão por parte do titular de dados. O uso de linguagem simplificada contribui para uma comunicação eficaz e para o empoderamento do titular em relação aos seus direitos de privacidade. 3. Disponibilidade Constante: O canal de atendimento deve estar disponível de forma constante para que os titulares de dados possam contatar o agente de tratamento e exercer seus direitos conforme necessário. Isso pode incluir a disponibilidade de serviços de atendimento ao cliente por telefone, e-mail, chat online ou outros meios de comunicação, garantindo que os titulares possam entrar em contato quando necessário. Além disso, algumas informações específicas devem ser disponibilizadas de forma clara e acessível no canal de atendimento, incluindo: • Prazo: Informações sobre os prazos para resposta às solicitações dos titulares de dados, conforme estabelecido pela legislação aplicável ou pelas políticas internas da organização. • Política de Privacidade: A política de privacidade da organização, que deve descrever como os dados pessoais são coletados, usados, compartilhados e protegidos pela empresa. • Padrões de Segurança: Informações sobre os padrões de segurança adotados pela organização para garantir a privacidade e proteção dos dados pessoais dos titulares. ";"615485": "Sim, os operadores têm responsabilidades na concretização dos direitos dos titulares de dados, porém essa responsabilidade está limitada ao escopo de suas atividades específicas. Conforme estabelecido no artigo 39 da LGPD, os operadores devem cooperar com os controladores para o atendimento aos direitos dos titulares de dados, desempenhando seu papel operacional de maneira adequada de acordo com as instruções fornecidas pelo controlador. A responsabilidade dos operadores está relacionada principalmente à execução das atividades de tratamento de dados pessoais em conformidade com as instruções do controlador. Isso inclui garantir a segurança dos dados, adotar medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados e garantir a disponibilidade, integridade e confidencialidade dos dados. Além disso, os operadores devem cooperar com os controladores no atendimento aos direitos dos titulares de dados, fornecendo as informações e assistência necessárias para garantir o exercício desses direitos. Isso pode incluir a prestação de suporte técnico para responder a solicitações de acesso, retificação, exclusão ou portabilidade de dados, conforme exigido pela LGPD. No entanto, a responsabilidade efetiva dos operadores está condicionada ao cumprimento de suas obrigações operacionais específicas e à observância das instruções e diretrizes fornecidas pelos controladores. Em caso de não atendimento a essas obrigações, os operadores podem ser responsabilizados nos termos da LGPD e sujeitos às sanções previstas na legislação. Portanto, os operadores devem cooperar ativamente com os controladores para garantir o cumprimento dos direitos dos titulares de dados, desempenhando seu papel operacional de maneira diligente e em conformidade com as disposições da LGPD. ";"615486": "A adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor (SAC), estabelecidos pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais, poderia não ser viável por algumas razões: 1. Aplicabilidade Limitada: As disposições do Decreto nº

11.034 se aplicam apenas aos serviços regulados pelo Poder Executivo federal, como serviços de fornecimento de água, energia elétrica, entre outros. Portanto, estender essas diretrizes para a regulamentação da LGPD poderia criar um ônus adicional para empresas não reguladas pelo governo federal, especialmente as de pequeno porte, o que poderia ser desproporcional e oneroso. 2. Restrições Excessivas: Algumas diretrizes do Decreto nº 11.034, como a obrigatoriedade de disponibilidade ininterrupta do atendimento durante 24 horas por dia, sete dias por semana, e o tempo máximo de espera para atendimento telefônico, poderiam impor exigências muito rigorosas para empresas menores, tornando o cumprimento dessas regras impraticável ou financeiramente inviável. 3. Diferenças de Natureza: Os serviços regulados pelo SAC têm características específicas que podem não se aplicar ao tratamento de dados pessoais sob a LGPD. Enquanto o SAC lida com questões como cancelamento de contratos e reclamações sobre serviços, a LGPD trata da proteção dos dados pessoais dos titulares, exigindo abordagens e procedimentos distintos para atender aos direitos dos titulares de dados. Portanto, seria recomendável que, em vez de adotar diretamente as diretrizes do SAC para a regulamentação da LGPD, fosse prevista em regulamento a criação de um canal de atendimento específico para o exercício dos direitos dos titulares de dados, adaptado às necessidades e características do tratamento de dados pessoais realizado pelo agente de tratamento. Isso garantiria uma abordagem mais equilibrada e proporcional, levando em consideração as peculiaridades e demandas das empresas sujeitas à LGPD, especialmente as de menor porte. ";615487": "Um modelo de atendimento adotado por agentes privados que poderia servir como paradigma para o exercício dos direitos dos titulares de dados, considerando a capacidade de lidar com grandes volumes de demandas com economicidade, é o portal de privacidade implementado pela empresa Samsung no Brasil. O portal de privacidade da Samsung Brasil oferece um exemplo notável de como uma empresa pode gerenciar o exercício dos direitos dos titulares de dados de maneira eficiente e econômica. Alguns pontos que destacam a eficácia desse modelo são: 1. Transparência e Informação Adequada: A empresa apresenta de maneira clara e didática os parâmetros que orientam suas práticas de tratamento de dados, fornecendo informações detalhadas sobre como os dados são coletados, usados e protegidos. 2. Centralização e Acessibilidade: O portal oferece um ponto centralizado onde os titulares de dados podem exercer seus direitos de privacidade em diversas plataformas da empresa. Isso facilita o acesso dos titulares aos seus dados e simplifica o processo de exercício de direitos, promovendo uma experiência positiva para o usuário. 3. Política de Privacidade Transparente: A empresa disponibiliza sua política de privacidade de forma acessível e compreensível, permitindo que os titulares de dados entendam claramente seus direitos e como podem exercê-los. 4. Eficiência e Economia: Ao centralizar o exercício dos direitos dos titulares de dados em um portal único e integrado, a Samsung Brasil demonstra uma abordagem eficiente e econômica para lidar com grandes volumes de demandas, reduzindo custos operacionais e simplificando o processo tanto para os titulares quanto para a empresa. Portanto, o modelo de atendimento adotado pela Samsung Brasil por meio de seu portal de privacidade oferece um exemplo inspirador de como os agentes privados podem gerenciar o exercício dos direitos dos titulares de dados de forma eficiente, transparente e econômica. Essa abordagem pode servir como um paradigma para outras empresas que buscam implementar práticas de privacidade robustas e centradas no usuário. ";615491": "Sim, há hipóteses excepcionais em que o direito de confirmação da existência do tratamento pode ser negado. Uma dessas hipóteses é quando o pretendo titular de dados não é capaz de comprovar sua identidade. Nesse caso, o agente de tratamento pode justificar a negação da solicitação para resguardar a proteção dos dados pessoais que

possui em sua posse. Além disso, ao analisar legislações estrangeiras, como o regramento adotado pelo Reino Unido, identificamos duas situações em que a negação do direito de confirmação pode ser aplicada: 1. Manifestamente infundada: Uma solicitação pode ser considerada manifestamente infundada se o indivíduo claramente não tiver a intenção de exercer seu direito de acesso aos dados. Por exemplo, se o indivíduo fizer uma solicitação e depois oferecer para retirá-la em troca de algum benefício da organização, ou se a solicitação for maliciosa e utilizada para assediar a organização sem um propósito real além de causar perturbação. 2. Manifestamente excessiva: Uma solicitação pode ser considerada manifestamente excessiva se for claramente ou obviamente irrazoável, levando em consideração o equilíbrio entre a solicitação e o ônus ou custos envolvidos em lidar com ela. Isso pode incluir solicitações que sejam desproporcionalmente volumosas ou que sejam repetitivas em curtos períodos de tempo. Portanto, sugere-se que a negação do direito de confirmação da existência do tratamento pode ocorrer em casos em que a identidade do solicitante não possa ser comprovada ou quando a solicitação é considerada manifestamente infundada ou excessiva, de acordo com as disposições da legislação aplicável.

;"615492": "Partindo das informações referentes à experiência internacional, é crucial garantir que os titulares de dados tenham acesso às informações necessárias para identificar os controladores de seus dados, inclusive em casos de compartilhamento de dados pessoais. De acordo com as diretrizes do European Data Protection Board (EDPB) sobre o Regulamento Geral de Proteção de Dados (GDPR), os controladores devem fornecer aos titulares acesso às informações específicas sobre os destinatários de seus dados pessoais, quando possível. Aqui estão os principais pontos a serem considerados ao fornecer essas informações aos titulares: 1. Obrigação de acesso: O artigo 15 do GDPR estabelece o direito do titular de acessar suas informações pessoais e, portanto, os controladores devem garantir que os titulares tenham acesso às informações sobre os destinatários de seus dados. 2. Nomeação de destinatários específicos: A menos que o titular solicite de outra forma, o controlador deve fornecer os nomes específicos dos destinatários aos quais os dados foram ou serão divulgados, desde que seja possível identificá-los. 3. Categorias de destinatários: Se não for possível identificar os destinatários específicos, o controlador pode fornecer informações sobre as categorias de destinatários de forma tão específica quanto possível. Isso pode incluir o tipo de destinatário, setor, sub-setor e localização dos destinatários. 4. Transparência e justiça: É fundamental que as informações fornecidas aos titulares sejam transparentes e justas, conforme os princípios do GDPR. As informações sobre destinatários ou categorias de destinatários devem ser claras e compreensíveis para os titulares. 5. Exemplo prático: O EDPB fornece um exemplo prático de como essa informação pode ser apresentada na política de privacidade, indicando as categorias de destinatários, como "agências de viagens" ou "hotéis", e, em seguida, fornecendo os nomes específicos dessas empresas quando solicitado pelo titular.";"615489": "De acordo com o art. 39 da LGPD, o operador é obrigado a realizar as operações de tratamento conforme as instruções do controlador. Assim, a responsabilização do operador surge apenas quando ele desobedece as orientações do controlador. Nesse sentido, são aplicáveis os preceitos contidos no art. 42, §1º, I, da LGPD, considerando o operador como controlador para fins daquela operação, caso esteja agindo de forma independente em relação às instruções do controlador. Além disso, ao analisarmos a experiência internacional, o Guideline nº 1/2022 do European Data Protection Board, os dados que serão objeto da solicitação do titular de dados devem ser abrangidos pelas informações em posse dos operadores de dados. Portanto, é responsabilidade do operador cooperar com o controlador para o atendimento dessas solicitações, garantindo assim a transparência e o exercício efetivo dos direitos dos

titulares. Dessa forma, é fundamental que os operadores atuem em conformidade com as diretrizes estabelecidas pelo controlador e cooperem plenamente no fornecimento de informações solicitadas pelos titulares de dados, contribuindo para o cumprimento das disposições legais e para a proteção dos direitos dos indivíduos, sob pena de ter de arcar com possíveis responsabilizações em caso de descumprimento. ";615490": "No formato simplificado previsto no art. 19, inciso I, da LGPD, deveriam constar as seguintes informações mínimas sobre o tratamento de dados pessoais: 1. Confirmação da existência de tratamento: Deveria ser indicado de forma binária (sim ou não) se o controlador realiza o tratamento dos dados pessoais do titular. Essa confirmação é essencial para atender ao direito previsto no art. 18, inciso I, da LGPD, que garante ao titular o direito de obter do controlador a confirmação da existência de tratamento de seus dados pessoais. Essa indicação em formato binário permitiria ao titular dos dados ter uma compreensão clara e rápida sobre se seus dados estão sendo tratados pelo controlador, facilitando o exercício de seus direitos de proteção de dados. Além disso, essa informação poderia ser facilmente automatizada para garantir um atendimento imediato à solicitação do titular. ";615494": "Conforme estabelecido no Art. 9º da LGPD, o controlador tem o dever de fornecer as seguintes informações de forma clara, adequada e ostensiva para o atendimento do princípio do livre acesso dos titulares: • Finalidade específica do tratamento; • Forma e duração do tratamento, respeitando os segredos comerciais e industriais; • Identificação do controlador; • Informações de contato do controlador; • Informações sobre o uso compartilhado de dados pelo controlador e sua finalidade; • Responsabilidades dos agentes que realizarão o tratamento; • Direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD. No que se refere às informações sobre as operações que implementam decisões automatizadas, é relevante analisar a experiência internacional. O EDPB, em sua guideline 2016/679, estabelece a necessidade de explicação clara e simplificada do processo de profiling ou tomada de decisões automatizadas, conforme o princípio da transparência subjacente ao GDPR. Este mesmo princípio encontra-se presente na LGPD, em seu artigo 6, VI, que também exige a observância dos segredos comerciais e industriais, sendo este princípio aplicável igualmente às decisões automatizadas. ";615493": "De acordo com a orientação do European Data Protection Board (EDPB), expressa em sua guideline 1/2022, caso o titular não esteja plenamente satisfeito com as informações fornecidas pelo agente de tratamento, ele tem o direito de solicitar mais informações sem que isso caracterize uma nova requisição de dados. Esse entendimento é respaldado pelo EDPB ao afirmar que se o titular repetir um pedido de acesso inicial alegando que a resposta recebida não foi completa ou que não foram fornecidas razões para a recusa, esse pedido não deve ser considerado como uma nova solicitação, mas sim como um lembrete de uma primeira solicitação insatisfeita. Portanto, é crucial considerar que a requisição de acesso somente pode ser considerada como satisfatoriamente atendida quando o titular de dados demonstrar de forma conclusiva estar de acordo com o resultado de sua solicitação, seja através do transcurso do tempo, seja por manifestação expressa nesse sentido. Para garantir o pleno exercício do direito de acesso, é essencial que o agente de tratamento esteja preparado para fornecer informações adicionais ou esclarecimentos necessários, caso o titular não esteja totalmente satisfeito com as informações inicialmente disponibilizadas, conforme preconizado pelas diretrizes do EDPB. Além disso, é importante que a Autoridade Nacional de Proteção de Dados (ANPD) inclua a previsão da possibilidade de prorrogação do prazo de 15 dias previsto na LGPD em caso de pedido de acréscimo de informações por parte do titular. Ademais, o atendimento ao pedido deve ser em formato digital ou em papel alternativamente e não cumulativamente. ";615502": "No contexto da implementação do direito à

portabilidade dos dados, há setores que demonstram maior maturidade nos processos de negócio e tecnologia, possibilitando uma adoção mais imediata desse serviço a pedido do titular. Entre esses setores, destaca-se o setor bancário, que se encontra em um estágio avançado de implementação de sistemas de portabilidade de dados. Especificamente, desde 25 de outubro de 2021, entrou em vigor o "Sistema Financeiro Aberto" ou "Open Banking", uma iniciativa regulamentada pela Resolução Conjunta n.º 1 de 2020 do Banco Central do Brasil (Bacen). Esse sistema foi concebido como parte de uma série de medidas do Bacen para transformar o sistema financeiro em um ecossistema mais integrado. Nesse contexto, as bases de dados são padronizadas e tornadas interoperáveis, facilitando a livre circulação de dados entre diferentes agentes de tratamento. O setor bancário, portanto, pode servir como um paradigma para análise e teste para uma futura regulamentação do direito à portabilidade de dados pela ANPD. A experiência adquirida com o Open Banking pode oferecer valiosas lições sobre os desafios e oportunidades associados à implementação da portabilidade de dados em outros setores da economia. Além disso, a padronização e interoperabilidade estabelecidas no contexto do Open Banking podem servir como referência para o desenvolvimento de diretrizes e padrões para a portabilidade de dados em outros setores. Adicionalmente, a ANPD pode utilizar o setor de telecomunicação como paradigma de análise para o exercício do direito de portabilidade, uma vez que este setor já possui a previsão da portabilidade do código de telefone, conforme disposto na Resolução nº 460 de 19 de março de 2007 da Agência Nacional de Telecomunicações (Anatel), visando esta possibilidade a "facilidade de rede que possibilita ao usuário de serviço de telecomunicações manter o Código de Acesso a ele designado, independentemente de prestadora de serviço de telecomunicações ou de área de prestação do serviço".

615501: "Implementar um padrão de interoperabilidade para facilitar a portabilidade de dados enfrenta diversos desafios tecnológicos que precisam ser cuidadosamente considerados e endereçados. Alguns dos principais desafios incluem:

1. Interoperabilidade de sistemas: Um dos maiores desafios reside na interoperabilidade entre sistemas. Diferentes sistemas frequentemente utilizam formatos e linguagens de dados distintos, o que pode dificultar a comunicação entre eles. A falta de padronização pode tornar o processo de troca de dados entre diferentes agentes de tratamento complexo e dissonante.
2. Segurança da comunicação de dados: A transferência de dados entre sistemas representa um ponto crítico em termos de segurança. Dados em trânsito são suscetíveis a vulnerabilidades e ataques, o que pode resultar em violações de dados pessoais. Portanto, é essencial implementar medidas robustas de segurança para proteger a integridade e confidencialidade dos dados durante o processo de portabilidade.
3. Proteção de segredos comerciais: A portabilidade de dados pode envolver a transferência de informações sensíveis e estratégicas das organizações. A divulgação inadvertida de segredos comerciais durante o processo de portabilidade pode comprometer a vantagem competitiva das empresas. É necessário estabelecer mecanismos adequados para proteger os segredos comerciais durante a transferência de dados entre agentes de tratamento.
4. Delimitação dos dados elegíveis para portabilidade: Outro desafio importante é definir quais tipos de dados podem ser objeto de portabilidade. Alguns dados pessoais podem passar por processos de tratamento ou anonimização que dificultam sua transmissão ou rastreamento. Além disso, dados utilizados para o treinamento de sistemas de inteligência artificial podem apresentar desafios adicionais, uma vez que podem conter informações sensíveis e não estruturadas.

615505: "Para garantir a interoperabilidade e facilitar a portabilidade de dados, diversos aspectos devem ser objeto de padronização. Com base nos princípios estabelecidos pelo poder executivo federal e em outras fontes de referência, destacam-se os seguintes elementos: 1.

Intercâmbio coerente de informações e serviços entre sistemas: A interoperabilidade deve permitir o intercâmbio consistente de informações e serviços entre sistemas, possibilitando a substituição de componentes ou produtos sem comprometer as funcionalidades do sistema. Isso implica em padronizar formatos de dados e protocolos de comunicação para garantir a compatibilidade entre sistemas heterogêneos.

2. Transferência uniforme e eficiente de informações: A padronização deve garantir a capacidade de transferir e utilizar informações de maneira uniforme e eficiente entre diversas organizações e sistemas de informação. Isso requer a definição de formatos de arquivos de dados portáteis e a adoção de padrões de codificação e compressão que permitam a troca de informações de forma eficaz.

3. Interação e intercâmbio de dados entre sistemas: A interoperabilidade deve possibilitar a interação e o intercâmbio de dados entre dois ou mais sistemas de acordo com métodos definidos, garantindo que os resultados esperados sejam alcançados. Isso envolve o estabelecimento de protocolos de comunicação e APIs (Interfaces de Programação de Aplicações) que permitam a integração e interação entre sistemas distintos.

4. Compatibilidade entre componentes de sistemas diferentes: A interoperabilidade deve assegurar que dois ou mais componentes de um sistema, desenvolvidos por fornecedores diferentes e utilizando ferramentas distintas, possam atuar em conjunto. Isso requer a definição de padrões e protocolos de comunicação que permitam a integração de sistemas heterogêneos de forma transparente. Também é necessário definir princípios e regras de governança para orientar as relações entre os diferentes agentes envolvidos na portabilidade de dados, garantindo transparência, segurança e responsabilidade no uso e compartilhamento.

615503: "Consideramos que, de acordo com a legislação vigente, a disponibilização dos dados pessoais em formato interoperável representa um passo fundamental para o exercício do direito à portabilidade. Ao fornecer todos os dados de forma estruturada e compatível com sistemas de outros agentes de tratamento, o titular pode exercer um maior controle sobre suas informações e buscar novas oportunidades de utilização dos dados. No entanto, é essencial que o agente de tratamento forneça meios adequados para que o titular possa acessar, visualizar, transferir e, se necessário, retificar ou excluir os dados conforme sua vontade. Nesse sentido, a documentação comprovando o recebimento e a possibilidade de manuseio e uso dos dados pessoais pelo titular é um elemento importante para concluir o pedido de portabilidade de forma satisfatória. Essa documentação pode incluir informações sobre o formato dos dados, instruções de uso e quaisquer outras orientações relevantes para garantir que o titular possa exercer seus direitos de forma eficaz. Portanto, para considerar satisfeito o direito à portabilidade, é necessário não apenas que os dados sejam disponibilizados em formato interoperável, mas também que o titular tenha a capacidade de manusear e utilizar os dados de forma significativa, com o suporte necessário do agente de tratamento, devendo igualmente esta possibilidade ser documentável.

615504: "Analisando a experiência do open banking conduzido pelo Banco Central do Brasil (Bacen), observamos que a Resolução Conjunta n.º 1 estabelece obrigações para as instituições participantes em relação à interoperabilidade, sem definir padrões específicos. Em vez disso, a resolução exige que as instituições estabeleçam interfaces padronizadas, permitindo uma maior flexibilidade na implementação de soluções de interoperabilidade. Nesse sentido, a ANPD poderia adotar uma abordagem semelhante, permitindo que o setor privado defina padrões específicos de interoperabilidade, desde que essas estruturas sejam passíveis de fiscalização e estejam em conformidade com os princípios e diretrizes estabelecidos pela LGPD. Isso proporcionaria às empresas a flexibilidade necessária para desenvolver soluções adaptadas às especificidades de cada setor econômico, ao mesmo tempo em que garantiria a proteção dos dados pessoais dos titulares. Quanto ao

prazo para a implementação desses padrões de interoperabilidade, é razoável adotar um período semelhante ao estabelecido para o open banking. Dessa forma, sugerimos que a ANPD considere um prazo de dezoito meses a partir do recebimento da proposta de ecossistema de interoperabilidade de dados. Esse prazo permitiria às empresas tempo suficiente para desenvolver e implementar as soluções necessárias, garantindo uma transição suave e eficaz para um ambiente de portabilidade de dados interoperável.

","615511": "Para qualificar um dado como incompleto, inexato ou desatualizado, é importante estabelecer critérios objetivos que permitam identificar e avaliar essas características de forma clara e transparente. Considerando as diretrizes estabelecidas pelo Comitê de Supervisão Coordenada e outras boas práticas em proteção de dados, podemos definir os seguintes critérios: 1. Incompletude dos dados: Os dados devem ser considerados incompletos quando não contiverem todas as informações relevantes ou necessárias para a finalidade específica do tratamento. Isso pode incluir a ausência de campos obrigatórios, informações parciais ou dados que não abrangem completamente a situação ou contexto do titular. 2. Inexatidão dos dados: Os dados devem ser considerados inexatos quando contiverem informações imprecisas, incorretas ou falsas. Isso pode ocorrer devido a erros de digitação, atualização inadequada ou falta de verificação da precisão das informações. 3. Desatualização dos dados: Os dados devem ser considerados desatualizados quando não refletirem mais a realidade ou estiverem obsoletos em relação à finalidade do tratamento. Isso pode ocorrer devido a mudanças nas circunstâncias do titular, expiração da validade das informações ou falta de atualização periódica dos dados. É importante ressaltar que a qualificação de um dado como incompleto, inexato ou desatualizado deve levar em consideração a perspectiva do titular dos dados. O titular deve ter o direito de contestar e questionar a precisão e atualidade dos seus dados pessoais, desde que possa fornecer evidências documentais que fundamentem suas alegações.

","615514": "Existem situações em que a simples declaração do titular não seria suficiente para o exercício do direito à correção de seus dados pessoais. É essencial considerar os princípios de proporcionalidade e boa-fé, bem como garantir que o exercício desse direito não seja abusivo ou prejudicial para as partes envolvidas. Com base no guideline publicado pelo Information Commissioner's Office (ICO) do Reino Unido e nas disposições do art. 16 da UK GDPR (General Data Protection Regulation), que estabelece o direito à retificação de dados pessoais, podemos identificar algumas situações em que a simples declaração do titular pode não ser suficiente: 1. Justificativa plausível do agente de tratamento: Caso o agente de tratamento considere que os dados estão corretos e possua uma justificativa plausível para esse entendimento, ele deve comunicar isso ao titular. Essa justificativa pode se basear em evidências objetivas que demonstrem a precisão dos dados conforme estão sendo tratados. 2. Pedidos manifestamente infundados ou excessivos: Os pedidos de correção podem ser recusados se forem considerados manifestamente infundados ou excessivos. Isso inclui situações em que o titular não tem a intenção genuína de exercer seu direito à retificação ou quando o pedido se sobrepõe a outros já realizados. 3. Intenção maliciosa ou abusiva: Se o pedido de correção for utilizado de forma maliciosa, abusiva ou com a intenção de causar prejuízos à organização, o agente de tratamento pode se recusar a atender ao pedido. Isso inclui situações em que o pedido é utilizado para assediar a organização ou para obter vantagens indevidas. A ANPD pode adotar um entendimento similar ao ICO, estabelecendo critérios claros para a recusa de pedidos de correção que não atendam aos requisitos estabelecidos pela LGPD.

","615513": "Para avaliar a impossibilidade ou o esforço desproporcional no contexto do art. 18, § 6º, da LGPD, é necessário considerar critérios objetivos que permitam determinar quando um pedido de retificação, anonimização, bloqueio ou eliminação de

dados pode ser considerado excessivo ou manifestamente infundado. A fim de oferecer uma orientação clara sobre esses critérios, podemos nos basear nos exemplos fornecidos pelo Information Commissioner's Office (ICO) do Reino Unido e adaptá-los para o contexto da LGPD. Alguns critérios objetivos a serem considerados são:

1. **Intenção maliciosa ou assediadora:** Um pedido pode ser considerado manifestamente infundado se houver evidências de que o titular está agindo de forma maliciosa ou com a intenção de assediar a organização. Isso pode incluir casos em que o titular declara explicitamente sua intenção de causar perturbações ou faz acusações infundadas contra a organização ou seus funcionários.
2. **Benefícios oferecidos em troca:** Se o titular oferecer benefícios em troca da retirada do pedido de retificação, anonimização, bloqueio ou eliminação de dados, isso pode indicar que o pedido não é feito de forma genuína e pode ser considerado manifestamente infundado.
3. **Repetição excessiva ou sobreposição de pedidos:** Um pedido pode ser considerado excessivo se repetir o conteúdo de pedidos anteriores ou se estiver sobreposto a outras solicitações semelhantes. No entanto, é importante analisar cada caso individualmente para determinar se a repetição é justificada por motivos legítimos, como o tratamento inadequado de solicitações anteriores pelo controlador.
4. **Relação com informações completamente separadas:** Se um pedido estiver relacionado a um conjunto de informações completamente separado dos pedidos anteriores, ele não deve ser considerado excessivo, mesmo que aborde o mesmo assunto. Cada solicitação deve ser analisada considerando sua relevância e impacto específicos.

"615512": "Sim, existem situações excepcionais em que o direito de correção pode ser negado pelo controlador, desde que haja fundamentação legal e justificativa razoável para tal recusa. Ao analisar a experiência internacional, é possível usar como parâmetro as disposições do guideline publicado pelo Information Commissioner's Office (ICO) do Reino Unido, onde são evidenciados algumas dessas situações:

1. **Convicção de que os dados são precisos:** Se o controlador estiver convencido de que os dados pessoais contestados são precisos e verificados, ele pode informar ao titular que não irá alterar os dados. Nesse caso, o controlador deve explicar sua decisão e informar ao titular sobre seu direito de fazer uma reclamação à autoridade supervisora competente, como a ANPD, ou buscar recursos judiciais para fazer valer seus direitos.
2. **Aplicação de isenções legais:** O controlador pode recusar o pedido de retificação se aplicar uma isenção legal específica que justifique essa recusa, como quando o agente possui obrigação legal em manter o registro na forma como está apresentada em documento oficial, não podendo uma pessoa que utiliza nome social não alterado em sua documentação requisitar a correção de seus dados. As isenções variam de acordo com as disposições legais aplicáveis e devem ser examinadas cuidadosamente para determinar sua aplicabilidade a uma solicitação específica.
3. **Pedido manifestamente infundado ou excessivo:** O controlador pode recusar atender a uma solicitação de correção se considerar que o pedido é manifestamente infundado ou excessivo. Isso pode ocorrer quando o titular não tem a intenção genuína de exercer seu direito à correção ou quando o pedido é feito de forma abusiva, como parte de uma campanha para causar perturbações à organização. É importante ressaltar que a recusa em atender a um pedido de correção deve ser justificada de forma adequada e transparente, demonstrando ao titular as razões pelas quais o pedido foi considerado infundado, excessivo ou não aplicável. Além disso, o controlador deve informar ao titular sobre seus direitos de contestar a decisão.

"615517": "É fundamental considerar a necessidade de o titular fundamentar seu requerimento ao solicitar restrição de tratamento de dados pessoais, especialmente nos casos em que há contestação da exatidão dos dados, processamento ilegal, desnecessidade dos dados ou oposição ao tratamento. No entanto, ao analisar a experiência internacional, como o guideline

publicado pelo Information Commissioner's Office (ICO) do Reino Unido, observamos que existem situações em que a simples solicitação do titular pode ser suficiente, sem a necessidade de uma fundamentação explícita. Por exemplo, nos casos em que o titular contesta a exatidão de seus dados e o controlador está verificando a exatidão, ou quando os dados foram processados ilegalmente e o titular solicita a restrição, a simples solicitação do titular pode ser aceita sem a necessidade de uma fundamentação detalhada. No entanto, mesmo nessas situações, o controlador pode recusar o pedido se considerar que é manifestamente excessivo ou se houver outras razões válidas para a recusa. Nesse caso, o controlador deve informar ao titular os motivos pelos quais não está agindo, bem como seu direito de fazer uma reclamação à autoridade supervisora competente e sua capacidade de buscar recursos judiciais para fazer valer seus direitos. Portanto, embora a simples solicitação do titular possa ser suficiente em algumas situações, é importante que o controlador tenha a capacidade de avaliar a legitimidade do pedido e recusá-lo, se necessário, com base em critérios objetivos e razoáveis. Essa abordagem equilibra os direitos e interesses das partes envolvidas, garantindo a proteção adequada dos dados pessoais do titular e a conformidade com as disposições legais aplicáveis. Assim, um procedimento similar ao adotado pelo ICO do Reino Unido poderia ser considerado adequado no contexto da LGPD no Brasil.

","615516": "Sim, a anonimização e a eliminação podem ser adotadas alternativamente em situações específicas, desde que o agente de tratamento seja capaz de cumprir com o rigor técnico exigido para o processo de anonimização, conforme estabelecido pela LGPD (Lei Geral de Proteção de Dados). De acordo com as diretrizes fornecidas pela Autoridade Nacional de Proteção de Dados (ANPD) em sua consulta à sociedade sobre o Guia de Anonimização e Pseudonimização, o processo de anonimização de dados pessoais é considerado uma operação de tratamento de dados, sujeita a requisitos técnicos da LGPD. Isso inclui a necessidade de uma base legal para a coleta e tratamento dos dados para a finalidade de anonimização, transparência sobre o processo de coleta e tratamento, e o cumprimento de padrões técnicos e medidas de segurança para garantir que os dados sejam anonimizados de forma eficaz e irreversível. Portanto, se o agente de tratamento for capaz de realizar o processo de anonimização de acordo com os requisitos estabelecidos pela LGPD e garantir que os dados sejam efetivamente anonimizados, a anonimização pode ser uma alternativa viável à eliminação dos dados pessoais. No entanto, se o agente de tratamento não puder garantir o cumprimento adequado desses requisitos técnicos ou se a natureza dos dados pessoais não permitir uma anonimização eficaz, a eliminação dos dados deve ser realizada em conformidade com os princípios e disposições da LGPD. Portanto, a escolha entre anonimização e eliminação deve ser baseada na capacidade do agente de tratamento de garantir a conformidade com os requisitos legais e técnicos aplicáveis, bem como na natureza e sensibilidade dos dados pessoais envolvidos.

","615518": "O efeito da oposição prevista no art. 18, § 2º, da LGPD, quando a alegação do titular for considerada legítima, é crucial para garantir a proteção dos direitos e interesses do titular de dados. Nesse contexto, se o titular de dados alegar que o tratamento de seus dados pessoais está ocorrendo em desacordo com as disposições da LGPD e essa alegação for considerada legítima, o controlador deve agir prontamente para cessar o tratamento irregular e proteger os direitos do titular. Assim, os efeitos dessa oposição incluem:

1. Exclusão imediata dos dados pessoais: O controlador deve realizar a exclusão dos dados pessoais em questão, a fim de interromper qualquer situação lesiva aos interesses do titular. Isso implica a interrupção imediata do tratamento irregular e a remoção dos dados pessoais dos sistemas do controlador.
2. Instrução ao titular de seus direitos: O controlador deve informar ao titular sobre seu direito de fazer uma reclamação à Autoridade Nacional

de Proteção de Dados (ANPD) ou outra autoridade supervisora competente, bem como sobre a possibilidade de buscar a defesa de seus direitos por meio de ação judicial. Essas medidas são essenciais para garantir a conformidade com a LGPD e proteger os direitos fundamentais dos titulares de dados. Ao agir de acordo com a oposição legítima do titular, o controlador demonstra compromisso com a proteção dos dados pessoais e a conformidade com a legislação de proteção de dados vigente. ";615523": "Sim, a revogação do consentimento, conforme previsto no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base nesse consentimento. Essa obrigação está alinhada com as diretrizes internacionais, como as Diretrizes do European Data Protection Board (EDPB) sobre consentimento ao abrigo do Regulamento 2016/679 (GDPR). De acordo com essas diretrizes, os dados pessoais que foram coletados com base no consentimento do titular devem ser excluídos quando esse consentimento é retirado. Isso significa que o controlador tem a obrigação de eliminar os dados pessoais assim que o consentimento for revogado pelo titular. Além disso, caso o controlador deseje continuar o tratamento dos dados pessoais com base em outra justificativa legal após a revogação do consentimento, ele deve informar o titular sobre essa mudança e garantir que a nova base legal seja transparentemente comunicada ao titular. Isso está de acordo com o princípio da transparência, que é fundamental para garantir a proteção adequada dos direitos dos titulares de dados. Portanto, a revogação do consentimento implica na obrigação de eliminar os dados pessoais tratados com base nesse consentimento, a menos que exista outra base legal para o tratamento dos dados e que seja devidamente comunicada ao titular. ";615521": "Conforme o artigo 8º da LGPD, o requerimento de eliminação dos dados pessoais por parte do titular tem efeitos sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado. Nesse contexto, é importante considerar que a LGPD confere ao titular o direito de revogar o consentimento a qualquer momento, mediante manifestação expressa, conforme previsto no inciso IX do artigo 18. Entretanto, é fundamental que o agente de tratamento comunique ao titular a respeito da manutenção do consentimento mesmo após a solicitação de exclusão dos dados. Essa comunicação permite ao titular decidir se deseja ou não retirar esse consentimento remanescente. Se o consentimento for mantido, o agente de tratamento poderá prosseguir com o tratamento dos dados mesmo após a solicitação de exclusão, desde que os dados sejam coletados novamente de acordo com uma base legal válida e que respeite os direitos do titular. ";615617": "Seguem abaixo possíveis caracterizações destes conceitos 1. Decisão automatizada: Refere-se a qualquer processo de tomada de decisão que é automatizado, ou seja, que é realizado por um sistema computacional sem a intervenção humana direta ou significativa. Esta definição pode incluir uma ampla gama de sistemas, processos e algoritmos que são projetados para analisar dados e tomar decisões com base nessas análises. De acordo com a definição proposta por Rashida Richardson em seu trabalho "Defining and Demystifying Artificial Intelligence", uma "Sistema de Decisão Automatizado" é qualquer ferramenta, software, sistema, processo, função, programa, método, modelo e/ou fórmula projetados com ou usando computação para automatizar, analisar, ajudar, aumentar e/ou substituir decisões governamentais, julgamentos e/ou implementação de políticas. Esses sistemas podem impactar uma série de aspectos da vida, incluindo oportunidades, acesso, liberdades, segurança, direitos, necessidades, comportamento, residência e/ou status, por meio de previsão, pontuação, análise, classificação, recomendação, alocação, listagem, classificação, rastreamento, mapeamento, otimização, inferência, rotulagem, identificação, agrupamento, exclusão, simulação, modelagem, avaliação, fusão, processamento, agregação e/ou cálculo. 2. Decisão tomada unicamente com base em tratamento automatizado de

dados pessoais: Isso se refere a uma decisão que é tomada exclusivamente por um sistema automatizado, sem qualquer intervenção humana no processo de tomada de decisão. Isso significa que não há supervisão ou revisão humana envolvida na decisão final. Uma definição semelhante é proposta de regulamento da União Europeia para inteligência artificial ("AI Act"), que define um "Sistema de Inteligência Artificial" como software desenvolvido com uma ou mais das técnicas e abordagens listadas e que pode, para um conjunto dado de objetivos definidos pelo humano, gerar saídas como conteúdo, previsões, recomendações ou decisões que influenciam os ambientes com os quais interagem."

615618": "Para determinar quando um interesse está sendo efetivamente afetado, é necessário considerar diversos critérios, especialmente no contexto da LGPD. Aqui estão alguns pontos relevantes:

1. Impacto no titular de dados: Um interesse está sendo efetivamente afetado quando há um impacto significativo sobre o titular de dados. Isso pode incluir impactos tangíveis, como perda financeira, dano à reputação, discriminação injusta, negação de oportunidades ou outros prejuízos substanciais.
2. Natureza dos dados e decisões: O tipo de dados pessoais envolvidos e a natureza das decisões automatizadas também são importantes. Se a decisão automatizada diz respeito a dados altamente sensíveis ou é de grande importância para a vida do indivíduo, isso aumenta a probabilidade de que um interesse esteja sendo afetado.
3. Transparência e explicabilidade: A falta de transparência ou explicabilidade no processo de tomada de decisão automatizada pode indicar um risco maior de afetar os interesses dos titulares de dados. Se os titulares não entendem como as decisões são tomadas ou não têm acesso adequado às informações sobre o processo, isso pode indicar que seus interesses estão sendo afetados.
4. Probabilidade de erro ou viés: Se houver uma alta probabilidade de erro ou viés no processo de decisão automatizada, isso pode aumentar a probabilidade de que os interesses dos titulares de dados sejam afetados de maneira injusta ou prejudicial.
5. Evidências concretas de dano: Para que um interesse seja considerado efetivamente afetado, o titular de dados geralmente precisa fornecer evidências concretas de que foi prejudicado pela decisão automatizada. Isso pode incluir evidências de perdas financeiras, oportunidades negadas, danos emocionais ou outros impactos adversos."

615619": "Implementar o direito de revisão de decisões previsto no art. 20 da LGPD enfrenta diversos desafios práticos, especialmente no contexto de sistemas de inteligência artificial generativa. Aqui estão alguns dos principais desafios:

 1. Complexidade dos sistemas de IA generativa: Os sistemas de inteligência artificial generativa são extremamente complexos e podem envolver algoritmos de aprendizado de máquina que produzem resultados não facilmente compreensíveis pelos humanos. Isso torna difícil determinar como uma decisão específica foi tomada e quais foram os fatores considerados.
 2. Rastreabilidade das decisões: Em sistemas de IA generativa, pode ser desafiador rastrear e documentar o processo de tomada de decisão. Isso é especialmente verdadeiro em sistemas totalmente autônomos, onde é difícil determinar exatamente quando e como uma decisão foi tomada.
 3. Limitações na capacidade humana: Mesmo que seja possível revisar decisões automatizadas, os humanos podem ter dificuldade em entender e avaliar completamente as decisões tomadas por sistemas de IA complexos. Isso pode limitar a eficácia da revisão humana.
 4. Necessidade de especialização técnica: Para revisar adequadamente as decisões tomadas por sistemas de IA, os revisores humanos podem precisar de conhecimentos técnicos especializados em inteligência artificial e aprendizado de máquina. Isso pode representar um desafio adicional, especialmente em ambientes onde tais especialistas são escassos.
 5. Garantia de imparcialidade e objetividade: É crucial garantir que o processo de revisão de decisões seja imparcial e objetivo. Isso pode ser difícil de alcançar, especialmente se os revisores humanos tiverem interesses pessoais

ou vieses que possam influenciar sua análise. ";615620": "Sim, existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas, especialmente em casos em que seja tecnicamente impossível realizar essa revisão de forma eficaz. Isso pode ocorrer em sistemas de inteligência artificial generativa, nos quais os algoritmos complexos produzem resultados que são difíceis ou impossíveis de serem totalmente compreendidos ou rastreados pelos humanos. Nesses casos, a negação do direito de revisão pode ocorrer devido à falta de transparência nos algoritmos, à complexidade do processo de tomada de decisão automatizada e à dificuldade em rastrear e documentar o caminho seguido pelo algoritmo até chegar à decisão final. Se for tecnicamente inviável fornecer uma explicação clara e compreensível sobre como uma decisão foi tomada, o controlador pode negar o pedido de revisão. "

{ "615450": "-", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "615484": "Resumo da recomendação: Um canal de atendimento ao titular deve levar em conta critérios de efetividade, acessibilidade e redução de barreiras de acesso. Em relação a efetividade, é fundamental a demonstração por parte dos controladores que os canais de atendimento estão sendo efetivos e acessados pelos titulares. Ainda, é essencial a clareza nos mecanismos de resolução de problemas Em relação a acessibilidade, além de informações claras e compreensíveis, é grande importância que sejam consideradas medidas de acessibilidade como, por exemplo, descrições nas imagens, plugin de acessibilidade em Libras; legendas e janelas de Libras, fontes com boa legibilidade e adoção de layouts com cores em alto contraste, plugins de busca por comando de voz. Por fim, em relação a redução das barreiras de acesso, os canais de atendimento devem ser gratuitos e indicados no momento de início da relação entre o titular e o controlador. Ainda, a diversificação dos pontos de atendimento é fundamental para que os titulares consigam exercer seus direitos em sites, aplicativos, email, telefone e pontos físicos de atendimento (caso a organização possua instalações físicas). Por fim, é essencial garantir que sempre exista um canal de atendimento e exercício de direitos dos titulares em todos os pontos de coleta de dados entre o controlador e o titular. "615485": "-", "615486": "-", "615487": "-", "615491": "Resumo da recomendação: A Lei Geral de Proteção de Dados não prevê qualquer hipótese de exceção do direito de confirmação da existência do tratamento de dados, motivo pelo qual tal hipótese deve ser analisada de forma restritiva e excepcional. Contudo, vislumbra-se a hipótese em que a confirmação da existência da atividade de tratamento de dados coloca em risco outro bem jurídico de grande importância, e que, naquela situação específica, poderia sobrepor o direito do titular de ter este direito exercido. Excepcionalmente, situações em que um controlador realiza atividades de tratamento de dados única e exclusivamente no contexto de investigações sigilosas e prevenção a fraudes, que, pela mera confirmação da existência do tratamento de dado de um titular revelaria a esta informação que traria prejuízo à investigação ou ao combate à fraude, vislumbra-se a hipótese de negar este exercício de direito. Contudo, tal negativa deverá ser devidamente fundamentada e o titular deve ser informado ostensivamente acerca de peticionar à ANPD caso entenda que a negativa se mostra abusiva ou em desacordo com a disposição legal. "615492": "Os direitos do art. 18 ganham concretude a partir do pedido do titular. Como consequência, quando solicitado, o titular tem direito de saber informações sobre o uso compartilhado de seus dados pessoais de forma específica, não genérica, ou aplicável a qualquer titular de dados pessoais que o controlador solicitado realize. Assim, o titular deve, no mínimo, ser informado sobre o nome do controlador que recebeu os dados e a finalidade do uso compartilhado no caso específico para que possa exercer seus direitos também perante a esse controlador. Ainda, o art. 18 destaca que o controlador deve informar não apenas as entidades privadas com quem realizou uso compartilhado de dados de determinado titular, mas também as entidades públicas. Isso reforça o princípio da transparência e livre acesso da LGPD aplicável a qualquer tipo de controlador de dados. Esta entre o acesso pelo titular de toda cadeia de controladores que tem acesso a seus dados é comumente associada a preocupações relacionadas a proteção do segredo industrial. Várias das disposições da LGPD, inclusive a concretização de direitos, traz o sopesamento do segredo de negócio como um dos filtros para divulgação de informações. Ao mesmo tempo, a lei não oferece uma definição clara do que é um segredo comercial ou industrial,

de forma a tornar esses conceitos fluídos no âmbito da proteção de dados. Conforme as diretrizes do Grupo de Trabalho do Artigo 29, os controladores não podem usar o segredo comercial como justificativa para negar acesso a dados ou recusar fornecer informações ao titular dos dados. Portanto, o argumento do segredo de negócio só é válido em circunstâncias excepcionais e não pode ser invocado de maneira indiscriminada. Em vez de adotar uma abordagem de "tudo ou nada", é necessário buscar um nível de transparência adequado tanto para o titular dos dados quanto para a empresa que detém o direito de manter seus segredos comerciais. Por fim, a exceção do segredo industrial deve ser devidamente fundamentada pelo controlador, de forma específica para cada caso, e ser passível de questionamento.

615489: "Resumo da recomendação: A ANPD deve considerar o previsto pela LGPD em seu art. 9º e dar regulamentação concreta acerca dos parâmetros mínimos de transparência ali descritos, tendo como norte a efetividade da comunicação entre controlador e titular. É necessário que o titular de fato compreenda como se dá a atividade de tratamento de dados para que possa exercer sua autodeterminação informativa. Portanto, informações genéricas, confusas, em linguagem hermética e prolixa não são suficientes para o atendimento do dever de transparência. Ainda, além do previsto no art. 9º, a ANPD tem a oportunidade de estabelecer um novo requisito: o dever de os controladores informarem as fontes dos dados tratados. Essa informação, no contexto da transparência ativa, não exige o grau mais elevado de granularidade acerca das fontes, bastando que o controlador informe de quais meios vem os dados (coleta direta do titular, observação, inferência, coleta de bases de dados públicas, compartilhamento de dados com parceiros comerciais, etc.). Por fim, seria de grande importância para o fortalecimento da cultura de proteção de dados no Brasil que a ANPD incentivasse medidas de transparência inovadoras, como “tabelas nutricionais de proteção de dados” e selos que indiquem atividades de tratamento de dados que apresentem alto risco para os titulares.

615493: "Resumo da recomendação: O direito de acesso se consolida mediante a disponibilização das informações e dos dados ao titular, seja por meio eletrônico ou físico, em conformidade com os incisos I e II, § 2º do art. 19 da LGPD. Tal disponibilização deve contemplar elementos de acessibilidade, garantindo ao titular acesso completo às suas informações. No meio eletrônico, é essencial assegurar uma diagramação adequada para permitir a leitura por pessoas que utilizam leitores de tela e outras tecnologias assistivas. Já em meio físico, deve-se considerar a impressão em Braille para possibilitar a leitura por pessoas cegas ou com baixa visão.

615502: "615501: "615505: "615503: "615504: "Resumo da recomendação: A ANPD deve iniciar e impulsionar a implementação de soluções de portabilidade por meio de regulamentação específica sobre esse direito. É comum que, uma regulamentação sobre o tema ocorra de forma setorial, porém a interoperabilidade é um dos pilares para o desenvolvimento de uma infraestrutura pública digital, tema chave para a agenda digital do Brasil. Com isso, a portabilidade assume perspectiva geral, para além das implicações setoriais do tema. Nesse sentido, a ANPD é o órgão regulador que possui a competência legal definida para estabelecer parâmetros mínimos acerca desse direito e dialogar com órgãos setoriais para que as regulamentações setoriais possuam um mesmo nível adequado de proteção aos titulares de dados.

615511: "Resumo da recomendação: O maior ponto de controvérsia acerca do direito de correção de dados incompletos, inexatos ou desatualizados se dá em dados que não podem ter sua validade/veracidade verificados objetivamente. EX: Um birô de crédito atribui uma baixa avaliação de crédito a um titular, implicando que este possui altas chances de não pagar dívidas contraídas. Essa atribuição foi baseada no histórico de pagamentos e de recebimentos deste titular nos últimos 5 anos. Nesse caso, o score de crédito final

é um dado que não garante, por si só, elementos suficientes para ter sua veracidade apurada. Contudo, a análise dos dados de histórico de pagamentos e recebimentos, por sua vez, pode ser apurada. Portanto, se o score de crédito foi calculado com base em informações desatualizadas, ele passa a ser objeto de correção na medida em que os elementos objetivos que o embasam estão incorretos. Por este motivo, o direito à correção está intimamente ligado ao direito de acesso às informações. Caso o titular não tenha acesso aos dados que embasam alguma análise feita sobre ele pelo controlador, torna-se impossível o exercício de um direito previsto em lei. Além disso, recai sobre o controlador o ônus de demonstrar que análises e inferências feitas possuem algum lastro na realidade e podem ter sua acurácia mensurada em algum parâmetro. Essa discussão se relaciona ao chamado “direito a inferências razoáveis” e se mostra como uma importante janela de oportunidade para a ANPD fixar parâmetros mínimos para atividades de tratamento de dados que atribuem características ou comportamentos a titulares que não podem ser diretamente observados ou mensurados objetivamente.

,"615514": "Resumo da recomendação: Em primeiro lugar, é importante que o titular consiga demonstrar minimamente qual a informação que está imprecisa. Quando o pedido é ininteligível, não sendo possível compreender qual dado está incorreto e o que deve ser corrigido, o direito de correção fica prejudicado. Contudo, situações em que o erro envolve informações sobre crédito, registro criminal, situação familiar e outras informações que dizem respeito aos seus direitos fundamentais é preciso contar com documentos capazes de demonstrar o erro. Aliado a isso, ressaltamos que é papel do controlador esclarecer quais documentos servem de justificativa nesses casos e do porque somente a declaração do titular não é suficiente para que a correção ocorra. Ao mesmo tempo, é preciso que o controlador tenha cautela e respeite a proporcionalidade da documentação exigida. Ou seja, a solicitação de mais informações para proceder à correção deve versar somente para o necessário da comprovação, não sendo admitida solicitações de documentos que só trariam maiores dificuldades de acesso ao direito do titular. Ex: O titular mudou de nome e quer que o novo nome conste na base de dados do controlador. Para tanto, ele faz a solicitação de correção e o controlador informa que a correção depende de uma documentação que mostre o nome atual como o RG, a documentação que comprove a mudança de nome, a certidão de nascimento ou casamento e comprovante de residência. No caso em questão, é possível ver que o comprovante de residência é uma solicitação excessiva tendo em vista que não é adequada para averiguar a inexistência do dado a ser corrigido.

,"615513": "Resumo da recomendação: Cabe ressaltar que o dever de comunicar a correção a terceiros de quem o controlador compartilha dados é um dever legal previsto expressamente aliado a um dos princípios basilares da proteção de dados no Brasil. Tal obrigação tem como decorrência a exigência de que o controlador tenha medidas técnicas e organizacionais para poder informar parceiros de que um dado foi corrigido. Todavia, sabemos que as múltiplas atividades de tratamento e as tecnologias envolvidas podem ser um fator relevante na hora de informar com clareza e qualidade que um dado foi corrigido. Dito isso, ressaltamos alguns critérios objetivos: A quantidade de parceiros em que se compartilha os dados A complexidade técnica da correção. A quantidade de parceiros é um critério seguro pois quantificável e avaliável como elemento que dificulta a comunicação imediata da correção. Já o segundo elemento, diz respeito a impossibilidade de comunicação imediata da correção por conta do tempo de execução da própria correção, de modo que uma correção mais demorada, atrase o momento da comunicação imediata, bem como da qualidade dessa comunicação haja vista a complexidade com que foi executada. Reforça-se que esses critérios podem ser utilizados para justificar um prazo estendido para a correção ou eliminação dos dados, ou apresentação de solução

alternativa (ex: controlador apresentar anonimização como solução quando a eliminação é inviável) mas jamais o descumprimento da solicitação do titular. ","615512": "Resumo da recomendação: Existe uma certa dificuldade em exceções na qual o controlador pode se recusar a realizar a correção dos dados, tendo em vista que a correção colabora com o princípio da qualidade dos dados e seus fluxos em nossa sociedade. Contudo, existem dois elementos que podem ser utilizados para negar um pedido de correção:: Pedidos ininteligíveis Pedidos excessivos ou infundados Pedidos ininteligíveis são aqueles em que o pedido do titular não consegue esclarecer qual dado está inexato e precisa ser corrigido ou quando o titular não apresenta a documentação necessária para tanto. Já os pedidos excessivos ou infundados são aqueles em que o titular solicita múltiplas vezes sobre o mesmo assunto em um período de tempo curto, de forma que a resposta de um, responde a todos. Nesse caso, o controlador pode responder a uma solicitação e se recusar a responder as repetidas, alegando que a correção solicitada já foi realizada. Em qualquer dos casos, a recusa pela correção dos dados deve vir com uma justificativa, que deve conter: os motivos pelos quais a correção não foi feita; o direito de fazer uma reclamação à ANPD e a possibilidade do titular de buscar a seara judicial para a resolução do problema. Por fim, ressalta-se que esta pergunta possui íntima conexão com a pergunta anterior "Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?", motivo pelo qual é de grande importância uma regulamentação que garanta aos titulares o máximo de informações possíveis acerca de seus dados tratados pelo controlador para que controvérsias sobre a correção de um dado sejam mitigadas."","615517": "Os direitos dos titulares previstos na LGPD existem a partir do pressuposto da assimetria de poder e informações na relação entre titular e controlador. Desta forma, nenhum exercício de direitos deve se basear na capacidade técnica do titular de formular um pedido, mas sim na forma como o controlador fornece informações suficientes para que o titular possa compreender o tratamento de dados e se seu pedido tem legitimidade ou não. Nesse sentido, é desproporcional que o titular saiba avaliar a conformidade do tratamento para poder exercer tais direitos, pois trata-se de uma hipótese clara de inversão do ônus da prova. A LGPD prevê em dois momentos a inversão do ônus da prova, inicialmente em seu art.8º §2 da LGPD, ao dispor que o controlador precisa comprovar que cumpriu com os requisitos do consentimento, e no art. 42 §2º, em que se autoriza em processo judicial a inversão do ônus da prova quando "for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa". Tal disposição se assemelha a dos art.6, VIII;51, VI CDC e art 373, §1º CPC. que dispõem que a inversão do ônus da prova deve ocorrer quando for muito oneroso a comprovação pela parte. No caso em questão, a informação sobre o tratamento está de posse do controlador, razão pela qual é do controlador o dever demonstrar que cumpriu a lei após a manifestação do titular. ","615516": "-"","615518": "Resumo da recomendação: Diante de tal pergunta, duas respostas podem ser possíveis: Resposta 1: encerrar o tratamento de dados pessoais do titular que se opôs. Resposta 2: proceder à conformidade do tratamento. Como a proposição legal do art. 16 §2º estabelece que o direito à oposição deve ser exercido em caso de desconformidade com a lei, caso seja legítimo, o controlador precisa tomar medidas para que o tratamento esteja de acordo com a LGPD. Portanto, a resposta 2 parece ser a mais adequada. Opor-se ao tratamento de um dado também pode levar ao encerramento do tratamento no caso do legítimo interesse, onde a irregularidade do tratamento está na violação das legítimas expectativas do titular. Contudo, mesmo nesses casos, o encerramento do tratamento dos dados do titular é uma forma de conformidade. Vale lembrar que é uma boa prática que as comunicações com titulares de dados

como as do exemplo venham acompanhadas de uma interface que forneça um canal de atendimento e um canal de exercício ao direito à oposição no mesmo ambiente. Ex: o email tem que vir acompanhado com alguma opção de “fale conosco” e “quero me opor a esse tratamento de dados” Algo distinto é o pedido de eliminação, anonimização ou bloqueio dos dados, que visa impedir tratamentos de dados excessivos, desnecessários ou em desconformidade. Nesses casos, o pedido visa o encerramento do tratamento de dados pessoais do titular, razão pela qual essa deve ser a consequência caso ele seja legítimo nas hipóteses de tratamento excessivo ou desnecessário. No caso da desconformidade à lei, o agente de tratamento precisa adequar a atividade de tratamento ao mesmo tempo que exclui, anonimiza ou bloqueia o tratamento dos dados do titular. “615523”-“615521”-“615617”:

Nesse contexto, a palavra “unicamente” não deve ser interpretada de forma restritiva para descaracterizar a decisão como automatizada em qualquer envolvimento humano na tomada de decisão, mas apenas nos casos em que esse envolvimento é significativo, isto é, quando pode alterar ou influenciar o resultado da decisão. Essa interpretação afasta a tentativa de fabricação de interferência humana na tomada de decisão para afastar a aplicação do art. 20, o que confere maior carga protetiva aos titulares de dados. Tal interpretação é corroborada no contexto europeu, em que o Grupo de Trabalho do Artigo 29 (corroborado pelo EDPB) se manifestou pelo entendimento de que, para ser qualificado como participação humana, esta deve ser significativa para a tomada de decisão, ou seja, envolver pessoa com autoridade e competência para interferir no resultado – não meramente um ato simbólico. Nesse sentido, a Autoridade Espanhola de Proteção de Dados faz uma complexificação necessária da análise sobre a interferência humana significativa. Esta pode ser entendida quando a pessoa que participa da decisão: (i) tem competência ou autoridade para mudar o resultado; (ii) tem conhecimento e preparo para mudar o resultado da decisão automatizada; (iii) tem independência e diligência no exercício de sua competência, ou seja, quando não há pressões da organização ou externas que impeçam o agir pela pessoa, assim como a ausência do pré-condicionamento de aceitar a decisão automatizada como certa (viés da automação); (iv) pode exercer sua competência e qualificação, pois pode exercer a jurisdição no caso concreto, além de ter informações, recursos e tempo para exercer sua função de interferir na decisão. Portanto, é essencial que a análise da decisão automatizada e a participação humana significativa considere não apenas a decisão final, mas também eventuais decisões intermediárias [upstream] que possam também ter impactos potencialmente distribuídos ou observados com atraso em decisões posteriores [downstream] que afetarão os interesses dos titulares. “615618”:

De acordo com o Grupo de Trabalho do Artigo 29, no contexto do art. 22 do RGPD da União Europeia, a afetação de um interesse jurídico no âmbito de decisões automatizadas ocorre sempre que houver afetação em direitos ou no seu estatuto jurídico, como no caso de impactos na liberdade de reunião, recebimento de benefício social ou até mesmo participar de processos democráticos. Porém, diferentemente do acontece no âmbito do RGPD, o art. 20 da LGPD não define que a afetação de interesses deve ser meramente jurídica, assim como não prevê a possibilidade de afetar “significativamente de forma similar”. Consequentemente, a afetação de interesses pela lei brasileira pode ser entendida de forma mais ampla, não havendo necessidade da verificação de violação de um direito específico para que o art. 20 e seus direitos correlatos possam ser invocados. Como exemplo de afetação de interesses, podemos citar o caso de decisões que neguem eficácia ou deixem de promover direitos do titular de dados, negando ou limitando alguma perspectiva de promoção da pessoa humana, inclusive apenas por meio de ameaça de afetação de direitos. Em outras palavras, a tutela dada pelo art. 20 pode ter natureza preventiva, antes da concretização

em dano efetivo.";"615619": "Os desafios práticos para implementação do direito de revisão de decisões previsto no art. 20 da LGPD no Brasil giram em torno, principalmente, de três elementos: (i) concretizar o entendimento a respeito dos critérios para exercício do art. 20; (ii) a possibilidade (ou não) de a revisão ser realizada por pessoa humana e, em caso positivo, em quais situações (delimitação dos critérios); (iii) como garantir o direito de revisão nos casos em que o sistema é mais opaco em função da complexidade do algoritmo e, em caso de impossibilidade, como garantir medidas alternativas para o titular; (iv) como compatibilizar o direito de revisão do art. 20 da LGPD com a possível futura regulação de inteligência artificial que pode trazer um rol de direitos com a previsão de um novo direito de contestação, inclusive com participação humana (exemplo do que já acontece no Projeto de Lei 2338/2023). ";"615620": "-"

{ "615450": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Os prazos fixados na Lei nº 12.527/2011, a Lei de Acesso à Informação (LAI), consideram o atendimento por órgãos e entidades da Administração Pública a pedidos formulados por cidadãos a respeito de informações contidas em registros e documentos, processos administrativos, relatórios sobre uso de recursos públicos, resultados de auditoria, entre outras. O atendimento a requerimentos fundados na LAI leva, portanto, na maior parte das vezes, a que os responsáveis pelo funcionamento de um balcão de atendimento ao público, mantido pela Administração com esta finalidade, compartilhem documentos já produzidos com requerentes interessados em acessá-los. O atendimento a titulares de dados pessoais coloca os agentes de tratamento privados diante de situação diversa. Vasta é a gama de possíveis pedidos, alguns a demandar providências adicionais, que vão além do simples compartilhamento de informações consolidadas em documentos já existentes ou previamente elaborados. Muitas das vezes os agentes de tratamento terão de se debruçar sobre cada pedido para compreendê-lo e poder atendê-lo satisfatoriamente, além de terem de recuperar informações nem sempre mantidas de forma consolidada e que correspondam exatamente ao pedido formulado pelo titular dos dados. Noutras tantas vezes o atendimento aos titulares implicará na tomada de ações concretas, que em nada se assemelham ao simples compartilhamento de informações ou documentos. Nesse contexto, a LAI não parece um bom ponto de aproximação para a regulação dirigida ao atendimento dos pedidos formulados pelos titulares aos agentes de tratamento atuantes no setor privado. Uma proposta alternativa segue na resposta da ABERT à pergunta seguinte (l.b). ",b.

Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Idealmente o prazo, na visão da ABERT, deve ser de no mínimo 30 (trinta) dias úteis, em linha com o que dispõe o artigo 12, 3, do GDPR. Esse prazo deve poder ser prorrogado (mediante aviso ao Titular de forma clara e formal), por igual período, ante a complexidade do processo de cada companhia para análise e atendimento das solicitações. A complexidade envolvida para o pleno atendimento de solicitações de titulares varia conforme os setores de atuação de cada empresa, o volume de dados envolvidos e a natureza das atividades de tratamento, entre outros elementos. A ausência de um prazo adequado somado a essa pluralidade de complexidades, volumes e especificidades para atendimento pelos diferentes controladores impacta diretamente o titular. A depender do relacionamento entre o titular e o controlador, é possível que o histórico de dados seja bastante extenso, logo, envolvendo um volume de dados relevante. Neste contexto, sem prazos adequados (e sua possível prorrogação), a ABERT enxerga, além de um risco de inviabilidade de verificação e atendimento adequado pelo controlador, um risco associado ao titular, no que se refere à qualidade dos dados recebidos. Prazos excessivamente curtos possivelmente resultarão em dificuldades operacionais que levarão os controladores a deixarem de atender por completo as solicitações recebidas. Por fim, é importante mencionar que há um risco relevante a respeito dos limites da solicitação de confirmação ou de acesso, com efeitos tanto para o controlador quanto para o titular: o potencial excesso de informações solicitadas ou encaminhadas. A ABERT entende que esse excesso pode se configurar de duas formas: [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]

;"615484": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão

(ABERT): Na perspectiva da ABERT, as características fundamentais de um canal de atendimento para garantir efetividade na comunicação entre o titular e o agente de tratamento são a disponibilidade e a usabilidade. Nesse sentido, é essencial que este canal de atendimento esteja publicamente disponível e facilmente localizável em sites ou redes oficiais dos agentes de tratamento, priorizando a praticidade na construção de meios para que o titular possa exercer seus direitos. É igualmente essencial que o canal seja de fácil usabilidade – especialmente considerando a diversidade social e cultural dos titulares do nosso país – contendo o mínimo possível de etapas a serem percorridas, mas não sem o mínimo necessário para a adequada identificação da necessidade ou demanda do Titular.

;"615485": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): A ABERT entende que sim, há responsabilidade dos operadores, na medida das atividades de tratamento de dados que conduzirem. A cooperação dos operadores no atendimento aos direitos dos titulares pelos controladores está diretamente relacionada ao papel central que assumem em diversas atividades de tratamento, uma vez que os operadores são frequentemente responsáveis por sua realização direta. Por exemplo: uma empresa que presta serviços de processamento de folha de pagamento, atuando como operadora, detém acesso imediato e organizado a informações relevantes sobre os empregados do controlador; e não poderia se furtar a colaborar com o controlador com vistas ao exercício dos direitos desses empregados. Assim sendo, independentemente da existência de cláusula contratual nesse sentido, deve-se presumir a existência de um dever de colaboração dos operadores em relação aos controladores para análise e atendimento às solicitações de titulares. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]";

;"615486": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): O Decreto do SAC (Decreto nº 11.034/2022) foi desenhado para lidar com atendimento a consumidores de “serviços regulados pelo poder público federal”, leia-se: setores de água, energia, telecomunicações, saúde, seguros, financeiro e aviação. O Decreto tem em vista a solução de reclamações, a abertura e cancelamento de contratos de consumo, exercício do direito de arrependimento, discussões sobre cobranças indevidas e restituição de valores a partir de uma estrutura de atendimento criada na década de 1990 e início dos anos 2000, marcada pelo surgimento dos grandes players em setores de infraestrutura após as privatizações, como as companhias de energia e telecomunicações. O esforço da Senacon/MJ, ator importante na construção do Decreto do SAC, foi reduzir os altos índices de insatisfação com as empresas mais reclamadas, novamente: companhia aéreas, concessionárias de água e energia, prestadoras de serviços de telecomunicação, entre outras. Nesse contexto é que pareceu adequado impor aos grandes players desses setores as obrigações que constavam na primeira versão Decreto (2008) e que foram parcialmente mantidas no texto atualmente em vigor. Ainda que importantes lições possam ser retiradas do próprio Decreto do SAC e dos vários regulamentos setoriais dirigidos à regulação de direitos dos consumidores, pensar na adoção dos procedimentos ali previstos, pela ANPD, como solução para a regulamentação de aspectos das LGPD, não parece uma solução adequada. Na visão da ABERT, a regulação por analogia tende a ser mais negativa do que positiva do ponto de vista econômico e operacional, tendo em vista: [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]

;"615487": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Na visão da ABERT, não há no setor privado um modelo de atendimento que possa ser considerado como padrão. Considerando os diferentes perfis e portes de agentes de tratamento – todos eles sujeitos ao atendimento dos direitos do titular –

é importante que não existam modelos de atendimento padronizados obrigatórios, ainda que exemplos específicos possam ser vistos como boas práticas. A complexidade e o volume das solicitações podem variar consideravelmente de um setor para outro, mesmo considerando apenas empresas de grande porte. Utilizar como modelo a realidade de uma empresa com alta complexidade e alto volume de solicitações pode distorcer os parâmetros e prejudicar a implementação de um modelo realmente eficiente por empresas com estruturas menores ou volumes de solicitação reduzidos. Portanto, a sugestão da ABERT é que não exista um padrão obrigatório a ser implementado por agentes de tratamento.

;"615491": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Sim. A ABERT apresenta abaixo rol exemplificativo, com algumas hipóteses em que, a seu ver, o direito de confirmação poderá ser negado pelo agente de tratamento. A saber: i. Quando o titular não realiza a validação da sua identidade conforme solicitado pelo controlador: como se sabe, para o atendimento de solicitações de titulares, é imprescindível que o controlador realize a validação de identidade como medida de segurança, de modo a assegurar que a resposta seja enviada ao verdadeiro titular ou a seu representante legal devidamente autorizado, inclusive em obediência ao artigo 46 da LGPD ; ii. Segredo de negócio e confidencialidade: quando o titular solicitar a disponibilidade de informações desenvolvidas ou inferidas pelo controlador a partir dos seus dados que contenham informações relativas à estratégia de negócio, posicionamento de mercado ou relacionamento com seus clientes pelo controlador – todas consideradas segredo de negócio. Nestes casos, a ABERT entende que o cumprimento da solicitação não deve se sobrepor ao segredo comercial e industrial; iii. Requisições massivas em curto período: quando houver múltiplas requisições em um pequeno espaço de tempo que demandem esforço desproporcional do agente de tratamento para atendê-las, considerando os aspectos técnicos e operacionais envolvidos; neste contexto, cabe ressaltar que a ANPD e os próprios agentes de tratamento têm atuado para levar aos titulares cada vez mais conhecimento a respeito dos seus direitos, de modo que se torna possível que o volume inicial seja elevado, até que se caminhe em direção a patamares normais. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normalizacao@anpd.gov.br)]

;"615492": "Contribuições ABERT: No entendimento da ABERT, a menção, na Política de Privacidade publicamente disponível das categorias de destinatários com os quais o Controlador realiza o compartilhamento de dados pessoais já deve ser considerada suficiente para cumprir a disposição do artigo 9º da LGPD, que visa a promover o acesso facilitado a informações sobre tratamento de dados pessoais. A perspectiva adotada se baseia na premissa de que o excesso de informação, considerando a assimetria de conhecimento entre titulares e agentes de tratamento, pode mais facilmente confundir do que esclarecer os titulares. É de pouca utilidade para a esmagadora maioria dos titulares saber exatamente quais são as empresas específicas (CNPJ a CNPJ) com quem o controlador compartilha dados, além de essa informação poder representar, em alguns cenários, segredo de negócio (por exemplo, quais empresas realizam validação de identidade e verificação antifraude). Deste modo, a ABERT entende que o objetivo de proporcionar transparência e clareza ao titular de dados seja plenamente alcançado de forma adequada, ostensiva e razoável por meio da menção, na Política de Privacidade do agente de tratamento, das principais categorias dos destinatários, como provedores de nuvem, de pagamento e autoridades competentes. Caso o titular manifeste interesse em obter mais detalhes acerca das entidades públicas e privadas com as quais o controlador compartilha seus dados pessoais, incluindo detalhes como nome e CNPJ das respectivas empresas, estes esclarecimentos poderão ser obtidos mediante o exercício de direito garantido pela

legislação, ocasião em que o controlador poderá especificar e prover mais detalhes, apenas quando requisitado pelo titular. Por outro lado, especificamente no que diz respeito ao controlador, a ABERT entende, de igual modo, bastar a menção, na sua Política de Privacidade, do seu nome, CNPJ e respectivos canais oficiais de comunicação, cujos dados satisfarão quaisquer eventuais necessidades dos titulares, lhes permitindo o pleno gozo de seus direitos. ";615489": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Em linha com a resposta dirigida à questão "I.d", a ABERT entende que sim, há responsabilidade dos operadores, na medida das atividades de tratamento de dados que conduzirem. A cooperação dos operadores no atendimento aos direitos dos titulares pelos controladores está diretamente relacionada ao papel central que assumem em diversas atividades de tratamento, uma vez que os operadores são frequentemente responsáveis por sua realização direta. Como mencionado anteriormente, uma empresa que presta serviços de processamento de folha de pagamento, atuando como operadora, detém acesso imediato e organizado a informações relevantes sobre os empregados do controlador; e não poderia se furtar a colaborar com o controlador com vistas ao exercício dos direitos desses empregados. Assim sendo, independentemente da existência de cláusula contratual nesse sentido, deve-se presumir a existência de um dever de colaboração dos operadores em relação aos controladores para análise e atendimento às solicitações de titulares. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)];";615490": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Na visão da ABERT, entendemos que na declaração em formato simplificado, os dados constantes no atendimento pelo controlador serão dados cadastrais básicos. Por exemplo: nome completo, RG ou CPF, endereço, e-mail, telefone ou outros da mesma natureza. Ainda, no caso dos serviços ou fornecedores que tenham sites disponíveis com área logada pelo cliente-titular, a lista de dados habitualmente visíveis nos menus comumente denominados "Meu Perfil", "Sua Conta", "Seus Dados" ou semelhantes já devem servir como a própria declaração simplificada, a qual estará, portanto, disponível ao titular em tempo integral. Naturalmente, para as empresas que não ofereçam essa possibilidade, o processo de atendimento deve ser realizado por meio da geração de um relatório pelo controlador e encaminhado ao titular em formato de fácil acesso e considerando mecanismos de segurança. ";615494": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Sob a perspectiva da ABERT, para garantir a transparência e o direito à informação, o controlador deve prover informações mínimas e essenciais referentes à finalidade do tratamento de dados, descrição das categorias dos dados pessoais coletados, informações genéricas referentes ao compartilhamento de dados com terceiros (como melhor exposto na resposta à pergunta "II.b"), bem como os direitos que poderão ser exercidos pelos titulares, além da disponibilização de canais oficiais de comunicação com o agente de tratamento – que deve dispor de equipes multidisciplinares adequadas (internas ou terceirizadas) para gerir e analisar as solicitações dos titulares de dados pessoais – bastando que as informações supracitadas constem na sua Política de Privacidade. Não obstante, a ABERT entende que as informações acerca dos critérios e procedimentos utilizados em decisões automatizadas não devem figurar entre as informações mínimas a serem fornecidas ao titular, sem que haja requerimento específico. Pensamos que tal divisão esteja em linha com a LGPD, que separa o pedido relacionado a critérios e procedimentos utilizados para decisões automatizadas (art. 20, §1º) das demais obrigações relacionadas ao fornecimento de informações aos titulares. ";615493": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Conforme estabelecido no artigo 19, § 2º da LGPD, o

titular dos dados possui a prerrogativa de escolher o formato de recebimento dos dados pessoais relacionados ao direito de acesso, seja em formato físico ou digital. Não obstante, é importante também observar o disposto no § 1º deste mesmo dispositivo, que estipula que os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso. Considerando o avanço tecnológico contínuo no cenário atual, é inegável afirmar que o armazenamento de dados em formato físico, tanto por pessoas físicas quanto jurídicas, tornou-se obsoleto. A ABERT entende que a disponibilização dos dados pessoais em formato eletrônico deve ser priorizada. Este posicionamento não apenas está em conformidade com a LGPD, mas também proporciona um ambiente mais seguro e idôneo para a finalidade pretendida: disponibilização de documentos ao titular de dados pessoais, sem as desvantagens e riscos inerentes à documentação em papel (extravio, sigilo, transporte, custos, entre outros). Em outras palavras, embora a LGPD contenha disposições específicas a respeito, a ABERT reforça o seu entendimento de que a disponibilização dos dados pessoais em formato eletrônico deve ser preferível por conferir maior segurança aos documentos, além de maior praticidade e economicidade aos controladores que, atualmente, possuem a quase totalidade de seus dados armazenados de forma digital.

","615502": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): A instituição de portabilidade, tomada como um instrumento regulatório, tem em vista reduzir custos de mudança suportados por usuários de serviços concorrentes, que possuam a mesma utilidade para o consumidor final. No setor de telecomunicações, com a portabilidade (instituída já há alguns anos), os consumidores deixaram de suportar a perda de seu número de contato telefônico ao “mudar” de operadora e passaram a poder mantê-lo, levando-o consigo para a nova operadora de sua escolha. Nesse contexto, mais apenas do que uma mera praticidade para os consumidores, a instituição da portabilidade representa uma verdadeira ferramenta de fomento à competição, já que os consumidores deixam de ser desencorajados pelo custo de mudança antes suportado e se veem em condições de seguir adiante, trocando de operadora, com maior facilidade. Considerado esse efeito habilitador da competição a portabilidade passou a ser exigida no setor de telecomunicações, sendo levada a outros setores, como o de serviços financeiros. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]","615501": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Como mencionado na questão anterior, temos um cenário de absoluta incerteza, no qual não se sabe ao certo quais dados seriam objeto de interoperabilidade ou em que termos essa interoperabilidade seria implementada. Somente após o preenchimento dessas lacunas parece, à ABERT, possível que se possa pensar em quais sistemas operacionais serviriam de ponto de contato entre agentes e, então, pensar nos desafios tecnológicos relacionados. De toda sorte, parece evidente que a vasta gama de diferentes sistemas desenvolvidos e implementados pelos respectivos times de TI das empresas representam um desafio importante – ainda que se esteja tratando de um mesmo setor de atividade econômica. Vale lembrar que mesmo nos casos em que diferentes agentes de tratamento contratarem um dado sistema, provido por um mesmo fornecedor, é comum que esses sistemas passem por processos de customização. Sistemas customizados dificilmente utilizam os mesmos campos e parâmetros e podem apresentar dificuldades significativas para simples exportação e importação dados com a equivalência esperada, ainda que em formato interoperável. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]","615505": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): A partir da perspectiva da ABERT,

destacamos a importância de uma discussão técnica com especialistas capacitados neste tema para identificar os aspectos que devem ser padronizados para garantir a interoperabilidade. É fundamental abordar questões como a estrutura dos dados, protocolos de comunicação e segurança da informação para garantir uma interoperabilidade eficaz entre os diferentes agentes de tratamento de dados. E evitar que se crie o risco de compartilhamento indevido e não desejável de dados entre diferentes agentes de tratamento que passem a operar de forma interconectada. Esses são apenas alguns dos aspectos que devem ser considerados na padronização para promover uma interoperabilidade consistente e abrangente. Uma colaboração técnica e especializada será essencial para identificar e implementar os padrões necessários nesse processo. ","615503": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): sem contribuições.", "615504": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Como mencionado na questão anterior, temos um cenário incerto, no qual não se sabe quais dados seriam objeto de interoperabilidade ou em que termos essa interoperabilidade seria implementada. Somente após o preenchimento dessa lacuna parece, à ABERT, possível que se possa pensar em quais sistemas operacionais serviriam de ponto de contato entre agentes e daí pensar nos desafios tecnológicos relacionados. A partir desse ponto seria, sim, razoável permitir que as empresas de um mesmo setor se reúnam para debater padrões de interoperabilidade específicos para suas atividades.", "615511": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): A ABERT entende que um dado é considerado incompleto quando faltam informações que estariam diretamente associadas a ele (por exemplo, somente o sobrenome em um cadastro que depende do nome completo para poder alcançar sua finalidade). Um dado inexato seria aquele que parece estar correto, porém algum erro no momento da coleta ou posteriormente levou à inexatidão (exemplos são anos de nascimento errados ou grafias equivocadas no nome ou endereço do titular). Já o dado desatualizado é aquele que estava completo e correto no passado, mas não mais reflete a realidade do titular (por exemplo, endereço ou telefone antigos cadastrados em vez dos atuais). Vale observar, porém, que dados desatualizados nem por isso deixam de ser úteis, como por exemplo nos cenários de combate à fraude, em que o histórico de endereços ou telefones anteriores é crucial para a atividade. ","615514": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Para que o pedido possa ser atendido, é imprescindível que o titular demonstre por quais motivos os dados existentes estão incompletos, inexatos ou desatualizados, bem como confirme a veracidade dos dados por ele apresentados como corretos, não bastando, portanto, na grande maioria das situações, a simples declaração do titular para o exercício do direito à correção. Infelizmente, um dos principais vetores de fraudes nas empresas é a falsa correção de informações por quem se passa por um titular – o exemplo mais conhecido é a alteração de endereço de entrega em um e-commerce, para que o produto seja enviado ao fraudador e não para o titular. Na visão da ABERT, solicitações de correção devem ser revisadas com cuidado antes que as alterações pretendidas sejam implementadas, tendo em vista que seu atendimento implica na substituição de informações no banco de dados dos agentes de tratamento envolvidos. Por esse motivo, essas solicitações só devem ser atendidas após conferência dos dados apontados como incompletos, inexatos ou desatualizados e confirmação da veracidade dos dados apontados pelo titular como corretos, evitando-se com isso a prática de fraudes e a eliminação de dados originais verídicos. ","615513": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): No entendimento da ABERT, a impossibilidade ou o esforço desproporcional devem ser considerados de acordo com os aspectos técnicos e

operacionais envolvidos. Além disso, como se sabe, os direitos dos titulares não são absolutos. Certos direitos, por exemplo, podem ser eventualmente restringidos pelos direitos dos agentes de tratamento sobre seus segredos empresariais, situação em que caberá ao controlador explicar ao titular as razões pelas quais algumas de suas solicitações não serão atendidas. Nesse sentido, vale conferir as orientações e exemplos do Information Commissioner's Office (ICO) sobre requisições infundadas: [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]

","615512": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Sim, a ABERT entende que o direito de correção poderá ser negado pelo controlador sempre que a requisição do titular se mostrar infundada ou manifestamente abusiva, o que deverá ser avaliado no caso concreto, com base nos parâmetros mencionados na resposta à questão anterior ("IV.c"), bem como nos casos em que não houver validação de identidade do titular, ou, ainda, se houver dúvidas razoáveis sobre as informações apresentadas pelo titular."

","615517": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Sim. Na visão da ABERT, é fundamental que solicitações de anonimização, bloqueio ou eliminação apenas devam ser atendidas em casos especiais, após rigorosa análise interna dos dados pessoais indicados pelo titular e revisão das atividades de tratamento, tendo em vista que o atendimento ao pedido do titular implica reconhecer que o controlador não está cumprindo com as exigências da LGPD. A qualificação aqui é extremamente importante: dados desnecessários referem-se àqueles que não são úteis nem pertinentes para a finalidade que justifica o seu tratamento; dados excessivos são considerados àqueles supervenientes aos necessários para atingir a finalidade que justifica o seu tratamento e dados tratados em desconformidade com a LGPD são aqueles cujo tratamento é ilegal. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]

","615516": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): No entendimento da ABERT, a anonimização e a eliminação de dados pessoais podem ser adotadas de forma alternativa, considerando situações específicas, já que o que realmente importa é o resultado prático, ou seja, a impossibilidade de reutilização dos dados pessoais. Ademais, a escolha específica entre anonimização e eliminação pode depender de circunstâncias particulares, as quais um titular de dados, considerando uma pessoa média, pode não conseguir diferenciar com clareza. Na esmagadora maioria dos casos, os titulares exercem seu direito solicitando a exclusão das informações sem, no entanto, compreender que, segundo a legislação, há uma distinção entre os direitos relacionados à anonimização e à eliminação de dados, bem como que a eliminação completa de dados muitas vezes não poderá ser realizada, inclusive para o cumprimento de obrigações legais e regulatórias ou o exercício regular de direitos. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normatizacao@anpd.gov.br)]

","615518": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): O artigo 18, § 2º da LGPD estabelece a possibilidade de o titular dos dados pessoais se opor a um tratamento específico realizado por um controlador quando a base legal para o tratamento dos dados pessoais não for o consentimento e quando, no seu entendimento, houver descumprimento da legislação. Segundo a visão da ABERT, se a alegação do titular for considerada legítima pelo controlador, o resultado prático desta ação consiste na interrupção do tratamento de dados pessoais do titular que vinha sendo realizado até então, bem como a suspensão de novas atividades de tratamento, paralisando quaisquer novos usos dos dados pessoais desse titular. Isso indica, inclusive, que o controlador talvez necessite realizar a eliminação de

dados pessoais, a depender da atividade de tratamento questionada. A eliminação, todavia, pode não ser a medida mais adequada caso a organização também utilize os dados para outras finalidades que não tenham sido objeto de oposição do titular. Nestes casos, o controlador deve se certificar de que os dados não serão utilizados para as finalidades às quais o titular se opôs, podendo prosseguir com outras atividades de tratamento realizadas com os mesmos dados e que tenham outras finalidades. [CONTINUA. Versão completa segue no documento complementar enviado ao endereço de e-mail indicado pela ANPD (normalizacao@anpd.gov.br)]

;"615523": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Não. A ABERT entende não haver um direito absoluto que implique na eliminação automática dos dados pessoais tratados pelos agentes de tratamento, ainda que com base na revogação do consentimento do titular. Como se sabe, quando o titular revoga seu consentimento para o tratamento de dados pessoais, pode também solicitar a eliminação desses dados, com algumas exceções. No entanto a LGPD nos parece clara ao prever que a eliminação e a revogação do consentimento são direitos distintos e que a realização deste não implicará, automaticamente, na execução daquele (vide, por exemplo, art. 8º, §5º, da LGPD). A revogação do consentimento pelo titular possui efeitos não retroativos, mas, sim prospectivos (ex-nunc), não gerando, portanto, automaticamente, o dever de eliminação dos dados pessoais tratados com base nesse consentimento. É sempre necessária solicitação expressa do titular, a qual será avaliada, e que, eventualmente, poderá não ser atendida. Isso porque o atendimento a uma solicitação de eliminação dos dados pessoais tratados com o consentimento do titular implica na exclusão de tais informações de banco de dados ou sistemas, o que pode gerar consequências gravosas caso não seja avaliada a pertinência de manutenção desses mesmos dados pessoais por outros motivos, particularmente em razão de obrigações legais, cumprimento de contratos, exercício regular de direitos ou outras razões. Em muitos cenários, o consentimento se refere apenas a finalidades determinadas, e não se aplica para todos os tratamentos realizados pelo controlador, justificando-se assim a manutenção desses dados para outras finalidades vinculadas a esses outros tratamentos.

;"615521": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Na visão da ABERT, a requisição de eliminação de dados pessoais tratados sob o amparo de consentimento anteriormente manifestado não deve afetar os tratamentos realizados até a revogação do consentimento, os quais ficam ratificados de acordo com o art. 8º, §5º. Ainda que o titular requeira expressamente a eliminação de seus dados pessoais tratados com base em consentimento fornecido para finalidade específica, há de ser avaliado pelo controlador eventual dever de retenção dos dados por obrigação legal ou regulatória, outras finalidades previstas no artigo 16 da LGPD, ou, ainda a utilização dos dados afetados com base em outras hipóteses legais.

;"615617": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): No entendimento da ABERT, decisão automatizada consiste no tratamento de determinado conjunto de dados por um software, o qual identifica, correlaciona e analisa certas informações sobre determinado indivíduo sem intervenção humana. A partir destas informações, esse mesmo software toma uma decisão acerca do (ou associa um determinado predicado ao) indivíduo em questão. Evidentemente, pode haver cenários em que uma decisão seja tomada por humanos a partir de tratamento automatizado (por exemplo, criação automática de score de crédito utilizado para manualmente se decidir pela concessão de empréstimo ou não). Nesse caso, estaríamos falando de uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais, mas não de uma decisão automatizada.

;"615618": "Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Quando há consequências relevantes para o

titular de dados pessoais, notadamente impossibilidade de contratar produtos ou serviços, ter acesso negado a serviços essenciais, bem como em cenários de análise de sua situação de saúde e crédito. A simples existência de perfis, por exemplo, não deve ser interpretada como uma atividade que afeta significativamente o interesse do titular; é preciso compreender a finalidade da criação desse perfil.”; 615619: “Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Para a ABERT, os desafios práticos incluem a compreensão do conceito de “direito à revisão”. Esse direito não significa que os titulares possam forçar a mudança de uma decisão automatizada, mas sim de solicitar que esta seja revista. Ou seja, não é o direito de obrigar que uma decisão diferente seja tomada, senão de solicitar que a decisão automatizada original seja avaliada e, caso erros sejam efetivamente constatados, que ela possa ser modificada. Deste modo, em diversos cenários, não haverá nada a ser modificado na decisão original. Em outras palavras, o direito à revisão não implica o direito de obter um resultado diferente nem de controlar o resultado do tratamento e a decisão tomada; trata-se do direito de compreender os motivos pelos quais uma determinada decisão foi tomada, sem que isso implique obrigar o controlador a alterar a decisão. Por fim, a ABERT ressalta que o direito à revisão de decisões automatizadas não poderá ser exercido quando a automatização for acompanhada por supervisão humana, caso em que já conta, ao longo do seu processo, com algum tipo de curadoria. Nestes casos, sequer há de se falar em direito à revisão, dado que, conforme o art. 20 da LGPD, o titular “tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais”. ”; 615620: “Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT): Sim, para que o titular possa solicitar a revisão mencionada no caput do artigo 20 da LGPD, a ABERT entende que ele deve ter condições de demonstrar que a decisão automatizada afeta, de modo significativo, seus interesses. Caberá aqui, portanto, que o titular justifique o pedido de revisão, explicitando o porquê de a decisão afetar significativamente seus interesses e qual é alteração pretendida. Evidentemente, quanto maior for a importância dos direitos em jogo relativos à decisão automatizada, mais simples será ao titular fazer essa demonstração. Não parece razoável imaginar que o controlador tenha como atender bem à solicitação do titular se não souber ao certo de qual revisão está se tratando. Em primeiro lugar, é possível que decisão cuja revisão esteja sendo solicitada não seja resultante de tratamento automatizado. Em segundo, o controlador precisa entender qual a revisão pretendida. Em alguns casos pode ser evidente que o titular deseja que uma negativa de crédito seja revertida em concessão de crédito, mas essa é uma situação simples que nem sempre se repetirá. Em suma, parece necessário que todo pedido conte com alguma descrição de seu objeto para que se possa respondê-lo adequadamente. Pedidos de revisão do tipo “solicito revisão da decisão automatizada destinada a definir meu perfil pessoal” tendem a levar a uma resposta do mesmo calibre. Essa é uma situação de ‘perde-perde’, que leva à ineficiência, na qual o controlador será impelido a uma resposta padrão, o titular não conseguirá alterar a situação em que se encontra e tampouco a ANPD terá bases sólidas para intervir se assim for necessário. ”

{ "615450": "Sem contribuições.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "Sem contribuições.", "615484": "Para assegurar a efetividade na comunicação entre o titular e o agente de tratamento, sugere-se que o canal de atendimento contenha as seguintes características: Seja disponibilizado em vários locais de fácil acesso, como por exemplo no site do agente de tratamento e na Política de Privacidade do Site; Contenha linguagem simples e de fácil entendimento, ou seja, o titular deve ser capaz de entender que o canal de contato é designado para o atendimento dos direitos dos titulares; Solicite os dados necessários para confirmar a identidade/legitimidade dos titulares, para que a solicitação seja válida; Seja objetivo, ou seja, o titular deve conseguir solicitar os seus direitos de maneira rápida e eficaz. A título exemplificativo, sugere-se que o titular não ultrapasse tempo maior que 5 (cinco) minutos para realizar a solicitação. Dessa forma, caso o canal seja acessado através de formulário, recomenda-se que o formulário não seja muito extenso, de modo a impedir ou onerar o titular no exercício de seus direitos; Por fim, recomenda-se que sempre seja fornecida uma resposta ao titular, mesmo em caso de negativa/impossibilidade de atendimento. ", "615485": "Sem contribuições.", "615486": "Entende-se que não seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor (SAC), estabelecido pelo Decreto nº 11.034/2022. Isso porque o Decreto do SAC estabelece a necessidade de atendimento telefônico de forma obrigatória, bem como que o atendimento não está condicionado ao fornecimento de dados pelo titular. Entende-se que estabelecer a obrigatoriedade de atendimento telefônico para atender as solicitações dos titulares trata-se de uma prática onerosa para as empresas que deverão disponibilizar uma linha de telefone específica de acesso ininterrupto durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, conforme dispõe o Decreto em seu artigo 4º, sendo que existem outras formas mais eficazes de atendimento a titular de dados, como e-mail ou chat de atendimento ou formulário de solicitação. Ainda, para que seja possível atender os direitos dos titulares em conformidade com a LGPD, é necessário comprovar a legitimidade do titular, tendo em vista que os direitos devem ser exercidos pelo próprio titular ou pelo seu representante legal devidamente constituído. Dessa forma, o atendimento não condicionado ao fornecimento de dados do titular macula a LGPD, na medida em que os agentes de tratamento precisam se certificar de que aquela solicitação é legítima, sob pena de ocorrência de incidente de segurança com dados pessoais. Por fim, o Decreto estabelece, em seu Art. 13, que as demandas serão respondidas no prazo de 7 (sete) dias corridos. Tal prazo não pode ser considerado como um prazo razoável para atender os direitos dos titulares, tendo em vista que alguns direitos necessitam de prazos maiores para serem atendidos de modo eficaz. ", "615487": "Sem contribuições.", "615491": "Sim. Primeiramente vale ressaltar que os direitos dos titulares não são absolutos e os agentes de tratamento podem se negar a atender o direito de confirmação da existência de tratamento, a depender do caso concreto. A título exemplificativo, pode-se citar as seguintes hipóteses: Ausência de comprovação da legitimidade do titular; Cumprimento de obrigação legal ou determinação judicial que determine o dever de sigilo; Existência de investigações ou processos judiciais em caráter sigiloso; Existência de pedidos repetitivos ou excessivos, configurando-se como abuso de direito; ou Identificação de má-fé ou práticas ilícitas nas solicitações de atendimento aos direitos. ", "615492": "Sem contribuições.", "615489": "Sem contribuições.", "615490": "Sem contribuições.", "615494": "Sem contribuições.", "615493": "Sem contribuições.", "615502": "Sem

contribuições.;"615501": "Sem contribuições.;"615505": "Sem contribuições.;"615503": "Sem contribuições.;"615504": "Sem contribuições.;"615511": "Sem contribuições.;"615514": "Sem contribuições.;"615513": "Sem contribuições.;"615512": "Sem contribuições.;"615517": "Sim, entende-se que é necessário que o titular de dados fundamente a sua solicitação. No momento do pedido de eliminação, bloqueio ou anonimização dos dados, o titular deve fornecer ao agente de tratamento as informações necessárias para que ele consiga analisá-las de forma efetiva e entender se realmente existe alguma desconformidade com a LGPD e tomar as providências necessárias em caso de irregularidade ou legitimidade do titular em exercer o pleito. Ainda, ressalta-se que a instrução do pedido do titular traz uma maior segurança jurídica para todas as partes envolvidas, na medida em que afasta o envio de inúmeras solicitações infundadas de titulares que possuem apenas o objetivo de ingressar com ações na via judiciária e agir de má-fé em relação aos agentes de tratamento. Tal medida otimiza a atuação dos agentes de tratamento e permite um atendimento de maior qualidade aos titulares de dados que, de fato, pretendem exercer seus direitos de maneira bem-intencionada, valorizando o caráter colaborativo entre titular e controlador de dados. ";615516": "Sem contribuições.;"615518": "Sem contribuições.;"615523": "Sem contribuições.;"615521": "Sem contribuições.;"615617": "Sem contribuições.;"615618": "Sugere-se que os critérios para determinar quando um interesse está sendo efetivamente afetado se assemelhe aos critérios já estabelecidos pela ANPD em sua página sobre o relatório de impacto à proteção dos dados pessoais (RIPD). São eles: Quando o tratamento puder impedir o exercício de direitos; Quando o tratamento puder impedir a utilização de um serviço; Quando o tratamento puder ocasionar danos (materiais e/ou morais) aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. ";615619": "Sem contribuições.;"615620": "Sem contribuições."

{ "615450": "ABRADEE: A princípio entendemos que sim, faz sentido.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "ABRADEE: 1: Em casos de sobreposição regulatória que apresente prazos conflitantes para atendimento a um mesmo tipo de demandas ao titular, quer seja consumidor ou outra categoria de titular, face aos desafios regulatórios de cumprimento a legislação, sugere-se que devam ser considerados os prazos previstos na LGPD ou aqueles que tenham sido objeto de regulamentação pela ANPD. 2: Com relação ao início da contagem do prazo de atendimento às demandas do titular, sugerimos que seja considerado para início de contagem a inexistência de pendências do titular no processo de validação de identidade. ", "615484": "ABRADEE: 1. Validação positiva do titular; 2. Quando necessário, envio de informações adicionais (quando necessárias e solicitadas ao titular informações adicionais, importante que ele as forneça para que seja possível a verificação completa da solicitação e atendimento desta); ", "615485": "ABRADEE: Necessária regulamentação sobre obrigação do operador comunicar ao Controlador sobre eventual exercício de direito de titular recebido em seu canal, além de providenciar e enviar, quando o caso, as informações/documentações necessárias para que o Controlador possa efetivamente atender a demanda do titular. Nas situações em que o operador deixar de comunicar o controlador ou se negar a fornecer as informações e documentações necessárias para fins de atendimento ao requerimento do titular ou deixar de apresenta-las em tempo hábil ao Controlador, responderá o operador nos termos do art. 42, §1º, I da LGPD, devendo, em caso de processo de fiscalização e sancionador, tal fato ser considerando uma agravante ao Operador e, quando comprovado o atendimento pelo Controlador de todas as medidas por ele possível para atendimento ao titular, atenuante ao Controlador, nos termos da Res. 04 da ANPD ", "615486": "ABRADEE: Entendemos que sim e que seria muito importante um Decreto específico e com regras claras para os canais de atendimento de exercício de direito dos titulares.", "615487": "-", "615491": "-", "615492": "-", "615489": "ABRADEE: Necessária regulamentação sobre obrigação do operador comunicar ao Controlador sobre eventual exercício de direito de titular recebido em seu canal, além de providenciar e enviar, quando o caso, as informações/documentações necessárias para que o Controlador possa efetivamente atender a demanda do titular. Nas situações em que o operador deixar de comunicar o controlador ou se negar a fornecer as informações e documentações necessárias para fins de atendimento ao requerimento do titular ou deixar de apresenta-las em tempo hábil ao Controlador, responderá o operador nos termos do art. 42, §1º, I, da LGPD , devendo, em caso de processo de fiscalização e sancionador, tal fato ser considerando uma agravante ao Operador e, quando comprovado o atendimento pelo Controlador de todas as medidas por ele possível para atendimento ao titular, atenuante ao Controlador, nos termos da Res. 04 da ANPD. ", "615490": "ABRADEE: Entendemos serem os Dados cadastrais", "615494": "ABRADEE: Finalidade do tratamento, Base legal, categoria dos titulares, categoria dos dados pessoais (comuns ou sensíveis), finalidade da decisão automatizada.", "615493": "ABRADEE: Sim", "615502": "-", "615501": "-", "615505": "-", "615503": "ABRADEE: Sim", "615504": "-", "615511": "ABRADEE: Sugerimos que sejam considerados os parâmetros regulatórios para fins de cadastramento e atualização cadastral já previstos, bem como que na ausência de atualização cadastral por parte de clientes, não possam os Controladores serem responsabilizados por aquele dado de sua base estar incompleto, inexato ou desatualizado. ", "615514": "ABRADEE: Quando o titular não for validado no processo de validação positiva ou, quando o for, nos casos em que o

dado corrigido precise estar igual ao de bases oficiais, como por exemplo, nome completo com documentos oficiais emitidos por órgãos públicos. ","615513": "ABRADEE: 1. Casos em que dados sejam compartilhados com controladores autônomos por força de obrigação legal regulatória; 2. Quando o tratamento envolver muitos agentes de tratamento ou alto volume de dados, trazendo esforço desproporcional para o Controlador; 3. Impossibilidade de comunicação simples, como e-mail, por exemplo, com outro agente de tratamento. ","615512": "ABRADEE: Não desde que o titular seja validado no processo de validação positiva e, que, assim o sendo, não deixar de apresentar, quando necessário, documentos oficiais emitidos por órgãos públicos. ","615517": "ABRADEE: Sim, uma vez que a solicitação do titular deverá demonstrar a razão pela qual ele entende que o tratamento se deu de forma irregular e apresente comprovações de suas alegações, como por exemplo, prints de tela, mensagens recebidas, entre outros. Tal fato se faz necessário até para possibilitar ao encarregado de proteção de dados avaliação do requerimento e, se for o caso, adoção de providências necessárias junto as áreas responsáveis de suas organizações. ","615516": "ABRADEE: Sim, poderiam ser alternativas, pois para o titular o efeito será o mesmo na prática, qual seja, o tratamento não mais ocorrerá. Além disso, a depender do tipo de sistema utilizado para armazenamento dos dados, não se faz possível tecnicamente a eliminação dos dados, mas tão somente a anonimização. ","615518": "ABRADEE: Neste caso, o Controlador adotará providências para que o tratamento seja corrigido ou, não sendo possível, excluído. No caso do requerimento ser objeto de processo de verificação de verossimilhança das alegações, será concedido ao Controlador o direito ao contraditório e ato contínuo, caso ANPD entender que o requerimento for legítimo, deverão ser aplicadas medidas orientativas ao Controlador. ","615523": "ABRADEE: Não, a revogação implicaria em cessar o tratamento, mas não na eliminação dos dados, pois estes ainda podem ser utilizados para finalidades diversas autorizadas por bases legais diversas e pelo período de retenção prevista para tanto, como no caso de armazenamento dos dados para exercício de direito em processos judiciais ou administrativos. ","615521": "ABRADEE: Os efeitos não seriam retroativos, mas o requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado deverá acarretar a efetiva eliminação dos dados ou em sua anonimização. ","615617": "ABRADEE: Entendemos que uma decisão automatizada é tomada exclusivamente por meios automatizados, sem intervenção humana. Nesse caso, a decisão é feita por algoritmos ou sistemas de inteligência artificial, sem a interferência de um ser humano no processo de tomada de decisão. Por outro lado, entendemos que uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é aquela em que a análise e a conclusão são feitas exclusivamente com base nas informações coletadas e processadas automaticamente, sem a intervenção de um indivíduo no processo de tomada de decisão. Exemplos disso podem incluir a avaliação do perfil ou comportamento, com base em dados pessoais, para determinar aspectos como crédito, capacidade de pagamento, perfil de consumo, etc. ","615618": "ABRADEE: (i) Sempre que afetar direito fundamental do titular; (ii) Quando não for possível garantir o atendimento ao princípio de autodeterminação informativa; (iii) possibilidade de discriminação em relação ao titular dos dados, por exemplo. ","615619": "ABRADEE: (i) Atender plenamente o direito de revisão sem comprometer a garantia de sigilo aos segredos industrial e comercial previstos na lei; (ii) Estabelecer critérios objetivos de auditoria no que tange as decisões automatizadas; (iii) Distinguir o que é processo automatizado, que é a forma de executar um processo, da decisão automatizada de fato; (iv) Justificar critérios de negócio, que podem ser excludentes, de critérios discriminatórios, frente à interpretação dos titulares. ","615620": "- "

{“615450”:"A ABRANET entende que, ainda que à primeira vista possa parecer adequada a transposição dos prazos da Lei de Acesso à Informação (LAI) aos prazos da LGPD, em razão da aparente proximidade do exercício destes direitos, na prática, percebe-se a irrazoabilidade destes prazos no âmbito dos direitos dos titulares. Isso porque, ao contrário da LAI que somente prevê uma espécie de direito – o direito de acesso à informação –, a LGPD dispõe sobre uma miríade de direitos mais complexos e completamente distintos entre si, nomeadamente, direito de acesso, confirmação, correção, anonimização, eliminação, portabilidade, informação sobre entidades com as quais o dado foi compartilhado, revogação do consentimento e revisão de decisões tomadas unicamente com base em tratamentos automatizados. Desta forma, considerando o escopo restrito da LAI e necessidade de implementação de procedimentos, técnicas e ferramentas muito mais complexos no âmbito da LGPD entende-se que aplicar a mesma lógica pode levar a resultados indesejados. Acresce-se a esse cenário as diferenças intrínsecas entre agentes públicos (que estão sujeitos à LAI) e privados: considerando a multiplicidade de formas de organização empresarial no âmbito privado, variando de micro e pequenas empresas a multinacionais, é possível que, ao se adotar os procedimentos da LAI, não seja possível que essa gama diversa se adapte aos prazos estabelecidos. Por exemplo, a exclusão ou correção de dados cujos servidores de armazenamento estejam fora do país e dependam de autorização hierárquica pode ser mais morosa. Vale observar que o GDPR europeu prevê um prazo de 30 dias para o cumprimento dos direitos dos titulares. Ou seja, mesmo a União Europeia, referência em proteção de dados pessoais, confere prazo bem maior para o cumprimento das obrigações. Por todo exposto, a ABRANET considera benéfico e adequado a implementação de um prazo de, pelo menos, 60 dias.”,b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?:“Para fins de diferenciação na definição de prazos, conforme apregoa o §4º do art. 19, entende-se que seria adequado considerar tanto a complexidade do tema sobre qual versa o direito (ou seja, os fatores que dificultariam ou retardariam o atendimento ao direito) quanto os fatores ligados à capacidade dos agentes de determinado setor em atender aquela determinação. Nesse sentido, menciona-se como relevante a complexidade dos direitos, o volume de dados tratados, a quantidade de tipos de dados tratados, a existência de regulamentação (setorial ou não) incidente sobre os dados tratados e sobre as atividades de tratamento dos agentes – fatores que, conforme exigência legal de diligência no tratamento destes dados, poderiam dificultar ou atrasar a observância – a existência de autoridades setoriais que possam influir sobre o exercício dos direitos, entre outros. Ainda, entende-se que seria prudente considerar, sobretudo, a estrutura da cadeia produtiva em relação aos dados e a quantidade de agentes distintos que necessariamente serão envolvidos nas atividades de tratamento – cenários, por exemplo, em que o cumprimento do direito demanda acionar muitos operadores certamente implicarão maior demora no cumprimento. Por fim, importante que sejam ratificados os prazos diferenciados previstos no Regulamento de Agentes de Pequeno Porte, que estabelece a concessão de prazo em dobro para estes agentes no atendimento das solicitações dos titulares.”,“615484”:"O principal é que o canal esteja adequado pensando no relacionamento já existente entre titular e agente de tratamento. Exigir, por exemplo, que uma rede social, que se relaciona inteiramente de forma online com o titular, tenha um canal por telefone não faz sentido para o próprio usuário. Além disso, entende-se relevante que o canal se atente para algum mecanismo de verificação da identidade do titular, até para que se

garanta que o direito está sendo exercido por uma pessoa que efetivamente está apta a exercê-lo.";"615485": "A responsabilidade do operador pelo atendimento dos direitos dos titulares dependerá: (i) das responsabilidades estabelecidas contratualmente ou negocialmente entre o controlador e operador; (ii) do domínio da situação de fato – ou seja, a influência do operador no exercício e atendimento dos direitos dos titulares; e (iii) da existência e do cumprimento das instruções do controlador pelo operador. Sabe-se que o regime de responsabilização adotado pela LGPD prioriza a responsabilidade dos controladores sem, no entanto, eximir os operadores de responder por eventuais descumprimentos e desconformidades com as instruções do controlador e com a própria lei, hipóteses nas quais poderão ser responsabilizados. Nesse sentido, em relação aos direitos dos titulares, deve ser facultado aos agentes de tratamento estabelecerem, conforme as peculiaridades do caso concreto, como deverá ser a cooperação e quem será responsável por cada aspecto do atendimento dos direitos dos titulares. A ABRANET entende que as partes dos contratos (controlador e operador) são as mais bem posicionadas para fazer tal definição no caso concreto, sendo desnecessária estipulação adicional da ANPD, na medida em que a LGPD já é clara em incluir os operadores na cadeia de responsabilização.";"615486": "A ABRANET entende como inviável a aplicação de diretrizes e procedimentos análogos ao referido decreto, em razão das diferenças intrínsecas entre as exigências do decreto – que é informado e inserido dentro do sistema consumerista, exclusivamente para agentes de setores regulados – e o sistema de proteção de dados e a realidade dos agentes de tratamento. Nesse sentido, menciona-se a impossibilidade e irrazoabilidade da aplicação, por exemplo, dos arts. 4º e 5º do decreto, que dispõem sobre a obrigatoriedade do atendimento telefônico. Diversos serviços ofertados a titulares de dados não são comumente oferecidos por meio telefônico – por exemplo, o acesso a uma rede social é feito por meio de aplicativo/browser –, portanto a alteração do modal de atendimento para o modal telefônico tende a ser contraintuitivo e mais oneroso para o titular. Ainda, é importante frisar que as equipes de SAC são responsáveis pelo atendimento ao consumidor sobre assuntos distintos, de fato ou de direito, o que justifica a alocação de recursos e pessoal para robustecer esse atendimento. Já os times responsáveis pelo atendimento ao titular de dados, cujo foco é mais especializado e técnico, geralmente resumem-se a uma equipe de pessoas ou, ainda, a uma única pessoa, geralmente pessoa física (“encarregado”). No entanto, apesar de menores, estes últimos possuem desafios ligados não só ao atendimento do titular como também de adequação geral à LGPD, evidenciando a diferença de escopo entre um e outro. Por fim, os prazos apontados no decreto (7 dias corridos) são inviáveis e demasiadamente exíguos para o atendimento dos direitos dos titulares, conforme mais bem explicitado na pergunta “a”.";"615487": "A ABRANET entende que não existe um modelo único que pode ser considerado paradigmático, até porque uma das premissas do atendimento aos direitos do titular é que ele seja adaptado à situação concreta de tratamento e à relação existente entre agente e titular. Assim, necessariamente modelos diversos serão necessários. De toda maneira, entende-se que privilegiar mecanismos de atendimento online, até pensando na factibilidade de cumprimento de alguns direitos, como portabilidade, é o ideal.";"615491": "A ABRANET entende que deve ser excetuada o direito de confirmação da existência do tratamento, quando (i) há obrigação judicial ou legal de sigilo/confidencialidade, (ii) o titular está sendo investigado por fraude, (iii) há comprometimento do segredo comercial e industrial e (iv) há impossibilidade material ou dificuldade exorbitante em se determinar tal informação. Nesse sentido, as hipóteses de exceção ao exercício do direito do titular serviriam como uma baliza adequada e suficiente para salvaguardar o interesse público e empresarial, sem comprometer o exercício legítimo do direito de confirmação da

existência do tratamento nas demais hipóteses. Ademais, como referência, a regulação europeia prevê hipóteses excepcionais para o não fornecimento de informações ao titular. O art. 14 do GDPR, por exemplo dispõe que, quando os dados utilizados não forem recolhidos junto do titular, é possível que o responsável pelo tratamento não forneça informações quando (i) “o titular dos dados já tenha conhecimento das informações”; (ii) se comprove a impossibilidade de disponibilizar a informação ou que o esforço envolvido seja desproporcionado; (iii) a obtenção ou divulgação dos dados estejam expressamente previstas na legislação interna, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; e (iv) existirem obrigações legais que limitem informação sobre o tratamento, incluindo confidencialidade e sigilo. Desse modo, a ABRANET entende que tais exceções previstas na legislação europeia também poderiam ser adotadas no Brasil.

,"615492": "Quanto aos dados de identificação do controlador, devem ser fornecidas as informações de identificação previstas no art. 9º, incisos III e IV da LGPD. Em casos de uso compartilhado dos dados pessoais, em primeiro lugar, destaca-se que nem toda hipótese de compartilhamento ensejará o fornecimento aos titulares, de forma detalhada, de informações, por exemplo, compartilhamentos dentro do mesmo controlador. Para a identificação dos controladores, é suficiente e útil ao titular compartilhar informações gerais sobre o tratamento, a finalidade (de forma geral), e o tipo de entidade receptora ou fornecedora dos dados de uso compartilhado. Há razões suficientes para não se compartilhar a denominação social e o CNPJ dos parceiros no uso compartilhado, tanto em razão de segredo industrial e comercial quanto em razão da segurança dos titulares, uma vez que possíveis agentes maliciosos que conheçam vulnerabilidades destes parceiros poderão utilizar-se dessa informação para vulnerar a segurança dos dados financeiros dos titulares.

,"615489": "A ABRANET entende que suas colocações no item “1, d” auxiliam a responder esse questionamento.”

,"615490": "A ABRANET considera suficiente para fins do art. 19, I da LGPD a disponibilização de dados que possam ser transmitidos de maneira inteligível, tendo em vista os mecanismos e o aparato técnico do responsável pelo tratamento de dados naquele momento. Dessa forma, entende como razoável o fornecimento das seguintes informações: (i) confirmação da existência de tratamento, (ii) dados fornecidos pelo titular no cadastro ou nas interações cadastrais (como alterações e complementações nos campos específicos) e (iii) informações mínimas e dados relacionados aos produtos e serviços contratados ou utilizados pelo titular.”

,"615494": "Entende-se que as informações mínimas e suficientes para a transparência ativa são aquelas apresentadas pelo art. 9 da LGPD, com ressalvas ao item V. Quanto aos critérios de decisões automatizadas, trata-se de tópico sensível, vez que muitas das vezes envolve, direta ou indiretamente, segredos industriais e de negócio. Nesse sentido, a ABRANET compreende que somente deverá ser exigível dos agentes de tratamento a disponibilização de informações gerais e fundamentais do tratamento de dados pessoais com decisões automatizadas, restringindo-se às informações sobre a lógica geral do funcionamento e sobre as possíveis consequências esperadas das decisões. Para além da proteção dos direitos de propriedade intelectual do controlador, potencialmente afetados por essas informações, há a finalidade de proteger o sistema de combate às fraudes, algo de particular relevância para instituições financeiras.”

,"615493": "Considerando os diferentes custos associados à modalidade de disponibilização física (como custo de impressão, transporte, envio, entre outros), somados ao fato de que a LGPD expressamente define que o cumprimento do direito de acesso deve ser gratuito, bem como a suficiência e difusão de práticas digitalizadas hoje em dia, faz-se necessária uma reflexão sobre a necessidade da entrega dos relatórios em papel. Nesse sentido, a ABRANET entende que a ANPD poderia indicar como meio preferencial e padrão o

formato digital, tendo em vista a eficiência do processo. Caso o titular solicite por meio impresso, deverá indicar expressamente a escolha ao agente de tratamento, que deverá analisar a adequação e relevância do pedido."615502": "Em primeiro lugar, há de se salientar que, apesar de previsto na agenda regulatória, a portabilidade em si (ou seja, o que constitui o direito e seus precisos contornos) nunca foi regulamentada pela ANPD. Para a melhor compreensão, regulamentação e observância deste direito pelos agentes de tratamento, é necessário que a ANPD estabeleça, de forma clara, o que constitui a portabilidade, quais são os agentes sujeitos (ou seja, quem deve enviar dados para quem, se somente para empresas atuantes no mesmo ramo, para fornecedores ou para qualquer um, independente da ligação na cadeia produtiva), quais são os dados efetivamente portáveis (por exemplo, há amplo debate sobre se dados inferidos pelo agente de tratamento estariam sujeitos à essa regra) e os seus limites, e entre outros fatores basilares."615501": "Os desafios são inúmeros e extremamente complexos. Novamente, eles variarão enormemente a depender da definição adotada de portabilidade, como destacado na questão anterior. Cabe ainda destacar que a LGPD não fala em direito à interoperabilidade, mas sim à portabilidade, e essa é uma distinção importante de ser levada em consideração pela ANPD no processo de regulamentação. De toda forma, os desafios incluem a definição de padrões comuns de escopo, formato de dados, delimitação de escopo, setores aplicáveis, participantes obrigatórios, compatibilidade tecnológica, padrão de conexão entre sistemas/ferramentas e padrões e requisitos técnicos de implementação, como medidas de segurança e aquelas relacionadas à integridade dos dados. Ainda, adicionam-se às dificuldades os ônus e custos elevados relacionados à implementação em si, considerando também o esforço nada desprezível para que os dados e arquivos sejam convertidos em formato padrão."615505": "Para além da resposta ao item anterior, destaca-se que, de acordo com a experiência internacional, a estruturação de padrões pelo próprio setor privado no âmbito da portabilidade, é mais eficaz que legislações estritas e inflexíveis sobre o tema."615503": "Considerando os desafios tecnológicos apontados anteriormente, entende-se que tal proposta seria positiva, uma vez que reduz ou mitiga questões apontadas, sobretudo de compatibilidade de tecnologias, permitindo que, com a disponibilização para o titular de todos os seus dados, em formato interoperável, lhe seja conferida autonomia, que é o cerne da efetividade do direito à portabilidade. Desta forma, a ABRANET acredita que essa disponibilização seria suficiente e empoderaria o titular. Ademais, se e quando um padrão de interoperabilidade for definido, utilizá-lo também significaria o cumprimento do direito à portabilidade. Ressalta-se, porém, as inúmeras dificuldades no estabelecimento de tais padrões, bem como a já mencionada distinção entre portabilidade e interoperabilidade, que devem ser levadas em consideração pela ANPD em seu processo de regulamentação."615504": "Certamente é não só razoável, como necessário que o setor privado possa definir padrões de interoperabilidade específicos para certas atividades econômicas, e inclusive para certos segmentos ou setores. Novamente, porém, ressalta-se que o direito à portabilidade não é igual à interoperabilidade e que a complexidade em definir prazos para quaisquer adequações decorre de uma questão anterior, qual seja, definir com precisão quais são os destinatários das regras de portabilidade, o escopo de dados a serem portados etc. Haverá diferenças muito grandes do que constituiriam prazos razoáveis, a depender dessas definições e do nível de maturidade do setor."615511": "A ABRANET entende que, ainda que observado o princípio da boa-fé, o custo operacional atrelado ao direito de correção e o esforço necessário para a observância desse direito é alto, além do risco apresentado em caso de erro. Por isso, a ABRANET entende que esse custo e esse risco podem ser significativamente reduzidos se forem estabelecidos requisitos mínimos

para as solicitações. Nesse sentido, citam-se: (i) erro material prejudicial ou potencialmente prejudicial ao titular, conforme argumentado em solicitação do titular; (ii) dado desatualizado ou incompleto, conforme comprovado por titular. No caso de atividade reguladas, como mercado financeiro – que demanda uma diligência maior prevista em dispositivo legal – há de se observar as normas estabelecidas pelo regulador setorial, bem como as respectivas responsabilidades, que poderão ocasionar demanda por dados adicionais.

,"615514": "Entende-se que, para atividades reguladas, a não observância dos requisitos estabelecidos em lei pode ser suficiente para não acolher a declaração como suficiente. Nos demais casos, elenca-se: (i) incapacidade de o titular demonstrar legitimidade para o exercício do direito de correção; (ii) correções de natureza puramente subjetivas em dados que não estejam objetivamente incorretos, desatualizados ou incompletos e; (iii) alteração solicitada não corresponder aos elementos comprobatórios apresentados pelo titular em solicitação."

,"615513": "De início, considera-se que os casos de co-controladoria não ensejam necessidade de informação, nos termos do art. 18, §6º. Para demais situações, poderão ser critérios a serem considerados para fins de impossibilidade ou esforços desproporcionais: (i) atualidade do uso compartilhado – é possível que o uso compartilhado seja consideravelmente antigo, de modo que o controlador possa ter perdido contato ou este tenha deixado de existir, ou ainda que o uso compartilhado tenha sido realizado com vistas a uma única atividade de tratamento, já finda; (ii) quantidade de controladores no uso compartilhado – em casos em que múltiplos controladores utilizam os mesmos dados, é possível que a delimitação de cada um seja desproporcional para fins de atualização; (iii) viabilidade prática e os custos e recursos necessários para processamento da comunicação; (iv) volume, complexidade e quantidade dos tipos de dados objetos de alteração; (v) presença (ou não) de representante legal dos demais controladores no Brasil; e (vi) no caso de correção de dados, na relação de controlador/operador, quando o operador não precisar daqueles dados atualizados para as finalidades que foi contratado para cumprir – por exemplo, se o operador foi contratado para fazer uma entrega ao titular, e esta entrega já foi realizada, mas o titular mudou de endereço, não há razão para compartilhar os dados atualizados."

,"615512": "São casos em que o direito à correção pode ser negado (i) impossibilidade por lei, regulamento, decisão judicial ou administrativa que impeça a alteração dos dados; (ii) dados já excluídos e/ou anonimizados; (iii) se a alteração dos dados prejudicar exercício regular de direitos do controlador e; (v) alterações com objetivo fraudulento ou de má-fé."

,"615517": "A ABRANET entende ser necessária a fundamentação do requerimento pelo titular, comprovando a desnecessidade dos dados ou a excessividade/desconformidade do tratamento. A fundamentação é relevante para identificar a inadequação e eventualmente solucioná-la, para viabilizar a resposta por parte do agente de tratamento perante a solicitação, e, inclusive, para possibilitar eventual esclarecimento por parte do agente, em caso de negativa legítima da solicitação apresentada. Caso contrário, corre-se inclusive o risco de os agentes de tratamento receberem muitos pedidos infundados, o que prejudicaria enormemente o fluxo de suas atividades (inclusive aquelas de resposta a pedidos legítimos e relevantes de direitos dos titulares). É importante que sejam criados incentivos para que estes pedidos sejam feitos em casos em que o titular realmente tenha boas razões para crer que o tratamento usa dados desnecessários, é excessivo, ou em que há descumprimento de obrigação legal, a fim de proteger tanto os cidadãos quanto as atividades dos agentes de tratamento."

,"615516": "A ABRANET entende que a decisão de adoção do procedimento de anonimização ou eliminação cabe aos agentes de tratamento, que deverão considerar as situações específicas do caso, visto que os procedimentos são, conforme preconiza a própria LGPD, equivalentes no que diz respeito ao tratamento de dados

personais. Isto é, ambos encerram o ciclo de tratamento e afastam a aplicação da LGPD a partir daquele momento. "615518": "Depreende-se da redação no art. 18, § 2º, da LGPD que o direito de oposição ao tratamento estaria vinculado às hipóteses de dispensa do consentimento. Nestes casos observado o descumprimento de outras disposições da LGPD, notadamente os direitos do titular e os princípios da lei, o titular teria a prerrogativa de opor-se ao tratamento. O efeito prático do direito de oposição, uma vez verificada a legitimidade da alegação, seria a cessação do tratamento de dados pessoais fundamentado na hipótese de dispensa de consentimento. Por isso mesmo, é importante destacar que o atendimento à solicitação do titular por parte dos agentes de tratamento não deve implicar presunção imediata de descumprimento da LGPD ou ser entendido como reconhecimento do próprio agente de tratamento de que a LGPD foi descumprida. Primeiro porque é preciso que os incentivos aqui estejam alinhados – se todos os pedidos forem tratados com presunção de correção, os agentes de tratamento seriam colocados numa posição complexa, em que todos os esforços de adequação seriam presumidamente tomados como irrelevantes. Segundo, porque é relevante que os titulares não façam alegações de toda natureza, mas sim concentrem seus esforços em pedidos legítimos, cujo atendimento efetivamente permitirá um melhor atendimento aos seus direitos. "615523": "A ABRANET, em consonância com o estabelecido pelo art. 8º, §5º da LGPD, entende que a revogação do consentimento não implica automaticamente a exclusão dos dados tratados com base no consentimento anteriormente autorizado. Ainda, da redação do parágrafo depreende-se a existência de uma demarcação clara entre um evento e outro: “[...] ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação [...]”. Neste sentido, a exclusão deve ocorrer apenas mediante a solicitação expressa do titular, conforme o art. 18, VI, observadas as exceções para conservação dos dados previstas nos incisos do art. 16.”615521": "A ABRANET entende que, da interpretação do art. 8º, §5º da LGPD, a revogação do consentimento não implica automaticamente a exclusão dos dados, devendo estar vinculada ao requerimento expresso do titular. No entanto, apenas se o tratamento não possui nenhuma outra base legal para execução, a solicitação do titular deve ser atendida, caso o consentimento seja revogado e a eliminação de tratamentos anteriormente realizados amparados pelo consentimento revogado seja requerida. "615617": "A ABRANET entende que, primeiramente, esta diferença cogitada pela ANPD não encontra amparo legal. A LGPD não diferencia estas categorias de tratamento em qualquer momento. Mais importante, porém, é que a aplicabilidade de eventual diferenciação seria extremamente complexa. Se a diferença semântica entre os conceitos partir da premissa de que uma decisão automatizada é aquela de fato inteiramente feita de modo automático, enquanto uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais na realidade for uma decisão não inteiramente automatizada, mas informada exclusivamente por tratamento automatizado, seria de se questionar se essa segunda categoria sequer existe. Uma decisão tomada por uma pessoa e que considere única e exclusivamente uma variável é inviável, porque elementos múltiplos afetam o indivíduo nesse processo, muitos deles sequer cognoscíveis. A experiência daquela pessoa, seu contexto social, entre diversos outros fatores, sempre serão critérios relevantes para a tomada de decisão. Ou seja, entende-se que essa é uma diferença semântica que, para além de não encontrar amparo na LGPD, leva a problemas relevantes de aplicabilidade concreta. "615618": "A consideração semântica do conceito de interesse do titular em seu uso tradicional, sem qualquer tipo de qualificante, estende a aplicabilidade do direito e o ônus aos agentes. Para além disso, uma extensão indevida do conceito de interesse parece contrariar o próprio intuito da LGPD – afinal, se a premissa fosse que o titular

pudesse se opor irrestritamente a qualquer tratamento automatizado, a lei teria expressamente feito esta definição. Por isso, é fundamental restringir, para fins de razoabilidade, a interpretação para interesses legítimos, pactuados contratualmente ou tutelados por normas e regulamentações, de forma a limitar a confusão com o mero “aborrecimento” com as decisões. Além disso, a afetação do interesse deve ser justificada, ou seja, é importante que haja uma explicação razoável e concreta para tal. Um exemplo muito simples pode ajudar a concretizar a preocupação – se uma pessoa acessa uma rede social e vê um anúncio nessa rede sobre viagens para Barcelona, faz sentido dizer que seu interesse foi violado, caso ela preferisse visualizar viagens para o Rio de Janeiro? Certamente não é o caso, e não é isso que a LGPD visa tutelar. ”615619”:”Os principais desafios são: (i) volume dos dados – a depender do número de pedidos, o agente de tratamento pode em concreto ter que duplicar sua estrutura de tratamentos; (ii) proteção dos segredos de negócio - há a legítima preocupação de que eventual revisão ou explicação de decisões automatizadas possam expor segredos de negócio, tutelados por propriedade intelectual, a depender do nível de detalhamento exigido; (iii) prevenção à fraude e mecanismos similares – da mesma forma, expor os critérios utilizados para consideração da fraude pode ajudar golpistas e inutilizar o tratamento, fragilizando a segurança e usabilidade dos serviços.”615620”:”Entende-se como razoável que a negativa de direito ocorra quando o pedido não se enquadrar nos critérios apontados como “interesse afetado”, evidentemente, e quando incorrerem nos desafios apresentados. Ou seja, quando se tornar impossível a explicação sem prejudicar direito tutelado por propriedade intelectual ou quando se tratar de casos de prevenção à fraude.”

{ "615450": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Para que as companhias tenham segurança nas respostas, é fundamental que prazo pertinente a esse cenário diverso seja concedido, sob pena de tornar inviável o atendimento adequado. Deste modo, sugerimos o prazo de 1 mês, prorrogável por até 3 meses, nos termos do art. 12(3), do GDPR, o que recomendamos seja seguido como referência por esta Autoridade. ", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Os seguintes critérios devem ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD: (i) Teor da Solicitação - complexidade do pedido; (ii) Urgência do pedido; (iii) Impacto ao titular; (iv) Complexidade para a solução; (v) Tamanho do agente de tratamento; (vi) volume de titulares/dados tratados. Sobretudo no que se refere à declaração clara e completa presente no inciso II do art. 19, compreendemos que é pertinente prazo estendido, conforme critérios acima, tendo em vista a necessidade de apuração interna do agente de tratamento. ", "615484": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Canal de atendimento que possua: (i) Meios de identificação do titular; (ii) Linguagem simples e acessível para compreensão do titular; (iii) Canal eletrônico com boa usabilidade e direcionamento; (iv) gratuito; (v) seguro. ", "615485": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Sim, o operador possui responsabilidade na concretização dos direitos dos titulares, sobretudo em situações nas quais: (i) for diretamente acionado pelo titular, cooperando para indicação de correto canal junto ao controlador, se o caso; (ii) apoiando o controlador com subsídios implantação de medidas razoavelmente necessárias para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação pelo controlador. ", "615486": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Não, o tema deve ser tratado de forma diferenciada. Questões relacionadas ao atendimento ao consumidor poderão diferenciar-se em demasiado no tocante à natureza de requisições de titulares, sobretudo em determinados segmentos do mercado, como o setor da saúde. Algumas obrigações de difícil aplicação na norma requerem, por exemplo: (i) disponibilidade ininterrupta - durante vinte e quatro horas por dia, sete dias por semana; (ii) pluridade de canais; (iii) obrigatoriedade de atendimento telefônico; (iv) acesso inicial não condicionado ao fornecimento prévio de dados pelo consumidor, (v) prazo de atendimento de demandas no prazo de sete dias corridos, contado da data de seu registro; (vi) horário de atendimento não inferior a oito horas diárias dentre outras. As justificativas incluem: (i) não é necessário um serviço de atendimento ininterrupto para cumprir com a LGPD; (ii) o atendimento ao cliente pode ser feito durante o horário comercial e por diferentes canais, como e-mail; (iii) a identificação prévia do titular de dados é recomendada para direcionar o atendimento e apurar violações; (iv) o tempo mínimo de funcionamento do SAC pode variar de acordo com a natureza dos serviços oferecidos pelas empresas, e se diferencia do prazo já previsto na LGPD (15 dias); (v) o contato direto com o atendente nem sempre é necessário, e o tempo máximo de espera para atendimento da solicitação depende de análises específicas; (vi) pode ser necessário solicitar repetição da demanda para coletar informações necessárias junto ao titular; (vii) meios digitais podem ser suficientes para atender solicitações dos titulares; (viii) o prazo de 5 dias corridos para atender solicitações pode ser curto, especialmente considerando o histórico do titular. ", "615487": "[Contribuições em nome da Associação

Nacional de Hospitais Privados - ANAHP] Consideramos que o modelo de Ouvidoria do Gov.br é um sistema que pode ser utilizado como paradigma no tocante ao setor público. Inclusive, a indicação de métricas para a calcular a efetividade dos atendimentos realizados e a satisfação do público. No tocante ao setor privado, uma das alternativas é utilizar os indicadores e as métricas implementadas pelo IBRC - Instituto Brasileiro de Relacionamento com o Cliente. ","615491":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Eventualmente, quando o tratamento de dados pessoais estiver relacionado a procedimentos de investigação e/ou auditorias, a fim de proteger o processo, seria possível a negativa. Quando o titular não tenha comprovado a sua identidade ou não apresentado informações mínimas para o cumprimento do pedido; quando o titular atuar de má-fé (apresenta solicitações repetitivas ao controlador sem justificativa aparente.");615492":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Razão social, CNPJ, Nome Fantasia e/ou Marca e DPO.";615489":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Cooperação na indicação de correto canal do controlador, se o caso ou apoio ao controlador com subsídios para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação.";615490":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] A declaração deve poder contemplar apenas os dados cadastrais (nos termos do artigo 11, § 2º do Decreto 8.771/2016) no formato em que se encontram, isto é, aqueles constantes no cadastro do titular junto à organização, se existentes, visto que tendem a ser os dados prontamente disponíveis para a organização fornecer aos respectivos titulares. ","615494":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Dados pessoais tratados para a tomada de decisão e finalidades do tratamento.";615493":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Sim, tanto a disponibilização digital quanto em formato de papel satisfazem os direitos do titular. No entanto, o fornecimento em papel deve considerar o volume de dados e ser oferecido apenas se o cliente não tiver acesso digital ou preferir o formato físico, com os custos repassados ao solicitante. A prioridade deve ser sempre o formato digital, dada a disponibilidade de meios tecnológicos seguros.";615502":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Telecomunicações e Setor Financeiro. No que se refere aos atores do segmento de saúde, incluindo entes públicos e privados, compreende-se que não há maturidade em processos que permita assegurar a Portabilidade na forma de dados interoperáveis no momento, considerando, dentre outros elementos, a sensibilidade, volumetria e formato dos dados.";615501":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Com referência ao setor da saúde, é possível citar: (i) Integrações entre plataformas que operam dados; (ii) formato válido de dados; (iii) qualidade de dados; (iv) operações e estrutura de tecnologia; (v) multidisciplinariedade de sistemas. Atualmente existem diversos mecanismos de coleta dados, cada um com sua particularidade e operação. Para que a interoperabilidade de dados fosse realizado, deveria inicialmente existir uma padronização no formato de coleta de dados e armazenamento de metadados, bem como sanitização do conjunto para que todo ele permaneça legível. ","615505":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Prioritariamente o formato de dados, protocolos e terminologias comuns. Em seguida a padronização das ferramentas operadoras de dados, o caminho de transferência, o processo de transferência e, por fim, a sanitização das bases.";615503":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Sim.";615504":"[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Sim, é razoável que o setor privado possa definir os padrões de

interoperabilidade, por segmentos de atividade - pois cada cenário possui desafios específicos. O prazo deverá ser determinado de acordo com o mercado que o operador atua, sendo que, no tocante à área da saúde, compreende-se prazo inferior a 12 (doze) meses demasiado desafiador, sugerimos o prazo de, pelo menos, 05 (cinco) anos.

","615511": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Compreendemos que os seguintes aspectos devem ser observados: Dado Inexato: Quando contém informações incorretas, imprecisas ou desatualizadas. Isso pode ocorrer devido a erros de entrada de dados, falhas de comunicação ou mudanças nas circunstâncias que tornam as informações obsoletas. Dado Desatualizado: Quando as informações que ele contém estão obsoletas ou não refletem a situação atual. Isso pode ocorrer quando os dados não são atualizados regularmente para acompanhar mudanças no tempo, como atualizações de status, alterações de contexto ou novos desenvolvimentos. No que se refere ao contexto ou consideração situacional para enquadramento do dado, deve ser considerado o último registro do dado, com evidências de data.

","615514": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] A simples declaração do titular não seria suficiente nos casos de: (i) solicitação genérica, como, por exemplo, sem indicação do dado a ser corrigido e/ou onde consta desatualizado; (ii) solicitações de correção sem comprovação da identidade do titular; (iii) situações em que é necessária a validação/cadastro por meio de comprovação documental e não é apresentado o documento para correção/atualização.

","615513": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Os critérios objetivos para avaliar a impossibilidade ou o esforço desproporcional conforme o art. 18, §6º da LGPD envolvem: (i) considerações sobre a complexidade da infraestrutura dos agentes de tratamento envolvidos; (ii) formato dos dados (iii) padrão de interoperabilidade; (iv) tipo de solicitação, (v) implicações da não recepção pelos demais da solicitação e (vi) volume de agentes a serem comunicados. Por fim, é necessário levar em conta desafios para que seja informado ao outro controlador "imediatamente", conforme menciona a legislação - devendo a ANPD fornecer critérios mais claros quanto ao prazo fornecido.

","615512": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Em circunstâncias excepcionais, o direito de correção pode ser negado pelo controlador em situações em que o pedido de correção é feito para informações que não necessitam de alteração, como quando os dados estão corretos e precisos. Além disso, o direito de correção pode ser negado quando as correções demandam comprovação por meio de documentos, e o titular não forneceu a documentação necessária para comprovar a necessidade da correção.

","615517": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] É essencial que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado, pois isso possibilita aos agentes de tratamento a verificação de inconsistências internas, melhorando seus programas de governança ou de seus parceiros, fornecedores e demais agentes que realizam o tratamento em seu nome ou juntamente a eles. A fundamentação permite que o controlador analise as alegações do titular e ofereça esclarecimentos adicionais, se necessário, sobre o tratamento de dados considerados desnecessários, excessivos ou em desconformidade.

","615516": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Sim, considerando situações específicas, a anonimização e a eliminação podem ser adotadas alternativamente pelos agentes de tratamento. Respeitando os limites de finalidade do tratamento de dados, bem como os riscos de reidentificação e as possibilidades legais e regulatórias, essa alternativa pode ser aplicada, especialmente em setores sensíveis como o da saúde, onde essa flexibilidade pode promover a

inovação em ferramentas voltadas para a saúde. Além disso, essa escolha pode atender às solicitações dos titulares quanto à cessação do tratamento de seus dados pessoais, ressalvadas as hipóteses legais de exceções. A adoção de medidas de anonimização ou eliminação pode ser considerada de forma alternativa, levando em conta que a anonimização remove as características de dados pessoais, mitigando substancialmente os riscos para os titulares de dados. ";615518": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] É necessário que o agente de tratamento, mesmo agindo de boa-fé e tendo conhecimento da possível configuração de tratamento inadequado dos dados, se comprometa proativamente com as medidas necessárias para correção do processo e as devidas comunicações, se o caso. ";615523": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Não necessariamente. A revogação do consentimento do titular, conforme estipulado no art. 18, IX, da LGPD, não automaticamente exige a eliminação dos dados pessoais tratados com base nesse consentimento. O titular precisa expressar explicitamente o desejo de eliminar seus dados. Além disso, é importante considerar que os dados tratados até a revogação do consentimento são válidos e podem ser retidos por obrigação legal ou regulatória, como exceções previstas no art. 16 da LGPD e em normativas específicas. ";615521": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Considerando o art. 8º da LGPD, é importante observar que os tratamentos realizados sob o amparo do consentimento anteriormente manifestado podem ser mantidos pelos agentes de tratamento em determinados casos, conforme previsão legal e normativas setoriais. Por exemplo, a conservação de dados em órgãos e estudos de pesquisas clínicas, conforme o art. 16, inciso II da LGPD, e o Guia Orientativo para fins de Tratamento acadêmicos e para realização de estudos e pesquisas elaborado pela ANPD. Isso se deve ao fato de que certos tratamentos, como os dados clínicos em pesquisas, não podem ser removidos sem afetar o resultado estatístico da pesquisa. Assim, o direito de revogação do consentimento deve estar em consonância com as normas do setor e respeitar os limites previstos pela LGPD. ";615617": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Uma decisão automatizada geralmente implica que, embora o processo de tomada de decisão possa ser automatizado, ainda pode haver alguma forma de intervenção humana no processo. Isso inclui a definição dos critérios ou regras que o algoritmo deve seguir, revisão periódica dos resultados gerados pelo sistema automatizado ou a possibilidade de os indivíduos afetados contestarem a decisão e obterem uma revisão humana. Por outro lado, uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais implica que não há intervenção humana significativa no processo de tomada de decisão. Isso significa que a decisão é totalmente gerada pelo sistema automatizado, sem revisão ou intervenção humana durante todo o processo. ";615618": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Recomendamos que os elementos abaixo sejam considerados: 1 - Natureza dos direitos afetados: Avaliar se os direitos fundamentais ou interesses legítimos dos indivíduos estão sendo comprometidos, tais como privacidade, liberdade de expressão, liberdade de associação, entre outros. 2 - Gravidade do impacto: Determinar a gravidade do impacto sobre os indivíduos afetados, considerando se a decisão automatizada pode resultar em consequências significativas, como perda de oportunidades, discriminação, prejuízos financeiros ou reputacionais. 3 - Abrangência da decisão: Analisar se a decisão automatizada tem um alcance amplo e afeta um grande número de pessoas ou se é direcionada a indivíduos específicos. 4 - Transparência e explicabilidade: Verificar se os critérios e algoritmos utilizados na tomada de decisão automatizada são transparentes e compreensíveis, permitindo que as pessoas entendam como suas

informações foram usadas e como a decisão foi tomada. 5 - Possibilidade de contestação: Avaliar se as pessoas têm meios eficazes para contestar ou contestar a decisão automatizada, garantindo o direito de corrigir informações imprecisas ou contestar decisões injustas."615619": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD envolvem a complexidade dos algoritmos, a interpretação dos resultados, o acesso aos dados, o conhecimento técnico necessário, o tempo e recursos requeridos, bem como a efetividade das correções. Além disso, há o desafio de dar transparência ao titular de dados sobre os critérios utilizados no processo de decisões automatizadas, considerando que diferentes estruturas e sistemas podem envolver segredo de negócio das companhias. Além disso, importante que se defina que garantir a revisão nas decisões não garante mudança no resultado anteriormente tomado, a menos que haja alteração nos critérios utilizados pelos controladores ou dados novos e/ou atualizados. Superar esses desafios demanda uma abordagem colaborativa entre reguladores, profissionais da área, desenvolvedores de tecnologia e usuários finais para garantir que os direitos de revisão sejam efetivos e que as decisões automatizadas sejam justas, transparentes e precisas."615620": "[Contribuições em nome da Associação Nacional de Hospitais Privados - ANAHP] Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas. Isso pode ocorrer quando não houver cabimento nas hipóteses previstas no art. 20 da LGPD, que incluem afetação aos interesses, definição de perfil pessoal, profissional, de consumo, de crédito ou aspectos da personalidade, bem como eventualmente normas setoriais relacionadas à matéria. Além disso, elencamos algumas circunstâncias em que o direito de revisão podem vir e ser negados: 1 - Obrigação legal: Se a decisão automatizada for exigida ou autorizada por lei, o controlador pode não ter a capacidade de alterá-la ou revisá-la. 2 - Risco à segurança: Se a divulgação das informações utilizadas na decisão automatizada representar um risco à segurança, integridade ou confidencialidade dos sistemas ou dados, o direito de revisão pode ser negado. 3 - Proteção de direitos de terceiros: Se a revisão da decisão automatizada violar os direitos ou interesses legítimos de terceiros, como segredos comerciais ou propriedade intelectual, o controlador pode ser impedido de realizar a revisão. 4 - Decisões manifestamente infundadas: Se a solicitação de revisão for considerada manifestamente infundada ou excessiva, o controlador pode recusar a revisão, desde que comunique claramente os motivos para tal decisão. É importante observar que, mesmo nessas circunstâncias, o controlador deve informar claramente os motivos para negar o direito de revisão e fornecer mecanismos para que os indivíduos contestem essa decisão, quando aplicável."

{ "615450": "[Brasscom] Primeiramente, é importante destacar que, no que se refere aos incisos I e II do artigo 19 da LGPD, já existem prazos estabelecidos para a resposta do controlador. Assim, no que diz respeito à confirmação da existência ou acesso aos dados, a ANPD apenas poderia desviar dos prazos ali estabelecidos no caso de setores específicos, como prevê o §4º do artigo 19. Quanto aos demais direitos previstos nos incisos III a IX do artigo 18, de fato é necessário que haja uma elucidação em relação ao prazo para seu atendimento. A proposta de seguir os prazos da Lei nº 12.527/2011 é inadequada, considerando as diferentes lógicas subjacentes aos direitos estabelecidos por essa lei e pela LGPD. Enquanto a LGPD visa possibilitar que um titular específico exerça seus direitos em relação aos seus dados pessoais perante o controlador, a LAI tem o objetivo de regular o acesso a informações públicas. Assim, no contexto da LGPD, o controlador precisa primeiro garantir a autenticação do titular, o que envolve uma série de procedimentos (como a confirmação da identidade e a verificação do meio de exercício do direito, incluindo se é feito por meio de procurador), impactando o tempo necessário para atender a esses direitos. Essa realidade não se aplica à LAI. Além disso, os prazos previstos pela LAI (20 dias, com a possibilidade de prorrogação por mais dez dias, conforme previsto pelo caput do artigo 11 e seu §2º) são demasiadamente exíguos para o atendimento dos direitos previstos nos incisos III a IX do artigo 18 da LGPD. Nesse sentido, destaca-se que o GDPR estabelece, em seu artigo 12.1, que os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Assim, recomenda-se que a ANPD siga o prazo estabelecido pelo GDPR, ou seja, de 30 (trinta dias), podendo haver prorrogação por mais 60 (sessenta) dias, caso necessário, devendo o termo inicial ser a data de autenticação do titular. (Continuação vide e-mail).", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD? "[Brasscom] Compreende-se que a lógica utilizada para diferenciar os prazos previstos incisos I e II do artigo 19 é o nível de detalhamento das informações fornecidas, visto que o inciso I fala da confirmação de existência ou do acesso a dados pessoais em formato simplificado, enquanto o inciso II fala de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento. Porém, como a própria LGPD já estabelece os prazos para atendimento aos direitos previstos em tais incisos, entende-se que a presente questão se refere ao §4º do artigo 19, que dispõe sobre a possibilidade da Autoridade dispor, de forma diferenciada, acerca dos prazos previstos nos incisos I e II do caput no caso de setores específicos. Nesses casos, para setores que precisam de tempo adicional para atender aos direitos previstos nos incisos I e II do artigo 19 da LGPD, uma alternativa seria seguir o prazo previsto pelo GDPR, em seu artigo 12.1.: os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Para definir quais setores poderiam se beneficiar de um prazo diferenciado, a ANPD pode considerar uma série de critérios, por exemplo: o volume dos pedidos recebidos, os tipos de requisições recebidas por aquele setor especificado, a complexidade de tais requerimentos e dos sistemas nos quais os dados são tratados, dentre outros, dados esses que a ANPD já tem conhecimento pela atividade de sua Ouvidoria e os relatórios que produz. " "615484": "[Brasscom] Para garantir a efetividade da comunicação entre o titular dos dados e o agente de tratamento, algumas medidas são essenciais: (i) É

fundamental que as informações sobre os direitos dos titulares e os procedimentos para exercê-los sejam divulgadas de maneira clara e simplificada. (ii) Importante disponibilizar ao titular meios de exercer todos os direitos conferidos pela LGPD. (iii) Antes de atender aos direitos do titular, é necessário autenticar sua identidade de acordo com os padrões estabelecidos pelo controlador. (iv) O atendimento ao requerimento deve ser realizado de forma gratuita, porém, a ANPD deve coibir o exercício de direitos de forma abusiva, indicando exemplos de requerimentos que poderiam ser configurados como tal. Contudo, ao se debruçar sobre as características dos canais de atendimento disponibilizados aos titulares, a Autoridade deve levar em conta a diversidade dos agentes de tratamento, levando em consideração aspectos como tamanho e estrutura organizacional. Da mesma forma, a ANPD precisa reconhecer que as organizações lidam com o exercício dos direitos dos titulares de maneiras diversas, adaptando-se à realidade específica de cada uma e sendo elas as mais hábeis a determinar as características daquele canal. Nesse contexto, destaca-se um estudo realizado pela International Association of Privacy Professionals (The State of Data Rights, 2020, p. 46-57, disponível em: <https://iapp.org/resources/article/the-state-of-data-rights/>) . Além disso, é preciso que se considere que os titulares podem apresentar desafios adicionais à comunicação. Por exemplo, um pedido genérico de dados por parte do titular pode resultar em um atendimento falho devido à imprecisão da solicitação, exigindo esclarecimentos adicionais. Em complemento, a tendência dos titulares em utilizar outros meios de comunicação ao invés daqueles indicados pelo controlador e sua recusa em fornecer informações necessárias podem complicar o processo de atendimento, mesmo quando o canal de comunicação está disponível e acessível. (Continuação vide e-mail).";"615485": "[Brasscom] Inicialmente, é preciso que se considere que o atendimento, pelo operador, às suas obrigações legais é essencial para a concretização dos direitos dos titulares. Nesse sentido, destaca-se o dever de manter registros de operações de tratamento de dados pessoais (artigo 37) e realizar o tratamento segundo as instruções fornecidas pelo controlador (artigo 39). No que tange às obrigações específicas que deverão ser impostas ao operador para permitir o atendimento adequado dos direitos dos titulares por parte do controlador, é preciso que essas sejam estabelecidas contratualmente de acordo com negociações a serem feitas entre as partes, podendo incluir: assistência técnica e operacional; notificação em prazo adequado sobre o recebimento de requerimento de exercício de direito; dentre outras. ";"615486": "[Brasscom] A abordagem semelhante ao SAC para atender aos direitos dos titulares é inviável por diversos motivos: 1) Múltiplos canais: A disponibilização de vários canais pode gerar complexidade operacional, custos adicionais e fragmentação de recursos. 2) Disponibilidade 24/7: Manter disponibilidade ininterrupta é impraticável para muitas organizações, especialmente as de menor porte, e pode comprometer a qualidade do atendimento devido à necessidade de análises cuidadosas e consultas legais. 3) Atendimento telefônico obrigatório: Impor o atendimento telefônico restringe a flexibilidade dos controladores, ignorando as preferências dos titulares e limitando a acessibilidade e a comodidade. 4) Acesso não condicionado aos dados: Embora a autenticação seja crucial, exigir acesso não condicionado pode comprometer a privacidade e a segurança dos dados. 5) Condições mínimas para atendimento telefônico: Estabelecer condições mínimas pode gerar burocracia e custos adicionais, sem necessariamente melhorar o atendimento. 6) Opções de acesso em documentos impressos: A obrigação de incluir opções de acesso em documentos impressos pode ser excessiva, especialmente em um mundo digitalizado. 7) Parâmetros pormenorizados para acompanhamento: Definir parâmetros rígidos pode ser inadequado, não considerando a diversidade das organizações e das demandas dos titulares. 8) Prazo de resposta: O prazo estabelecido

pode ser exíguo e inviável para muitas organizações, diferentemente do GDPR, que prevê um prazo mais realista. ","615487": "[Brasscom] Não há um modelo ideal. As organizações devem ter liberdade para estabelecer o formato de atendimento mais adequado às suas particularidades e às necessidades dos titulares. Isso é crucial, pois muitas empresas já investiram recursos significativos em sistemas de atendimento aos titulares, e a implementação de um novo modelo poderia representar desafios estruturais e desperdício de investimentos anteriores. Essa liberdade também se alinha à lógica de gestão de riscos da LGPD. Assim, é fundamental que as organizações mantenham a flexibilidade para determinar o formato de atendimento mais adequado às suas particularidades e às exigências dos titulares dos dados. Essa abordagem é justificada por diversos motivos: - Flexibilidade: As empresas possuem estruturas, processos e sistemas variados, não havendo uma solução única. Permitir que elas determinem seus próprios formatos de atendimento possibilita uma adaptação mais eficaz às suas realidades individuais e às demandas dos titulares. - Inovação: Ao conceder às organizações a liberdade de definir seus formatos de atendimento, incentiva-se a inovação e o surgimento de novas soluções e tecnologias que aprimoram a experiência do titular e a eficiência do processo. - Personalização: Cada empresa tem uma compreensão única das necessidades e preferências de seus titulares. Conceder a elas autonomia para determinar seus formatos de atendimento viabiliza a personalização das soluções para melhor atender às expectativas dos usuários. - Eficiência econômica: Permitir que as empresas estabeleçam seus próprios formatos de atendimento abre espaço para a busca por soluções mais econômicas e eficientes, considerando suas capacidades financeiras e operacionais. Portanto, embora seja importante que a ANPD forneça orientações claras e elucidativas, é igualmente crucial que as organizações tenham autonomia para determinar como implementar essas diretrizes de forma a melhor atender às necessidades dos titulares e garantir a conformidade com a legislação de proteção de dados. ","615491": "[Brasscom] Inicialmente, para fins de uma resposta mais completa à presente questão, a Brasscom gostaria de remeter esta Autoridade ao item 4 da contribuição submetida via e-mail que trata sobre os limites do direito de acesso. Além disso, apesar da resposta ter sido incluída na seção dedicada ao direito de acesso e do tópico do documento submetido por e-mail também se referir especificamente a esse direito, a reflexão se aplica a todos os direitos previstos na LGPD. De forma resumida, a presente associação gostaria de destacar que nenhum direito individual deve ser tido por absoluto, devendo a ANPD estar atenta e coibir o exercício abusivo de direitos. Esse raciocínio não deve ser diferente na interpretação da LGPD quanto aos direitos conferidos aos titulares de dados pessoais. No que se refere ao direito de confirmação da existência de tratamento, são exemplos de hipóteses que justificam a negativa da confirmação: i) o solicitante não confirmou a identidade do titular de dados; ii) a solicitação tem intenções maliciosas e está sendo evidentemente usada para assediar, de forma recorrente, uma organização sem nenhum propósito real a não ser causar transtorno; (iii) quando o controlador indica o canal correto para o exercício dos direitos (ex: OneTrust, e-mail específico) e o titular insiste reiteradamente em realizar o exercício por canal diverso ; (iv) quando um titular de dados evidentemente formula o pedido de acesso com um intuito diverso daquele que justifica o próprio direito e (v) quando formula pedidos idênticos e repetidos após já ter sido atendido pelo controlador. ","615492": "[Brasscom] A informação individualizada sobre todos os destinatários dos dados pessoais, além de possivelmente revelar dados de outras pessoas físicas que eventualmente não permitiram essa revelação, pode expor dados comercialmente estratégicos do controlador, tutelados pelos segredos comercial e industrial. Assim, a divulgação nominal pode ensejar um problema concorrencial, o que violaria um dos

princípios da LGPD. Por essa razão, entendemos que a obrigação de prestar as informações sobre o compartilhamento de dados poderia se limitar à indicação das categorias de destinatários e à finalidade para os quais são tratados, o que atenderia ao princípio da transparência e o pedido de acesso do titular dos dados. Eventual fornecimento de dados mais específicos sobre entidades com as quais o compartilhamento é realizado poderia ser realizado caso o titular não ficasse satisfeito com os dados fornecidos, seguindo a lógica do repasse de informações em camadas, como sugere a Agencia Española de Protección de Datos (“AEPD”) (mais detalhes podem ser encontrados nos seguinte link: [; bem como na submissão feita pela Brasscom por e-mail](#)) ou a critério do controlador, respeitada a legislação vigente. “;615489”:[Brasscom] Inicialmente, é preciso que se considere que o atendimento, pelo operador, às suas obrigações legais é essencial para a concretização dos direitos dos titulares. Nesse sentido, destaca-se o dever de manter registros de operações de tratamento de dados pessoais (artigo 37) e realizar o tratamento segundo as instruções fornecidas pelo controlador (artigo 39). No que tange às obrigações específicas que deverão ser impostas ao operador para permitir o atendimento adequado dos direitos dos titulares por parte do controlador, é preciso que essas sejam estabelecidas contratualmente de acordo com negociações a serem feitas entre as partes, podendo incluir: assistência técnica e operacional; notificação em prazo adequado sobre o recebimento de requerimento de exercício de direito; dentre outras.”;615490”:[Brasscom] O caput do artigo 19 regula a possibilidade de exercício de dois direitos distintos, o direito de confirmação da existência do tratamento (artigo 18 I da LGPD) e o direito de acesso aos dados pessoais tratados (artigo 18 II da LGPD). Partindo da premissa que o titular de dados exerceu o direito de acesso, solicitando uma declaração simplificada, para atender ao requisito do inciso I do artigo 19 da LGPD, que estabelece a necessidade de uma declaração em formato simplificado sobre o tratamento de dados pessoais, é crucial que o controlador forneça as informações essenciais que permitam aos titulares entenderem como seus dados estão sendo tratados. Assim, conforme estabelecido no caput do artigo 19, deve-se garantir o acesso dos titulares aos dados pessoais que estão sendo tratados, nos limites do que foi solicitado. “;615494”:[Brasscom] As informações que devem ser disponibilizadas ao titular sobre o tratamento de seus dados, independentemente de requerimento, encontram-se previstas pelo artigo 9º da LGPD (finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei), as quais estarão previstas na Política de Privacidade e Proteção de Dados do agente de tratamento. Para além disso, no que tange às informações objeto de requerimento pelos titulares, a Brasscom gostaria de citar novamente como um bom exemplo aquele recomendado pela Agencia Española de Protección de Datos, que sugere que recomenda que as informações sejam repassada “em camadas” aos titulares (mais detalhes podem ser encontrados nos seguinte link: [; bem como na submissão feita pela Brasscom por e-mail](#)). “;615493”:[Brasscom] A questão apresenta certa ambiguidade em relação ao seu objetivo, mas parece indagar se o direito de acesso seria considerado atendido quando o agente de tratamento disponibiliza os dados pessoais em formato digital ou em papel, de acordo com a escolha do titular. Nesse sentido, o §2º do artigo 19 da LGPD estabelece que o controlador deve atender ao direito de acesso conforme requerido pelo titular, devendo sempre ser considerada a razoabilidade do pedido. Isso significa que, se o titular especificar sua preferência por um formato específico (digital ou papel), o controlador deve fornecer

no formato solicitado, desde que não demande um esforço desproporcional, caso em que poderá o controlador preferir o formato digital. Nesse sentido, é importante considerar que os formatos podem variar dependendo dos próprios dados pessoais a serem fornecidos e da forma de contato normalmente mantida entre titular e controlador. Por exemplo, para relações usualmente mantidas em ambiente virtual, o formato digital via portal de privacidade, e-mails ou área logada pode ser preferível. Por fim, cabe também observar que prazos diferenciados poderão ser estabelecidos a depender do formato escolhido pelo titular.

Um aspecto que não diz respeito especificamente ao questionamento apresentado pela Autoridade, mas que a Brasscom considera relevante trazer à atenção da ANPD, envolve situações em que é feito um pedido de acesso a um controlador que detém um grande volume de dados do titular. Nesses casos, como destacado pelo guia sobre direito de acesso do European Data Protection Board (“EDPB”, disponível no seguinte link:), é importante que se considere que: (Continuação vide e-mail);“615502”:[Brasscom] O tema da portabilidade demanda uma análise mais pormenorizada antes de recomendações serem feitas, na medida em que se apresenta como um tema complexo e transversal, havendo maior ou menor aplicabilidade a depender do setor econômico e/ou atividade desenvolvida pelo controlador. Assim, é crucial que a Autoridade promova um debate mais amplo com os setores envolvidos, dada a variabilidade na maturidade para implementar o direito à portabilidade. Ademais, um conhecimento mais aprofundado do cenário internacional e de diretrizes, padrões e boas práticas adotadas a respeito do tema pode fornecer substrato extremamente rico para endereçar diversos aspectos que emergem do tema. A complexidade de tal tema pode ser demonstrada, por exemplo, no setor de telecomunicações, no qual é garantia aos consumidores a portabilidade numérica (mais informações sobre sua configuração podem ser encontradas no Código de Boas Práticas do setor disponível neste link:). Pela portabilidade específica deste setor, permite-se a migração de um contrato de prestação de serviço de uma prestadora de serviço de telecomunicações para a outra por meio do “Código de Acesso” (número de telefone do titular). Nesse sentido, o anexo (disponível aqui:) que atualmente dispõem sobre tal portabilidade aborda detalhadamente diversos temas, são exemplos: abrangência e objetivos da portabilidade; definições; características da portabilidade; direitos e deveres dos usuários; direitos e deveres das prestadoras; preços cobrados; modelo de portabilidade; etc. Nessa toada, levantamos alguns temas meramente exemplificativos que precisam ser elucidados por esta Autoridade antes de regulamentar o direito de portabilidade: i) definição de portabilidade e interoperabilidade; ii) quais dados devem ser portáveis; (Continuação vide e-mail);“615501”:[Brasscom] Os desafios tecnológicos para implementação de um padrão de interoperabilidade para o direito de portabilidade são diversos e abrangentes. Eles envolvem a complexidade das operações, a diversidade de formatos de dados e metadados, bem como as ferramentas e protocolos de comunicação adotados pelo mercado de cada setor e indústria. Além da complexidade sistêmica envolvida, existe também uma diversidade de práticas entre os diferentes agentes econômicos, o que dificulta ainda mais uma harmonização entre os diferentes interesses e ações. Dessa maneira, uma abordagem que estimule a discussão entre setores, a fim de promover uma maior flexibilidade por meio da autorregulação, é uma opção para que sejam adotadas soluções condizentes com as necessidades individuais das organizações. ”;“615505”:[Brasscom] ”;“615503”:[Brasscom] Sim, é adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibiliza para o titular todos os seus dados pessoais em formato interoperável, caso esse tenha sido o pedido feito pelo titular. Os Guidelines do Working Party 29 (disponível aqui: <<https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-right-data->

portability-under-regulation-2016679_en>) sobre portabilidade elucidem que esse direito também pode abranger a transmissão de dados pessoais de um controlador para outro, caso essa tenha sido a solicitação do titular. No entanto, é importante observar que esse aspecto do direito de portabilidade não: 1) implica na obrigação para os controladores adotarem e manterem sistemas de processamento que sejam tecnicamente compatíveis; 2) os torna responsáveis pelo tratamento realizado pelo próprio titular dos dados ou por outra empresa que receba os dados pessoais; 3) gera uma obrigação específica de verificar a qualidade dos dados antes de transmiti-los; e 4) impõe uma obrigação ao controlador de reter os dados pessoais por mais tempo do que o necessário ou além de qualquer período de retenção especificado. ";615504": "[Brasscom] Sim, é razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas no contexto da portabilidade de dados. Isso se justifica pelo fato de que diferentes setores podem ter necessidades e características específicas em relação à transferência de dados entre diferentes sistemas e plataformas. Permitir que o setor privado participe ativamente no estabelecimento desses padrões pode levar a soluções mais adequadas e eficientes para as empresas e os consumidores dentro de cada setor. No entanto, é importante ressaltar que esses padrões de interoperabilidade não deveriam ser obrigatórios. Embora possam ser úteis como referências ou guias para as empresas, a imposição de padrões específicos poderia restringir a flexibilidade das organizações para encontrar soluções que melhor atendam às suas necessidades individuais. Além disso, a definição de prazos para a implementação desses padrões deve levar em consideração a complexidade das atividades econômicas envolvidas, bem como o tempo necessário para que as empresas se adaptem e implementem as mudanças necessárias. ";615511": "[Brasscom] Para qualificar um dado como incompleto, inexato ou desatualizado, a situação concreta deve ser considerada à luz dos princípios da qualidade e finalidade estabelecidos pela LGPD. Embora o princípio da qualidade exija a exatidão dos dados, é importante reconhecer que essa exigência pode variar de acordo com a finalidade do tratamento. Por exemplo, em situações como o cadastro em um e-commerce, pode ser aceitável que o titular forneça apenas um dos seus sobrenomes, enquanto em contextos mais formais, como o preenchimento de uma escritura de imóvel, a precisão dos dados é crucial. O Information Commissioner's Office ("ICO", a posição pode ser encontrada no seguinte link:) defende que ao receber uma solicitação de retificação, o controlador deve tomar medidas razoáveis para verificar a precisão dos dados e retificá-los, se necessário. Essas medidas devem levar em consideração a natureza dos dados pessoais e sua utilização. Quanto maior for a necessidade de precisão dos dados, maior deve ser o esforço para verificar sua exatidão e retificá-los, especialmente se os dados forem utilizados para tomar decisões significativas que afetem o indivíduo ou terceiros. Além disso, é fundamental que se estabeleça claramente os limites desse direito, garantindo que ele se aplique apenas a dados genuinamente incompletos, inexatos ou desatualizados. Esse direito não deve ser usado para revisar eventos passados, e os controladores devem ter a possibilidade de solicitar aos indivíduos evidências específicas que comprovem a incorreção das informações retidas. É crucial ainda que tais aspectos se refiram apenas a fatos, excluindo opiniões. Isso é essencial para proteger a liberdade de expressão. A ANPD deve deixar claro que a retificação deve se aplicar exclusivamente a dados que são factualmente incompletos, inexatos ou desatualizados e não a dados com os quais o indivíduo simplesmente discorda. ";615514": "[Brasscom] É preciso considerar que o direito de correção está estreitamente relacionado com o princípio da qualidade dos dados que garante, aos titulares, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu

tratamento. Nesse sentido, o controlador deve ter a possibilidade de requerer aos titulares comprovação de que os dados estariam incompletos, inexatos e desatualizados. O Information Commissioner's Office ("ICO", mais informações podem ser encontradas aqui:), por exemplo, pontua que, ao receber um pedido de correção, o controlador deve adotar medidas razoáveis para se certificar da qualidade dos dados e para retificá-los, se necessário, levando em consideração os argumentos e as provas fornecidas pelo titular. Nesse sentido, são exemplos específicos em que a simples declaração do titular não seria suficiente para o exercício do direito à correção: situação em que haja dúvida sobre a veracidade dos dados; ausência de documentação comprobatória; eventual alteração em bases públicas; impossibilidade de confirmação de tratamento de dados do titular e/ou de confirmação da sua identidade; dentre outras.";"615513": "[Brasscom] Para avaliar a impossibilidade ou o esforço desproporcional conforme o art. 18, § 6º, da LGPD, é crucial considerar cada situação de forma concreta e individualizada. Isso significa que não há uma lista definitiva de critérios objetivos que se apliquem uniformemente a todas as circunstâncias. Em vez disso, é necessário analisar cuidadosamente os detalhes específicos de cada pedido de correção, eliminação, anonimização ou bloqueio de dados pessoais. Essa abordagem personalizada permite que se leve em conta uma série de fatores contextuais que podem influenciar a viabilidade de atender à solicitação. Por exemplo, o volume de solicitações, o tamanho e recursos disponíveis do controlador, o número de agentes envolvidos no tratamento dos dados e os eventuais prejuízos à atividade do controlador são considerações importantes a serem ponderadas. Dessa forma, ao lidar com pedidos de acesso aos dados pessoais, é essencial que o controlador avalie cada caso individualmente, levando em conta os diversos aspectos que podem afetar a capacidade de atender à solicitação de forma adequada e dentro dos parâmetros estabelecidos pela LGPD. Isso assegura que os direitos dos titulares de dados sejam respeitados de maneira efetiva, ao mesmo tempo em que reconhece as limitações e desafios enfrentados pelos controladores na gestão e proteção desses dados. ";"615512": "[Brasscom] Considerando o princípio da qualidade dos dados e a própria disposição do inciso III do artigo 18, o controlador poderá se recusar a atender ao pedido do titular caso entenda, primeiramente, que os dados estão completos, exatos e atualizados. Além disso, caso o titular não forneça os documentos necessários para o atendimento a tal direito, o controlador também poderá negá-lo. Em complemento, a ANPD também deverá elucidar que o direito de correção: (i) não equivale a uma revisão do passado (por exemplo, uma mudança de nome ou de estado civil não deverá ter efeitos retroativos), o que poderia inclusive afetar o cumprimento a eventual obrigação legal;; e (ii) deve se aplicar apenas a fatos e não a opiniões, de forma a salvaguardar a liberdade de expressão (essas opiniões são defendidas pelos Centre for Information Policy Leadership no seguinte documento:). Por fim, reitera-se os pontos trazidos em relação aos limites do exercício abusivo de direito, nos termos da resposta à questão II.a desta Tomada de Subsídios e do item 4 do documento submetido por essa Associação por e-mail. ";"615517": "[Brasscom] Sim, nos termos do inciso IV do artigo 18, é preciso que o titular fundamente e comprove que os dados são desnecessários, excessivos ou que estão sendo tratados em desconformidade legal para fins de exercício dos direitos de anonimização, bloqueio ou eliminação. Portanto, é importante que a ANPD esclareça aos titulares de dados que a anonimização, bloqueio ou eliminação não são direitos irrestritos, sendo necessário, para seu atendimento, a existência de dados considerados desnecessários, excessivos ou a ocorrência de tratamento em desconformidade legal. Além disso, é importante ressaltar ainda que a anonimização, bloqueio ou eliminação não devem ser realizados se o controlador estiver tratando os dados pessoais de acordo com uma base legal válida,

pois nesse caso os dados continuarão sendo necessários e seu uso será legalmente justificado. Além disso, os dados também poderão ser mantidos nos casos previstos no artigo 16 da LGPD. Isto é, os dados poderão ser armazenados para: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

","615516": "[Brasscom] Sim, tanto a anonimização quanto à eliminação são medidas que podem ser adotadas de forma alternativa, dependendo das circunstâncias específicas, sendo ambas reconhecidas pela Lei Geral de Proteção de Dados Pessoais. O artigo 12 da LGPD estabelece que os dados anonimizados não são considerados como dados pessoais. Isso significa que, ao anonimizar os dados de acordo com os critérios definidos pela legislação, eles perdem sua natureza de identificadores pessoais, proporcionando uma alternativa viável à eliminação completa dos dados. Além disso, o inciso IV do artigo 16 da LGPD autoriza a conservação dos dados pessoais exclusivamente para uso do controlador, desde que os dados sejam anonimizados. Essa disposição legal reconhece que a anonimização dos dados oferece um nível adequado de proteção à privacidade, permitindo que o controlador mantenha os dados para fins específicos, desde que não possam ser acessados por terceiros. Portanto, a LGPD reconhece tanto a anonimização quanto à eliminação como medidas equivalentes para garantir a proteção dos dados pessoais, proporcionando às organizações a flexibilidade necessária para escolher a abordagem mais adequada às suas necessidades e à natureza dos dados em questão. "

","615518": "[Brasscom] Caso o titular se oponha ao tratamento de dados realizado com base em uma das hipóteses de dispensa de consentimento, e essa oposição seja considerada legítima, o controlador deverá interromper a operação de tratamento, a menos que consiga justificá-la com base em outra fundamentação legal. No entanto, mesmo diante da possibilidade de que a oposição legítima estaria fundada em tratamento de dados em descumprimento da LGPD, isso não deveria, por si só, configurar infração para fins de aplicação de sanções administrativas perante a ANPD. Isso porque o nível de exigência, comprovação e apuração deve ser mais elevado, devendo ser respeitado o trâmite de apuração da ocorrência garantindo a ampla defesa do agente de tratamento. Ademais, espera-se que a ANPD possa auxiliar os agentes de tratamento na tarefa de adequar suas atividades de tratamento, abrindo prazo para essa adequação no caso concreto - e promover, assim, o incremento de maturidade da cultura de proteção de dados no Brasil e a atuação responsiva da autoridade - e não que aplique sanções a partir de situações isoladas e que podem ser absolutamente pontuais. Assim, o efeito de considerar o pedido realizado pelo titular nos termos do §2º do artigo 18 legítimo seria a necessidade de atendimento ao pedido e, conseqüentemente, a indução à conformidade legal. Com o atendimento de tal pedido, o direito de oposição, nos termos do referido dispositivo, perde seu fundamento. "

","615523": "[Brasscom] A revogação do consentimento, conforme prevista no art. 18, IX, da LGPD, não necessariamente implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular. Isso porque pode haver outra base legal que justifique o tratamento desses dados, por exemplo, quando os dados são necessários para o cumprimento de um contrato entre o controlador e o titular dos dados ou para o adimplemento a uma obrigação legal. Assim, destaca-se que, muitas vezes, as empresas precisam dos dados pessoais para diversos propósitos, e o tratamento pode ser baseado em mais de uma base legal. Portanto, a revogação do consentimento não significa automaticamente que o controlador deva apagar os dados, especialmente se houver outra base legal que justifique o tratamento para certo fim (esse é o

entendimento defendido nos Guidelines on consent under Regulation 2016/679 do Working Party 29, disponível aqui:). Outra circunstância que pode exigir que o controlador mantenha os dados é a necessidade de saber como agir em determinada situação (por exemplo: no caso do titular que não quer receber propagandas, é preciso guardar os dados para garantir que o direcionamento não será feito). Por fim, é importante que se considere que a revogação do consentimento não deve gerar efeitos retroativos. Isso significa que, se o consentimento foi concedido para uma determinada operação de tratamento - como um processo de autenticação para a execução de uma transação (operação X) - a sua revogação não deve afetar retroativamente a operação já realizada. Em outras palavras, uma vez que uma operação foi concluída com base no consentimento válido naquele momento, a revogação subsequente do consentimento não deve invalidar a legalidade dessa operação.

","615521": "[Brasscom] Na ausência de outra base legal, os dados devem ser eliminados. Caso tenham sido compartilhados, é necessário notificar os entes com quem foram compartilhados. No entanto, em determinadas circunstâncias, é essencial que o controlador mantenha os dados para orientar suas ações em situações específicas. Por exemplo, se um titular expressar o desejo de não receber mais propagandas, é necessário manter os dados para garantir que o direcionamento não ocorra. Contudo, é fundamental ressaltar que o tratamento realizado com base no consentimento anteriormente à revogação permanece legal."

","615617": "[Brasscom] Uma decisão tomada unicamente com base em tratamento automatizado é aquela em que não há envolvimento humano no processo de tomada de decisão. Isso significa que a decisão é tomada inteiramente por tratamento automatizado, sem qualquer intervenção ou influência direta de seres humanos. Além disso, é preciso que se considere que, ao tratar da LGPD e especificamente do artigo 20, necessariamente está a se tratar de decisões automatizadas que envolvam o tratamento de dados pessoais. "

","615618": "[Brasscom] "

","615619": "[Brasscom] A implementação do direito de revisão de decisões, conforme previsto no art. 20 da LGPD, enfrenta uma série de desafios práticos significativos. Um dos principais desafios reside na complexidade dos sistemas que utilizam aprendizado de máquina e inteligência artificial. Esses sistemas muitas vezes tomam decisões automatizadas com base em algoritmos complexos, tornando difícil explicar de forma clara aos titulares os motivos por trás de uma decisão específica. Além disso, a potencial exigência de intervenção humana para revisar e explicar as decisões automatizadas pode gerar gastos adicionais de recursos para as organizações, isso porque, a necessidade de envolvimento humano para revisar e explicar essas decisões pode aumentar os custos operacionais e administrativos. Outro desafio é fornecer explicações claras e acessíveis aos titulares sem comprometer os direitos de propriedade intelectual e segredos comerciais das organizações. O fornecimento das informações exigidas pelos §1º do artigo 20 pode entrar em conflito com a necessidade de proteger informações confidenciais e estratégicas da empresa, criando um desafio adicional na implementação desse direito. Além disso, a manutenção de registros detalhados sobre as decisões tomadas e os processos envolvidos pode exigir investimentos significativos em sistemas de registro e armazenamento de dados. Isso pode representar um desafio especialmente para organizações que lidam com grandes volumes de dados e decisões automatizadas em escala. Ainda, a implementação efetiva do direito de revisão de decisões também está sujeita a custos financeiros relacionados à atualização e adaptação dos sistemas de informação e processos organizacionais para garantir a conformidade com os requisitos da LGPD. Esses custos podem ser substanciais, especialmente para pequenas e médias empresas. (Continuação vide e-mail)."

","615620": "[Brasscom] Sim, quando: não há enquadramento nos termos do artigo 20 ("decisões tomadas unicamente com base em tratamento automatizado

de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade”); a resposta possa revelar algoritmo ou lógica de programação, bem como violar direitos de propriedade intelectual e segredo comercial; e caso a revisão seja impossível, pela técnica ou pela prática. "

{ "615450": "Sim, sobretudo para o setor da saúde, no qual as solicitações dos direitos dos titulares podem apresentar questões de alta complexidade a depender do contexto, considera-se que o prazo de 20 (vinte) dias, conforme mencionado no § 1º do art. 11, e, sobretudo, a possibilidade de prorrogação do prazo por mais 10 (dez) dias, em conformidade com o §2º do mesmo artigo, garantiria maior efetividade do cumprimento de resposta ao exercício dos direitos pelos agentes de saúde.", b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?: "Os seguintes critérios devem ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD: (i) Teor da Solicitação; (ii) Urgência do pedido; (iii) Impacto ao titular; (iv) Complexidade para a solução; (v) Tamanho do agente de tratamento; (vi) volume de titulares/dados tratados. Sobretudo no que se refere à declaração clara e completa presente no inciso II do art. 19, compreendemos que é pertinente prazo estendido, conforme critérios acima, tendo em vista a necessidade de apuração interna do agente de tratamento. ", "615484": "Canal de atendimento que possua: (i) Meios de identificação do titular; (ii) Linguagem simples e acessível para compreensão do titular; (iii) Canal eletrônico com boa usabilidade e direcionamento.", "615485": "Sim, o operador possui responsabilidade na concretização dos direitos dos titulares, sobretudo em situações nas quais: (i) for diretamente acionado pelo titular, cooperando para indicação de correto canal junto ao controlador, se o caso; (ii) apoiando o controlador com subsídios para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação pelo controlador.", "615486": "Não, o tema deve ser tratado de forma diferenciada. Questões relacionadas ao atendimento ao consumidor poderão diferenciar-se em demasiado no tocante à natureza de requisições de titulares, sobretudo em determinados segmentos do mercado, como o setor da saúde. Algumas obrigações de difícil aplicação na norma requerem, por exemplo: (i) disponibilidade ininterrupta - durante vinte e quatro horas por dia, sete dias por semana; (ii) pluralidade de canais; (iii) obrigatoriedade de atendimento telefônico; (iv) acesso inicial não condicionado ao fornecimento prévio de dados pelo consumidor, (v) prazo de atendimento de demandas no prazo de sete dias corridos, contado da data de seu registro; (vi) horário de atendimento não inferior a oito horas diárias dentre outras. As justificativas incluem: (i) não é necessário um serviço de atendimento ininterrupto para cumprir com a LGPD; (ii) o atendimento ao cliente pode ser feito durante o horário comercial e por diferentes canais, como e-mail; (iii) a identificação prévia do titular de dados é recomendada para direcionar o atendimento e apurar violações; (iv) o tempo mínimo de funcionamento do SAC pode variar de acordo com a natureza dos serviços oferecidos pelas empresas, e se diferencia do prazo já previsto na LGPD (15 dias); (v) o contato direto com o atendente nem sempre é necessário, e o tempo máximo de espera para atendimento da solicitação depende de análises específicas; (vi) pode ser necessário solicitar repetição da demanda para coletar informações necessárias junto ao titular; (vii) meios digitais podem ser suficientes para atender solicitações dos titulares; (viii) o prazo de 5 dias corridos para atender solicitações pode ser curto, especialmente considerando o histórico do titular.", "615487": "Consideramos que o modelo de Ouvidoria do Gov.br é um sistema que pode ser utilizado como paradigma no tocante ao setor público. Inclusive, a indicação de métricas para a calcular a efetividade dos atendimentos realizados e a satisfação do público. No tocante ao setor privado, uma das alternativas é utilizar os indicadores e as métricas implementadas pelo IBRC - Instituto Brasileiro de Relacionamento com o Cliente.

;"615491": "Eventualmente, quando o tratamento de dados pessoais estiver relacionado a procedimentos de investigação e/ou auditorias, a fim de proteger o processo, seria possível a negativa. "; "615492": "Razão social, CNPJ, Nome Fantasia e/ou Marca e DPO."; "615489": "Cooperação na indicação de correto canal do controlador, se o caso ou apoio ao controlador com subsídios para atendimento da solicitação em prazo hábil para o cumprimento no disposto na legislação."; "615490": "Considerando que o formato simplificado prevê que o relatório seja encaminhado imediatamente, a informação mínima que pode ser fornecida é sobre a Existência do tratamento: Sim ou não. Em caso positivo, ficará facultado a cada controlador complementar ou não a requisição com informações adicionais, se assim entender pertinente."; "615494": "Dados pessoais tratados para a tomada de decisão e finalidades do tratamento."; "615493": "Sim, tanto a disponibilização digital quanto em formato de papel satisfazem os direitos do titular. No entanto, o fornecimento em papel deve considerar o volume de dados e ser oferecido apenas se o cliente não tiver acesso digital ou preferir o formato físico, com os custos de impressão repassados ao solicitante. A prioridade deve ser sempre o formato digital, dada a disponibilidade de meios tecnológicos seguros."; "615502": "Telecomunicações e Setor Financeiro. No que se refere aos atores do segmento de saúde, incluindo entes públicos e privados, compreende-se que não há maturidade em processos que permita assegurar a Portabilidade na forma de dados interoperáveis no momento, considerando, dentre outros elementos, a sensibilidade, volumetria e formato dos dados."; "615501": "Com referência ao setor da saúde, é possível citar: (i) Integrações entre plataformas que operam dados; (ii) formato válido de dados; (iii) qualidade de dados; (iv) operações e estrutura de tecnologia; (v) multidisciplinariedade de sistemas. Atualmente existem diversos mecanismos de coleta dados, cada um com sua particularidade e operação. Para que a interoperabilidade de dados fosse realizado, deveria inicialmente existir uma padronização no formato de coleta de dados e armazenamento de metadados, bem como sanitização do conjunto para que todo ele permaneça legível. "; "615505": "Prioritariamente o formato de dados, protocolos e terminologias comuns. Em seguida a padronização das ferramentas operadoras de dados e por fim a sanitização das bases."; "615503": "Sim."; "615504": "Sim, é razoável que o setor privado possa definir os padrões de interoperabilidade, por segmentos de atividade - pois cada cenário possui desafios específicos. O prazo deverá ser determinado de acordo com o mercado que o operador atua, sendo que, no tocante à área da saúde, compreende-se prazo inferior a 12 (doze) meses demasiado desafiador. "; "615511": "Compreendemos que os seguintes aspectos devem ser observados: Idado Inexato: Quando contém informações incorretas, imprecisas ou desatualizadas. Isso pode ocorrer devido a erros de entrada de dados, falhas de comunicação ou mudanças nas circunstâncias que tornam as informações obsoletas. Dado Desatualizado: Quando as informações que ele contém estão obsoletas ou não refletem a situação atual. Isso pode ocorrer quando os dados não são atualizados regularmente para acompanhar mudanças no tempo, como atualizações de status, alterações de contexto ou novos desenvolvimentos. No que se refere ao contexto ou consideração situacional para enquadramento do dado, deve ser considerado o último registro do dado, com evidências de data."; "615514": "A simples declaração do titular não seria suficiente nos casos de: (i) solicitação genérica, como, por exemplo, sem indicação do dado a ser corrigido e/ou onde consta desatualizado; (ii) solicitações de correção sem comprovação da identidade do titular; (iii) situações em que é necessária a validação/cadastro por meio de comprovação documental e não é apresentado o documento para correção/atualização. "; "615513": "Os critérios objetivos para avaliar a impossibilidade ou o esforço desproporcional conforme o art. 18, §6º da LGPD envolvem: (i) considerações sobre a complexidade da infraestrutura

dos agentes de tratamento envolvidos; (ii) formato dos dados (iii) padrão de interoperabilidade; (iv) tipo de solicitação, (v) implicações da não recepção pelos demais da solicitação e (vi) volume de agentes a serem comunicados. Por fim, é necessário levar em conta desafios para que seja informado ao outro controlador "imediatamente", conforme menciona a legislação - devendo a ANPD fornecer critérios mais claros quanto ao prazo fornecido.,"615512": "Em circunstâncias excepcionais, o direito de correção pode ser negado pelo controlador em situações em que o pedido de correção é feito para informações que não necessitam de alteração, como quando os dados estão corretos e precisos. Além disso, o direito de correção pode ser negado quando as correções demandam comprovação por meio de documentos, e o titular não forneceu a documentação necessária para comprovar a necessidade da correção. ","615517": "É essencial que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado, pois isso possibilita aos agentes de tratamento a verificação de inconsistências internas, melhorando seus programas de governança ou de seus parceiros, fornecedores e demais agentes que realizam o tratamento em seu nome ou juntamente a eles. A fundamentação permite que o controlador analise as alegações do titular e ofereça esclarecimentos adicionais, se necessário, sobre o tratamento de dados considerados desnecessários, excessivos ou em desconformidade. ","615516": "Sim, considerando situações específicas, a anonimização e a eliminação podem ser adotadas alternativamente pelos agentes de tratamento. Respeitando os limites de finalidade do tratamento de dados, bem como os riscos de reidentificação e as possibilidades legais e regulatórias, essa alternativa pode ser aplicada, especialmente em setores sensíveis como o da saúde, onde essa flexibilidade pode promover a inovação em ferramentas voltadas para a saúde. Além disso, essa escolha pode atender às solicitações dos titulares quanto à cessação do tratamento de seus dados pessoais, ressalvadas as hipóteses legais de exceções. A adoção de medidas de anonimização ou eliminação pode ser considerada de forma alternativa, levando em conta que a anonimização remove as características de dados pessoais, mitigando substancialmente os riscos para os titulares de dados. ","615518": "É necessário que o agente de tratamento, mesmo agindo de boa-fé e tendo conhecimento da possível configuração de tratamento inadequado dos dados, se comprometa proativamente com as medidas necessárias para correção do processo e as devidas comunicações, se o caso. ","615523": "Não necessariamente. A revogação do consentimento do titular, conforme estipulado no art. 18, IX, da LGPD, não automaticamente exige a eliminação dos dados pessoais tratados com base nesse consentimento. O titular precisa expressar explicitamente o desejo de eliminar seus dados. Além disso, é importante considerar que os dados tratados até a revogação do consentimento são válidos e podem ser retidos por obrigação legal ou regulatória, como exceções previstas no art. 16 da LGPD e em normativas específicas. ","615521": "Considerando o art. 8º da LGPD, é importante observar que os tratamentos realizados sob o amparo do consentimento anteriormente manifestado podem ser mantidos pelos agentes de tratamento em determinados casos, conforme previsão legal e normativas setoriais. Por exemplo, a conservação de dados em órgãos e estudos de pesquisas clínicas, conforme o art. 16, inciso II da LGPD, e o Guia Orientativo para fins de Tratamento acadêmicos e para realização de estudos e pesquisas elaborado pela ANPD. Isso se deve ao fato de que certos tratamentos, como os dados clínicos em pesquisas, não podem ser removidos sem afetar o resultado estatístico da pesquisa. Assim, o direito de revogação do consentimento deve estar em consonância com as normas do setor e respeitar os limites previstos pela LGPD. ","615617": "Uma decisão automatizada geralmente implica que, embora o processo de tomada de decisão possa ser

automatizado, ainda pode haver alguma forma de intervenção humana no processo. Isso inclui a definição dos critérios ou regras que o algoritmo deve seguir, revisão periódica dos resultados gerados pelo sistema automatizado ou a possibilidade de os indivíduos afetados contestarem a decisão e obterem uma revisão humana. Por outro lado, uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais implica que não há intervenção humana significativa no processo de tomada de decisão. Isso significa que a decisão é totalmente gerada pelo sistema automatizado, sem revisão ou intervenção humana durante todo o processo.";"615618": "Recomendamos que os elementos abaixo sejam considerados: 1 - Natureza dos direitos afetados: Avaliar se os direitos fundamentais ou interesses legítimos dos indivíduos estão sendo comprometidos, tais como privacidade, liberdade de expressão, liberdade de associação, entre outros. 2 - Gravidade do impacto: Determinar a gravidade do impacto sobre os indivíduos afetados, considerando se a decisão automatizada pode resultar em consequências significativas, como perda de oportunidades, discriminação, prejuízos financeiros ou reputacionais. 3 - Abrangência da decisão: Analisar se a decisão automatizada tem um alcance amplo e afeta um grande número de pessoas ou se é direcionada a indivíduos específicos. 4 - Transparência e explicabilidade: Verificar se os critérios e algoritmos utilizados na tomada de decisão automatizada são transparentes e compreensíveis, permitindo que as pessoas entendam como suas informações foram usadas e como a decisão foi tomada. 5 - Possibilidade de contestação: Avaliar se as pessoas têm meios eficazes para contestar ou contestar a decisão automatizada, garantindo o direito de corrigir informações imprecisas ou contestar decisões injustas.";"615619": "Os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD envolvem a complexidade dos algoritmos, a interpretação dos resultados, o acesso aos dados, o conhecimento técnico necessário, o tempo e recursos requeridos, bem como a efetividade das correções. Além disso, há o desafio de dar transparência ao titular de dados sobre os critérios utilizados no processo de decisões automatizadas, considerando que diferentes estruturas e sistemas podem envolver segredo de negócio das companhias. Além disso, importante que se defina que garantir a revisão nas decisões não garante mudança no resultado anteriormente tomado, a menos que haja alteração nos critérios utilizados pelos controladores ou dados novos e/ou atualizados. Superar esses desafios demanda uma abordagem colaborativa entre reguladores, profissionais da área, desenvolvedores de tecnologia e usuários finais para garantir que os direitos de revisão sejam efetivos e que as decisões automatizadas sejam justas, transparentes e precisas.";"615620": "Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas. Isso pode ocorrer quando não houver cabimento nas hipóteses previstas no art. 20 da LGPD, que incluem afetação aos interesses, definição de perfil pessoal, profissional, de consumo, de crédito ou aspectos da personalidade, bem como eventualmente normas setoriais relacionadas à matéria. Além disso, elencamos algumas circunstâncias em que o direito de revisão podem vir e ser negados: 1 - Obrigação legal: Se a decisão automatizada for exigida ou autorizada por lei, o controlador pode não ter a capacidade de alterá-la ou revisá-la. 2 - Risco à segurança: Se a divulgação das informações utilizadas na decisão automatizada representar um risco à segurança, integridade ou confidencialidade dos sistemas ou dados, o direito de revisão pode ser negado. 3 - Proteção de direitos de terceiros: Se a revisão da decisão automatizada violar os direitos ou interesses legítimos de terceiros, como segredos comerciais ou propriedade intelectual, o controlador pode ser impedido de realizar a revisão. 4 - Decisões manifestamente infundadas: Se a solicitação de revisão for considerada manifestamente infundada ou excessiva, o controlador pode recusar a revisão, desde que comunique claramente os motivos para tal

decisão. É importante observar que, mesmo nessas circunstâncias, o controlador deve informar claramente os motivos para negar o direito de revisão e fornecer mecanismos para que os indivíduos contestem essa decisão, quando aplicável."

elucidações e complementações); e (iii) o pedido foi realizado por meio do canal correto para fins de atendimento, o que muitas vezes está ligado ao item (i). Tais aspectos não visam dificultar o exercício de direitos, mas sim garantir um atendimento seguro e adequado, em conformidade com a LGPD. No que diz respeito ao item (ii), uma alternativa seria fornecer ao titular respostas em camada, isto é, atender aquilo que é possível diante das circunstâncias, solicitando esclarecimentos que viabilizem o atendimento do direito do titular, suspendendo o prazo até que os esclarecimentos sejam prestados.

b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

Entende-se que a distinção entre os prazos estabelecidos nos incisos I e II do artigo 19 da LGPD se baseia no nível de detalhamento das informações solicitadas. Enquanto o inciso I trata da confirmação de existência ou acesso a dados pessoais em formato simplificado, o inciso II aborda uma declaração mais abrangente, incluindo a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento.

No que tange ao inciso I, é necessário esclarecimento quanto ao que se entende por atendimento imediato. Organizações de variados tamanhos e setores possuem realidades distintas de tratamento de dados, bem como números diversos de titulares e sistemas envolvidos, de modo que a interpretação conferida a este termo deve levar em consideração que o cumprimento depende de tempo hábil para processamento do pedido pelos agentes de tratamento. Nesse contexto, a questão pode ser desenvolvida a partir do §4º do artigo 19, que permite à Autoridade definir prazos diferenciados dos previstos nos incisos I e II do artigo 19 da LGPD para setores específicos.

Nos caso em que setores específicos necessitam de tempo adicional para cumprir com os direitos de confirmação de existência ou o acesso a dados pessoais, seria possível (i) adotar entendimento flexível quanto à margem de cumprimento “imediato” (ex.: a partir da solicitação o sistema pode levar até 48 horas para gerar os dados em formato simplificado); e (ii) seguir o previsto pelo GDPR, conforme disposto em seu artigo 12(3): os direitos dos titulares devem ser atendidos em um mês, com a opção de prorrogação por até dois meses, levando em consideração a complexidade e o volume de solicitações.

Nesse sentido, o Information Commissioner's Office (ICO) dispõe sobre a possibilidade do setor privado estender o prazo de resposta (no caso, o GDPR do Reino Unido) por mais dois meses se a solicitação for complexa ou incluir outros tipos de solicitações relacionadas aos direitos dos indivíduos que devem ser atendidas simultaneamente, como em caso de pedidos acumulados de eliminação e de portabilidade de dados. (Disponível em: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-should-we-consider-when-responding-to-a-request/>>).

A Data Protection Commission (DPC) também destaca os critérios de complexidade e múltiplos pedidos, bem como fornece exemplos que podem ser adotados no caso brasileiro, como: (i) indisponibilidade de imediato de grande quantidade de dados no sistema; (ii) necessidade de emprego de recursos extras para cumprimento do pedido; (iii) envolvimento considerável de dados de terceiros; e (vi) necessidade de suprimir informações de terceiros ou que envolvam segredo de negócio. (Disponível em:

<https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf>).

c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Para garantir uma comunicação eficaz entre o titular e o agente de tratamento, a Câmara-e.net destaca a importância de a ANPD fornecer orientações claras sobre vários aspectos. Estes incluem:

- (i) A importância de a Autoridade reconhecer a necessidade de cautela na autenticação do titular e possivelmente sugerir boas práticas para o tema;
- (ii) A necessidade de a Autoridade afirmar explicitamente que o processo de autenticação dos titulares antes do atendimento a solicitações relacionadas aos seus direitos é legítimo, e que cabe ao controlador determinar a melhor forma de realizá-lo, inclusive indicando quais dados deve ou não coletar para o cumprimento dessa função, considerando sua realidade organizacional, situação específica e riscos envolvidos, entre outros fatores;
- (iii) Estabelecer que o prazo para atender aos direitos dos titulares deve começar a partir do dia subsequente à validação de um pedido como legítimo, o que implica na autenticação do titular, na clareza do pedido e no seu encaminhamento por canal adequado;
- (iv) Reconhecer a liberdade do controlador para definir a abordagem mais apropriada para o atendimento dos titulares, como a utilização de um canal unificado ou a disponibilização de diversos canais;
- (v) Deixar claro que o formato da resposta ao titular deve ser determinado pelo controlador, levando em consideração a realidade organizacional e outras circunstâncias relevantes.

Ao avaliar as características dos canais de atendimento aos titulares, é fundamental que a Autoridade leve em conta a diversidade dos agentes de tratamento, considerando fatores como tamanho e estrutura organizacional. É importante destacar que as organizações lidam de maneiras diversas com os direitos dos titulares, adaptando-se à sua realidade específica e sendo as mais indicadas para determinar as características desses canais. Nesse sentido, um estudo conduzido pela International Association of Privacy Professionals (The State of Data Rights, 2020) ressalta essas variações e suas implicações.

Além disso, é crucial considerar que os titulares podem apresentar desafios adicionais à comunicação. Por exemplo, pedidos genéricos de dados podem resultar em atendimentos deficientes devido à falta de precisão na solicitação, requerendo esclarecimentos adicionais. Além disso, as preferências dos titulares por outros meios de comunicação e sua relutância em fornecer informações necessárias, bem como em realizar a autenticação necessária podem complicar ou até inviabilizar o processo de atendimento, mesmo quando o canal de comunicação está disponível e acessível. Portanto, é fundamental reconhecer que a eficácia da comunicação entre as partes não é exclusivamente responsabilidade do controlador, mas depende de atos de boa-fé de ambos os lados.

d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

É fundamental reconhecer que a execução adequada das obrigações legais pelo operador é essencial para garantir os direitos dos titulares. Isso inclui a obrigação de manter registros das operações de tratamento de dados pessoais (conforme estabelecido no artigo 37) e de conduzir o tratamento de acordo com as instruções do controlador (conforme estipulado no artigo 39).

Quanto às responsabilidades específicas que devem ser atribuídas ao operador para viabilizar o adequado atendimento dos direitos dos titulares pelo controlador, é necessário estabelecê-las por meio de contrato, após negociações entre as partes. Essas responsabilidades podem abranger aspectos como suporte técnico e operacional, notificação tempestiva do recebimento de solicitações de exercício de direitos ou de solicitações de esclarecimento provenientes da Autoridade, entre outras.

e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

A adoção de abordagens semelhantes às do Serviço de Atendimento ao Consumidor (“SAC”) apresenta desafios significativos quando aplicada ao atendimento dos direitos dos titulares. Vários aspectos tornam essa estratégia inadequada:

- 1) Disponibilidade contínua: Manter um serviço disponível 24 horas por dia, 7 dias por semana, é impraticável para muitas organizações, especialmente as de menor porte. Além disso, o atendimento adequado aos direitos dos titulares muitas vezes requer análises detalhadas, cooperação entre equipes e, por vezes, consultas legais, o que torna difícil manter uma disponibilidade ininterrupta.
- 2) Imposição do atendimento telefônico: Tornar o atendimento telefônico obrigatório limita a flexibilidade dos controladores para escolher o melhor meio de comunicação, desconsiderando as preferências e necessidades dos titulares. Isso pode, ainda, não ser eficaz para respostas mais complexas, considerando o que foi disposto no item anterior, e prejudicar a acessibilidade e conveniência para os titulares.
- 3) Acesso irrestrito aos dados: Embora a autenticação seja essencial para proteger os dados dos titulares, exigir acesso irrestrito pode comprometer a privacidade e segurança dessas informações.
- 4) Padronização excessiva do atendimento telefônico: Estabelecer requisitos rígidos para o atendimento por telefone pode resultar em burocracia e custos adicionais para as organizações, sem necessariamente melhorar a qualidade do serviço prestado.
- 5) Inclusão obrigatória de opções de contato em documentos impressos: Exigir opções de contato em todos os documentos impressos pode ser excessivo e desnecessário, especialmente considerando o ambiente digital predominante.
- 6) Rigidez nos parâmetros de acompanhamento das demandas: Definir parâmetros muito específicos pode ser inadequado e inflexível, não levando em conta a diversidade das organizações, as necessidades dos titulares e a complexidade para elaboração de respostas às solicitações.

- 7) Prazos de resposta apertados: O prazo de sete dias corridos estabelecido pelo Decreto nº 11.034/2022 pode ser desafiador para muitas organizações, especialmente quando comparado ao prazo mais flexível previsto pelo GDPR.

Essas considerações ressaltam a importância de adaptar as práticas de atendimento dos direitos dos titulares às especificidades de cada organização, às particularidades de cada direito garantido pela LGPD, e às necessidades dos próprios titulares.

f. Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

É fundamental reconhecer que alguns elementos necessitam de esclarecimentos por parte da ANPD, conforme destacado na resposta à questão “c” da presente Seção. No entanto, é crucial que as organizações tenham liberdade para estabelecer o formato de atendimento mais adequado às suas particularidades e às necessidades dos titulares dos dados.

Essa abordagem se justifica por diversos motivos:

Flexibilidade: As organizações possuem estruturas, processos e sistemas diferentes, o que significa que não há uma abordagem única que sirva para todas. Possibilitar que as organizações determinem seu próprio formato de atendimento permite adaptar-se de forma mais eficiente às suas próprias realidades e às demandas dos titulares.

Inovação: Ao permitir que as organizações tenham liberdade para definir seus próprios formatos de atendimento, incentiva-se a inovação e o desenvolvimento de novas soluções e tecnologias que possam melhorar a experiência do titular e a eficiência do processo.

Personalização: Cada organização pode ter uma compreensão diferente das necessidades e preferências dos seus titulares. Permitir que elas determinem seu próprio formato de atendimento possibilita a personalização das soluções para melhor atender às expectativas dos usuários.

Eficiência econômica: Ao dar liberdade às organizações para estabelecerem seu próprio formato de atendimento, possibilita-se a busca por soluções mais econômicas e eficientes, levando em conta as capacidades financeiras e operacionais de cada organização.

Portanto, embora seja importante que a ANPD forneça orientações claras e elucidativas, é igualmente crucial que as organizações tenham autonomia para determinar como implementar essas diretrizes de forma a melhor atender às necessidades dos titulares e garantir a conformidade com a legislação de proteção de dados.

II. INFORMAÇÕES SOBRE O TRATAMENTO (ART. 18, INCISOS I, II, VII E VIII):

a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Primeiramente, é importante destacar que, embora a questão tenha sido abordada na seção dedicada ao direito de acesso, esta reflexão se estende a todos os direitos previstos na LGPD.

Sobre os limites dos direitos dos titulares, é importante que se considere que nenhum direito individual deve ser considerado absoluto. Essa mesma lógica se aplica à interpretação da LGPD em relação aos novos direitos concedidos aos titulares de dados pessoais.

Dentro desse contexto, existem valores e considerações legais que limitam o exercício dos direitos de acesso e outros direitos estabelecidos pela LGPD. Esses incluem: (i) a liberdade de expressão; (ii) necessidade de cumprimento de obrigação legal; (iii) a condução de investigações e processos internos; (iv) os direitos e liberdades de terceiros; (v) informações confidenciais e dever de sigilo; (vi) a proteção da propriedade intelectual e, de maneira mais ampla, dos segredos empresariais; e (vii) a impossibilidade de verificação da titularidade do solicitante. Além disso, é necessário coibir o exercício abusivo dos direitos, comportamento expressamente condenado pela legislação nacional (conforme o artigo 187 do Código Civil).

Nesse sentido, pode haver recusa em atender a um pedido quando seu exercício for abusivo, o que pode ser determinado pelo excesso do pedido ou pela má-fé na solicitação. Como exemplos de condutas de má-fé, podem-se citar: (i) a ausência de intenção genuína de exercer o direito, buscando apenas prejudicar o controlador com solicitações infundadas; (ii) solicitações maliciosas feitas com o intuito de assediar a organização sem propósito legítimo; (iii) insistência em usar um canal inadequado para o exercício dos direitos, apesar das orientações do controlador; (iv) direcionamento do pedido a um funcionário específico por motivos pessoais; ou (v) envio sistemático de múltiplos pedidos sem aguardar o prazo de resposta.

Por outro lado, pedidos excessivos podem incluir: (i) solicitações flagrantemente desproporcionais; (ii) repetição de pedidos já atendidos sem justificativa para informações adicionais; (iii) renovação de pedidos dentro de um curto intervalo de tempo sem motivo válido; (iv) formulação do pedido com intenções diferentes das que justificam o direito; (v) descon sideração das normativas que regem o tratamento de dados; (vi) exposição de dados de terceiros; ou (vii) solicitações específicas sobre medidas técnicas e administrativas adotadas pelo controlador, quando envolvem segredos comerciais, conforme ressalta o artigo 19, inciso II, da LGPD.

b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

Entendemos que a obrigação de fornecer informações sobre o compartilhamento de dados deve se restringir à indicação das categorias de destinatários e às finalidades para as quais os dados são tratados, o que atende ao princípio da transparência e às solicitações de acesso dos titulares dos dados. Nesse sentido, é importante considerar que a divulgação nominal das entidades públicas e privadas com as quais o controlador compartilhou dados pode acarretar uma série de problemáticas. São exemplos:

- 1) **Aspectos concorrenciais:** Revelar as entidades com as quais o compartilhamento é realizado pode proporcionar uma vantagem competitiva a determinadas empresas, o que pode distorcer o mercado e prejudicar a concorrência.
- 2) **Propriedade intelectual e segredo de empresa:** Em muitos casos, as informações sobre as entidades com as quais os dados são compartilhados são consideradas confidenciais e estratégicas para a empresa. Divulgá-las nominalmente pode comprometer a propriedade intelectual e o segredo empresarial, especialmente se a

restrição a essas informações representar um valor econômico significativo para a empresa.

- 3) **Confidencialidade contratual:** Em alguns casos, as organizações podem estar sujeitas a acordos de confidencialidade que as proíbem de divulgar a identidade das entidades com as quais compartilham dados. Isso pode ocorrer em contratos comerciais ou parcerias estratégicas, nos quais a confidencialidade é essencial para proteger os interesses das partes envolvidas.

Sugerimos que, caso o titular não esteja satisfeito com os dados fornecidos inicialmente, seja adotada uma abordagem de repasse de informações em camadas, como recomendado pela Agência Espanhola de Proteção de Dados (“AEPD”). Isso permitiria um fornecimento mais específico de informações sobre as entidades com as quais o compartilhamento é realizado, garantindo ao mesmo tempo a proteção dos interesses comerciais e legais das organizações envolvidas. Mais detalhes sobre essa abordagem podem ser encontrados no seguinte link: <https://www.aepd.es/en/rights-and-duties/know-your-rights/right-information>.

c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?

É fundamental reconhecer que a execução adequada das obrigações legais pelo operador é essencial para garantir os direitos dos titulares. Isso inclui a obrigação de manter registros das operações de tratamento de dados pessoais (conforme estabelecido no artigo 37) e de conduzir o tratamento de acordo com as instruções do controlador (conforme estipulado no artigo 39). Quanto às responsabilidades específicas que devem ser atribuídas ao operador para viabilizar o adequado atendimento dos direitos dos titulares pelo controlador, é necessário estabelecê-las por meio de contrato, após negociações entre as partes. Essas responsabilidades podem abranger aspectos como suporte técnico e operacional, notificação tempestiva do recebimento de solicitações de exercício de direitos, entre outras.

d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

Para atender ao requisito do inciso I do artigo 19 da LGPD, que estabelece a necessidade de uma declaração em formato simplificado sobre o tratamento de dados pessoais, entendemos que bastaria o fornecimento de uma cópia dos dados pessoais do solicitante, a depender da extensão daquilo que foi solicitado pelo titular. Nesse formato simplificado, deve-se evitar que nele se encaixem pedidos genéricos ou excessivos relacionados “a todos os dados em posse do controlador” ou “tudo que tenha sobre mim”, mas sim atrelar a um contexto / serviço / funcionalidade determinada, que deve estar expressa no requerimento do titular (ex.: “fornecer os meus dados cadastrais em posse do controlador”, “histórico de minha transação financeira”, “histórico de meus pedidos” etc.). Além disso, é importante que a Autoridade esclareça que o fornecimento da declaração em formato simplificado é suficiente para fins de cumprimento do direito de acesso, salvo se o titular expressamente solicitar a declaração completa.

e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

As informações destinadas ao titular sobre o tratamento de seus dados, sem necessidade de solicitação específica, estão definidas no artigo 9º da LGPD e, portanto, estarão nas políticas de privacidade externas do controlador. Estas incluem a finalidade específica do tratamento, a modalidade e o prazo do tratamento, respeitando os segredos comerciais e industriais, a identificação e os detalhes de contato do controlador, informações sobre o compartilhamento de dados pelo controlador, considerando apenas as categorias de destinatários e sua finalidade, as responsabilidades dos agentes encarregados do tratamento e os meios para exercício dos direitos do titular, com destaque para os direitos listados no artigo 18 da lei. É importante esclarecer que, devido à complexidade de algumas dessas informações, elas poderão ser fornecidas de forma mais ampla, inclusive para permitir o entendimento do titular.

Em relação ao exercício dos direitos dos titulares, entende-se que a LGPD requer que o controlador oriente os titulares a respeito do meio de seu exercício, capacitando-os. Contudo, não requer informações publicamente disponibilizadas sobre os critérios e procedimentos utilizados na decisão automatizada, sendo que essas informações requerem a solicitação do titular, dentro do contexto do artigo 20 da LGPD.

Além disso, no contexto das informações solicitadas pelos titulares, a Câmara-e.net gostaria de reiterar a abordagem recomendada pela Agencia Española de Protección de Datos, que propõe a disponibilização dessas informações em camadas aos titulares. Mais detalhes sobre essa metodologia podem ser consultados no seguinte link: <<https://www.aepd.es/en/rights-and-duties/know-your-rights/right-information>>.

f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

A questão suscita certa ambiguidade em relação ao seu propósito, porém, parece estar questionando se o direito de acesso é considerado satisfeito quando o agente de tratamento disponibiliza os dados pessoais em formato digital ou em papel, de acordo com a escolha do titular. O parágrafo 2º do artigo 19 da LGPD estipula que o controlador deve cumprir o direito de acesso conforme solicitado pelo titular. Isso implica que, caso o titular especifique sua preferência por um formato específico (digital ou papel), o controlador deve fornecer os dados nesse formato. No entanto, na ausência de especificação por parte do titular, cabe ao controlador selecionar o meio que considere mais adequado para disponibilizar os dados.

Além disso, entendemos que o formato da entrega “em papel”, advinda da requisição de “forma impressa”, deve ser interpretada à luz das evoluções tecnológicas recentes. Atualmente, serviços podem ser desenvolvidos e prestados inteiramente em formato digital, de modo que se faz necessário que a Autoridade possibilite que a escolha pelo titular em receber os dados de forma impressa inclua a via do documento digital em que se permite a sua impressão pelo titular, o que inclusive é condizente com os fundamentos da LGPD nos quais, dentre outros, se incluem o desenvolvimento econômico, tecnológico e a inovação.

III. PORTABILIDADE DOS DADOS (ART. 18, INCISO V):

a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

É fundamental destacar que, antes de determinar se um certo setor possui maturidade para atender aos pedidos de portabilidade, várias questões precisam ser esclarecidas (definição de portabilidade e interoperabilidade, limites técnicos e legais, consentimento de terceiros, responsabilidade dos agentes de tratamento, limites diante de direitos de propriedade intelectual e segredo de negócio, etc). Logo, esse tema deve ser discutido em tomadas de subsídios e consultas públicas para compreensão e esclarecimento das complexidades envolvidas no atendimento a um eventual pedido do titular para a portabilidade de seus dados.

Para alguns dos associados da Câmara-e.net, a portabilidade de dados não representa um desafio significativo. Um exemplo notável é a abordagem da Google, que oferece aos seus usuários a portabilidade de dados há mais de uma década. Desde 2007, a empresa investiu em uma equipe dedicada à facilitação da exportação de dados de seus produtos, culminando no desenvolvimento do Google Takeout, que permite o download de dados de mais de 70 produtos da Google (mais informações podem ser encontradas aqui: <<https://blog.google/outreach-initiatives/public-policy/building-data-portability-help-consumers-choose/>>). Além disso, em 2018, Google, Apple, Meta, Microsoft, Twitter e SmugMug lançaram o Projeto de Transferência de Dados (DTP), uma iniciativa que visa simplificar a portabilidade de dados em nível global. O DTP desenvolveu um framework de tecnologia de código aberto que alimenta recursos de transferência direta de dados em serviços como Google Takeout, Transferência de Informações do Facebook e Página de Dados e Privacidade da Apple (mais informações encontram-se disponíveis aqui: <<https://dtinit.org/our-work>>). Outros associados, por sua vez, cumprem o direito à portabilidade por meio de soluções próprias ou de terceiros.

No entanto, é importante ressaltar que a associação é composta por membros de diversos setores e que a maturidade para lidar com a portabilidade de dados pode variar consideravelmente. Portanto, antes de fazer recomendações específicas, é crucial realizar uma análise detalhada, assim, recomendamos que a Autoridade promova um debate específico com os setores envolvidos para compreender melhor a situação.

b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

Os desafios para a implementação do direito à portabilidade vão desde aspectos legais, por exemplo, o que realmente é a portabilidade de dados e quais dados podem estar sujeitos a ela, até técnicos, por exemplo, como permitir que indivíduos movam, copiem ou transfiram facilmente dados pessoais em diferentes plataformas de maneira segura e protegida. Entretanto, dado que a portabilidade de dados requer adoção de medidas administrativas e técnicas para desenvolvimento ou aprimoramento das tecnologias específicas para a sua implementação, poucas orientações até o momento foram fornecidas aos responsáveis pelo tratamento de dados no que diz respeito à conformidade.

Levando em consideração os diversos campos de ação do setor privado e os diferentes estágios de maturidades em tecnologia de cada organização, a ANPD deve fornecer esclarecimentos e apresentar exemplos concretos, no sentido de explicar as circunstâncias nas quais este direito é aplicável, quais os limites quanto ao alcance dos pedidos e abrangência do fornecimento de dados, bem como permitir que as organizações tenham flexibilidade para entender e adotar o melhor formato de atendimento aos pedidos de portabilidade para cada uma, em respeito às melhores práticas dos seus setores, possibilitando maior eficiência na adaptação das diferentes

realidades em estrutura, processos e sistemas, devendo haver especial atenção da ANPD quanto a preservação dos segredos comerciais e industriais, expressamente ressalvados no artigo 18 inciso V da LGPD.

c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

As organizações devem ter flexibilidade e autonomia para escolha do melhor formato para a transmissão dos dados, respeitando um formato que seja de uso corrente e garanta a interoperabilidade, o que não implica exigir que os responsáveis pelo tratamento tenham que necessariamente manter sistemas compatíveis.

A ANPD deve focar, portanto, no desenvolvimento de padrões e boas práticas que permitam a comunicação de sistemas, arquivos e/ou ferramentas sem que, com isso, se dê preferência a uma delas em detrimento das demais. Isso porque, o mercado é dinâmico e a tecnologia evolui a níveis exponenciais, sendo plausível que o mercado se autorregule nas formas de interação e comunicação para a implementação da interoperabilidade. Cabe à ANPD, portanto, orientar e trazer exemplos concretos, sem limitar as vias técnicas possíveis.

d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?

Embora a LGPD não traga essa possibilidade de forma expressa no artigo 18, inciso V, o artigo 40 permite a compreensão no sentido de que uma vez fornecidos os dados para o titular em formato interoperável, conforme futuro Regulamento da ANPD, o direito de portabilidade poderá ser considerado com atendido, nos moldes do que é previsto no GDPR. Isso porque se o próprio titular optar por solicitar os dados pessoais a certo controlador em formato interoperável, é porque entende que seu direito será melhor atendido dessa forma. Assim, entendemos ser importante que a ANPD disponha sobre padrões de modo flexível, permitindo aos agentes adequar-se segundo as práticas consolidadas e o contexto das atividades de tratamento específicas de seus nichos, levando em consideração fatores como: (i) os segredos comercial e industrial; (ii) a carga financeira ou técnica excessiva ou irrazoável para o porte da empresa; (iii) os direitos e a privacidade de terceiros; (iv) a quantidade e complexidade dos dados solicitados; (v) o volume de solicitações.

É relevante observar que este aspecto do direito de portabilidade não deve:

- 1) Impor aos controladores a obrigação de adotar e manter sistemas de processamento tecnicamente compatíveis;
- 2) Responsabilizar o agente de tratamento transmissor pelo tratamento realizado pelo próprio titular dos dados ou por outro agente de tratamento receptor dos dados pessoais;
- 3) Estabelecer uma obrigação específica de verificar a qualidade dos dados antes da transmissão;
- 4) Exigir que o controlador retenha os dados pessoais por mais tempo do que o necessário ou além de qualquer período de retenção especificado.
- 5) Incluir informações que revelem segredos comercial e industrial, como categorias de segmentação de titulares de dados, trazendo, em exemplos, os critérios ou as informações mínimas que poderiam ser assim consideradas.

e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

É plausível permitir que o setor privado desempenhe um papel na definição de padrões de interoperabilidade específicos para diferentes atividades econômicas no âmbito da portabilidade de dados. Essa abordagem se justifica pela diversidade de necessidades e características que os diversos setores podem apresentar em relação à variedade de formatos de dados tratados e à transferência de dados entre sistemas e plataformas distintas. Envolvendo o setor privado nesse processo, podemos esperar soluções mais adaptadas e eficazes tanto para empresas quanto para consumidores dentro de cada setor.

Embora possam servir como referências úteis ou diretrizes para as empresas, esses padrões específicos não podem ser interpretados como uma imposição, o que poderia limitar a capacidade das organizações de encontrar as soluções mais adequadas às suas necessidades individuais ou de seus setores.

No que se refere ao estabelecimento de prazos, considerando que a definição pelo setor privado será apenas uma sugestão, não haveria que se falar em prazo para a implementação desses padrões.

IV. CORREÇÃO DOS DADOS TRATADOS (ART. 18, INCISO III):

a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

A fim de avaliar a qualidade de um dado, considerando se está incompleto, inexato ou desatualizado, é necessário analisar a situação específica à luz dos princípios da qualidade e finalidade estabelecidos pela LGPD. Embora o princípio da qualidade demande a exatidão dos dados, é relevante entender que essa exigência pode variar conforme a finalidade do tratamento. Por exemplo, em um cadastro de e-commerce, pode ser aceitável que o titular forneça apenas um dos seus sobrenomes, enquanto em procedimentos mais formais, como o registro de uma escritura de imóvel, a precisão dos dados torna-se mais crucial.

O Information Commissioner's Office ("ICO", disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/#ib5>) destaca que, ao receber um pedido de retificação, o controlador deve adotar medidas razoáveis para verificar a precisão dos dados e corrigi-los, se necessário. Essas medidas devem levar em conta a natureza dos dados pessoais e sua finalidade de uso. Quanto maior for a necessidade de precisão da informação, mais esforço será necessário para verificar e corrigir sua exatidão, especialmente se os dados forem fundamentais para decisões significativas que impactam o indivíduo ou terceiros.

Adicionalmente, é essencial estabelecer claramente os limites desse direito, assegurando que ele se aplique apenas a dados genuinamente incompletos, inexatos ou desatualizados. Esse direito não deve ser utilizado para revisar eventos passados, e os controladores devem ter o direito de solicitar ao indivíduo evidências específicas que comprovem a incorreção das informações retidas. É crucial ainda que tais evidências se refiram exclusivamente a fatos,

excluindo opiniões, em respeito à liberdade de expressão. A ANPD deve deixar claro que a retificação se aplica exclusivamente a dados que são factualmente incompletos, inexatos ou desatualizados, e não a dados com os quais o indivíduo simplesmente discorda.

b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

É relevante destacar a estreita relação entre o direito de correção e o princípio da qualidade dos dados, que visa garantir aos titulares a exatidão, clareza, relevância e atualização dos dados conforme necessário para cumprir a finalidade do seu tratamento. Nesse contexto, é fundamental que o controlador tenha a possibilidade de solicitar aos titulares (i) elementos suficientes para comprovar a autenticidade do titular-requerente para evitar incidente de segurança; (ii) evidências de que os dados estão incompletos, inexatos ou desatualizados; e (iii) as informações necessárias e comprovadas para fins de correção. Por exemplo, o Information Commissioner's Office ("ICO", para mais informações consulte: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/>) destaca que, ao receber uma solicitação de correção, o controlador deve adotar medidas razoáveis para verificar a qualidade dos dados e corrigi-los, se necessário, levando em consideração os argumentos e as evidências apresentadas pelo titular.

c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.

Para determinar a impossibilidade ou o esforço desproporcional, conforme definido no art. 18, § 6º, da LGPD, é fundamental examinar cada caso de maneira específica e individualizada. Não existe uma lista definitiva de critérios objetivos que se apliquem uniformemente a todas as situações. Em vez disso, é necessário uma análise dos detalhes específicos de cada solicitação de acesso aos dados pessoais.

Essa abordagem personalizada permite considerar uma variedade de fatores contextuais que podem influenciar a capacidade de atender à solicitação. Por exemplo, o volume de solicitações, os recursos disponíveis para o controlador, o tamanho da equipe responsável pelo tratamento dos dados e os possíveis impactos nas operações do controlador são aspectos relevantes a serem ponderados.

Portanto, ao lidar com solicitações de acesso aos dados pessoais, é essencial que o controlador avalie cada situação individualmente, levando em conta os diversos fatores que podem afetar a capacidade de atender à solicitação de maneira adequada e em conformidade com a LGPD. Isso garante o respeito efetivo aos direitos dos titulares de dados, ao mesmo tempo em que reconhece os desafios e limitações enfrentados pelos controladores na gestão e proteção desses dados.

d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

Considerando os preceitos do princípio da qualidade dos dados e as disposições do inciso III do artigo 18, é facultado ao controlador recusar o atendimento ao pedido do titular caso julgue que os dados estejam completos, precisos e atualizados. Ademais, a falha na verificação da autenticidade e a ausência dos documentos necessários fornecidos pelo titular também pode

fundamentar a negativa do controlador. Acrescenta-se que a ANPD deve esclarecer que o direito de correção não implica em uma revisão retroativa, visando, assim, evitar possíveis implicações legais decorrentes de mudanças passadas, e que deve ser restrito a fatos, preservando a liberdade de expressão (essas opiniões são defendidas pelos Centre for Information Policy Leadership no seguinte documento: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world_8_july_2020_.pdf>).

Além disso, reitera-se os pontos trazidos em relação aos limites do exercício abusivo de direito, o que pode ser verificado pelo excesso do pedido, e até mesmo pela má-fé na solicitação dos dados. Como condutas de má-fé podem ser consideradas as seguintes situações, entre outras: (i) o indivíduo claramente não tem intenção de exercer o seu direito, mas procura retaliar ou incomodar o controlador de seus dados com pedidos descabidos; (ii) a solicitação tem intenções maliciosas e está sendo evidentemente usada para assediar, de forma recorrente, uma organização sem nenhum propósito real a não ser causar transtorno; (iii) quando o controlador indica o canal correto para o exercício dos direitos (ex: OneTrust, e-mail específico, campo específico em seu website) e o titular insiste reiteradamente em realizar o exercício por canal diverso; (iv) o pedido é feito a um funcionário específico contra o qual fica evidente que o requerente tem algum rancor pessoal; ou (v) quando o titular envia sistematicamente pedidos de correção para o controlador sem sequer aguardar o decurso do prazo para resposta.

Já como excessivos, podem ser considerados os seguintes exemplos: (i) quando o pedido é flagrantemente desproporcional (pedidos que desvirtuam o intuito da lei; pedidos coletivos utilizados para retaliação contra o controlador); (ii) se a solicitação repete pedidos anteriores já respondidos sem detalhar o que adicionalmente corrigir; (iii) quando o pedido renova um anteriormente feito e devidamente respondido num intervalo inferior a 6 (seis) meses, salvo justo motivo, como por exemplo a atualização do banco de dados.

Além desses, o controlador pode restringir o direito de correção, ainda que demonstrada as evidências de sua declaração, em casos que possam, exemplificativamente: (i) obstruir uma investigação, inquérito, procedimento oficial ou legal; (ii) prejudicar a prevenção, a detecção, a investigação ou o processo de infrações penais ou a execução de penalidades, bem como procedimentos de combate a fraudes ou ilícitos, incluindo os ocorridos na internet; (iii) violar os direitos e as liberdades de terceiros, incluindo a liberdade de expressão.

V. ANONIMIZAÇÃO, BLOQUEIO, ELIMINAÇÃO E OPOSIÇÃO NO CASO DE TRATAMENTO IRREGULAR (ART. 18, IV E § 2º):

a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Sim, de acordo com o inciso IV do artigo 18, o titular deve apresentar justificativas e evidências que indiquem que os dados são desnecessários, excessivos ou estão sendo tratados em desconformidade com a legislação, a fim de exercer os direitos de anonimização, bloqueio ou eliminação. Assim, é fundamental que a ANPD esclareça aos titulares que forneçam recursos suficientes para os agentes de tratamento analisarem as solicitações, sobretudo em relação à

identificação do possível problema que ocasionou o pedido. Em muitos casos, o titular se opõe ao tratamento com alegação de irregularidade, mas que na verdade é uma incompreensão ou falta de conhecimento da legislação nacional e da regulamentação setorial no tema, por falta de leitura dos contratos que fazem parte (Termos de Uso, Política de Privacidade ou demais contratos de prestação de serviço), e até mesmo por desconhecimento da existência de outras bases legais para além de seu consentimento.

É importante ressaltar ainda que a anonimização, bloqueio ou eliminação não devem ser realizados se o controlador estiver tratando os dados pessoais de acordo com uma base legal válida (por exemplo: cumprimento de obrigação legal ou regulatória pelo controlador, como é o caso do artigo 16 da Resolução BCB nº96/2021, para o exercício regular de direitos em processo judicial, administrativo ou arbitral e prevenção à fraude e à segurança do titular), pois nesse caso os dados continuarão sendo necessários e seu uso será legalmente justificado.

Além disso, os dados também poderão ser mantidos nos casos previstos no artigo 16 da LGPD.

Outro aspecto relevante sobre o direito de eliminação, bloqueio ou anonimização que não foi objeto de questionamento, mas que está abrangido na presente questão diz respeito à necessidade de esclarecimento pela ANPD no sentido de que o controlador não precisa apresentar uma prova conclusiva da operação realizada, bastando sua declaração nesse sentido. Isso se justifica pela natureza impraticável de se produzir uma prova negativa, especialmente considerando a complexidade dos sistemas de armazenamento e processamento de dados. Exigir tal prova poderia impor ônus desproporcionais aos controladores. Portanto, a declaração do controlador, acompanhada de medidas adequadas de boa-fé, deve ser considerada suficiente para atestar a exclusão, bloqueio ou anonimização dos dados, garantindo a efetividade dos direitos de privacidade dos titulares sob a LGPD.

b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

Sim, tanto a anonimização quanto à eliminação são medidas que podem ser consideradas de forma alternativa, dependendo do contexto específico, sendo ambas reconhecidas pela Lei Geral de Proteção de Dados Pessoais.

O artigo 12 da LGPD estipula que os dados anonimizados deixam de ser considerados dados pessoais. Isso implica que, ao seguir os critérios definidos pela legislação para anonimização, os dados perdem sua capacidade de identificar indivíduos, oferecendo uma alternativa viável à eliminação completa dos dados.

Além disso, o inciso IV do artigo 16 da LGPD permite a retenção de dados pessoais pelo controlador, desde que os dados sejam anonimizados e utilizados exclusivamente por ele. Essa disposição legal reconhece que a anonimização dos dados oferece um nível suficiente de proteção à privacidade, permitindo que o controlador mantenha os dados para usos específicos, desde que não possam ser acessados por terceiros.

Portanto, a LGPD reconhece tanto a anonimização quanto à eliminação como medidas equivalentes para garantir a proteção dos dados pessoais, oferecendo às organizações a flexibilidade necessária para escolher a abordagem mais adequada às suas necessidades e à natureza dos dados envolvidos.

c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

Se a alegação do titular for considerada legítima de acordo com o art. 18, § 2º, da LGPD, isso implica que o controlador deve atender ao pedido formulado pelo titular. Essa obrigação de cumprimento do pedido não apenas satisfaz as demandas individuais do titular, mas também induz o controlador à conformidade legal com a LGPD. Com o atendimento de tal pedido e a consequente conformidade legal, o direito de oposição, nos termos do referido dispositivo, perde seu fundamento.

VI. REVOGAÇÃO DO CONSENTIMENTO (ART. 18, VI E IX):

a. A revogação do consentimento prevista no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular? Explique

A revogação do consentimento, conforme estipulado no art. 18, IX, da LGPD, não implica necessariamente na obrigação de eliminar os dados pessoais tratados com base nesse consentimento. Isso se deve à possibilidade de existir outra base legal que justifique o tratamento desses dados, como em casos em que são necessários para o cumprimento de um contrato entre o controlador e o titular dos dados, ou para o cumprimento de uma obrigação legal.

É importante ressaltar que, frequentemente, as empresas precisam dos dados pessoais para uma variedade de propósitos, e o tratamento pode ser fundamentado em mais de uma base legal, conforme se extrai do artigo 16 da LGPD. Portanto, a revogação do consentimento não implica automaticamente na exclusão de todos os dados, tampouco afeta o tratamento de dados realizado até o momento em que a eliminação foi solicitada, sendo, em princípio, legítimo o tratamento de dados realizado até então. Esse entendimento é corroborado pelos Guidelines on consent under Regulation 2016/679 do Working Party 29, que destacam a complexidade das bases legais para o tratamento de dados (disponível em: <https://ec.europa.eu/newsroom/article29/items/623051>).

Além disso, um exemplo prático é a necessidade do controlador de reter os dados para garantir o cumprimento das preferências do titular. Nesse cenário, é necessário manter certos dados para assegurar que determinado tratamento não ocorra, o que evidencia a importância de considerar diferentes bases legais para o tratamento de dados pessoais.

b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

Na falta de outra base legal para o tratamento, a eliminação dos dados é obrigatória. Quando os dados foram compartilhados, é crucial notificar os entes com quem foram compartilhados. No entanto, em certas situações específicas, é imprescindível que o controlador mantenha certos dados para orientar suas ações. Por exemplo, se um titular manifestar o desejo de não receber mais propagandas, é necessário manter os dados para garantir que o direcionamento não ocorra. É importante destacar, contudo, que o tratamento realizado com base no consentimento anterior à revogação continua legalmente válido.

Portanto, nas situações em que os dados tenham outras finalidades a eles atreladas (por exemplo, contrato vigente, obrigação legal ou regulatória, legítimo interesse para combate à fraude, defesa judicial etc), o regime do artigo 18, IV, da LGPD é que deve ser aplicado, considerando que os dados serão mantidos não pelo consentimento já revogado, mas sim para dar cumprimento às demais situações que justificam a sua retenção, que envolvem as demais bases legais do art. 7º ou 11 da LGPD.

VII. DECISÕES BASEADAS EM TRATAMENTO AUTOMATIZADO (ART. 20, CAPUT):

a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

Uma decisão tomada unicamente com base em tratamento automatizado é aquela na qual não há participação humana no processo de tomada de decisão. Isso implica que a decisão é completamente gerada por meio de processamento automatizado, sem qualquer intervenção ou influência direta de indivíduos. Além disso, é importante observar que, ao discutir a LGPD e, mais especificamente, o artigo 20, está a se debater decisões automatizadas que envolvam o tratamento de dados pessoais e que necessariamente afetem os interesses dos titulares de dados envolvidos.

b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

Para determinar quando um interesse está sendo efetivamente afetado, a ANPD deve levar em consideração, no cenário brasileiro, critérios ou situações em que: (i) o indivíduo é impossibilitado - ilegalmente - de exercer regularmente seus direitos previstos pelo ordenamento jurídico de modo prolongado, causando efeitos negativos que comprometam o exercício de direitos fundamentais; (ii) o indivíduo é - ilegalmente - prejudicado em seu acesso a serviços, por exemplo, relacionado a educação, saúde, transporte etc.; (iii) o indivíduo sofre com situações ilícitas, com impactos graves ou prejudiciais, como em caso de discriminação.

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

A aplicação do direito de revisão de decisões, conforme delineado no art. 20 da LGPD, enfrenta uma série de desafios práticos consideráveis. Um dos principais obstáculos reside na complexidade dos sistemas que empregam tecnologias de aprendizado de máquina e inteligência artificial. Estes sistemas frequentemente geram decisões automatizadas com base em algoritmos intrincados, dificultando a explicação clara aos titulares sobre os motivos subjacentes a uma decisão específica.

Ademais, a possível necessidade de intervenção humana para revisar e explicar as decisões automatizadas pode acarretar custos adicionais de recursos para as organizações. Isso decorre do fato de que a participação humana pode elevar os custos operacionais e administrativos, sem que, necessariamente, ganhe-se em capacidade intelectual, eficiência ou que se potencialize seus efeitos mitigatórios, já que o humano possui acesso a menos informações ou variáveis do que os inputs fornecidos na decisão automatizada.

Outro desafio está em fornecer explicações claras e acessíveis aos titulares sem comprometer os direitos de propriedade intelectual e segredos comerciais das organizações. A divulgação das informações requeridas pelos §1º do artigo 20 pode entrar em conflito com a necessidade de resguardar informações confidenciais e estratégicas da empresa, criando uma complexidade adicional na aplicação desse direito.

Além disso, a manutenção de registros detalhados sobre as decisões tomadas e os processos envolvidos pode demandar investimentos significativos em sistemas de registro e armazenamento de dados. Isso pode representar um desafio para pequenas e médias empresas.

Por fim, a efetiva implementação do direito de revisão de decisões também está sujeita à definição do que seria “afetar interesses”, o que se espera seja definido pela ANPD de forma razoável.

d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

Sim, o controlador pode negar o direito de revisão sobre decisões automatizadas quando: (i) a decisão possuir alguma participação humana ou a decisão automatizada não impactar de forma relevante os interesses do titular, o que não se enquadra nos termos do artigo 20 da LGPD, afastando a sua incidência (em linha com os itens “a” e “b” acima); (ii) a resposta pode revelar algoritmo, informações do código fonte ou a lógica de programação, violando direitos de propriedade intelectual e segredo comercial; e (iii) quando a revisão é inviável, seja por questões técnicas ou práticas.

Informações mínimas: sugere-se que as informações para garantir a transparência no tratamento dos dados pessoais e identificação dos controladores sejam fornecidas aos titulares de forma sucinta (apenas com os elementos essenciais).

Implementação da interoperabilidade: Para assegurar a capacidade de interação entre sistemas é necessário estabelecer um layout padronizado de comunicação (definido em comum acordo pelas associações representativas do setor) que viabilize o compartilhamento de dados não apenas pelas grandes empresas, mas também pelos pequenos e médios empresários, por meio da adoção de arquivos simplificados sempre que compatível com a demanda (Ex.: casos em que não haja um volume muito grande de dados).

II. RESPOSTA AOS ITENS DA TOMADA DE SUBSÍDIOS SOBRE OS DIREITOS DOS TITULARES.

i. BLOCO 1 Relacionamento entre o controlador e o titular

a. É razoável para o setor privado, para o atendimento aos direitos do titular de dados pessoais, a adoção de prazos similares aos previstos na Lei nº 12.527, de 18 de novembro de 2011? Em caso negativo, o que tornaria o atendimento inviável nos prazos previstos e quais seriam os prazos razoáveis?

Ainda que os temas tratados na Lei nº 12.527 ("LAI") e na Lei Geral de Proteção de Dados ("LGPD") possam, à primeira leitura, ser considerados similares, não se pode deixar de ressaltar suas diferenças conceituais, pois, ao passo em que a primeira busca regulamentar o acesso dos cidadãos exclusivamente a informações públicas, objetivando a transparência do poder público, a LGPD busca estabelecer regras para o tratamento de dados pessoais dos cidadãos conferindo extensa gama de direitos a serem observados em benefício dos titulares por entidades públicas e privadas. O tratamento das informações e as tratativas no escopo da LAI são menos morosos que o tratamento de dados pessoais e outros procedimentos necessários para atendimento aos direitos dos titulares pela LGPD.

Diante do exposto, recomenda-se que seja determinado o prazo para primeira resposta no período de até 1 (um) mês da solicitação, podendo ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos - a exemplo do disposto no artigo 12.1 do GDPR.

Outrossim, propõe-se que a ANPD estabeleça contagem de prazos em dias úteis, excluindo o dia do começo e incluindo o dia do vencimento, em linha com o estabelecido nos Arts. 218 a 235 do CPC e pela GDPR.

c Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Em primeiro lugar, para garantir a efetividade na comunicação entre o titular e o agente de tratamento, a ABIPAG entende relevante que haja autonomia das organizações para estabelecer o formato de atendimento. Sem prejuízo, também propõe: **(i)** Identificação do titular solicitante a fim de permitir que o controlador atue de maneira assertiva na demanda; **(ii)** Possibilidade de solicitação de informações complementares pelos agentes para que possam identificar o titular requerente, desde que respeitadas as diretrizes de proteção de dados pessoais; e **(iii)** Disponibilidade do canal nos principais meios de comunicação e divulgação do agente de tratamento (ex.: sites e aplicativos). Modelo comum no mercado é a utilização de formulários de solicitação integrados em sistemas de atendimento e a realização de pedidos por e-mail com padrões de informações.

d Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

A ABIPAG considera que o operador desempenha um importante papel na execução adequada das obrigações legais, o que inclui a manutenção dos registros das operações de tratamento de dados pessoais e o tratamento dos dados em acordo com as instruções do controlador. Neste sentido, entende-se que a responsabilidade deve ser estabelecida contratualmente entre as partes e haja cooperação entre controlador e operador para assegurar a proteção dos dados pessoais de forma eficaz.

e Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor (“SAC”), estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

No lugar de uma abordagem padronizada, sugere-se que haja autonomia para adoção de práticas no contexto específico de cada organização e de acordo com as necessidades dos

titulares. Entende-se que aplicação de medidas como SAC poderiam se mostrar proibitivas para organizações de menor porte - sobretudo diante da complexidade de implementação.

f Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

Não. Conforme reforçado anteriormente, a ABIPAG entende que a autonomia das organizações na definição do formato de atendimento é fundamental para possibilitar a adaptação às suas especificidades e às necessidades dos titulares dos dados.

ii. Bloco 2: Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII)

a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Sim. A ABIPAG entende que tal direito não é absoluto, podendo sofrer limitação com o intuito de assegurar a proteção da liberdade de expressão, a conformidade com a lei, a realização de investigações, a proteção dos direitos de terceiros, a preservação de informações confidenciais, a defesa da propriedade intelectual e a prevenção de abusos. Para fins exemplificativos, elencam-se os casos em que a confirmação da existência do tratamento possa comprometer informações estratégicas ou sigilosas de uma instituição, ocasião em que a legislação pode permitir a negativa desse direito com base na proteção do direito comercial.

b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

Para evitar desafios como vantagens competitivas indevidas, violação de segredos empresariais, dentre outros similares, a ABIPAG sugere que as informações fornecidas para identificação dos controladores, mesmo em casos de compartilhamento de dados pessoais, limitem-se a indicar as categorias de destinatários e as finalidades do tratamento dos dados.

d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

Sugere-se que a declaração simplificada sobre o tratamento de dados pessoais inclua os dados pessoais tratados e suas finalidades, observado o escopo solicitado pelo titular. Devem constar também os dados de identificação do titular solicitante e a justificativa para a manutenção dos grupos de dados identificados e encaminhados – exigência que poderá ser cumprida com simples remissão ao aviso de privacidade do controlador, por exemplo.

e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

A ABIPAG acredita que, para assegurar transparência e direito à informação, o controlador deve divulgar, conforme os artigos 9º e 18º da LGPD, informações como a finalidade do tratamento, modalidade, prazo, identificação do controlador, detalhes de contato, informações sobre compartilhamento de dados e suas finalidades, responsabilidades dos agentes de tratamento e direitos do titular. Adicionalmente, recomenda-se a criação e ampla divulgação de avisos de privacidade e disponibilização de informações em camadas para facilitar o entendimento dos titulares. Estas informações incluiriam aspectos relacionados à adoção de decisões automatizadas e os agrupamentos de dados pessoais necessários na avaliação, como dados de contato, biométricos, entre outros.

f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

Sim, entende-se que haverá satisfação do direito do acesso se o agente de tratamento disponibilizar as informações no formato escolhido pelo titular (digital ou em papel), conforme determina o parágrafo 2º do artigo 19 da LGPD. Se o titular não especificar sua preferência, o controlador tem a liberdade de escolher o formato mais adequado para disponibilizar os dados, sendo que, no caso da necessidade de encaminhamento dos dados em papel, seja considerada a possibilidade de repasse do custo para os titulares de dados.

iii. BLOCO 3: Portabilidade dos dados (art. 18, inciso V)

a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

Setor financeiro, em que o projeto de implementação do Open Finance apresenta-se como um grande sucesso, pois possibilitou o acesso a dados e históricos financeiros, beneficiando os usuários finais com a melhoria de produtos e serviços bancários que lhe eram oferecidos, bem como facilitando o acesso ao crédito. Contudo, considerando que a maturidade para lidar com a portabilidade pode variar entre os setores, a ABIPAG recomenda que ANPD promova debates e estudos aprofundados, incluindo análises internacionais e consultas públicas, antes que seja realizada uma recomendação específica.

b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

A ABIPAG entende que, para além dos desafios tecnológicos de implementação de um layout padrão que garanta a compatibilidade de todos os agentes, existem desafios relacionados à implementação em si, tais como atribuição de quem será o ente responsável pela base que permitirá a interoperabilidade, definição de custos, garantia de segurança cibernética dos dados e afins. Por essa razão, para que haja efetividade em eventual regulação, a ABIPAG recomenda que a ANPD promova um amplo debate com os agentes controladores antes de disciplinar o tema.

c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

Para assegurar a capacidade de comunicação entre sistemas, é importante avaliar a viabilidade da padronização, visando possibilitar a transferência de dados em formatos compreensíveis e facilmente acessíveis. Para além disso, a ABIPAG ressalta que entende relevante que eventual padronização não se restrinja a integrações complexas via API, mas também seja viabilizado, sempre que possível, o compartilhamento em formatos de exportação menos complexos, como planilhas e PDFs, assegurando a utilização da funcionalidade por pequenos e médios empresários.

e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

Entende-se que a participação do setor privado é indispensável para definição dos padrões obrigatórios de interoperabilidade, devendo ser definidos em comum acordo pelas principais associações representativas do setor. É importante que essas associações também estejam envolvidas em discussões futuras acerca dos prazos de implementação, considerando que possuem conhecimento prático da complexidade das atividades exercidas por seus associados, bem como do tempo necessário para se adaptarem às novas exigências.

iv. Bloco 4 Correção dos dados tratados (art. 18, inciso III):

a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

Sugere-se que, para que um dado seja qualificado como incompleto, inexato ou desatualizado, é importante considerar critérios objetivos, como a verificação da fonte dos dados, a data da última atualização, a precisão das informações e a integridade dos registros.

b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

Entende-se que a declaração do titular não seria suficiente para exercer o direito à correção caso a alteração interfira no princípio da qualidade do dado que exige exatidão. Nestas instâncias, a correção deve ser avaliada, pois pode gerar complexidades para outros direitos regulares do controlador.

c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD?

A ABIPAG entende que não há critérios objetivos passíveis de aplicação a todas as situações. Por essa razão, a associação sugere uma abordagem individualizada para cada solicitação de acesso a dados pessoais. Para tanto, é essencial que haja análise de aspectos como o número de entidades envolvidas, a diversidade dessas entidades, a complexidade da cadeia de compartilhamento, a variação na sensibilidade dos dados e os recursos disponíveis para o controlador. Encontrar o equilíbrio adequado entre transparência e eficiência é fundamental, garantindo que a divulgação das entidades envolvidas seja proporcional às circunstâncias específicas de cada caso.

Além disso, é importante considerar a proporcionalidade entre o esforço necessário para atender à solicitação de acesso e os benefícios reais para o titular dos dados. Em alguns casos, o fornecimento de acesso pode demandar um esforço desproporcional em relação aos benefícios que o titular obterá com esta informação. Nestes casos, faz-se necessária a avaliação criteriosa para garantir equilíbrio entre os direitos do titular e as limitações do controlador.

Portanto, a ABIPAG destaca a importância de uma abordagem flexível e contextualizada para a avaliação da impossibilidade ou esforço desproporcional previstos no art. 18, § 6º, da LGPD. Esta abordagem busca conciliar a proteção dos dados pessoais com a viabilidade operacional das empresas, garantindo um tratamento equilibrado para todas as partes envolvidas.

d. Exemplifique. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

A ABIPAG acredita que o controlador pode recusar o atendimento caso entenda que os dados estejam completos, precisos e atualizados, isto é, em conformidade com o princípio da qualidade dos dados e a disposição do art. 18, III da LGPD ou quando o titular não fornece documentação adequada que comprove a inexistência dos dados. Cabe também ressaltar que, abusos no exercício desse direito, como pedidos feitos de má-fé ou excessivos, podem fundamentar a negativa. Exemplos de má-fé incluem intenções de retaliação ou assédio ao controlador sem propósito legítimo, solicitações maliciosas ou pedidos feitos de forma repetitiva sem justificativa válida.

v. BLOCO 5 Anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e § 2º):

a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Sugere-se aplicação da regra prevista no art. 18, IV da LGPD para os casos em que haja solicitação de anonimização, bloqueio ou eliminação de dados, ou seja, que o titular fundamente e comprove a desnecessidade, excessividade ou desconformidade legal dos dados, ainda que não o faça lastreado em fundamentos legais.

b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

Sim, pois trata-se de alternativa permitida pela LGPD levando em consideração o contexto específico do tratamento e da organização, bem como a particularidade de cada cenário. Instituições com grandes volumes de armazenamento em nuvem enfrentam desafios financeiros ao considerar a eliminação de dados, dada a necessidade de revisão e exclusão em larga escala. Em contrapartida, a anonimização emerge como uma alternativa mais viável, preservando dados para análise estatística sem comprometer a privacidade dos titulares.

c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

Quando um titular apresenta uma alegação legítima de oposição ao tratamento de seus dados, o controlador tem a responsabilidade de agir conforme a lei. Isto pode envolver a suspensão da atividade de tratamento ou a realização de modificações para garantir a legalidade do processo. Além disso, é importante que os dados coletados ilegalmente sejam excluídos ou anonimizados, uma vez que caso seja, sua manutenção sem fundamento legal também poderia constituir uma violação. Nesse contexto, a transparência é outra obrigação do controlador, podendo ser necessário que este informe ao titular as medidas adotadas em resposta à sua alegação de oposição. Isto pode incluir mudanças nas práticas de tratamento ou até mesmo a suspensão do tratamento, se for o caso.

vi. Revogação do consentimento (art. 18, VI e IX):

b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

Conforme previsto no art. 8º da LGPD, o requerimento de eliminação de dados pessoais gera efeitos sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado. Na mesma linha, entende-se que os tratamentos realizados com base no consentimento anteriormente concedido pelo titular dos dados permaneceriam válidos, até que haja requerimento de eliminação, nos termos do inciso VI do art. 18 da referida Lei. Dessa forma, entende-se que a revogação do consentimento mediante manifestação expressa do titular não invalida os tratamentos realizados

anteriormente, reforçando a importância do requerimento de eliminação para cessar tais atividades.

vii. Decisões baseadas em tratamento automatizado (art. 20, caput)

a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

Uma decisão automatizada é aquela em que o processo de tomada de decisão é realizado por meio de algoritmos ou sistemas computacionais, sem intervenção humana direta. Uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais é aquela em que não há qualquer participação ou interferência humana no processo de tomada de decisão, sendo totalmente conduzida por algoritmos ou sistemas computacionais. Essas decisões são baseadas somente nos dados pessoais fornecidos e processados, sem a análise ou consideração de informações adicionais por parte de uma pessoa.

b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

Sugere-se que sejam considerados os seguintes critérios: (i) quando há impacto significativo na vida do titular dos dados (Ex.: decisões relacionadas a emprego, crédito ou acesso a serviços essenciais) ou quando há uso de dados sensíveis; (ii) quando não há explicações ou transparência em processos decisórios que podem gerar consequências substanciais, como negação de serviços ou restrição de direitos; e (iii) quando há violação de direitos fundamentais, como o direito à não discriminação ou à privacidade. Esses aspectos são importantes para garantir que as decisões automatizadas respeitem os princípios de equidade e transparência, protegendo os interesses dos titulares dos dados.

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

A ABIPAG identifica desafios como: **(i)** a criação de sistemas e processos capazes de rastrear e analisar as decisões automatizadas, bem como garantir a transparência e a explicabilidade dessas decisões para os titulares dos dados; **(ii)** o desenvolvimento de mecanismos que permitam que os titulares contestem e solicitem a revisão de decisões automatizadas, especialmente quando essas decisões são complexas ou baseadas em

algoritmos; e **(ii)** a falta de recursos nas organizações para lidar com as solicitações de revisão de decisões de forma oportuna e eficiente, especialmente considerando a possibilidade de um grande volume de solicitações, e a falta de documentação e regras padronizadas sobre os critérios de decisões automatizadas, o que pode dificultar ainda mais o processo de revisão.

Nesse sentido, a ABIPAG recomenda o desenvolvimento de diretrizes bastante objetivas para orientar as organizações sobre como cumprir suas obrigações de revisão de decisões sob a LGPD, garantindo uma abordagem uniforme e apropriada em todos os casos.

d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

A negativa do direito de revisão sobre decisões automatizadas pode ocorrer quando há razões técnicas, legais ou de segurança que justifiquem a não divulgação ou revisão detalhada da decisão ao titular dos dados. A ABIPAG entende que a revisão deverá ser feita dentro do limite da tecnologia, ou seja, dentro dos casos em que seja possível executá-la.

Sendo o que servia para o momento, a ABIPAG se coloca à inteira disposição da ANPD para prestar esclarecimentos adicionais que se façam necessários.

Atenciosamente,

ABIPAG – ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS

- **Tipo de Direito:** Dependendo do tipo de direito, tempo maior pode ser necessário para atendê-lo. Assim, direitos como “acesso simplificado” (19, I), anonimização ou retificação, devem ter prazo menor, do que o de “acesso completo” (19, II), portabilidade ou exclusão por exemplo.
- **Complexidade da Solicitação:** Solicitações complexas e que envolvam diversos pedidos em um só devem ter prazo sequenciais e individualizados – por exemplo, direito de acesso, retificação e exclusão simultâneos devem ter prazo individuais e sucessivos para atendimento.
- **Natureza do Dado:** Quão mais sensíveis os dados, maior a tendência de segurança no seu tratamento, logo, maior a complexidade para atender a pedidos dos titulares – como acesso e exclusão, por exemplo.
- **Volume de dados:** em geral, quanto maior o volume de dados objeto do tratamento, mais complexa será o atendimento de eventual solicitação.
- **Tipo de Serviço e amplitude da clientela:** em linhas gerais, organizações que, por sua natureza, lidam com um volume significativo da população (como provedores de conexão, linhas aéreas, instituições financeiras...) tendem a ter um volume de solicitações significativamente superior ao da maioria dos agentes regulados, o que pode demandar tratamento diferenciado.
- **Necessidade de aplicação de isenções:** como dados pertencentes ou relacionados a outros titulares.

Q- c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

R- Entendemos que para canal de atendimento ser suficientemente efetivo, ele deve atender aos seguintes requisitos:

- **Amplamente divulgado:** o acesso ao Portal de Privacidade e/ou Aviso de Privacidade contendo o canal deve ser facilmente visível na experiência do usuário, com o canal de atendimento claramente identificado e acompanhado de instruções claras sobre como utilizá-lo.
- **Acessível para a pessoa-média:** Isto é, deve ser facilmente acessível pela maioria das pessoas, como: endereço de correio eletrônico, número de telefone ou formulário em um *website*;
- **Linguagem simples:** deve utilizar de linguagem clara e acessível para garantir que as informações sejam compreendidas facilmente pelo titular e prestar informações em formato inteligível, que não demande conhecimento prévio para acessar a resposta.
- **Gratuito (como regra):** Inexistência cobrança por parte do Controlador e os eventuais custos necessários para alcançar o canal de comunicação não apresentem óbice considerável para o exercício de direitos à pessoa-média – ex: embora acesso à internet ou a uma linha telefônica envolva custos, ele são razoáveis e, em regra, não serão óbice ao exercício de direitos – por outro lado, demandar que o titular envie solicitação por correspondência física, com cópia de documentos autenticados, pode representar custo proibitivo. É importante apenas deixar claro que em situações de abuso do exercício regular de direitos pelo titular (exemplo: titular que reiteradamente exerce seus direitos de acesso) o agente de tratamento poderá cobrar do titular de dados os valores exatos despendidos para tal atendimento.

- **Permitir a Fundamentação:** O titular deve ser capaz de fundamentar o seu pedido, explicar os seus motivos e/ou ofertar mais detalhes a respeito de sua solicitação, inclusive o resultado que deseja alcançar.
- **Seguro:** considerando a tecnologia utilizada, o agente de tratamento deve adotar cuidados razoáveis para garantir a segurança do canal de comunicação escolhido (ex. criptografia dos dados em trânsito).
- **Suportado por procedimentos adequados:** os agentes regulados devem estruturar fluxos de atendimento e estabelecer prazos para o atendimento das requisições de acordo com a legislação vigente, inclusive direcionando a demanda para o Encarregado, sempre que adequado o seja.

Q- d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

R- Apesar de não existir obrigação legal expressa a respeito do dever de cooperação por parte dos Operadores, é razoável deduzir que esse dever está diretamente relacionado à necessidade de serem observadas as instruções lícitas do Controlador. Adicionalmente, em atenção às boas-práticas, é recomendável que isso seja incluído (e tipicamente o é) no contrato entre o controlador e o operador.

Dito isso, o dever de cooperação por parte do operador deve ser entendido como a obrigação de empregar esforços razoáveis para que o controlador consiga atender à solicitação apresentada ao titular, observado o escopo do contrato entre as Partes.

Desde que relacionado ao objeto da relação entre as partes, podemos delimitar essa obrigação de duas formas, em linha com o item 8.3.1 da NBR ISO/IEC 27701: (i) fornecer as informações que sejam razoavelmente necessárias para atender às solicitações de determinado titular (ex. fornecer cópia dos dados pessoais ou lista de suboperadores que porventura tenham tido acesso aos dados do titular); (ii) implementar as medidas técnicas e administrativas que sejam razoavelmente necessárias para o atendimento da solicitação (ex. executar *script* para descartar ou alterar determinado dado).

Outrossim, é importante que o Operador mantenha o registro das operações de tratamento, de forma a facilitar o atendimento destes direitos, e mantenha o Controlador informado de suas capacidades e limitações, bem como das ações concretamente executadas para o atendimento de suas orientações.

Q- e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

R- Entendemos que não, pelos seguintes motivos:

- Considerando que a LGPD não determinou nenhum modelo mandatório de canal de atendimento, pelo que, qualquer canal de atendimento razoável, deve ser encarado como perfeito cumprimento das obrigações legais por parte do controlador, posição, inclusive, adotada na União Europeia, conforme se extrai da *Guideline* 01/2022/EDPB, não nos parecem adequadas as seguintes diretrizes constantes na norma legal em análise: (i) operar por diversos canais de atendimento integrados (Art. 2º); (ii) Atendimento telefônico obrigatório (art. 5º); (iii) Necessidade de registro numérico ou outro tipo de procedimento eletrônico (art. 12º)

- A exigência de múltiplos canais e atendimento contínuo pode ser impraticável devido à complexidade e custos de segurança para proteção de dados. Além disso, o atendimento telefônico para os direitos dos titulares previstos na LGPD não se equipara às tratativas no âmbito da legislação consumerista, já que as demandas exigem análise, compreensão e avaliação, conforme exigido pela legislação.
- É impossível também garantir a disponibilidade ininterrupta (art. 4º, *caput*), pois: (i) garantir a disponibilidade absoluta dos canais de comunicação é impossível, sendo a interrupção ou a redução de disponibilidade, consequência, inclusive, da necessidade de manutenção dos sistemas; (ii) o atendimento de solicitações de titulares em regra depende da prévia análise de profissionais de privacidade especializados, inclusive, para verificar a adequação da solicitação apresentada – profissionais especializados e que cuja manutenção requer o dispêndio de valores significativos.
- Considerando que a validação prévia da identidade do titular é uma boa-prática decorrente da necessidade de se atender ao princípio da segurança e encontra previsão tanto em códigos de conduta setoriais nacionais (SARB nº 25/FEBRABAN), quanto na *Guideline* 01/2022/EDPB, não entendemos adequadas as diretrizes relativas à(ao) (i) **não-vinculação do contato inicial ao fornecimento de dados pessoais (art. 4º, §4º)**; e (ii) **termo inicial do prazo contado a partir do registro da demanda (Art. 13º)**.
- **Necessidade de inclusão do canal de atendimento em todo documento na contratação do serviço (art. 7º)**: entendemos, com base na redação do art. 9º da LGPD, que é suficiente que o canal para o exercício de direitos dos titulares seja incluído no Aviso de Privacidade.
- **Os direitos garantidos pela LGPD dizem respeito aos dados pessoais dos titulares e não são o foco dos serviços prestados (art. 14º)**

R- f. Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

R- Existem modelos de atendimento já adotados, que permitem o tratamento de grande volume de solicitações, por meio de ferramentas tecnológicas (ex. OneTrust, Securiti.ai...) que tornam o processo de resposta às solicitações de direitos, no mínimo, parcialmente automatizado.

Essas soluções geralmente são conectadas às bases de dados, e, quando diante de solicitação do titular, podem, dentre outros: (i) realizar varreduras, identificando, por meio de certos identificadores (ex. CPF), se dados do titular são armazenados, quais dados e em quais bases; (ii) fornecer ao titular a possibilidade de baixar os dados ao seu respeito; e (iii) gerar (e até mesmo executar) *scripts* destinados à eliminação e modificação de dados.

A problemática é: muitas dessas soluções tecnológicas possuem custo para a sua implantação, especialmente no atual momento de considerável desvalorização do real em relação ao dólar, pelo que, mesmo as soluções nacionais, muitas vezes não são acessíveis para as organizações em geral, não devendo, portanto, ser tornados obrigatórios, mas como recomendações de boas práticas.

II. Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII):

Q- a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

R- Sim. Existem situações em que é razoável que seja negado o direito de confirmação da existência do tratamento:

- Quando a confirmação puder causar prejuízos significativos ao agente de tratamento ou à sociedade. Podemos trazer alguns exemplos típicos, em que é razoável manter o tratamento em sigilo: (i) dados relacionados a suspeitas e investigações de fraude, em âmbito privado; (ii) dados relativos a suspeitas e investigações de financiamento ao terrorismo ou lavagem de dinheiro; (iii) investigações de incidentes; (iv) dados relacionados a operações de tratamento resguardadas por segredos comerciais.
- Quando o titular não tenha comprovado a sua identidade, em atenção a requisição razoável de prova por parte do controlador; ou
- Quando o titular atue de má-fé, por exemplo, apresenta solicitações repetitivas ao controlador sem justificativa aparente.
- Quando a confirmação da existência do tratamento de dados pessoais poderia revelar informações que constituem segredo de negócio da empresa, comprometendo sua vantagem competitiva no mercado;
- Durante o curso de investigação e auditorias internas, quando essa divulgação possa prejudicar o desfecho dos trabalhos;
- Casos em que a confirmação possa ser óbice ao exercício de um direito (ex. direito de defesa em uma ação trabalhista);
- Quando a confirmação puder afetar os direitos de privacidade ou outras liberdades fundamentais de outra pessoa;
- Quando o controlador estiver submetido a uma obrigação legal de sigilo;
- Quando a informação puder colocar em risco a defesa e a segurança nacional ou a segurança do Estado e da sociedade;
- Se uma solicitação for claramente ou obviamente irrazoável, considerando-se desproporcional em relação ao ônus ou custos envolvidos no seu atendimento. Deve-se, ainda, levar em consideração todas as circunstâncias da solicitação, incluindo: a natureza das informações solicitadas; o contexto da solicitação e o relacionamento entre o controlador e o indivíduo; se a recusa em fornecer as informações ou mesmo reconhecer se a empresa as detém pode causar danos substanciais ao indivíduo; e os recursos disponíveis.

Q- b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

R- A avaliação precisará ser sempre casuística e atentar aos requisitos concretos.

Para a identificação do controlador responsável pela operação de tratamento, entendemos suficiente a indicação do nome empresarial ou marca pelo qual ele é comumente conhecido.

Em relação ao compartilhamento de dados pessoais, no entanto, consideramos que o dinamismo no compartilhamento e o volume considerável de operações possa tornar a nomeação individual dos controladores uma prática inexequível. Em razão disso, entendemos razoável, enquanto regra, que seja fornecida a categoria de controladores, como seu respectivo setor empresarial, e a finalidade do compartilhamento.

Q- c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?

R- Conforme informado na resposta ao questionamento do item 1.d, a responsabilidade dos operadores deve ser de apresentar o suporte necessário aos respectivos controladores. Assim, caso lhes seja apresentada alguma solicitação de direito, eles devem direcionar os titulares para o controlador, jamais devendo atender à solicitação sem prévia autorização do controlador.

Q- d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

R- Considerando que o formato simplificado requer que os dados sejam fornecidos imediatamente (prazo que entendemos deva ser entendido como em até 2 dias úteis), tal pedido deve poder contemplar apenas os dados cadastrais (nos termos do artigo 11, § 2º do Decreto 8.771/2016), no formato em que se encontram, isto é, aqueles constantes no cadastro do titular junto à organização, se existentes, visto que tendem a ser os dados prontamente disponíveis para a organização fornecer aos respectivos titulares, e a identificação do controlador responsável.

Q- e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

R- A LGPD já determina, em seu art. 9º, quais informações devem ser proativamente fornecidas pelo controlador. Os quesitos presentes no artigo devem ser interpretados à luz das normas técnicas aplicáveis, especialmente a ABNT NBR ISO/IEC 29184 e em posicionamentos da ANPD (ex. Nota Técnica nº 49/2022/CGF/ANPD), do seguinte modo:

- **Finalidade específica do tratamento:** descrição suficiente a permitir ao titular entender de forma clara e imediata o propósito para o qual os seus dados serão utilizados, esclarecendo-se quais categorias de dados serão utilizadas para quais propósitos.
- **Forma do tratamento:** indicando o método, momento e a localização da coleta dos dados pessoais, o método de seu uso (inclusive se envolverá tomada de decisão automatizada) e a jurisdição legal em que os dados ficarão armazenados (isto é, se haverá transferência internacional).
- **Duração do tratamento:** isto é, o prazo identificado, ou identificável, em que os dados serão retidos.
- **Identificação do controlador:** seu nome empresarial, podendo incluir o seu CNPJ.

- **Informações de contato do controlador:** entendemos tratar-se do contato do Encarregado ou, para os agentes de tratamento de pequeno porte, o canal para o exercício de direitos que fala o art. 11, §1º, do Regulamento de Agentes de Tratamento de Pequeno Porte.
- **Informações acerca do uso compartilhado de dados pelo controlador e a finalidade:** com quais agentes de tratamento (ou categorias de agentes de tratamento) poderão ser compartilhados dados, quais dados e com quais finalidades.
- **Responsabilidades dos agentes que realizarão o tratamento:** Complemento ao item anterior, identificando a função/papel dos agentes de tratamento (ou categoria de agentes de tratamento) no processo.
- **Direitos do titular:** Fornecer aos titulares uma listagem com seus direitos conferidos pelo art. 18º, da LGPD. Embora a legislação não obrigue, o fornecimento de informações a respeito de direitos previstos em outros artigos, como àqueles constantes no art. 20º, deve ser visto como uma boa prática.

Especificamente em relação aos Processos de Tomada de Decisão Automatizada, entendemos que devem ser fornecidos a categoria de dados tratados e a respectiva finalidade.

Q- f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

R- Sim. Ressalvado se o titular solicitar informação adicional sobre o tratamento, entendemos como razoável que o fornecimento de cópia digital dos dados pessoais seja adequado a satisfazer os direitos de acesso.

No entanto, caso o titular requeira que as informações sejam fornecidas em formato impresso, entendemos por razoável que o agente de tratamento possa requerer que o titular arque com os custos razoáveis do fornecimento das informações nesse formato (ex. custos de impressão e envio).

III. Portabilidade dos dados (art. 18, inciso V):

Q- a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

R- Atualmente, entendemos que apenas os setores regulados, com iniciativas em vigor ou desenvolvimento para se permitir a portabilidade de dados (como o setor financeiro e o setor securitário) se encontram parcialmente aptos a implementar o direito de portabilidade de forma suficientemente madura, seguindo-se os *frameworks* já estabelecidos pelas respectivas regulações setoriais.

Q- b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

R- Os desafios são inúmeros e extremamente complexos. Implementar padrão de interoperabilidade global, aplicável a todos os agentes de tratamento, tende a enfrentar problemáticas técnicas, dentre as quais:

- **Padrões setoriais:** a existência de múltiplos padrões já bem estabelecidos e pacificados nos diferentes setores – o que, se não for problema intrasetorial, pode tornar o compartilhamento de dados com controlador que não integre o setor do agente de tratamento de origem consideravelmente dificultado.

- **Obsolescência acelerada:** o rápido desenvolvimento tecnológico faz com que padrões rapidamente sejam substituídos, pelo que padrão adequado, na atualidade, para manter a interoperabilidade, pode não o ser dentro de alguns anos.
- **Variedade tecnológica:** as organizações tendem a utilizar diferentes aplicações e sistemas, inclusive operacionais, que podem se utilizar de diferentes linguagens e protocolos de comunicação, o que pode dificultar significativamente a interoperabilidade.
- **Necessidade de definição de padrões comuns:** para garantir a interoperabilidade é necessário definir padrões comuns de escopo e de dados e de participantes, compatibilidade tecnológica, padrão de conexão entre sistemas e ferramentas e padrões e requisitos técnicos de implementação, como medidas de segurança, inclusive quanto à integridade dos dados.
- **Custos significativos:** a interoperabilidade requer investimento significativo para a sua implementação, bem como deve ser considerada a existência de esforço sensível para que os dados e arquivos sejam convertidos em formato padrão.

Q- c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

R- Considerando que o direito de portabilidade afeta a todos os agentes de tratamento, inclusive os de pequeno porte, entendemos que o processo de padronização deve: *(i) ser residual, isto é, apenas aplicável quando inexistir regulação (ou autorregulação) setorial sobre o tema;* *(ii) ser suficientemente preciso para tornar a portabilidade exequível;* e *(iii) ser suficientemente amplo, de modo a permitir que todos os agentes de tratamento, inclusive os de pequeno porte, possam atendê-lo.* Tendo isso em consideração, em nosso entendimento a ANPD deve priorizar quatro itens:

- **O formato em que os dados devem ser fornecidos, priorizando-se formatos simples e amplamente acessíveis:** sendo recomendável que os dados sejam fornecidos de forma estruturada e, preferencialmente, em formatos tipicamente de simples manuseio e tipicamente utilizados para exportar dados para sistemas e aplicações de *internet* ou facilmente exportáveis para bancos de dados, como o XLSX, CSV ou JSON.
- **O caminho da transferência:** na inexistência de ferramentas setoriais específicas, entendemos que os dados devem poder ser transferidos por quaisquer meios razoavelmente seguros e acessíveis.
- **Medidas mínimas de segurança e criptografia devem ser aplicadas durante o processo de transferência:** por exemplo, estabelecendo a necessidade de se garantir a criptografia dos dados em trânsito.
- **O processo de transferência:** entendemos que devem ser definidos: *(i) o dever do titular de assegurar, e fornecer ao agente de tratamento de origem, as informações necessárias para permitir com que o agente de tratamento de origem execute seu processo de transferência, conforme orientações deste;* *(ii) os papéis e responsabilidades individuais dos agentes de tratamento;* e *(iii) o prazo mínimo com que o agente de tratamento de origem deve manter os dados e as informações disponibilizados ao agente de tratamento de destino.*

Q- d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?

R- Sim. Considerando que, nessas hipóteses, o titular pode, por si só, compartilhar seus dados com os demais controladores,

conforme acerto direto com estes, entendemos que o fornecimento aos titulares dos dados ao seu respeito será suficiente para o atendimento do direito à portabilidade.

Q- e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

R- Sim. Além de razoável, é também desejável, tendo em vista que permite que as organizações do setor privado, em suas associações setoriais, adotem os mecanismos mais adequados para cada setor.

Na União Europeia, essa cooperação é valorizada e incentivada como parte dos esforços para promover a interoperabilidade em todos os setores e indústrias. O WP29, por exemplo, em suas “guidelines on the right to data portability”, incentiva a cooperação entre as partes interessadas da indústria e associações comerciais para desenvolver um conjunto comum de padrões e formatos interoperáveis, com o objetivo de atender ao direito à portabilidade de dados.

Quanto ao prazo de definição e implantação deste padrão, utilizando o *Open Finance* como parâmetro, cujo marco inicial se deu no início de 2020 (Resolução Conjunta nº 01/2020) e atualmente se encontra em sua última etapa de implantação, iniciada em meados de 2023, sugerimos o prazo de, pelo menos, 05 (cinco) anos.

IV. Correção dos dados tratados (art. 18, inciso III):

Q- a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

R- Como regra geral, um dado só deve ser considerado impreciso, incompleto ou desatualizado se estiver (ou puder ser) sujeito a verificação objetiva, indicando a falta de qualidade na informação. Em outras palavras, a informação deve poder ser objetivamente comprovada como inacurada, seja por ser historicamente imprecisa ou por ter se tornado imprecisa ao longo do tempo. Seguindo esse critério de objetividade, os dados devem ser considerados:

- **Incompletos:** (i) quando estiverem ausentes informações essenciais e campos obrigatórios, elementos de identificação; (ii) quando as informações forem parciais ou fragmentadas; e (iii) quando os dados apresentarem inconsistência;
- **Inexatos:** quando os dados não refletirem a realidade objetiva, por exemplo, não identificando adequadamente os titulares de dados – o que pode transcorrer, por exemplo, quando o agente regulado se utilizava de fontes de dados não confiáveis.
- **Desatualizados:** quando os dados refletirem informações que, embora tenham correspondido a realidade objetiva no passado, já não o fazem; e quando forem obsoletos para a finalidade do tratamento.

Tomando esse requisito de objetividade, existem situações em que a verificação de quaisquer dos cenários acima se fará impossível, por se tratarem de realidades subjetivas ou probabilísticas. Assim, dados que sejam previsões probabilísticas, derivados de análises estatísticas, meramente opinativos (representando inferência sobre alguém), resultantes de testes e questionários preenchidos pelo titular (como testes comportamentais) ou de qualquer outra forma que não possam ser objetivamente comprovados como imprecisos de maneira razoável, não devem ser considerados inverídicos, mesmo que o titular desses dados deles discorde.

Essa regra tem exceções apenas nos casos em que for demonstrado que os dados objetivamente verificáveis que, porventura, fundamentam as informações não-verificáveis não são precisos, completos ou atualizados. Nessas situações, é possível solicitar a correção desses dados objetivamente verificáveis e, uma vez corrigidos, a atualização das informações que dependem deles, mesmo que não possam ser objetivamente verificadas por outros meios.

Exemplificamos: embora o titular não possa solicitar a correção de sua pontuação de crédito em dada instituição, por entender que ele é melhor pagador do que a pontuação aponta, caso alguma informação utilizada no cálculo da pontuação se encontre inacurada ou desatualizada, poderá pedir a sua correção e, feita a correção, que a pontuação seja atualizada.

Q- b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

R- Entendemos que existem situações em que é possível pressupor a possibilidade de a organização condicionar a retificação a algum processo de validação:

- O dado não se enquadra na regra de verificabilidade objetiva proposta no questionamento 4.a;
- Existe razoável probabilidade de dano ao titular ou a terceiros. Por exemplo, se o titular recebe documentação financeira (ou confidencial) em seu endereço, como cartão de crédito, por exemplo, é razoável que a organização valide o endereço, antes de retificá-lo;
- Existe razoável probabilidade de dano ao agente de tratamento. Por exemplo: o titular participa de programa de fidelidade de um varejista e afirma identificou erro em seu histórico de compras, que faz com que ele detenha menos pontos do que deveria (Ex. compra de alto valor não foi registrada). Retificar o histórico de compras sem que o titular comprove a realização da compra implicaria em possível prejuízo ao varejista.
- Existe razoável probabilidade de dano a sociedade. Por exemplo: se a correção dos dados puder prejudicar investigações oficiais, a proteção da segurança pública, a segurança nacional ou os direitos e liberdades de terceiros.
- Existe obrigação legal de validar a informação, como aquelas requeridas às instituições financeiras de validar os dados cadastrais de seus clientes (art. 16, da Circular BCB nº 3.978/2020).
- A solicitação possa ser razoavelmente considerada manifestamente infundada ou excessiva. Por exemplo, se um titular faz repetidos pedidos de correção de um dado, que já foi verificado por diversas vezes como um dado exato, completo e atual.

Essa validação não necessariamente implicará na necessidade de coleta de informação adicional junto ao titular, podendo se operar por outros meios, especialmente pela comparação com informações detidas por birôs de dados.

Q- c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, §6º, da LGPD? Exemplifique

R- Igualmente, a avaliação do esforço desproporcionado deve ser uma avaliação casuística. No entanto, entendemos que alguns requisitos objetivos devem ser considerados em sua elaboração:

- O volume de pessoas a serem notificadas, tendo em vista que influencia no volume de recursos que deve ser alocado para se proceder a comunicação;
- Custo mensurado para o atendimento da solicitação, tendo em vista que quanto maior o custo expectável, maior as chances do agente de tratamento não conseguir arcar com os mesmos.
- Capacidade econômica do agente de tratamento, tendo em vista que influencia no volume de recursos que o agente de tratamento consegue alocar para realizar a comunicação, sem afetar suas operações habituais de negócio;
- O momento em que se operou o compartilhamento, tendo em vista que influencia a utilidade da comunicação – quanto mais tempo decorreu entre o momento do compartilhamento e o momento da retificação, menor a sua utilidade;
- Os efeitos que a comunicação (ou ausência dela) podem previsivelmente surtir no titular, inclusive, considerando eventuais salvaguardas adotadas para resguardar o titular de eventuais danos decorrentes da inexistência das informações.
- Volume e complexidade dos dados objeto da solicitação, uma vez que quanto maior o volume de dados e a sua complexidade, maior tende a ser o impacto ao agente regulado na comunicação às pessoas afetadas;
- Solicitação manifestamente infundada ou excessiva, por exemplo, solicitações repetitivas sem justificativa ou solicitações em massa que impõem uma carga administrativa desproporcional.

Q- d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

R- Entendemos que o direito de correção poderá ser negado em quaisquer das seguintes hipóteses:

- A informação que se busca retificar não é objetivamente verificável, conforme descrito na resposta ao questionamento 4.a ou, sendo objetivamente verificáveis, foram julgados acurados com base na evidência disponível;
- É razoável, ou mesmo legalmente mandatório, validar a informação fornecida pelo titular, nos termos do questionamento 4.b, e essa validação não é possível – por exemplo, o titular se recusou a fornecer o comprovante de residência para alterar o seu endereço;
- Os dados, ainda que equivocados, precisem ser mantidos para fins históricos, inclusive em razão de obrigação regulatória;
- O titular atua de má-fé, exercendo seu direito de retificação de forma abusiva, com objetivos outros, que não o de garantir a qualidade dos dados ao seu respeito;

- Não seja possível verificar a identidade do titular; e
- O atendimento seja excessivo, notadamente quando da apresentação de pedidos repetitivos, sobrepostos ou em volume excessivo.

V. Anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e § 2º):

Q- a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

R- Sim. As obrigações e os encargos das organizações que tratam dados já são demasiadamente pesadas, tendo em vista a LGPD, outras leis e regulamentações setoriais, e os custos com segurança, de forma geral. O cumprimento do princípio da necessidade, da obrigação de não tratar dados excessivos (art. 6º, III), e a conformidade com a legislação e normas aplicáveis, são obrigações dos agentes de tratamento de dados pessoais. Portanto, é de se pressupor que, sendo obrigações, já haverá o seu natural cumprimento, sob pena de denúncias aos órgãos competentes, como a ANPD (além de órgãos setoriais), e respectivas fiscalizações.

Há que se impor regras para os requerimentos dos titulares, sob pena de inviabilizar a conformidade. A título de exemplo, suponha que um titular solicite a exclusão de seus dados pessoais do banco de dados de *marketing* de uma empresa. No entanto, ele não fornece fundamentação para sua solicitação e não demonstra que os dados são desnecessários para os fins do tratamento ou que a empresa está tratando os dados de forma excessiva. Além disso, o titular não aponta nenhuma desconformidade ou descumprimento legal por parte da empresa em relação ao tratamento de seus dados.

Sem a fundamentação clara, prova da desnecessidade dos dados ou da excessividade do tratamento, a empresa pode não ter o embasamento necessário para justificar a eliminação dos dados. A empresa não poderia simplesmente excluir os dados sem justificativa, e ainda estaria sujeita a reclamações do titular ou ações judiciais por não atender à sua solicitação.

Q- b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

R- Sim. A anonimização pode ser considerada a melhor alternativa, a depender da situação específica, como no caso em que os dados são tratados para fins estatísticos. A anonimização pode ser opção mais adequada, pois permite a utilização dos dados de forma agregada, sem identificar os titulares. Entretanto, se os dados já não forem mais necessários para nenhuma finalidade legítima e sua retenção representar risco para os titulares e ao agente de tratamento, a eliminação é a medida cabível. Portanto, a anonimização e a eliminação podem ser adotadas alternativamente, dependendo das circunstâncias específicas e das necessidades do tratamento.

Ainda, tendo em vista que dados anonimizados deixam de ser considerados dados pessoais, para fins da LGPD (art. 12), deve ser considerada cumprida a obrigação do agente de eliminar os dados pessoais ao término do tratamento (art. 16, *caput*). Outrossim, dados anonimizados podem desempenhar importante estímulo às atividades econômicas, apoiando os agentes regulados no aprimoramento de suas atividades.

Q- c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

R- O efeito prático da alegação do titular resultaria na cessação imediata do tratamento contestado, protegendo assim os seus direitos. O controlador deve tomar todas as medidas técnicas e administrativas para garantir que a interrupção seja efetiva, tais como a suspensão de compartilhamentos de dados com terceiros e a eliminação dos dados de seus sistemas.

VI. Revogação do consentimento (art. 18, VI e IX):

Q- a. A revogação do consentimento prevista no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular? Explique.

R- Não. O § 5º do art. 8º da LGPD legitima os tratamentos de dados pessoais realizados antes da revogação do consentimento, ou seja, sob a égide do consentimento anteriormente concedido, e ressalta: “enquanto não houver requerimento de eliminação”. Portanto, a revogação não implica na obrigação de eliminação automática, mas somente se houver o requerimento expresso por parte do titular.

Outrossim, é importante destacar que algumas particularidades podem impossibilitar a eliminação dos dados pessoais, mesmo se exercido o direito de eliminação pelo titular, devendo cada caso ser avaliado isoladamente, em acordo com suas especificidades técnicas. Por exemplo: não necessariamente os dados utilizados na operação de tratamento lastreadas no consentimento são utilizados exclusivamente para aquela operação, podendo ser mantidos para a persecução de outras finalidades, lastreadas em outras bases legais, notadamente eventual obrigação legal.

Q- b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

R- Em regra, caso haja o requerimento de eliminação de dados sob a égide do consentimento anteriormente concedido, os dados deverão ser efetivamente eliminados pelo controlador. No entanto, existem situações excepcionais que os dados pessoais podem ser razoavelmente mantidos, dentre elas: (i) quando presente uma das exceções previstas no art. 16º da LGPD; e/ou (ii) o dado seja razoavelmente necessário para outra operação de tratamento, que não seja fundamentada no consentimento revogado.

VII. Decisões baseadas em tratamento automatizado (art. 20, caput)

Q- a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

R- A diferença entre decisão automatizada e decisão tomada unicamente com base em tratamento automatizado de dados está no nível da intervenção humana e do controle exercido sobre a referida decisão.

Por exemplo, sistema automatizado que recebe os dados financeiros do cliente, como histórico de crédito, renda e dívidas. Com base nessas informações, em conjunto aos critérios definidos pela instituição financeira, o sistema gera automaticamente decisão sobre se o cliente é aprovado ou rejeitado para o empréstimo. Neste caso, o processo é

automatizado, mas pode haver alguma intervenção humana para configurar os parâmetros do sistema, ajustar os critérios de aprovação, ou revisar exceções. Essa intervenção humana pode adicionar certo grau de supervisão e controle à decisão final.

No caso da decisão tomada unicamente com base em tratamento automatizado de dados, o sistema automatizado toma a decisão sem intervenção humana significativa. Ou seja, o sistema é programado para analisar os dados do cliente e, com base em algoritmos pré-definidos, determinar se o empréstimo é aprovado ou rejeitado. Não há revisão humana dos critérios de aprovação ou consideração de circunstâncias especiais do cliente. A decisão é totalmente determinada pelo tratamento automatizado dos dados, sem influência humana direta.

Q- b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

R- Em alinhamento com o Regulamento Europeu, entendemos que um interesse deve ser considerado como “relevantemente afetado”, quando, a decisão possui efeito jurídico relevante ou a este assemelhado – isto é, acarreta repercussões tangíveis na vida do titular, influenciando seu status legal, direitos ou liberdades individuais. Entendemos que essas situações se concretizam quando pelo menos um dos seguintes critérios for satisfeito:

- A decisão, de qualquer modo, afeta a esfera jurídica de uma pessoa, isto é: o conjunto de seus direitos e suas obrigações jurídicas. Por exemplo: decisão que determina o acesso a um produto/serviço por um titular, ou os termos com os quais esse acesso se procederá.
- A decisão impede ou dificulta a produção de efeito jurídico desejado pelo titular, por exemplo, denegando acesso a determinado produto/serviço.
- A decisão afeta substancialmente processo decisório que modifica (ou impede a modificação) da esfera jurídica de uma pessoa – ou seja, ainda que a decisão, por si só, não afete a esfera jurídica do titular, é esperado que ela influencie substancialmente decisões que o façam (ex. pontuações de crédito).
- Embora a decisão não necessariamente afete a esfera jurídica do titular, pode surtir efeitos significativos nos objetos resguardados por seus direitos fundamentais. Por exemplo, decisão que, se equivocada, pode levar ao falecimento do titular.

São exemplos de decisões que satisfazem aos critérios acima àquelas que afetam significativamente o titular em relação a sua situação financeira, saúde, reputação, oportunidade de emprego, formação profissional, seu comportamento, a capacidade de realizar escolhas sobre a sua vida, dentre outros.

Q- c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

R- O maior desafio que se impõe na revisão de decisões automatizadas se refere à complexidade técnica sobre a explicação dessa decisão. Para que o direito à revisão exista, é necessário que o titular tenha possibilidade de apresentar sua percepção sobre como os dados devem ser tratados, de onde possam decorrer erros, discriminações ou mesmo porque um determinado dado ou fator não se aplica ao tratamento. Assim, o direito à explicação pode ser considerado um pressuposto para o exercício de outros direitos.

Há correntes doutrinárias que discutem se esse direito à explicação estaria ou não contemplado no ordenamento jurídico brasileiro, ou até mesmo se seria exequível, tendo em vista possíveis opacidades, que consistem em resultados ininteligíveis nas decisões automatizadas. Isso porque o cérebro humano pode não conseguir identificar o que efetivamente determina o resultado de um modelo algorítmico muito complexo.

Ainda que especialistas dos agentes regulados consigam compreender o racional que levou a uma dada decisão, considerando o volume significativo de parâmetros envolvidos, transpô-los aos titulares de forma inteligível, por si só, tende a ser um desafio significativo.

Além disso, é necessário preservar os segredos comercial e industrial, que por vezes podem ter direta relação com as formas pelas quais o resultado foi atingido.

Outro desafio consiste em assegurar que os processos de revisão sejam transparentes, justos e imparciais, sem comprometer a eficiência e a agilidade das operações automatizadas.

Ainda podem surgir desafios de cunho operacional: na medida em que a sociedade se digitaliza um maior volume de decisões é tomada de forma exclusivamente automatizada, o que pode gerar maior demanda e, conseqüentemente, dificuldade operacional na implementação de processos efetivos de revisão.

Esses desafios demandam não apenas esforços técnicos e operacionais, mas também abordagem cuidadosa e colaborativa entre os setores público e privado, de modo que não haja regulamentação excessiva, com a imposição de obrigações que barrem o desenvolvimento econômico, tecnológico e a inovação (fundamentos da proteção de dados, nos termos do art. 2º, V).

Q- d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

R- Entendemos que podem subsistir algumas situações em que seja razoável que o Controlador denegue o direito de revisão da decisão automatizada. Muito embora entendamos a necessidade de análise casuística, sendo impossível esgotar todas as hipóteses em uma única lista, destacamos as seguintes situações:

- **A decisão envolveu participação humana relevante:** existindo intervenção humana relevante (isto é, apta a alterar o resultado), tendo em vista que o direito previsto no art. 20, *caput*, da LGPD, é limitado às decisões tomadas unicamente por meios automatizados;
- **O titular não forneceu nenhum fundamento apto a modificar a decisão:** o exercício de revisão possui como pressuposto o fornecimento, pelo titular, de argumentos capazes de modificar o entendimento sobre o assunto. Se estes não são apresentados, é impossível proceder a revisão da decisão;
- **Caso, por questões de segredo comercial, o controlador não possa fornecer as informações a que se referem o art. 20, §1º, da LGPD:** sem o fornecimento de informações a respeito do processo decisório, não é possível, em regra, o fornecimento de argumentos pelo titular aptos a modificar a decisão, pelo que inviável o atendimento do direito de revisão;
- **A revisão da decisão não apresenta qualquer utilidade ao titular:** são aquelas situações em que a decisão já produziu e esgotou os seus efeitos, pelo que sua revisão não trará qualquer benefício real ao titular;

- **O titular atua de má-fé:** exercendo seu direito de revisão de forma abusiva, com objetivos outros, que não o de garantir a qualidade dos dados ao seu respeito;
- **Não seja possível revisar a decisão sem comprometer segredo comercial e/ou industrial do controlador ou de terceiros,** por exemplo, caso a decisão faça uso, no todo ou em parte, de um sistema fornecido por terceiro.
- **Quando a revisão manual de decisões automatizadas for tecnicamente ou praticamente inviável,** naquelas situações em que o esforço para realizá-la seja desproporcional aos efeitos concretos no titular de dados, considerando a complexidade, o volume dos processos e de parâmetros envolvidos na decisão.
- **O atendimento seja excessivo:** notadamente quando da apresentação de pedidos repetitivos, sobrepostos ou em volume excessivo.

Rony Vainzof | Caio Lima | Jean Santana | Alexandra Lopes
VLK Advogados

- b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

Assim como nos prazos previstos no artigo 19, o principal critério que deveria ser levado em consideração para a diferenciação de prazos é a **complexidade da solicitação**.

O grau de complexidade da solicitação de um titular pode variar significativamente de acordo com o direito exercido e com as características do caso concreto. Os seguintes fatores podem influenciar:

- ☐ **Quantidade de dados pessoais envolvidos:** Solicitações que envolvem grande volume de dados podem ser mais complexas devido à necessidade de analisar uma grande quantidade de informações. Isso pode incluir dados provenientes de diversas fontes ou armazenados em diferentes sistemas, exigindo esforços adicionais para garantir uma resposta precisa e completa.
- ☐ **Necessidade de cooperação com terceiros:** quando há a necessidade de cooperação com terceiros, o processo pode ser mais complexo, pois é preciso estabelecer uma comunicação eficiente e coordenar esforços entre diferentes partes.
- ☐ **Natureza das atividades do controlador:** se o controlador estiver envolvido em atividades altamente regulamentadas, como serviços financeiros e de saúde, as solicitações relacionadas podem exigir medidas para garantir a conformidade do atendimento.

A análise da complexidade deve ser feita caso a caso. Se não for possível atender à requisição dentro do prazo previsto, é comum em outras legislações permitir ao controlador a prorrogação do prazo, como por exemplo, por até 2 meses na GDPR⁴, 30 dias na PIPEDA⁵ e 45 dias na CCPA⁶. Em qualquer situação, é fundamental que o controlador informe ao titular sobre o andamento da solicitação, qualquer prorrogação de prazo e sua justificativa.

- c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Em primeiro lugar, é essencial avaliar a forma utilizada para a viabilização do canal de atendimento. Conforme as diretrizes do *Article 29 Working Party*, em “*Guidelines on Transparency Under Regulation*”,⁷ o canal utilizado deve levar em conta a interação entre o responsável pelo tratamento e o titular dos dados, assim como a forma de coleta dos dados. Por exemplo, disponibilizar canais de atendimento exclusivamente online pode não ser viável quando o serviço prestado pelo agente de tratamento é realizado exclusivamente por meios físicos.

⁴ União Europeia. Regulamento (UE) 2016/679 (GDPR). Artigo 12, parágrafo 3. Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

⁵ Comissário de Privacidade do Canadá. Acesso à Informação Pessoal: Guia de Boas Práticas para Empresas - Comissário de Privacidade do Canadá. Disponível em: <https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/api_bus/>.

⁶ California Consumer Privacy Act (CCPA). Seção 1798.130(a)(2).

⁷ Article 29 Working Party. Guidelines on Transparency Under Regulation 2016/679. 2018. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Nesses casos, é importante considerar a necessidade de meios alternativos adequados. Por exemplo, é possível possibilitar o atendimento de requisições de forma presencial ou até mesmo por meio de interações telefônicas.

Outro ponto de importância é a necessidade de os canais de comunicação considerarem as **características individuais do público** com o qual o agente de tratamento interage, levando em conta fatores como idade, necessidades especiais e outras características específicas.

Nesse sentido, é essencial garantir que, quando as ações são direcionadas às crianças com idade suficiente para estarem alfabetizadas, qualquer informação e comunicação sejam transmitidas de forma simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, conforme estabelece o artigo 14, parágrafo 6º da LGPD.

Da mesma forma, se um responsável pelo tratamento estiver ciente de que seus serviços são utilizados por outros membros vulneráveis da sociedade, incluindo pessoas com deficiência ou pessoas que possam ter dificuldade em acessar as informações, as vulnerabilidades desses titulares de dados devem ser consideradas ao construir seus canais de atendimentos.

- d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

Enquanto os controladores têm a responsabilidade primária de garantir que o tratamento de dados ocorra em conformidade com a LGPD, os operadores têm o dever de auxiliar os controladores no cumprimento de suas obrigações, inclusive no atendimento de solicitações de direitos de titulares.

Nesse sentido, entende-se que o operador tem a **obrigação de assistir** o controlador no atendimento de solicitações de direitos. Isso envolve a implementação de medidas técnicas e organizacionais apropriadas, as quais devem ser aplicadas de acordo com a viabilidade técnica e operacional do operador, considerando seus recursos, capacidades e o contexto específico da atividade de tratamento confiada a ele.

Para determinar o **grau exigido de assistência**, é necessário considerar a natureza do tratamento realizado e o tipo de atividade atribuída ao operador no caso concreto. Em certas circunstâncias, a assistência pode se limitar ao encaminhamento ágil de solicitações recebidas. Entretanto, em situações específicas, o operador pode ter deveres técnicos mais específicos, como responsabilidades pela correção de dados inexatos ou execução de solicitações de eliminação, especialmente quando responsável por atividades como extração e gerenciamento de dados pessoais ou interação direta com o titular, o que pode ser objeto de negociação contratual entre as partes.

Embora etapas do gerenciamento de solicitações possam ser terceirizadas para o operador, a responsabilidade pelo cumprimento dessas solicitações permanece com

o controlador. Portanto, a avaliação da admissibilidade das solicitações dos titulares e a conformidade com os requisitos estabelecidos pela LGPD devem ser conduzidas de acordo com as diretrizes estabelecidas pelo controlador, que é responsável por repassar essas orientações aos operadores.

- e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

Entendemos que grande parte das diretrizes gerais do Decreto nº 11.034 (“Decreto”) podem servir de parâmetro para o estabelecimento de normas para o atendimento de direitos de proteção de dados. Entretanto, destaca-se as seguintes diretrizes específicas que **não** deveriam ser adotadas:

- ☐ **Canais de solicitações integrados:** entende-se que o melhor formato para solicitar o exercício dos direitos estabelecidos na LGPD seja um canal único, diferentemente do previsto no artigo 2º do Decreto. As solicitações relacionadas à proteção de dados pessoais podem requerer processos específicos e especializados para atender a cada tipo de solicitação de direito, além de prazos distintos. No mercado, a centralização de solicitações de proteção de dados em um único canal, gerenciado por uma equipe especializada em proteção de dados, tem sido preferível.
 - ☐ **Vedação ao não fornecimento prévio de informações:** Em consonância com o exposto acima e abordado nesse documento, entende-se que previamente ao fornecimento de informações ao titular e/ou atendimento de suas solicitações relativas à proteção de dados, deverá ser validada a identidade do titular, para sua própria segurança, em sentido contrário ao que está previsto no artigo 3º, § 4º do Decreto.
 - ☐ **Prazos:** entende-se que o prazo de 07 dias, previsto no artigo 13 do Decreto é insuficiente para atendimento das solicitações de exercício de direitos, conforme indicado nas contribuições do item I.(a).
- f. Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

Em relação ao atendimento, um modelo que poderia ser considerado como paradigma, especialmente para lidar com grandes volumes de demandas com economicidade, é o adotado por algumas grandes plataformas digitais e empresas de tecnologia. Estas empresas frequentemente implementam sistemas avançados de automação e atendimento digital para gerenciar solicitações dos titulares.

Um exemplo prático pode ser observado em grandes provedores de serviços online, como plataformas de redes sociais, provedores de e-mail ou empresas de comércio eletrônico. Essas organizações costumam oferecer interfaces online intuitivas e centralizadas para que os usuários possam exercer seus direitos de proteção de dados.

- ☐ **Chatbots e assistência virtual:** Implementação de chatbots e assistentes virtuais para interação inicial com os usuários, fornecendo informações sobre

proteção de dados, esclarecendo dúvidas comuns e até mesmo auxiliando na submissão inicial de solicitações.

- ☐ **Formulários online:** Disponibilização de formulários online específicos para diferentes tipos de solicitações, permitindo que os usuários submetam suas demandas de forma estruturada.
- ☐ **Foco em autoajuda:** prioridade na promoção da autoajuda, disponibilizando recursos educacionais que capacitam os usuários a compreenderem e exercerem seus direitos de proteção de dados de maneira independente.
- ☐ **Automatização de respostas padrão:** Utilização de sistemas automatizados para lidar com solicitações comuns e rotineiras, proporcionando respostas instantâneas e eficientes. Isso reduz a carga de trabalho manual e acelera o tempo de resposta.
- ☐ **Atualização em tempo real:** Fornecimento de atualizações em tempo real sobre o status das solicitações, permitindo que os usuários acompanhem o progresso e recebam informações transparentes sobre o tratamento de seus pedidos.

No entanto, acreditamos que a criação desses canais não deveria ser imposta às empresas, as quais deveriam ter a liberdade de determinar por si mesmas o método mais eficaz de atender aos direitos dos titulares de dados, visando aprimorar seu programa de governança interno.

II. Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII)

- a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Existem hipóteses excepcionais para negar o direito de confirmação da existência do tratamento de dados pessoais. Essa negação pode ocorrer nas seguintes circunstâncias:

- ☐ Quando o fornecimento dessa confirmação puder revelar informações confidenciais ou sensíveis sobre terceiros, infringindo seus direitos à privacidade e proteção de dados.
- ☐ Em situações em que a divulgação da informação resultaria em riscos significativos para a segurança nacional, ameaçaria a prevenção ou investigação de atividades criminosas, ou colocaria em perigo a vida e integridade física de indivíduos. Nesses casos, a negação desse direito pode ser justificada como medida necessária para equilibrar os direitos de proteção de dados com a proteção de interesses mais amplos da sociedade.
- ☐ Quando os interesses legítimos do controlador se sobrepõem aos do titular dos dados. Poderá ser negado o provimento de um direito ao titular a fim de resguardar os interesses do controlador ou operador. Por exemplo, quando ocorre o tratamento de dados pessoais para a prevenção de fraudes ou garantia da segurança de colaboradores, a eventual confirmação do tratamento poderia impedir a realização de tais atividades legítimas⁸.
- ☐ Em casos de solicitações manifestamente infundadas ou excessivas, como quando o titular de dados faz solicitações repetitivas em um curto período, ou se a pessoa está fazendo uma solicitação apenas para obter algo em troca da

⁸ União Europeia. Regulamento (UE) 2016/679 (GDPR). Artigo 14(5)(b). Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

organização, ou ainda se estiver usando as leis de proteção de dados para assediá-la organização⁹.

b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

Quanto à identificação dos controladores, o art. 9º, III, da LGPD estabelece que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados com a identificação do controlador, devendo ser disponibilizadas informações que permitam a identificação do responsável pelo tratamento, como a razão social, nome fantasia, e CNPJ.

Como regra geral, entendemos que o agente pode indicar em suas políticas de privacidade e documentos de transparência disponibilizado aos titulares as categorias de agentes de tratamento com os quais seus dados foram compartilhados, bem como informações sobre a finalidade do compartilhamento dos dados pessoais, sem a necessidade de listar nominalmente os parceiros.

Contudo, caso o titular solicite informações sobre o compartilhamento, por meio do direito de previsto no artigo 18º, VII, o titular deve ter o direito de receber informações mais detalhadas a respeito das entidades públicas e privadas com as quais houve o uso compartilhado dos dados, indicando nominalmente os terceiros¹⁰, quando isso não ferir os segredos comerciais da companhia.

c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?

Conforme mencionado anteriormente, os operadores têm a obrigação de colaborar com os controladores para assegurar o cumprimento das obrigações relacionadas ao tratamento de dados. Esse apoio inclui a garantia de que os titulares possam efetivamente exercer seus direitos, incluindo o direito de obter informações sobre o tratamento de seus dados pessoais.

No que se refere ao direito de obtenção de informações, a obrigação dos operadores varia de acordo com a natureza do tratamento e as atividades específicas atribuídas a eles no caso concreto. Assim, os operadores devem auxiliar os controladores na obtenção de informações sobre o tratamento, fornecendo dados como os propósitos do tratamento, categorias de dados pessoais envolvidos, destinatários, prazo de armazenamento e os direitos dos titulares, respeitando os limites técnicos e operacionais sob os quais estão envolvidos.

Ressalta-se que, embora partes do processo de gerenciamento de solicitações possam ser terceirizadas para os operadores, a responsabilidade pelo cumprimento dessas solicitações e contato com o titular dos dados permanece com o controlador.

⁹ União Europeia. Regulamento (UE) 2016/679 (GDPR). Artigo 12(5). Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>.

¹⁰ Article 29 Working Party. Guidelines on Transparency Under Regulation 2016/679. 2018. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

- d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

O art. 19, inciso I, da LGPD prevê a disponibilização imediata de uma declaração em formato simplificado quando solicitado pelo titular dos dados. Diante dessa exigência, entende-se que as informações mínimas sobre o tratamento de dados pessoais que deveriam constar dessa declaração são:

- ☐ **Confirmação se são ou não tratados dados pessoais do titular:** O primeiro aspecto essencial é informar ao titular se seus dados pessoais estão sendo tratados pelo controlador. Caso os dados não sejam tratados, a declaração deve afirmar isso de forma clara e objetiva.
 - ☐ **Tipos de dados pessoais tratados, se houver:** Se os dados pessoais do titular estiverem sendo tratados, a declaração em formato simplificado deve identificar os tipos de dados pessoais que estão sendo tratados (por exemplo: dados cadastrais, dados de saúde, informações financeiras, entre outras categorias).
- e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

As informações mínimas sobre o tratamento de dados pessoais que devem ser evidenciadas pelo controlador, independentemente de requerimento, para garantir a transparência e o direito à informação são:

- ☐ Finalidade do tratamento;
- ☐ Informações de contato do controlador;
- ☐ Informações acerca do uso compartilhado de dados; e
- ☐ Menção explícita aos direitos contidos no art. 18 da LGPD.

Em relação à transparência sobre os critérios e procedimentos utilizados para a decisão automatizada, considerando a complexidade técnica envolvida em tais tratamentos, muitas vezes dificultando sua compreensão para uma pessoa média, a simples divulgação desses critérios pode não ser suficiente para atingir os objetivos de transparência. Além disso, é importante destacar que empresas frequentemente consideram modelos de tomada de decisão como segredos comerciais ou industriais, o que limita a divulgação detalhada dessas informações e pode dificultar ainda mais a compreensão por parte do titular.

Em vez disso, sugere-se que as informações sobre tais procedimentos sejam apresentadas de maneira geral, e que permita ao titular compreender quais são as implicações práticas das decisões automatizadas durante o tratamento de dados realizado.

- f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

Sim, o direito de acesso pode ser considerado satisfeito quando o agente de tratamento disponibilizar uma cópia dos dados pessoais para conhecimento do titular. O cerne desse direito é garantir que os titulares tenham a capacidade de obter informações claras e compreensíveis sobre o tratamento de seus dados pessoais.

Conforme o entendimento do EDPB em “*Guidelines 01/2022 on data subject rights – Right of access*”¹¹ (p. 23) se o acesso aos dados é concedido por meio da disponibilização de uma cópia ao titular, o direito de acesso é cumprido. A obrigação de fornecer uma cópia atende aos objetivos do direito de acesso, permitindo que o titular dos dados esteja ciente e verifique a legalidade do tratamento.

III. Portabilidade dos dados (art. 18, inciso V)

- a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

O setor financeiro e de telefonia são exemplos que possuem maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade.

- ☐ **Setor Financeiro:** No setor financeiro, a portabilidade é regulada por resoluções específicas do Bacen: portabilidade de salário (Resolução n. 3.402/2006 e Resolução n. 4.292/2013), de crédito (Resolução n. 4.292/2013) e de cadastro (Resolução n. 2.835/2001). Além disso, em abril de 2019, foi introduzido no Brasil um conjunto de diretrizes (Aviso nº 33.455/2019) que serviram como o framework para a regulamentação do *open banking*. O framework estabelecido para viabilizar o *open banking conta com* especificações dos procedimentos de compartilhamento, como o conteúdo mínimo a ser compartilhado, os tipos de dados que podem ser compartilhados, requisitos de interoperabilidade, questões de segurança, bem como as ferramentas para obter consentimento do cliente.
- ☐ **Setor de Telefonia:** A portabilidade numérica, foi introduzida no Brasil em 2007 pela Anatel, por meio da Resolução nº 460/2007. Essa resolução cria um processo de portabilidade altamente detalhado, estabelecendo um conjunto de direitos e garantias do consumidor associados, e baseia-se em medidas específicas para enfrentar os desafios técnicos e de rede associados à implementação da portabilidade de números.

No entanto, além de definir setores com diferentes níveis de prontidão para implementar o processo de portabilidade de dados, é aconselhável estabelecer certas condições sob as quais pode ser justificado negar o direito à portabilidade dos dados, conforme orientações estabelecidas pela European Commission no documento “*Guidelines on the right to data portability (wp242rev.01)*”¹²:

¹¹ EDPB em “*Guidelines 01/2022 on data subject rights - Right of access*”. Disponível em https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

¹² *Guidelines on the right to data portability (wp242rev.01)*
<https://ec.europa.eu/newsroom/article29/items/611233>

- ☐ Atividades em que o processamento de dados não é realizado de forma automatizada, isto é, situações que envolvem documentos físicos; e
- ☐ Atividades nas quais os dados não são fornecidos pelos próprios titulares, a fim de proteger os segredos comerciais das companhias.

b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

Os principais desafios tecnológicos para implementar um padrão de interoperabilidade incluem:

- ☐ **Padronização dos dados:** isso envolve estabelecer formatos de dados comuns, como XML, JSON ou CSV, que possam ser compreendidos e processados por diferentes sistemas. Isso requer um acordo sobre a estrutura dos dados, os tipos de dados utilizados e as convenções de nomenclatura.
- ☐ **Compatibilidade de sistemas:** os sistemas de diferentes fornecedores podem ter arquiteturas, linguagens de programação e usar tecnologias diferentes. Integrar esses sistemas requer soluções que possam fazer a tradução entre eles, garantindo que os dados sejam interpretados corretamente em ambos os lados.
- ☐ **Segurança e Privacidade:** a interoperabilidade requer a troca de dados entre diferentes sistemas, o que pode aumentar os riscos de segurança e violação de privacidade. É necessário implementar medidas de segurança robustas, como criptografia, autenticação e controle de acesso, para proteger os dados durante a transferência e o compartilhamento.
- ☐ **Escalabilidade:** à medida em que a quantidade de dados e o número de usuários aumentam, os sistemas precisam ser capazes de lidar com essa carga adicional sem comprometer o desempenho. Isso requer arquiteturas escaláveis e a capacidade de adicionar recursos de forma dinâmica conforme necessário.
- ☐ **Gestão de identidade e acesso:** Para garantir que apenas usuários autorizados tenham acesso aos dados, é necessário implementar sistemas de gestão de identidade e acesso eficazes. Como exemplo, cita-se a experiência do setor financeiro, que estabelece um conteúdo mínimo que deve ser incluído na solicitação de portabilidade, além de obrigar as instituições a estruturarem um canal de comunicação eletrônica entre o banco remetente e receptor (Resolução nº 4.639, Bacen)

c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

Para garantir a interoperabilidade, considera-se que os seguintes aspectos devem ser padronizados:

- ☐ **Formato de dados:** Estabelecer um formato comum para representar e estruturar dados é fundamental. Isso inclui a definição de como as informações serão organizadas, quais tipos de dados são suportados e como são codificados.
- ☐ **Protocolos de comunicação:** definir protocolos padronizados para a comunicação entre sistemas é essencial. Isso abrange a forma como os

sistemas trocam dados, as regras para iniciar, encerrar e gerenciar conexões, e os métodos de autenticação e autorização.

- **Normas de segurança da informação:** Aspectos relacionados à segurança e privacidade dos dados também devem ser padronizados, incluindo métodos de autenticação, autorização, criptografia e controle de acesso.

d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?

Sim, é adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibiliza para o titular todos os seus dados pessoais em um formato interoperável, caso não exista pedido específico do titular de transferência para outro fornecedor.

Ao disponibilizar os dados em um formato interoperável, o agente de tratamento permite que o titular possa transferi-los para outro serviço ou plataforma de sua escolha, facilitando a mudança entre provedores de serviços e promovendo a concorrência no mercado.

e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

Sim, a autorregulação da portabilidade desempenha um papel importante em setores específicos da economia que já possuem práticas estabelecidas de portabilidade, como o setor financeiro, saúde complementar e telefonia. Essa abordagem permite que diferentes agentes desses setores se unam para superar obstáculos de falta de coordenação e especificidades técnicas envolvidas em medidas de portabilidade e interoperabilidade.

Por exemplo, no setor financeiro, a regulação do open banking envolveu uma ampla consulta pública para definir especificações detalhadas sobre o compartilhamento de dados. Para determinar os padrões tecnológicos e os procedimentos operacionais para projetar a interface e o protocolo de compartilhamento envolvidos no open banking, a Resolução Conjunta nº 1/2020 do Bacen estabelece que as instituições participantes devem assinar uma convenção que estabelece os padrões para o compartilhamento de dados, demonstrando assim um exemplo eficaz de autorregulação.

No setor de saúde, por exemplo, a ANS estabeleceu um Grupo de Trabalho sobre Portabilidade para revisar e propor novas regulamentações, contando com a participação de diversos stakeholders, incluindo provedores de saúde, associações do setor e organizações de proteção ao consumidor. Esse processo participativo e consultivo permitiu abordar preocupações específicas do setor, como o formato das solicitações de portabilidade, o prazo esperado para a aceitação ou negação das solicitações e a validação da portabilidade por meio da execução de um novo contrato entre consumidores e operadoras.

No setor de telecomunicações, a ANATEL também adotou um processo semelhante ao estabelecer padrões para a portabilidade de números, envolvendo consultas públicas, audiências e a participação de diferentes partes interessadas.

IV. Correção dos dados tratados (art. 18, inciso III)

a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

Diante da falta de uma definição legal para dados incompletos, imprecisos ou desatualizados na LGPD, é crucial interpretar esses termos conforme sua aplicação prática no contexto do tratamento. Os seguintes critérios podem ser considerados:

- ☐ **Precisão:** A autoridade de proteção de dados britânica, o ICO, define que “impreciso” significa incorreto ou enganoso quanto a qualquer questão de fato¹³. Ou seja, quando o dado pessoal não incluir todos os elementos necessários para identificar com precisão o titular em relação à realidade fática, no contexto do tratamento realizado (ex. ausência de um sobrenome, ausência de numeração de um endereço).
- ☐ **Consistência e veracidade:** quando o dado pessoal contiver erro em relação à realidade fática (por exemplo, atribuição errônea de profissão, sexo). A veracidade de um dado deve estar amparada por uma fonte confiável capaz de comprovar que os dados que se pretende atualizar/complementar são verdadeiros. Em alguns casos, pode ser necessário confrontar os dados com fontes externas. Além da consistência com informações externas, os dados também devem ser consistentes entre si. Por exemplo, informações como idade e data de nascimento devem ser coerentes entre si.
- ☐ **Integridade e atualidade:** quando o dado pessoal não tiver sido atualizado para refletir mudanças do titular (ex. estado civil, alterações de endereço, atualização de telefone, estado de emprego). Para tanto é importante considerar o decurso temporal de quando os dados pessoais foram coletados, pois dados coletados há mais tempo tem maior probabilidade de estarem desatualizados e, portanto, menos confiáveis para uso atual.
- ☐ **Rastreabilidade e auditoria:** registros e procedimentos para rastrear e auditar as alterações nos dados ao longo do tempo podem auxiliar a identificar quando e como ocorreram inconsistências ou desatualizações.

b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente

Considerando os efeitos adversos que a alteração indevida de um dado pessoal pode gerar, entendemos que nas seguintes situações é necessário adotar procedimentos mais rigorosos do que simplesmente aceitar a declaração do titular:

- (i) quando a solicitação envolver dados sensíveis;
- (ii) quando há potenciais riscos à segurança, confiabilidade ou integridade dos dados;
- (iii) quando há maior probabilidade de fraudes (como cadastros bancários);

¹³ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/#accurate_inaccurate

- (iv) quando a correção dos dados do titular puder afetar negativamente terceiros;
- (v) quando a legislação ou regulamentos setoriais estabelecerem regras específicas para a correção dos dados.

Nesses casos, a implementação de processos adequados de verificação e autenticação da identidade do titular é fundamental para garantir a correção precisa e segura dos dados pessoais.

c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.

Para avaliar a impossibilidade ou o esforço desproporcional em informar imediatamente aos agentes de tratamento sobre a correção, eliminação, anonimização ou bloqueio dos dados compartilhados, os seguintes critérios objetivos devem ser considerados:

- ☐ **Volume de agentes de tratamento envolvidos:** Se houver uma grande quantidade de agentes de tratamento com os quais os dados foram compartilhados, pode ser impraticável notificar a todos individualmente.
- ☐ **Tecnologias complexas:** Em situações em que os sistemas de informação são altamente complexos e dispersos, pode ser difícil identificar e notificar de forma eficiente aos agentes de tratamento sobre as atualizações necessárias nos dados compartilhados.
- ☐ **Custo excessivo:** Se os custos associados à notificação forem excessivos altos em relação aos recursos disponíveis.
- ☐ **Impacto para as operações:** Se a notificação exigir um tempo significativo ou recursos humanos que não estejam disponíveis, especialmente se isso afetar adversamente outras operações críticas da organização.
- ☐ **Riscos à segurança ou confidencialidade:** Se a notificação representar um risco substancial à segurança dos dados ou à confidencialidade das informações envolvidas.

d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

O direito de correção pode ser negado quando:

- (i) **não houver comprovação de identidade** do titular, ou não houver comprovação que o dado é incompleto, inexato ou desatualizado;
- (ii) a correção solicitada entra em **conflito com outros direitos ou interesses legítimos do controlador ou de terceiros**. Nesse sentido, o ICO¹⁴ exemplifica que um controlador não precisa atualizar dados mantidos para fins estatísticos, históricos ou de pesquisa, pois isso poderia prejudicar esse propósito. Por exemplo, a correção dos dados solicitada pelo titular pode afetar a liberdade de expressão ou o direito à informação de terceiros,

¹⁴ Information Commissioner's Office. UK GDPR guidance and resources. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accuracy/#accurate_inaccurate

especialmente em contextos jornalísticos ou de pesquisa, ao potencialmente modificar informações históricas, prejudicando o interesse público na divulgação dessas informações.

- (iii) a solicitação **for manifestamente infundada ou excessiva**. De acordo com o ICO¹⁵, uma solicitação pode ser “**manifestamente excessiva**” quando for claramente irracional em relação aos custos envolvidos no tratamento do pedido. Para determinar isso, é necessário considerar a natureza das informações solicitadas, o contexto do pedido e do relacionamento entre as partes, o potencial de danos para a pessoa caso o pedido seja recusado, os recursos disponíveis e a frequência das solicitações anteriores. E “**manifestamente infundado**” seria um pedido claramente sem base ou intenção legítima pelo titular, como intenções maliciosas, uso do pedido para assediar a organização, declarações para causar perturbações, acusações falsas, motivação pessoal contra funcionários específicos.

V. Anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e § 2º)

- a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Não é necessário que o titular fundamente sua solicitação, na medida em que a LGPD não traz essa obrigatoriedade. Tal exigência poderia ser considerada como uma forma de limitação ao exercício do direito.

Inclusive, caso os dados sejam considerados desnecessários, excessivos ou em desconformidade com a lei, a atividade por si só já estaria irregular, pois violaria o princípio da necessidade e qualidade dos dados, sendo dever do agente de tratamento comprovar o contrário.

- b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

Sim. O artigo 16 da LGPD, exige que os dados sejam eliminados após o término do tratamento, mas permite, em seu inciso IV, que o controlador mantenha os dados, para seu uso exclusivo, desde que sejam anonimizados.

Além disso, de acordo com o artigo 12 da LGPD, os dados anonimizados não são considerados dados pessoais, a menos que o processo de anonimização seja reversível. Assim, quando os dados são adequadamente anonimizados, eles perdem sua natureza de dados pessoais e, portanto, não estão mais sujeitos às regulamentações de proteção de dados.

¹⁵ Information Commissioner's Office. Manifestly unfounded and excessive requests. Disponível em: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>

Portanto, é possível interpretar que, caso seja do interesse do controlador, ele pode optar pela anonimização dos dados pessoais como alternativa à sua eliminação, já que ambas as opções têm o mesmo efeito para o titular, ou seja, o controlador deixará de tratar seus dados pessoais.

- c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

O artigo 18, § 2º, da LGPD estabelece que o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento da lei. Se a alegação do titular for considerada legítima, ou seja, se ficar comprovado que o tratamento dos dados pessoais violou as disposições da LGPD, o efeito da oposição é que o controlador deverá cessar imediatamente o tratamento dos dados pessoais em questão, interrompendo qualquer atividade de tratamento de dados pessoais que esteja sendo realizada de forma contrária à lei.

VI. Revogação do consentimento (art. 18, VI e IX)

- a. A revogação do consentimento prevista no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular? Explique.

A revogação do consentimento não deve implicar na obrigação de eliminar os dados tratados com base no consentimento, quando houver outra base legal que justifique a manutenção dos dados. A revogação do consentimento e a exclusão dos dados são direitos distintos previstos na LGPD.

O *European Data Protection Board* (EDPB)¹⁶, em linha com as *Guidelines* sobre o consentimento do *Article 29 WP*¹⁷, entende que, uma vez retirado o consentimento, a organização precisa garantir que os dados sejam eliminados, a menos que possam ser tratados com base em outro fundamento jurídico (p.ex., requisitos legais de retenção ou para cumprir um contrato).

No mesmo sentido, o ICO¹⁸ entende que será necessário interromper o tratamento de dados quando o consentimento for revogado, sem especificar a necessidade de eliminação. O ICO entende que, em alguns casos, poderá ser necessário manter um registo da retirada do consentimento para garantir o atendimento ao pedido do titular – por exemplo, uma revogação do consentimento para recebimento de e-mail marketing.

¹⁶https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

¹⁷ Guidelines on Consent under Regulation 2016/679 (wp259rev.01). Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en>

¹⁸Information Commissioner's Office. UK GDPR guidance and resources. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/#:~:text=%E2%80%9CThe%20data%20subject%20shall%20have,withdraw%20as%20to%20give%20consent.%E2%80%9D>

Ainda que a revogação do consentimento pelo titular seja uma das hipóteses que dão causa ao término do tratamento de dados, conforme art. 15, III da LGPD e, por consequência, exige a eliminação dos dados, conforme art. 16, existem situações em que haverá a necessidade de manutenção dos dados com fundamento em outra base legal. Quando um titular revoga seu consentimento, a revogação atinge apenas o tratamento fundamentado nessa base legal, não invalidando a manutenção dos dados para outras finalidades.

- b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

De acordo com o artigo 8º, § 5º, e o artigo 15, inciso III, da LGPD, a revogação do consentimento resultará no término do tratamento dos dados em questão, e os dados pessoais tratados com base nesse consentimento devem ser eliminados, a menos que se apliquem as exceções previstas no artigo 16 ou exista outras hipóteses de tratamento que possibilitem a manutenção dos dados pessoais para finalidades distintas.

De acordo com o § 5º do artigo 8º, os tratamentos realizados com base no consentimento anteriormente manifestado permanecem válidos enquanto não houver requerimento de eliminação. Isso implica que, quando o titular solicitar a eliminação dos dados, o consentimento anteriormente dado se tornará inválido, invalidando o tratamento que o tiver como fundamento. Contudo, entendemos que o controlador ainda pode realizar outros tratamentos que estejam fundamentados em outras bases legais.

A UK GDPR estabelece que a revogação do consentimento não afeta a legalidade do tratamento baseado no consentimento antes da sua retirada (art. 7(3))¹⁹. O entendimento do ICO nesse sentido é que o tratamento que estiver amparado no consentimento será interrompido, sem prejuízo da continuidade de outros tratamentos fundamentados em outras bases legais²⁰. A autoridade britânica entende que, em alguns casos, poderá ser necessário manter um registo da retirada do consentimento – por exemplo, para manter registos de que o consentimento foi revogado para finalidades de marketing direto. A manutenção dos dados pessoais para esse registo não depende do consentimento, desde que seja informado ao titular que essa manutenção é necessária, por exemplo, em razão de obrigação legal ou interesses legítimos do controlador.

VII. Decisões baseadas em tratamento automatizado (art. 20, caput)

- a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

A decisão tomada unicamente com base no tratamento automatizado é uma decisão tomada por meios automatizados, sem qualquer envolvimento humano. Nesse

¹⁹ União Europeia. Regulamento (UE) 2016/679 (GDPR). Artigo 7(3). Disponível <https://gdpr-info.eu/art-7-gdpr/>

²⁰ Information Commissioner's Office. UK GDPR guidance and resources. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/how-should-we-obtain-record-and-manage-consent/>

sentido, o ICO²¹, esclarece que um tratamento poderá ser considerado como unicamente automatizado caso a interferência humana seja apenas de inserção de dados pessoais, para que possam assim ser tratados de forma automatizada, sendo a tomada de decisão, em si, realizada por um sistema automatizado.

Sobre este posicionamento, as *Guidelines* sobre a tomada de decisões individuais automatizadas do *Article 29 WP*²², aprovadas pelo EDPB, também estabelecem que em decisões "exclusivamente" baseadas no tratamento automatizado não há envolvimento humano no processo de decisão. Para ser considerada a participação humana, o responsável pelo tratamento deve assegurar que qualquer controle da decisão seja significativo, e não apenas uma ação simbólica no sistema, ou seja, deve ser realizada por alguém que tenha autoridade e competência para alterar a decisão.

Desta forma, uma decisão será considerada automatizada (e não tomada unicamente com base em tratamento automatizado), caso haja intervenção humana para avaliar e interpretar o resultado de uma decisão automatizada, antes de aplicá-la ao titular, devendo assim existir uma intervenção humana ativa, e não apenas passiva informando os dados para análise.

b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

Podemos interpretar que um interesse do titular está sendo afetado quando a decisão tomada unicamente com base em tratamento automatizado gerar riscos às liberdades civis e aos direitos fundamentais do titular dos dados. Os critérios para tal avaliação podem incluir:

- ☐ **Impacto na esfera individual:** a decisão automatizada tem um impacto significativo na esfera individual do titular dos dados. Isso pode ser determinado pela natureza e gravidade das consequências da decisão para o titular, como aspectos como a privacidade, a liberdade pessoal, a reputação, a autonomia e a capacidade de tomar decisões sobre a própria vida.
- ☐ **Consequências adversas:** a decisão automatizada tem consequências significativas para o titular, como restrições de acesso a serviços essenciais, limitações de oportunidade de emprego ou graves prejuízos financeiros.
- ☐ **Potencial discriminatório:** a decisão automatizada pode resultar em discriminação injusta ou tratamento diferenciado, em comparação com outras pessoas ou grupos, por exemplo com base em características como raça, etnia, religião, orientação sexual, gênero, idade, entre outras.

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

Considerando que não há necessidade de a revisão ser realizada por pessoa natural, entendemos que os desafios que potencialmente seriam enfrentados pelas empresas ficam significativamente reduzidos. Contudo, é importante garantir que a revisão da decisão e eventuais questionamentos por parte do titular sobre funcionamento dos

²¹ What does the UK GDPR say about automated decision-making and profiling?. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/#id2>

²² https://www.cnil.fr/sites/cnil/files/atoms/files/20171025_wp251_enpdf_profilage.pdf

algoritmos e o processo de tomada de decisão não comprometam os segredos comerciais e industriais do agente de tratamento.

- d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

Sim. Segundo a LGPD, apenas as decisões baseadas exclusivamente em tratamento automatizado de dados e que impactem os direitos dos titulares necessitam de revisão. Situações que não atendam a esses critérios podem ter o pedido de revisão recusado.

	o atendimento aos direitos dos titulares estabeleça que, para cada nova solicitação de exercício de direito formulada por um titular, inicia-se a contagem de um novo prazo, ainda que, no decorrer de uma comunicação com o agente de tratamento relacionada a uma solicitação inicial, o titular busque exercer outro direito.
c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?	A escolha sobre as características do canal de atendimento para garantir sua efetividade deve ser feita pelo agente de tratamento. Isso porque os elementos que compõem o binômio “características-efetividade” tendem a variar de acordo com o modelo de negócio e a organização das atividades do agente de tratamento. Por exemplo, para um agente de tratamento que lida com os titulares apenas de forma presencial, será mais eficiente a disponibilização de um formulário impresso a ser preenchido por escrito, ao passo que para um agente de tratamento que não possua presença física (seja no Brasil ou no exterior) e se relacione virtualmente com os titulares, será mais eficiente a disponibilização online do canal na plataforma em que ocorrem as interações. O mais importante é que a ANPD evite regular ou dar orientações sobre os canais de comunicação que possam trazer ônus excessivo ou desmensurado, principalmente considerando o princípio da liberdade dos modelos de negócios promovidos na internet, prevista no art. 3º da Lei 12.965/14 (Marco Civil da internet). A ANPD deveria focar seus esforços em orientar os agentes de tratamento sobre a necessidade de que, observadas a pluralidade e as especificidades dos modelos de negócios existentes no mercado, os direitos dos titulares sejam atendidos eficazmente. Por fim, com o objetivo de garantir a efetividade da comunicação e, ao mesmo tempo, a segurança do atendimento dos direitos dos titulares, é importante que a ANPD oriente os agentes de tratamento sobre as medidas a serem implementadas para verificar a identidade do titular. Sobre esse ponto, não parece necessário que o agente de tratamento sempre requeira apresentação de documentos adicionais do titular, especialmente nos casos em que a solicitação ocorrer no âmbito de uma relação contínua entre o agente e o titular. No entanto, entendemos que a ANPD deve esclarecer quando a solicitação desses documentos é recomendável e quando pode ser dispensada. Essa possibilidade é reconhecida por outras autoridades de proteção de dados fora do Brasil, a exemplo do ICO no Reino Unido e da CNIL na França.

	Além disso, com esse mesmo objetivo, a ANPD também deve orientar os agentes de tratamento sobre como proceder em caso de solicitações de exercícios de direitos formuladas por terceiros (por exemplo, por pais, representantes legais, procuradores etc.). Sobre esse ponto, parece razoável que seja admitido o exercício de direitos dos titulares por terceiros nas hipóteses já previstas no ordenamento jurídico vigente, especialmente no Código Civil (por exemplo, tutela, curatela e representação), mediante apresentação de documentos que comprovem os poderes do terceiro ao agente de tratamento. Essa possibilidade é reconhecida por outras autoridades de proteção de dados fora do Brasil, a exemplo do ICO no Reino Unido. Fontes: ICO – Reino Unido (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-of-access/#responding) CNIL – França (https://www.cnil.fr/fr/cnil-direct/question/exercice-de-mes-droits-informatique-et-libertes-dois-je-fournir-obligatoirement)
d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?	As obrigações de atendimento aos direitos dos titulares previstas no Capítulo III da LGPD aplicam-se especificamente ao controlador de dados pessoais. Nesse sentido, entende-se que a solicitação de exercício de direito do titular deve ser feita ao controlador, no âmbito da relação controlador-titular. Não obstante, deve ser facultada aos agentes de tratamento a possibilidade de regularem entre si quem será responsável, sob a ótica operacional, por atender (todas ou determinadas) solicitações de exercício de direitos de titulares. Em certas circunstâncias, o operador poderá ser o único agente capaz de operacionalizar a solicitação do titular (por exemplo, quando fizer a gestão do canal de solicitações ou do servidor onde estão hospedadas as informações do controlador). No entanto, entende-se que o atendimento do direito do titular pelo operador somente deverá ser feito mediante instruções do controlador (que poderá se dar de maneira mais genérica pela via contratual ou pontualmente, à medida em que solicitações sejam recebidas). Em qualquer caso, o operador não deve se antecipar e tomar a decisão de atender à solicitação do titular por iniciativa própria, sob pena de atuar fora das instruções do controlador e ser equiparado a um controlador (art. 42, §1º, I). Por fim, é importante que a ANPD deixe clara a possibilidade de que, sempre que procurado por um titular de dados que deseje exercer algum dos direitos previstos pela LGPD e desde que a identificação seja possível,

	o operador indique ao titular os dados de contato do controlador. Essa possibilidade está alinhada com a previsão do art. 18, §4º, II da LGPD e garantirá maior efetividade ao atendimento da solicitação do titular.
e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?	O Decreto nº 11.034/2022, que regulamenta o Serviço de Atendimento ao Consumidor ("Decreto" e "SAC"), é destinado aos fornecedores dos serviços regulados pelo Poder Executivo Federal. Dessa forma, a adoção do referido ato normativo como parâmetro pela ANPD pode impor aos agentes de tratamento a obrigação genérica de implementarem medidas desproporcionais para cumprir com os requisitos previstos no Decreto, o que representaria ônus excessivo ao exercício de diversas atividades econômicas. As especificidades dos canais de comunicação com os titulares irão variar de acordo com diversos elementos, que podem sim considerar a eventual atuação dos agentes de tratamento em setores regulados, mas que também deverão ser consistentes com os diferentes portes, recursos disponíveis e modelos de negócio desses agentes. Nesse sentido, importante reiterar que a LGPD é uma lei de aplicação horizontal, que impacta quase todo tipo de negócio no Brasil. Assim, orientar a forma de atendimento aos titulares com base em um único parâmetro pode representar baixa efetividade do cumprimento de direitos previstos na LGPD. Dentre os requisitos previstos no Decreto que podem ser desproporcionais a depender da estruturação do agente de tratamento, destaque-se: (i) acesso ao SAC de modo ininterrupto, durante vinte e quatro horas por dia, sete dias por semana; e (ii) atendimento telefônico obrigatório com horário de atendimento não inferior a oito horas diárias, com atendimento humano. Enfatizando a resposta à pergunta "c" deste Bloco I, entende-se que a ANPD deve evitar regular ou dar orientações sobre as diretrizes e procedimentos a serem implementados para o atendimento dos direitos de titulares que possam ser demasiadamente específicos ou restritivos. A ANPD deveria focar seus esforços em orientar os agentes de tratamento sobre a necessidade de que, observadas a pluralidade e as especificidades dos modelos de negócios existentes no mercado, os direitos dos titulares sejam atendidos eficazmente.
Bloco II - Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII)	

c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?	A eventual falta de clareza na identificação do controlador, especialmente em casos envolvendo diversos agentes de tratamento, pode representar um desafio para o exercício dos direitos dos titulares. Na prática, o titular, ao tentar exercer seus direitos, pode encontrar dificuldades de identificar o responsável final pelo tratamento dos seus dados. Para solucionar essa dificuldade, é importante que a ANPD esclareça que os operadores, ainda que não devam tomar decisões em relação ao atendimento dos direitos dos titulares sem instruções prévias dos controladores, devem atuar de forma transparente na comunicação com os titulares. Isso está em linha com o art. 9 da LGPD, que não limita expressamente o cumprimento da obrigação de divulgação de informações sobre o tratamento ao controlador. Nesse sentido, na medida da sua participação e considerando a dinâmica específica da respectiva atividade de tratamento, o operador deveria ter a prerrogativa de fornecer informações ao titular acerca do tratamento dos seus dados. A prerrogativa do operador de indicar ao titular dos dados quem é o agente de tratamento responsável por atender às solicitações de exercício de titulares não deve depender de acordo entre controlador-operador, já que é essa premissa que garantirá ao titular acesso a outras informações ou possibilidade de exercício dos direitos previstos na LGPD. Por outro lado, a forma e o conteúdo das informações que serão divulgadas pelo operador ao titular de dados poderá ser objeto de deliberação entre os agentes de tratamento (pela via contratual, por exemplo), desde que essa deliberação não represente empecilhos para que o titular consiga ter acesso efetivo às informações que deseje.
f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?	Entende-se que sim, o direito de acesso pode ser considerado satisfeito quando o agente de tratamento disponibilizar os dados pessoais ao titular em ambos os formatos, eletrônico ou impresso. No entanto, ainda que a LGPD preveja, no §2º do art. 19, que a escolha sobre o formato é do titular, acredita-se que a ANPD deve relativizar essa possibilidade de escolha diante da diversidade dos modelos de negócio no mercado e a variação dos recursos disponíveis a depender do porte do agente de tratamento. Nesse sentido, tem-se como exemplo entidades que tratam dados coletados a partir de fontes públicas legítimas e que possuem um volume considerável de informações sobre determinado titular. A solicitação de acesso às informações na via impressa pode representar custos altos à empresa, diante do volume de dados (e, logo, no material necessário à impressão), principalmente considerando que essa mesma

	solicitação pode ser feita por uma multiplicidade de titulares. Ainda nesse exemplo, a entrega dos dados em formato impresso dificultaria ao próprio titular a sua interpretação. Diante desse cenário, desde que garantido o acesso gratuito às informações (em linha com ao art. 6º, IV da LGPD), ainda que não no formato de preferência do titular, entende-se que deve ser considerado satisfeito o direito de acesso do titular.
Bloco III - Portabilidade dos dados (art. 18, inciso V)	
b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?	Não obstante a importância de que seja assegurado ao titular o direito de portabilidade, a ANPD deve ser cautelosa na regulamentação desse direito para não impor obrigações financeiras excessivas e tecnicamente impraticáveis pelas entidades sujeitas à LGPD. Entende-se que os desafios tecnológicos enfrentados para implementação de um padrão de interoperabilidade derivam, na verdade, da multiplicidade de perfis de agentes de tratamento existentes. Assim, a ANPD deve buscar um equilíbrio entre a efetividade do direito à portabilidade e a viabilidade da implementação de medidas técnicas pelos agentes de tratamento, à luz de aspectos econômicos e estruturais. Isso deverá considerar os diferentes modelos de negócio presentes no mercado e a diferença em relação aos recursos disponíveis para implementar mecanismos técnicos que possibilitem a portabilidade, respeitada a diversidade dos agentes de tratamento. A discrepância entre a forma de organização e o porte dos agentes de tratamento, que ocorre em função do escopo horizontal de aplicação da LGPD, demonstra que, no âmbito da regulação do direito à portabilidade, não há uma solução tecnológica "one size fits all". É muito importante que a ANPD esteja atenta a esse aspecto para evitar a criação de obrigações que representem entraves aos agentes de tratamento e que sejam implementáveis apenas por uma parcela desses agentes, resultando em exclusão da outra parcela.

	É fundamental também levar-se em consideração o aspecto tecnológico da interoperabilidade de dados, em particular a rápida evolução da tecnologia nessa área. Formatos de dados que eram considerados como “padrão de mercado” há poucos anos hoje já são vistos como limitados em sua capacidade de representação das estruturas de informação utilizadas na maioria das bases de dados. A definição excessivamente rígida de um padrão pode levar ao engessamento do setor e ao atraso tecnológico do país como um todo, por obrigar o mercado ao uso de formatos de dados ultrapassados. Diante do cenário acima, é importante que a ANPD busque ativa e especificamente contribuições do mercado acerca de aspectos tecnológicos para viabilização do atendimento desse direito. Através de consultas públicas direcionadas e diálogos abertos com diversos setores da sociedade, a ANPD poderá regular e propor orientações que sejam eficientes, equitativas e sustentáveis para todos os atores envolvidos. A criação de um sandbox regulatório, bem como um foro de autorregulação envolvendo agentes de tratamento, também podem ser medidas efetivas.
c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?	De modo a subsidiar a discussão do tema, destaque-se o art. 20 do General Data Protection Regulation (GDPR), no qual é estipulado que os titulares de dados têm o direito de receber os dados pessoais que forneceram a um controlador em um formato que permita que os dados sejam facilmente transferidos para outro controlador de dados e que estabelece os seguintes requisitos objetivos a serem considerados pelo controlador: (i) Formato estruturado e de uso comum: os dados devem ser disponibilizados em um formato que seja organizado de forma estruturada e que seja amplamente reconhecido e utilizado no mercado, o que facilitaria a interoperabilidade e a utilização dos dados por diferentes sistemas e plataformas (por exemplo, CSV, XML e JSON), mas sem a obrigação de um formato específico; (ii) Leitura automática: o formato dos dados deve ser legível por máquina, o que significa que os dados devem ser apresentados de uma maneira que possa ser processada automaticamente por computadores e sistemas de TI através de programas e/ou bibliotecas de código-fonte disponíveis gratuitamente no mercado, não havendo, portanto, necessidade de intervenção humana; e (iii) Facilidade de transferência: o formato dos dados deve ser projetado de maneira que facilite a transferência dos dados para outro controlador de dados, caso o titular dos dados solicite, o que

	envolve a adoção de padrões comuns de interoperabilidade e a disponibilização de ferramentas ou APIs para facilitar a transferência de dados. O Considerando nº 68 do GDPR determina ainda que o direito do titular dos dados de transmitir ou receber dados pessoais que lhe digam respeito não deve criar a obrigação dos controladores adotarem ou manterem sistemas de tratamento tecnicamente compatíveis. Considerando a discrepância entre os diferentes perfis de agentes de tratamento e de modelos de negócios, essa regra também deveria ser considerada pela ANPD ao regular o direito à portabilidade. Pode ser somado a esses requisitos um quarto, a saber: (iv) Leitura humana: o formato dos dados, além de legível por máquina, deve também ser legível por uma pessoa através de qualquer programa de leitura/edição de texto disponibilizado junto com os principais sistemas operacionais de computador do mercado, ou através de um navegador de internet padrão do mercado. Essa regra garantiria que os agentes de tratamento de dados não possam criar um padrão esotérico de informações que dificulte a entrada de novos participantes, nem que se exclua a possibilidade de o titular avaliar as suas informações pessoais de maneira facilitada e gratuita.
d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?	Sim. E essa possibilidade é importante para garantir que todos os agentes de tratamento consigam viabilizar, financeira e tecnologicamente, o atendimento desse direito. De modo a subsidiar esse posicionamento, destaque-se o art. 20 do General Data Protection Regulation (GDPR), no qual é estipulado que os titulares de dados têm o direito de receber os dados pessoais que forneceram a um controlador em um formato que permita que os dados sejam facilmente transferidos para outro controlador de dados e que estabelece os seguintes requisitos objetivos a serem considerados pelo controlador: (i) Formato estruturado e de uso comum: os dados devem ser disponibilizados em um formato que seja organizado de forma estruturada e que seja amplamente reconhecido e utilizado no mercado, o que facilitaria a interoperabilidade e a utilização dos dados por diferentes sistemas e plataformas (por exemplo, CSV, XML e JSON);

	(ii) Leitura automática: o formato dos dados deve ser legível por máquina, o que significa que os dados devem ser apresentados de uma maneira que possa ser processada automaticamente por computadores e sistemas de TI, não havendo, portanto, necessidade de intervenção humana; e (iii) Facilidade de transferência: o formato dos dados deve ser projetado de maneira que facilite a transferência dos dados para outro controlador de dados, caso o titular dos dados solicite, o que envolve a adoção de padrões comuns de interoperabilidade e a disponibilização de ferramentas ou APIs para facilitar a transferência de dados. O Considerando nº 68 do GDPR determina ainda que o direito do titular dos dados de transmitir ou receber dados pessoais que lhe digam respeito não deve criar a obrigação dos controladores adotarem ou manterem sistemas de tratamento tecnicamente compatíveis. Considerando a discrepância entre os diferentes perfis de agentes de tratamento e de modelos de negócios, essa regra também deveria ser considerada pela ANPD ao regular o direito à portabilidade.
Bloco IV - Correção dos dados tratados (art. 18, inciso III)	
c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.	De maneira não exaustiva, destaque-se, por exemplo, controladores que possuam modelo de negócio legitimamente baseado na coleta de dados pessoais disponíveis publicamente e que, na eventual viabilidade do atendimento de uma solicitação de correção/eliminação/ anonimização/bloqueio de dados do titular, não deverão ser obrigados a comunicar ao(s) controlador(es) da base de dados pessoais pública, especialmente em casos em que não tiver vínculos contratuais com esse controlador.
d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.	Sim. As práticas de mercado que envolvem o tratamento de dados pessoais são diversas, assim como os modelos de negócios dos agentes de tratamento. Nesse sentido, a depender de como as atividades do controlador se estruturam, pode não ser possível atender a uma solicitação de correção do titular do dado. São os casos, por exemplo, de empresas que tratam dados obtidos de outras fontes legítimas, como bases públicas ou dados tornados manifestamente públicos pelo titular. Nessas situações, em que a base de dados do controlador derivará de uma outra fonte, a correção do dado pode não ser possível ou, ainda que o seja, pode não ser efetiva (uma vez que, ao extrair novamente informações da base de dados original, o dado continuará incorreto).

	A ANPD deve estar ciente dessas nuances específicas de determinados modelos de negócios legítimos e admitir a possibilidade de que o agente de tratamento não atenda à solicitação do titular nesses cenários. Isso, no entanto, não deve eximir o agente de tratamento da obrigação de informar ao titular sobre a origem dos dados e, quando possível, sobre os mecanismos disponíveis para solicitar sua correção na fonte original. O mesmo racional deve ser aplicado a solicitações de anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e §2º da LGPD).
Bloco V - Anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e § 2º)	
a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.	Sim. O titular, ao solicitar a exclusão de seus dados, deverá fornecer uma fundamentação clara para tal. Essa medida deve ter como objetivo garantir que a solicitação seja legítima e que o titular esteja ciente das implicações da exclusão. Em alguns casos, a despeito da fundamentação, entende-se que a exclusão de dados pelo agente de tratamento pode não ser viável à luz de eventuais obrigações legais ou regulatórias ou, ainda, na subsistência de um legítimo interesse do agente de tratamento (por exemplo, caso os dados venham a ser necessários para defesa de direitos no futuro). Nesses casos, acredita-se ser possível que o agente de tratamento informe o titular sobre as razões da impossibilidade de exclusão, desde que forneça justificativa razoável e fundamentada para tanto. É importante destacar ainda que a exclusão de dados do sistema do agente de tratamento nem sempre garantirá a sua completa remoção de todas as mídias ou backups. O titular deve estar ciente de que, mesmo após a exclusão da base de dados ativa do agente de tratamento, os dados poderão ainda ser mantidos em backups ou em outros sistemas por motivos de segurança ou recuperação de desastres. Por fim, especificamente nos casos de agentes de tratamento que tratem dados pessoais advindos de fontes públicas ou que foram manifestamente tornados públicos pelo titular, não se pode exigir desses agentes que (i) excluam os dados pessoais das fontes originais; e (ii) que não voltem a tratar esses dados pessoais, especialmente quando seu modelo de negócio for baseado em sistemas automatizados de extração de dados, caso os dados pessoais não sejam excluídos das fontes originais. Em situações nas quais os dados não são coletados diretamente do titular, como em modelos de negócios que os obtêm de fontes públicas

	ou de terceiros, o exercício do direito à exclusão pode ser limitado. A exclusão, nesses casos, deverá ocorrer de acordo com a viabilidade técnica e operacional e observando-se as especificidades do modelo de negócio do agente de tratamento.

Bloco VII - Decisões baseadas em tratamento automatizado (art. 20, caput)

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?	Há diversos desafios práticos na implementação do direito de revisão previsto no art. 20. O primeiro deles diz respeito ao fato de que o artigo condiciona o direito de revisão às decisões tomadas “unicamente” de forma automatizada. A interpretação do termo “unicamente” é subjetiva. Por exemplo, se uma decisão é tomada por um sistema, a partir do processamento de dados, mas o agente de tratamento é responsável por comunicar essa decisão ao titular, o fator humano na “comunicação da decisão” já deveria ser suficiente para se concluir que a decisão não foi tomada “unicamente” de forma automatizada? Ou o conceito demandaria uma intervenção humana mais substancial na decisão, como por exemplo, a interpretação de uma conclusão automatizada a partir de critérios considerados manualmente pelo agente de tratamento? Superada a dificuldade de definir que uma decisão é totalmente automatizada, parte-se para os desafios práticos para revisá-la. Quando o agente de tratamento fizer uso de sistemas complexos (por exemplo, aqueles baseados em <i>deep learning</i>), pode ser difícil identificar qual fator específico levou à decisão para a qual busca-se revisão (especialmente quando os sistemas forem compostos por algoritmos de “caixa preta” – “<i>black box</i>”, cujos processos e operações são inacessíveis). Além disso, a documentação do processo decisório pode ser incompleta ou inexistente nesses casos. A ANPD deve orientar os agentes de tratamento sobre de que modo viabilizar o direito de revisão nesses cenários, sem que as orientações representem barreiras ou desincentivo à inovação. Nesse sentido, é importante que a ANPD oriente os agentes de tratamento principalmente sobre (i) quando uma decisão será considerada tomada “unicamente” de forma automatizada, e (ii) em que consiste a revisão da decisão, especialmente em cenários em que essa revisão se demonstrar impossível considerando a tecnologia empregada. Considerando todas as nuances técnicas relacionadas à revisão de decisões automatizadas e, também, todas as discussões legislativas e regulatórias recentes envolvendo accountability e IA, entende-se que a ANPD deve propor mais iniciativas de participação pública especificamente direcionadas para esse tema (incluindo consultas públicas detalhadas e diálogos abertos com os diversos atores da sociedade), antes de regulamentar o dispositivo da LGPD em discussão. Os resultados do sandbox regulatório de IA e proteção de dados pessoais da ANPD também poderão contribuir para esse processo de regulamentação.

1.1. VERIFICAÇÃO DA AUTENTICIDADE DO TITULAR NO EXERCÍCIO DO DIREITO DE ACESSO

Atualmente, esta preocupação aparece de forma mais evidente no exercício do direito de acesso porque é o prazo que está definido na lei⁵, no entanto, esse desafio é uma constante presente antes do atendimento pelos controladores de qualquer direito exercido pelo titular, cujos prazos ainda serão trazidos por esta r. ANPD, segundo determina a LGPD.

Essa verificação a ser feita pelos controladores, qual seja, checar a autenticidade do titular assim que recebe um pedido exercendo seu direito de acesso, deve ocorrer antes do fornecimento da resposta, sob pena de o descuido poder ensejar um incidente de segurança. A cautela do controlador com a autenticidade do titular, conforme o contexto específico do pedido, visa exatamente a prover uma proteção de seus dados pessoais de forma mais eficaz, havendo, dever legal expresso neste sentido⁶, evitando-se assim acessos ou desvios ilícitos.

Para além do desafio de origem, da verificação da identidade sem uma coleta adicional excessiva de dados pessoais, há um desafio adicional nesse momento, no caso de organizações que oferecem serviços a uma ampla gama de consumidores, usuários finais, visto que as bases de dados com frequência são alvos de artifícios para criação de cadastro falso e/ou incompleto que, muito embora o controlador já adote uma série de medidas para evitá-los, podem passar sem detecção.

Nesse passo, diversas podem ser as situações nas quais os controladores se encontram quando recebem um pedido de acesso, como por exemplo:

- i) O pedido é feito pelo próprio titular com o qual o controlador já tem uma relação jurídica prévia, normalmente contratual; cumpre ao controlador confrontar os dados fornecidos por um titular, no momento do exercício de um direito previsto na LGPD, com os dados que possui sobre aquele titular em sua base de dados;
- ii) O pedido é apresentado por um titular com o qual o controlador ainda não tem qualquer relação jurídica e as informações dos titulares são coletadas licitamente pelo controlador por meio de bases de dados acessivelmente públicas ou por outros meios em que a coleta não foi obtida com o titular diretamente; esse controlador não terá em suas bases de dados informações cadastrais do titular, mas também terá que verificar de autenticidade do pedido, que, no caso, será através da coleta de mais dados pessoais para comprovar e assegurar que o titular-requerente é de fato o titular das informações requeridas;
- iii) O titular possui relação jurídica prévia com o controlador, porém os dados estão desatualizados; eventualmente alguns dados precisam ser coletados para permitir a verificação da autenticidade do titular;

⁵ V. artigo 19, II da LGPD

⁶ V. artigo 6º, inciso X e artigo 46 da LGPD.

- iv) O pedido que é apresentado por terceiro, seja representante legal ou voluntário: o controlador deve se certificar sobre a validade da representação, no sentido de exigir prova de que o representante legal efetivamente exerce esse papel e, na representação voluntária, que a procuração validamente lhe confere os poderes suficientes para exercer o direito pleiteado em nome do titular; e
- v) O contexto do pedido formulado é mais crítico e gera mais riscos ao titular de dados, a exemplo da verificação da autenticidade do titular para cumprir um pedido de acesso a exames realizados em um laboratório clínico, haja vista que envolve a saúde do titular (dado pessoal sensível): certamente uma certificação mais criteriosa é adequada.

Em toda e qualquer situação, de forma mais ou menos complexa, o controlador, antes do cumprimento de um pedido formulado por um titular de dados ou terceiro que o represente, deve proceder a verificação da autenticidade do titular, o que deve ser razoável e coerente com o zelo que o contexto específico requer.

Às vezes a situação poderá ser resolvida com o uso da tecnologia do duplo fator de autenticação (cadastro prévio; dados atualizados), que, inclusive, deveria ser incentivado, à vista do princípio da minimização da coleta. Aqui a verificação da autenticidade do titular poderia ocorrer com a confirmação de certos dados do cadastro, do número do cliente ou do contrato, desde que não sejam dados públicos, ou através do envio de um código numérico via SMS ou um e-mail cadastrado do titular, dentre outras medidas. Por exemplo, um cadastro recente numa loja comercial, não se deve esperar que o controlador colete mais dados ou comprometa investimento grande de recursos para a conferência da autenticidade do titular de dados antes do oferecimento da resposta.

Entretanto, outras vezes esse mecanismo não será suficiente ou viável (inexistência de cadastro; dados desatualizados) e deverá ser considerada legítima a verificação de identidade do titular por meio da obtenção de um documento de identificação na medida da necessidade do controlador. Essa possibilidade representa um meio factível e suficiente, compatível com o arcabouço principiológico da LGPD.

Todavia, em função do incremento significativo de fraude documental, apropriação de identidade e delitos informáticos no Brasil, notadamente, em alguns setores, como de Telecomunicações e Bancários, a utilização da biometria trouxe impactos positivos relacionados à gestão de riscos, em especial, no tocante à mitigação de fraudes e outros problemas de segurança relacionados com a autenticação de identidade do titular.

Desse modo, a implementação de novas soluções tecnológicas para autenticar clientes por meio do uso do processo biométrico, que está atrelado ao histórico de venda/contratação/alteração dos serviços, com objetivo de garantir maior segurança aos próprios clientes e mitigar riscos

relacionados com diversas modalidades de fraudes mostra-se razoável em função do volume de dados e titulares envolvidos, haja vista a necessidade de minimização dos riscos e a garantia da segurança nos processos de negócio desenvolvidos por alguns setores.

Por isso, a adequação da forma de verificação da autenticidade do titular diante do contexto específico do pedido feito pelo titular é de extrema relevância. Ao mesmo tempo em que a LGPD é estruturada com base na gestão de riscos, o que, por um lado, traz flexibilidade para o controlador de dados decidir seus meios de atuação, por outro são necessárias diretrizes desta r. Autoridade Nacional, que garantam o mínimo de segurança jurídica aos controladores durante o tratamento dos dados pessoais. Não se espera da ANPD a edição de regras específicas e prescritivas que sejam obrigatórias a todo e qualquer controlador, eis que tal conduta engessaria o desenvolvimento das atividades econômicas e a livre iniciativa, além de eventualmente extrapolar a realidade e as possibilidades técnicas dos controladores, porém se busca um direcionamento da ANPD de como endereçar as dificuldades práticas enfrentadas.

Nesse sentido, instrui a ICO (Autoridade de Dados do Reino Unido):

“Você pode pedir informações suficientes para julgar se o solicitante (ou a pessoa em nome da qual a solicitação é feita) é a pessoa responsável pelos dados. O ponto principal é que você deve ser razoável e proporcional sobre o que pede. Você não deve solicitar mais informações se a identidade do solicitante for óbvia para você. Este é particularmente o caso quando você tem um relacionamento contínuo com o indivíduo.

Você também não deve solicitar documentos de identificação formal, a menos que seja necessário. Primeiro, você deve pensar em outras maneiras razoáveis e proporcionais de verificar a identidade de um indivíduo. Você já pode ter medidas de verificação em vigor que pode usar, por exemplo, um nome de usuário e uma senha.

No entanto, você não deve presumir que em todas as ocasiões o solicitante é quem diz ser. Em alguns casos, é razoável pedir ao solicitante para verificar sua identidade antes de enviar as informações”.

Sendo assim, é razoável compreender que a verificação da autenticidade do titular, a ser realizada pelo controlador segundo os meios que entender possíveis para sua realidade, perpassa em diferenciar certos contextos para os quais são relevantes a relação jurídica existente entre o titular-requerente e o controlador, a natureza e o volume dos dados pessoais envolvidos no pedido do titular, assim como o risco da atividade desenvolvida pelo controlador.

Para auxiliar a contextualização do pedido, algumas perguntas podem ser realizadas pelo controlador diante de um requerimento feito por um titular:

- i) Qual o pedido formulado pelo titular?
- ii) O titular efetuou o requerimento pessoalmente, ou o requerimento foi feito por terceiro-procurador?
- iii) Existe relação jurídica prévia entre o titular-requerente e o controlador?

- iv) Quais os dados pessoais envolvidos no pedido?
- v) A natureza e volume dos dados pessoais, bem como a atividade desenvolvida pelo controlador geram qual nível de risco para os titulares?
- vi) Qual a natureza e o volume de dados que possuo daquele titular-requerente?
- vii) O pedido envolve dados pessoais sensíveis, ou de crianças e adolescentes? Exemplos: clínicas médicas, hospitais, seguradoras de saúde, escolas, clubes recreativos, associações religiosas, cadastros em redes sociais, dentre outros.

A abordagem do raciocínio apresentado encontra sólido respaldo na própria LGPD, que é construída – assim como inúmeros arcabouços de proteção de dados ao redor do mundo – em uma premissa de gestão de riscos, responsabilização e prestação de contas. Deste modo, seria salutar que esta respeitável Autoridade traçasse orientações considerando os critérios acima mencionados, de modo a guiar, a tomada de decisão do controlador.

Dito isto, sugerimos que, na normatização relativa aos direitos dos titulares, a ANPD deveria fazer constar as seguintes "Recomendações"⁷:

Recomendações referentes à verificação da autenticidade do titular que exerce direitos previstos na LGPD:

- i) O controlador deve proceder, sempre que possível, a verificação da autenticidade do titular que exerce um direito previsto na LGPD antes de atendê-lo para evitar incidentes de segurança;
- ii) O princípio da gestão de risco deve permear a decisão do controlador de como proceder essa verificação;
- iii) O controlador é livre para definir o rigor da verificação da autenticidade do titular adotada em cada caso, levando em conta, por exemplo, o contexto específico, a natureza e o volume dos dados pessoais envolvidos no pedido, os níveis de risco que o pedido do titular lhe impõe, além de outros fatores que entender relevantes;
- iv) Desde que possível, o controlador deverá evitar coletar dados pessoais adicionais para fins de verificação da autenticidade do titular que formula um pedido, sendo estimulado o uso de tecnologia de duplo fator de autenticação, ou equivalente;
- v) Caso o controlador não tenha relação prévia com o titular de dados, ou caso os dados estejam desatualizados, é legítima a coleta de documento de identificação para realizar a verificação da autenticidade;

⁷ De acordo com o item 4, do Anexo I, da Agenda Regulatória da ANPD para o biênio 2021-2022, divulgada pela Portaria nº 11, de 17/01/2021, da ANPD, Presidência da República, o tema "Direito dos Titulares" deve ser tratado através de uma Resolução.

- vi) A coleta de dados pessoais sensíveis, como a biometria, deve ser reservada a casos específicos, em que a sua necessidade seja justificada em virtude de particularidades dos controladores de dados, inclusive setoriais, como por exemplo, volume de titulares, natureza das atividades de tratamento realizadas, dados pessoais tratados e o interesse público, especialmente no que tange ao combate a fraudes e garantia de segurança aos titulares;
- vii) A verificação da validade do pedido feito por terceiro (representante legal/procurador) deve ser feita com cautela⁸. Neste caso, sugerimos, em prol da segurança jurídica e eficiência no atendimento do pedido, que esta r. Autoridade forneça um modelo de procuração, com poderes expressos para que os titulares possam voluntária e precisamente escolher o que pretendem solicitar no exercício do direito de acesso e autorização expressa e inequívoca para o recebimento dos dados em nome do titular, se essa for sua real intenção.

2. INÍCIO DA CONTAGEM DO PRAZO DO INCISO II DO ARTIGO 19 DA LGPD PARA OS DIREITOS DE CONFIRMAÇÃO DA EXISTÊNCIA E DE ACESSO A DADOS

2.1. SUSPENSÃO DO PRAZO ATÉ A VERIFICAÇÃO DA AUTENTICIDADE DO TITULAR

Em virtude da complexidade para a verificação da autenticidade do titular de dados, o momento do início da contagem do prazo do inciso II do artigo 19 é um aspecto que tem levantado inúmeros questionamentos pelos controladores que se preocupam em zelar pela segurança jurídica e evitar incidentes de segurança. Isso porque a verificação da autenticidade do titular pode afetar o prazo que os controladores dispõem, na LGPD, para resposta.

De acordo com a redação da LGPD, o atendimento a um requerimento do titular sobre (i) a confirmação da existência de tratamento ou (ii) o acesso aos dados deve ocorrer:

"I - em formato simplificado, imediatamente", ou

"II - por meio declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 dias, contado da data do requerimento do titular."¹⁰ (grifos nossos).

⁸ Segundo a autoridade de dados inglesa (ICO), a verificação da validade do pedido feito por terceiro deve ser feita pelo controlador que recebe o pedido de acesso em nome de um titular. O pedido deve ser respondido se o controlador estiver confortável e seguro com relação à legitimidade do requerimento. Isso não significa avaliar a idoneidade do terceiro, mas sim checar se a procuração atende os requisitos legais para seu cumprimento.

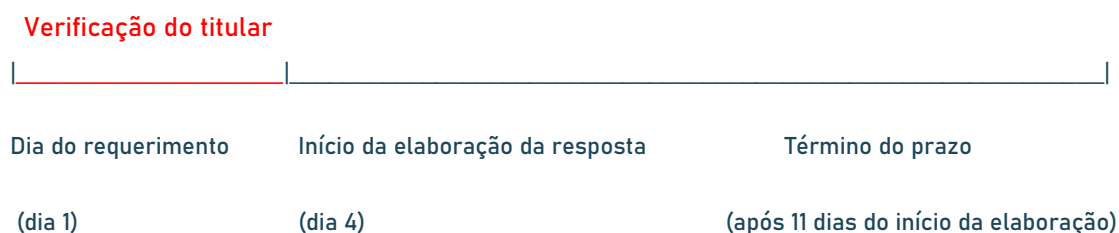
⁹ Inciso I do art. 19 da LGPD.

¹⁰ Inciso II do artigo 19 da LGPD.

A questão abordada no presente tópico se refere especificamente ao inciso II aqui transcrito, que determina o prazo de 15 dias, a contar do requerimento, para que o direito à confirmação da existência de tratamento ou o direito de acesso aos dados seja atendido por meio de declaração clara e completa.

Após o requerimento feito através de um pedido de confirmação da existência ou de acesso a dados pessoais, poderá haver uma janela de tempo da qual o controlador deve se valer para verificar a autenticidade do titular antes de o pedido formulado ser atendido. O controlador não pode fornecer uma resposta sem essa confirmação, sob pena de violar a lei¹¹ e incorrer em um incidente de segurança caso forneça dados pessoais a terceiros. Contudo a LGPD determina que o prazo de (até) 15 dias deve ser contado do requerimento do titular.

Uma linha de tempo pode melhor ilustrar essa tênue questão:



Como se percebe no exemplo hipotético acima, o prazo efetivo que o controlador teve para responder foi apenas de 11 dias, tendo em vista que levou 72 horas para a verificação do titular, para a validação de seu pedido. Na prática, não é incomum que o prazo necessário para a confirmação da autenticidade do pedido seja ainda maior, fazendo com que o controlador conte com uma exígua janela de tempo para atendimento do pedido do titular.

Isso pode ocorrer por diversos fatores, como dificuldades técnicas, multiplicidade de sistemas, natureza da atividade desenvolvida pelo controlador, volume de dados, dentre outros, e a depender do modelo de negócio da empresa e suas especificidades, essa verificação não poderá ser feita imediatamente. São exemplos situações que os controladores se deparam e que afetam diretamente o cumprimento do prazo em análise:

- i) O titular-requerente que, ao formular pedido, se recusa insistentemente em compartilhar qualquer dado, até mesmo o CPF, com o controlador para comprovação de sua identidade, o que prejudica o atendimento cauteloso do direito no prazo;

¹¹ V. artigo 44 e parágrafo único da LGPD.

- ii) O controlador disponibiliza um canal aos titulares para o exercício dos direitos, mas isso não é respeitado pelos titulares e os pedidos chegam de maneira pulverizada. No caso de pequenas empresas, a dificuldade pode ser o mapeamento dos dados pessoais que detém daquele titular-requerente; e
- iii) Em empresas de maior porte, a dificuldade pode passar em compilar todos os dados pessoais de todos os sistemas que utilizam para fornecê-los ao titular nesse exíguo período de tempo.

Não é possível, contudo, de antemão precisar o período que essa verificação leva para acontecer em todo e qualquer negócio, porquanto esse aspecto depende de diversas variáveis presentes no contexto específico.

Ademais, podem existir casos em que, numa primeira verificação, o controlador perceba que dados fornecidos pelo requerente não coincidem com os que constam em sua base de dados e que precisa, portanto, realizar uma checagem mais apurada de sua titularidade – como explicado no tópico anterior.

Em suma, quanto maior a dificuldade de verificação da autenticidade do titular, menor o tempo restante para o controlador responder ao pedido.

Sendo assim, ainda que se busque o atendimento de tais pedidos no menor prazo possível, na prática o prazo de 15 dias não deve ser contado do requerimento propriamente dito, mas sim após a verificação, pelo controlador-requerido da autenticidade do titular, ou seja, após a confirmação que o pedido foi feito por quem tem efetivamente o direito de acesso aos dados solicitados. Esse prazo de verificação seria, assim, entendido como um processo de validação do próprio pedido, com o início do prazo legal somente após a validação da legitimidade do pedido submetido.

Logo, a expressão “contado da data do requerimento do titular” deve ser interpretada como “contado da data do requerimento [legítimo] do titular”, sendo a legitimidade alcançada pela verificação da autenticidade do titular-requerente, no prazo de verificação razoável e adequado a cada negócio. Entendemos que a formalização desse entendimento em guia orientativo ou norma a ser editada pela ANPD seria um importante avanço na garantia da segurança jurídica afeta a construção do ambiente de proteção de dados no país.

Note-se que no White Paper produzido pela CIPL¹² com sugestões ao European Data Protection Board (EDPB) sobre como implementar os direitos dos titulares numa economia global dirigida por dados, há uma recomendação exatamente nesse sentido, qual seja, a de que o prazo de

¹² Center for Information Policy Leadership, White paper: “Data Subject Rights under the GDPR in a Global Data Driven and Connected World”, 08.07.2020

resposta a um pedido de acesso previsto no GDPR¹³ deveria ser contado a partir da confirmação adequada da identidade do titular-requerente.

Este prazo, por sua vez, poderia ser informado pelo próprio controlador, ao titular, quando do seu requerimento, considerando suas peculiaridades técnicas. Desta forma, haveria o devido zelo com a transparência ao titular, ao comunicá-lo sobre esse prazo de autenticação no momento da solicitação de um pedido de acesso, e com a própria segurança que se espera do controlador no tratamento dos dados pessoais, ao confirmar a legitimidade do requerimento antes de fornecer a resposta, num equilíbrio de conformidade com o que a lei exige.

Importante ressaltar que, às vezes, a demora na validação do pedido pode decorrer de uma inércia do próprio titular-requerente, que deixa de tomar alguma providência solicitada pelo controlador-requerido para tanto. Por conseguinte, tal demora deveria igualmente representar um impedimento para o início do prazo para resposta, na medida em que o controlador nada pode fazer se não ultrapassada essa etapa preliminar de validação do pedido pela autenticação do titular que, ao fim, beneficia o próprio titular dos dados.

Referida conduta confere segurança no tratamento dos dados pessoais e no atendimento aos direitos dos titulares, segurança esta que, inclusive, é exigida pela lei, em seu artigo 44. Dito de outra forma, o tratamento deve ser realizado de acordo com a segurança que dele se espera e certamente o titular de dados não espera que as empresas forneçam seus dados a terceiros não autorizados; tampouco os controladores, na sua lógica de gestão de riscos, querem dar margem a incidentes de segurança, como uma resposta descuidada a um pedido de acesso de suposto titular e sofrer a responsabilização consequente.

Como alternativa mais eficiente, poderia ser recomendado aos controladores de dados, quando sua estrutura assim o permitir, que fosse adotada uma ferramenta ou sistema automatizado de pedido de acesso, eventualmente separado por categorias de titulares (exemplo: cliente, usuário do site, funcionário, fornecedor, parceiro etc.), que facilitaria o rastreamento dos dados pessoais a partir de seu requerimento. Desta forma, uma vez verificada a autenticidade e a categorização do titular logo no pedido, a identificação dos dados nos sistemas do controlador seria muito mais ágil, prestigiando, com isso, a celeridade no atendimento ao direito solicitado.

Não obstante, ainda que a automatização do rastreamento dos dados pessoais seja, em prol da eficiência, estimulada, também devem ser consideradas pela ANPD as situações nas quais os sistemas ou bancos de dados dos controladores, por serem muito antigos, podem apresentar impossibilidade técnica de serem automaticamente rastreados. Nesse caso, é fundamental também

¹³ "Article 12 (3) of the GDPR: "(...) within one month of receipt of the request."

que a ANPD valide a opção do controlador em identificar e categorizar esses dados pessoais manualmente.

E mesmo que se adote o sistema ou ferramenta acima mencionada, ou se opte pela identificação manual dos dados pessoais constantes dos bancos de dados dos controladores, cumpre apresentar aqui outro aspecto pertinente ao tema que precisa ser endereçado pela ANPD, e que decorre do pedido do titular e que diz respeito à sua amplitude já que isso também afeta o prazo para seu atendimento.

2.2. SUSPENSÃO DO PRAZO PELA NECESSIDADE DE COMPREENSÃO DO PEDIDO FORMULADO PELO TITULAR

Para que o direito do titular seja devidamente atendido, seja no conteúdo, seja no tempo previsto em lei¹⁴, é também necessário que o controlador compreenda o que o titular pretende acessar, ou seja, quais informações busca obter.

Um pedido genérico, formulado por um titular que solicite todos seus dados existentes no controlador em todas as atividades de tratamento, como muitas vezes acontece, ensejará um atendimento falho e incompleto devido à imprecisão do requerimento. Um pedido nesses termos necessita de esclarecimento, de um complemento pelo titular de dados. Logo, a depender da quantidade de dados tratados e das operações de tratamento desenvolvidas, o controlador, por vezes, precisará solicitar esclarecimentos ao titular-requerente¹⁵ sobre o que ele pretende obter, porém sem que isso prejudique seu prazo para resposta.

Tal cuidado é expressamente sugerido pelo *CNIL*, em suas diretrizes sobre como atender um pedido de acesso¹⁶.

Uma maneira de se endereçar essa questão - em guia orientativo da Autoridade - seria a suspensão do prazo de resposta a requerimento genérico por dois motivos: primeiro, para a verificação da autenticidade do titular, amplamente discutida nos tópicos anteriores; segundo, para que o titular, a pedido do controlador, complemente seu pedido, se genericamente formulado. Nesse sentido, por mais que se deva honrar o direito do titular, deve haver, da parte do controlador, uma verificação de contexto para o atendimento pleno do pedido, respeitados os contornos da LGPD.

Alternativamente, e dentro do prazo definido no artigo em comento, deve-se permitir que controlador responda àquele pedido de acesso genérico e ilimitado “em camadas”, conforme sugere a Autoridade de Proteção de Dados espanhola (V. tabela no Anexo I a esse documento)¹⁷, ideia

¹⁴ V. Artigo 19, II da LGPD.

¹⁵ V. ICO guidelines em <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/#responding>

¹⁶ <https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces>

¹⁷ <https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf> (pg. 05 e ss)

igualmente defendida pela CIPL¹⁸. Por exemplo, numa primeira camada poderiam ser fornecidas informações mais básicas e sucintas¹⁹, inteligíveis à uma pessoa comum²⁰ e, caso ainda assim restem dúvidas, o titular poderá solicitar um segundo pedido com maior detalhamento e especificidades, renovando-se o prazo para o controlador responder.

As Cortes de Justiça de Amsterdã²¹ e da Alemanha²² chegaram a admitir a recusa ao cumprimento de pedidos de acesso em virtude de os requerimentos respectivos terem sido muito extensos e/ou indefinidos, podendo esta opção também ser validada pela ANPD.

Em resumo, um pedido genérico feito por um titular deveria autorizar, a critério do controlador de dados: (1) um pedido de esclarecimento ou complementação ao titular, com suspensão do prazo da resposta até manifestação do titular; ou (2) uma resposta genérica (“primeira camada”) e considerada válida; ou (3) a recusa de seu atendimento.

2.3. CONTAGEM EM DIAS ÚTEIS E HORÁRIO COMERCIAL

Relevante, por fim, trazer a questão sobre a natureza dos dias que devem ser considerados na contagem do prazo em análise²³, se dias úteis ou dias corridos, assim como o horário razoável de funcionamento dos controladores para tal fim.

No que se refere à natureza dos dias, visando ao alcance de uma interpretação razoável da lei e uma padronização de sua aplicação no território nacional para conferir uma previsibilidade ao titular dos dados, um parâmetro que poderia ser adotado seria o art. 219 do Código de Processo Civil brasileiro, que prevê sejam considerados apenas os dias úteis para os prazos estabelecidos em dias²⁴. Embora seja um dispositivo que se aplique aos prazos processuais em juízo, a lacuna da LGPD poderia ser suprida fazendo-se essa analogia. O Código de Processo Civil ainda determina que os dias úteis são de segunda a sexta-feira, excluídos os feriados²⁵.

¹⁸ V. CIPL, *White Paper*.

¹⁹ V. CIPL, *White Paper*.

²⁰ A referência à “pessoa comum” deve ser entendida como dados que são compreensíveis por todos, sem que seja necessária uma especialização técnica para sua compreensão.

²¹ *Amsterdam Court, 20/06/2019, ECLI:NL:RBAMS:2019:4418: “Request to healthcare institution for complete copies of the processing of personal data on the basis of the GDPR. In principle, right to copies pursuant to Article 15 GDPR. Partly rejected if the request is too indefinite and / or too extensive or if the data is not available at the care institution (or at least insufficiently substantiated after a dispute about the care institution).”* Disponível em: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:4418>

²² *Bundesarbeitsgericht, Urteil vom 27. April 2021 – 2 AZR 342/20: “The German Federal Labour Court released, on 27 April 2021, its decision regarding an employee’s right to access their entire email correspondence and any emails mentioning them by name. In particular, the Court found that the request, which was submitted under Article 15 of the General Data Protection Regulation (Regulation (EU) 2016/679) (‘GDPR’), was not specific enough under the applicable civil procedural rules. As a result, the Court held that the employer was not required to provide copies of the employee’s entire email correspondence, as well as any emails mentioning the employee by name.”* Disponível em *DataGuidance website*.

²³ V. art. 19 II da LGPD

²⁴ “Art. 219. Na contagem de prazo em dias, estabelecido por lei ou pelo juiz, computar-se-ão somente os dias úteis. Parágrafo único. O disposto neste artigo aplica-se somente aos prazos processuais.”

²⁵ “Art. 216. Além dos declarados em lei, são feriados, para efeito forense, os sábados, os domingos e os dias em que não haja expediente forense.”

Quanto ao horário de funcionamento para fins de resposta ao pedido de acesso, igualmente seria salutar considerar o horário de funcionamento dos estabelecimentos comerciais, que, em regra, ocorre das 9h às 18h, o que alcançaria uma gama ampla de controladores, garantindo uma interpretação uniforme e justa da lei. Ou seja, os direitos dos titulares seriam atendidos dentro do horário comercial e requerimentos feitos após às 18h seriam considerados como realizados no dia útil seguinte (de segunda a sexta-feira, exceto feriados).

Deste modo, sugerimos que, na normatização relativa aos direitos dos titulares, a ANPD deveria fazer constar as seguintes "Recomendações":

Recomendações referentes ao prazo previsto no artigo 19 II da LGPD:

- i) O início da contagem do prazo ocorrerá após a devida autenticação do titular feita pelo controlador;
- ii) Caso não seja possível a verificação imediata da autenticidade do titular, o controlador pode informar ao requerente, pelo mesmo meio em que foi contatado, o tempo que levará para proceder tal verificação, devendo o prazo para resposta passar a contar após essa verificação devidamente realizada;
- iii) Caso a verificação da autenticidade do titular dependa de alguma providência a ser cumprida pelo titular-requerente, como por exemplo a informação de um código que lhe tenha sido enviado por SMS ou e-mail, ou apresentação de um documento, o prazo para resposta não correrá até que a providência seja realizada;
- iv) Para que o direito de acesso seja cumprido dentro do prazo definido na LGPD, é recomendável:
 - sempre que possível, a disponibilização ao titular de dados de sistema ou ferramenta automatizada de pedido de acesso, separada por categoria de titular, de modo que haja uma identificação dos dados pessoais de uma forma mais célere e eficiente;
 - o titular deve peticionar através do meio disponibilizado pelo controlador, prestigiando a centralização de pedidos;
 - o titular deve formular pedido certo e determinado. Em caso de pedido genérico e ilimitado e, no intuito de viabilizar uma resposta dentro do prazo legal, é legítimo ao controlador, ao seu critério: (1) formular um pedido de esclarecimento ou complementação ao titular, com suspensão do prazo da resposta até a obtenção de uma resposta; (2) oferecer uma resposta mais básica, genérica, compreensível a uma pessoa comum, como uma primeira camada de resposta ao titular e, caso a resposta não seja suficiente, ao

titular de dados cabe solicitar um novo pedido apresentando mais detalhes e especificações, renovando-se o prazo para resposta do controlador; (3) recusar o atendimento do pedido.

- v) É cabível o rastreamento manual de dados pessoais para responder a um pedido de acesso realizado por titular, se assim o controlador dos dados entender conveniente; e
- vi) O prazo previsto no art. 19 II da LGPD será contado em dias úteis (de segunda a sexta-feira, exceto feriados), observado o horário comercial (das 9h às 18h).

3. DADOS DE PESSOAS JURÍDICAS X USO DE DADOS PESSOAIS NA ATUAÇÃO DE PESSOAS JURÍDICAS

Seguindo os exemplos do direito comparado, a LGPD, em seu artigo 1º, expressa e inequivocamente, limita o âmbito de sua aplicação aos dados de pessoas físicas. E tal restrição não poderia ser diferente na medida em que a justificativa de toda a construção da mencionada lei gira em torno da proteção aos direitos individuais fundamentais relacionados à pessoa humana, valor máximo do ordenamento jurídico dos estados democráticos de direito.

Portanto, a LGPD não tutela os dados de pessoas jurídicas, cuja personificação, como se sabe, é uma mera realidade jurídica²⁶ para aquisição de direitos e obrigações, sendo sua existência autônoma e independente das pessoas que a constituem – seus sócios.

As pessoas jurídicas tampouco se confundem com seus representantes legais, pois, ainda que sejam pessoas naturais, a vontade manifestada através deles não reflete e não diz respeito à vontade do indivíduo per se, mas à da entidade a qual representam. Eles falam em nome delas e não por si próprios. Tal premissa se encontra, inclusive, expressa no art. 49-A do Código Civil ao determinar que a pessoa jurídica não se confunde com a pessoa de seus sócios, associados, instituidores ou administradores.

Os dados das pessoas jurídicas por vezes podem se assemelhar aos das pessoas físicas, mas com eles não se confundem e esse aspecto é fundamental para correta aplicação da LGPD.

Como exemplos, podemos citar:

²⁶ Caio Mário da Silva Pereira, “Instituições de Direito Civil”, Vol. 01, p. 308

- i) O caso do nome comercial de uma pessoa jurídica que envolva o nome próprio de pessoas físicas. Como o nome comercial é de titularidade de uma pessoa jurídica, a finalidade de sua utilização não envolve esfera jurídica de uma pessoa física, mas sim a de uma pessoa jurídica propriamente dita, detentora, inclusive, de CNPJ. Logo, esse nome comercial, ante a titularidade, o contexto e a finalidade de sua utilização, não pode ser considerado dado pessoal e foge à proteção da LGPD, ainda que no meio dele exista um sobrenome de uma pessoa natural;
- ii) A linha telefônica de titularidade de pessoa jurídica, mas que é usada por representante da empresa; e
- iii) O endereço da pessoa jurídica que é o mesmo do sócio pessoa física; e
- iv) O endereço eletrônico corporativo.

Todos esses dados, quando se referirem à esfera jurídica da pessoa jurídica, não serão abrangidos pela lei, e não se confundem com dados das pessoas físicas, sejam elas seus sócios, ou seus representantes.

Situação diversa ocorre quando, numa relação jurídica travada pela pessoa jurídica, há o envolvimento de dados de qualificação dos sócios (pessoas físicas) ou dos representantes legais das pessoas jurídicas, como o nome, a qualificação, ou o número de telefone pessoais. Esses, sim, serão dados pessoais porquanto a esfera jurídica e a titularidade dos dados envolvidos são, realmente, do indivíduo e, quando tratados, se sujeitam à LGPD. De todo modo, são dados públicos, cujo tratamento é legítimo se em conformidade com a finalidade para a qual foram publicizados²⁷.

No Brasil, considerando a grande maioria de pequenas e médias empresas e a grande quantidade de pequenos empreendedores, temos as figuras de sociedades tais como MEI – Microempresa individual²⁸ e EIRELI – Empresa Individual de Responsabilidade Limitada²⁹, que possuem apenas um sócio e que, em alguns casos, dependendo da atividade desenvolvida, admitem inclusive a flexibilização do endereço da sede, que pode se confundir com o residencial.

Também nesses casos, embora as informações a respeito das referidas pessoas jurídicas façam com que se chegue a determinados dados de seus sócios, não se deve confundir as referidas sociedades com as pessoas físicas que as constituíram, não podendo elas, quando estiverem atuando em nome da pessoa jurídica, tampouco, exercer direitos de titulares.

Assim sendo, a devida distinção sobre os dados referentes às pessoas jurídicas e aqueles dados pessoais que dizem respeito aos seus sócios (pessoas físicas) ou seus representantes legais

²⁷ Artigo 7º, parágrafo 3º da LGPD.

²⁸ Criada pela Lei Complementar 128/2008.

²⁹ Criada pela Lei 12.441/2011.

e o esclarecimento da legitimidade de seu tratamento é de premente necessidade para resguardar a correta aplicação da LGPD.

Uma referência de extrema relevância diz respeito à Lei de Proteção de Dados de Singapura (PDPA) que, expressamente, exclui de seu âmbito de aplicação, como regra, os "*business contacts*"³⁰ ao afirmar em seu artigo 4 (5)³¹ "*Exceto quando houver ressalva expressa, as Partes III a VI não se aplicam às informações de contato comercial*". As partes da lei mencionadas, por sua vez, se referem aos seguintes tópicos: "*(III) Regras Gerais a Respeito da Proteção de Dados Pessoais; (IV) Coleta, Uso e Divulgação de Dados Pessoais; (V) Acesso e Correção dos Dados Pessoais; (VI) Cuidado com Dados Pessoais*".

É louvável e muito feliz a distinção feita pela própria lei de Singapura, o que denota necessidade clara quanto ao esclarecimento da diferença de tratamento de dados no contexto empresarial, com relação ao tratamento que é realizado num contexto que envolva a esfera jurídica, propriamente dita, daquele que diz respeito aos dados pessoais de sócios (pessoas físicas) ou representantes de pessoas jurídicas efetivamente.

Sendo assim, sugerimos que, na normatização relativa aos direitos dos titulares, a ANPD deveria fazer constar as seguintes "Recomendações":

Recomendações sobre a distinção de tratamento de dados no contexto empresarial e no contexto de titulares pessoas físicas:

- i) A LGPD se aplica às pessoas físicas e não às pessoas jurídicas. Logo, a titularidade dos dados, o contexto e a finalidade de sua utilização são critérios relevantes para a incidência ou não da lei³²;
- ii) Quando as relações jurídicas se referirem à atuação da pessoa jurídica, a LGPD será inaplicável.
- iii) No que concerne aos dados que se refiram aos sócios (pessoas físicas) ou seus representantes legais, são considerados pessoais e merecem a proteção da LGPD. Todavia, como são considerados dados públicos e seu tratamento - em especial, o acesso a eles -,

³⁰ Como "*business contacts*" (contato comercial), a lei de Singapura define como "*o nome de um indivíduo, nome da posição ou cargo, número de telefone comercial, empresa, endereço, endereço de correio eletrônico comercial ou fax comercial, número e qualquer outra informação semelhante sobre o indivíduo, não fornecido por ele para fins unicamente pessoais*";

³¹ Tradução livre. V. Data Protection Act 2012, de Singapura.

³² Nesse aspecto, vide decisão judicial proferida pelo TJSP, no processo de nº 1003381-18.2021.8.26.0566, que afastou a incidência da LGPD para dados de pessoas jurídicas no caso concreto, admitindo, contudo, a aplicação por analogia, dada a possibilidade de confusão de alguns dados com os da pessoa natural. Finalidade, boa fé e o interesse público que justificam a disponibilidade dos dados, sem comprometer a segurança, intimidade, honra e a imagem da pessoa jurídica.

desde que feito de boa-fé, para atuar e representar a pessoa jurídica, é perfeitamente justificado e legítimo, segundo a LGPD³³.

- iv) Os direitos das pessoas físicas (que também são sócios ou representantes de pessoas jurídicas) devem ser exercidos pelas pessoas físicas, titulares dos dados pessoais, ou procurador legítimo, com poderes específicos para o exercício dos direitos, e nunca pelas pessoas jurídicas que eles representam.

4. PONDERAÇÕES SOBRE O EXERCÍCIO DE DIREITO PELOS TITULARES

Neste tópico apresentamos, de uma forma mais abrangente, outros desafios relacionados à interpretação dos direitos dos titulares criados pela LGPD. Embora mais perceptíveis quando falamos do direito de acesso, são premissas que devem guiar o exercício de qualquer um dos direitos dos titulares.

Nesse particular, é indubitável a compreensão de que nenhum direito individual deve ser tido por absoluto³⁴, eis que a ordem jurídica consubstancia interesses muitas vezes contrapostos e que precisam ser ponderados nas situações concretas, de forma a garantir sua efetividade. Esse raciocínio não poderia ser diferente na interpretação da LGPD quanto aos novos direitos que conferiu aos titulares de dados pessoais. Não há dúvidas de que precisam ser observados em sua essência, eis que frutos de uma inovação legislativa legítima e louvável, porém, a amplitude dos direitos conferidos aos titulares de dados pessoais possui balizadores, conforme veremos.

É sabido que a LGPD dá margens para a definição de contornos equilibrados de normatização pela ANPD ao lhe conferir tal atribuição³⁵ e ao trazer como seus próprios fundamentos³⁶, além do respeito à privacidade, à autodeterminação informativa e outros importantes direitos relacionados ao indivíduo, valores diversos, igualmente imprescindíveis para a realidade brasileira. Portanto, também devem ser considerados na interpretação da LGPD os desenvolvimentos econômico e tecnológico e a inovação, a livre iniciativa e a livre concorrência.

Não obstante, a forma de exercício desses direitos também precisa ser melhor delineada pela ANPD para prestigiar a boa-fé, a própria finalidade da existência desses direitos e desincentivar a imposição de obrigações inexecutáveis, excessivas ou injustificáveis para os controladores de dados

³³ Parágrafo 3º do artigo 7º da LGPD.

³⁴ Premissa inclusive expressamente prevista no artigo 29 (2) na Declaração Universal de Direitos Humanos de 1948, da qual o Brasil é signatário.

³⁵ Artigo 55-J, principalmente incisos I, II, XIII, XX e parágrafo 5º da LGPD.

³⁶ Artigo 2º da LGPD.

peçoais, de forma a coibir o exercício abusivo de direito, comportamento expressamente repudiado pelo ordenamento jurídico nacional³⁷.

Os controladores vêm tendo dificuldades para o atendimento de alguns direitos dos titulares que, sem compreender seu real significado, extrapolam o razoável para, por exemplo, (i) exercem o pedido de acesso de forma extremamente ampla e vaga; (ii) solicitam informações confidenciais ou que envolvem terceiros; (iii) exigem o apagamento dos dados quando ainda há base legal que legitima o tratamento pelo controlador; (iv) confundem o direito à anonimização com o direito à eliminação e o bloqueio no tratamento de seus dados; ou (v) insistem em se opor a operações de tratamentos realizadas pelos controladores em perfeita consonância com a LGPD.

Nesse passo, a conceituação do abuso de direito pela doutrina, apesar de ampla, também pode ser definida como o exercício do direito de modo a contrariar e contradizer o valor que o próprio direito procura tutelar. Portanto, representaria uma violação a limites, não colocados pela existência de direitos de terceiros, mas definidos pelos elementos intrínsecos ao próprio direito, exemplificado como o seu valor ou sua função³⁸. Nesse contexto, o princípio da boa-fé, como princípio geral de direito, é fundamental para balizar os limites do exercício legítimo dos direitos criados pela LGPD aos titulares de dados.

Ademais, é importante ressaltar que existem outros valores e fatores, além do abuso de direito ou do princípio da boa-fé, que legalmente limitam o exercício do direito de acesso e de outros direitos previstos na LGPD, como (i) liberdade de expressão; (ii) investigações e processos internos; (iii) direitos e liberdades de terceiros; (iv) questões confidenciais; (v) propriedade intelectual e, de forma mais ampla, segredos de negócio, que também precisam ser esclarecidos e endereçados pela ANPD em sua normatização sobre direito dos titulares.

Nessa linha de ideias, na sequência abordaremos alguns direitos específicos, cujo exercício pelos titulares já apresenta inúmeros desses desafios para os controladores de dados.

4.1. DOS LIMITES AO EXERCÍCIO DO DIREITO DE ACESSO

Retornando ao direito de acesso, mas agora abordando com mais detalhes a forma de seu exercício, a Autoridade Espanhola de Proteção de Dados Pessoais, em precedente divulgado em seu website³⁹, invocou a violação do princípio da boa-fé para classificar certo pedido de acesso como abusivo e entendeu como válida a recusa do controlador em responder ao titular. No caso, o requerente havia desempenhado diversas funções no controlador (uma universidade) e formulou um pedido de acesso amplo, sem especificar o que pretendia. Mesmo diante da provocação da

³⁷ Artigo 187, do Código Civil: *"Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes"*.

³⁸ FERNANDES, Ilana Oliveira. "A Teoria do Abuso do Direito no Novo Código Civil", em: WebArtigos.com. Publicado em 16 de maio de 2007 <http://www.webartigos.com/artigos/a-teoria-do-abuso-do-direito-no-novo-codigo-civil/1646/>

³⁹ Em 15.04.2021. Disponível em: <https://www.aepd.es/es/documento/e-00739-2021.pdf>

universidade para esclarecer a solicitação, o titular-requerente reiterou o pedido antes feito sem indicar quaisquer detalhes. Por oportuno, transcrevemos trecho da decisão proferida pela Diretora da AEPD:

"No presente caso, conforme declarado no início desta Resolução, o reclamante pode obter o acesso desejado se esclarecer os termos de sua solicitação, eis que conhecedor das inúmeras funções que exerceu na entidade reclamada [uma Universidade]. Quando os direitos são exercidos ajustando-se formalmente aos requisitos estabelecidos pela Lei, mas de forma anormal, de modo que seu conteúdo essencial seja distorcido, incorre em um abuso de direito que o sistema jurídico em nenhum caso pode proteger." (grifos nossos).

Referido exercício abusivo do direito de acesso, assim como outros excessos semelhantes já têm sido percebidos e sofridos pela indústria, como por exemplo:

- i) O titular que insiste em receber a resposta por canal diverso do disponibilizado pelo controlador;
- ii) O titular (colaborador) que solicita acesso a investigações em andamento nas quais seja citado, mas que são sigilosas e afetam direito de terceiros; e
- iii) O titular insiste numa resposta por e-mail do controlador com informações sobre seus dados e cópia de seus contratos, quando esse acesso pode ser alcançado diretamente pelo titular mediante o login em seu cadastro, no site do controlador⁴⁰, dentre outros.

Deste modo, a necessidade de atuação da ANPD para traçar diretrizes norteadoras sobre os limites razoáveis ao exercício deste direito, em particular, é urgente e inevitável.

4.1.1 Do pedido de acesso sobre compartilhamento de dados

Dentro desse contexto vale mencionar a questão do compartilhamento de dados dos titulares porque, muitas vezes, o controlador se depara com pedidos de titulares exercendo seu direito de acesso numa extensão exacerbada, ao ponto de solicitar a indicação nominal de todos os terceiros, e todos os destinatários de dados pessoais com quem compartilhou dados pessoais. Porém, a informação individualizada sobre todos os destinatários dos dados pessoais, além de possivelmente revelar dados de outras pessoas físicas que eventualmente não permitiram essa revelação e pode expor dados comercialmente estratégicos do controlador, tutelados pelos segredos comercial e industrial. Assim, a divulgação desses nomes pode ensejar um problema concorrencial, o que violaria um dos princípios da LGPD⁴¹.

Por essa razão, entendemos que a obrigação de prestar as informações sobre o compartilhamento de dados poderia se limitar à indicação das categorias de destinatários e à

⁴⁰ V. CIPL White Paper.

⁴¹ Artigo 2º da LGPD: A disciplina da proteção de dados pessoais tem como fundamentos (...) Inciso VI - a livre iniciativa, a livre concorrência e a defesa do consumidor."

finalidade⁴² para os quais são tratados, o que atenderia o princípio da transparência⁴³ e o pedido de acesso do titular dos dados.

4.1.2. Do pedido de acesso sobre as bases legais

Outro aspecto concernente ao direito de acesso se refere à informação sobre as bases legais dos tratamentos realizados pelo controlador. A LGPD não prevê a obrigação de informar ao titular de dados as bases legais específicas das atividades de tratamento que realiza, tampouco há direito expresso nesse sentido no Capítulo III da LGPD, que trata de direitos dos titulares.

A comunicação ostensiva das informações sobre o tratamento de dados dos titulares, exigida no art. 9º da LGPD, é prestada com a política de privacidade e/ou proteção de dados disponibilizada pelo controlador que deveria poder (i) responder a um eventual pedido de acesso sem necessariamente informar as bases legais; e (ii) remeter o titular dos dados às disposições da sua política de privacidade e/ou proteção de dados, elaborada segundo os requisitos da lei, para obtenção de mais detalhes.

Preocupa uma abordagem onde toda e qualquer informação deva ser fornecida logo em um primeiro contato, o que poderá levar a uma falta de compreensão do titular leigo e não a um melhor entendimento do direito. Nesse sentido, uma abordagem seria a preferência por deixar de oferecer informação sobre todas as bases legais usadas no tratamento de seus dados pessoais em toda e qualquer operação, porém, na hipótese de o titular insistir na informação sobre a base legal relacionada a determinada (s) finalidade (s), por ele indicada (s) expressamente, poderia o controlador, num segundo momento de interação com o titular, fornecer essa informação, desde que a revelação não viole segredo comercial ou industrial.

Procurando endereçar as preocupações acima identificadas, trazendo maior segurança jurídica no contexto do exercício dos direitos dos titulares e a garantia de seu cumprimento pelos agentes de tratamento, fazemos a seguir as seguintes “Recomendações”, muitas delas inspiradas tanto na ICO, na CNIL e na AEPD, constem de Resolução sobre Direito dos Titulares a ser editada pela ANPD:

Recomendações sobre o exercício legítimo do direito de acesso pelos titulares:

- i) É preferível a disponibilização de um meio eletrônico para formulação do pedido de acesso pelo titular, devendo a resposta ser fornecida no mesmo formato, salvo se solicitado por outro meio;

⁴² V. artigo 9º inciso V da LGPD

⁴³ V. Artigo 6º VI da LGPD.

- ii) O titular, ao exercer seus direitos, deve utilizar o canal disponibilizado pelo controlador para tanto;
- iii) Sempre que possível, os pedidos que formulem direitos devem ser certos e determinados. Pedidos genéricos e amplos podem dificultar o atendimento a contento do titular e levam a respostas genéricas; a um pedido de esclarecimento ao titular-requerente por parte do controlador; ou à recusa na resposta, opção que caberia ao controlador;
- iv) Informações sobre os destinatários do compartilhamento realizados serão suficientes se indicarem a categoria de destinatários, juntamente com a finalidade do compartilhamento, podendo ser indicados exemplos, caso não viole segredos de negócios;
- v) Informações sobre bases legais utilizadas devem constar na Política de Privacidade e Proteção de Dados Pessoais do controlador. Entretanto, caso o titular insista na informação sobre a base legal relacionada a determinada (s) finalidade (s), o controlador poderá, num segundo momento de interação com o titular, fornecer essa informação desde que a revelação não viole segredo comercial ou industrial;
- vi) A recusa em responder um direito de acesso é possível quando o exercício do direito for abusivo, o que pode ser verificado pelo excesso do pedido, e até mesmo pela má-fé na solicitação dos dados⁴⁴.

Como condutas de má-fé podem ser consideradas as seguintes situações:

- O indivíduo claramente não tem intenção de exercer o seu direito de acesso, mas procura retaliar ou incomodar o controlador de seus dados com pedidos descabidos;
- A solicitação tem intenções maliciosas e está sendo evidentemente usada para assediar, de forma recorrente, uma organização sem nenhum propósito real a não ser causar transtorno;
- Quando o controlador indica o canal correto para o exercício dos direitos (ex: OneTrust, e-mail específico) e o titular insiste reiteradamente em realizar o exercício por canal diverso⁴⁵;
- O pedido é feito a um funcionário específico contra o qual fica evidente que o requerente tem algum rancor pessoal; ou
- Quando o titular envia sistematicamente diferentes pedidos para o controlador sem sequer aguardar o decurso do prazo para resposta.

⁴⁴ V. CIPL White Paper and ICO.

⁴⁵ Nesse particular, a ANPD já se manifestou no sentido de que o titular deve respeitar o meio disponibilizado pelo controlador para atendimento a seus direitos.V. <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado>

Como excessivos, podem ser considerados os seguintes pedidos:

- Quando o pedido é flagrantemente desproporcional. Como exemplos de experiências estrangeiras, podemos citar *nightmare letter*⁴⁶; pedidos amplos ou indefinidos⁴⁷; pedidos que desvirtuam o intuito da lei⁴⁸; pedidos repetidos em curto espaço de tempo; pedidos coletivos utilizados para retaliação contra o controlador⁴⁹. Todos esses tipos de pedidos precisam ser desencorajados pela ANPD;
- Se a solicitação repete pedidos anteriores já respondidos sem detalhar o que pretende de informações adicionais, sem prejuízo do direito do titular em ter acesso a informações de tratamento se seus dados foram atualizados;
- Quando o pedido renova um anteriormente feito e devidamente respondido num intervalo inferior a 6 (seis) meses⁵⁰, salvo justo motivo, como por exemplo a atualização do banco de dados;
- Quando um titular de dados evidentemente formula o pedido de acesso com um intuito diverso daquele que justifica o próprio direito, ou seja, ao invés de exercer o pedido de acesso para verificar a validade do tratamento de seus dados, assim o faz para colher informações para juntar em um outro processo qualquer⁵¹;
- O pedido desconsidera a existência de determinadas normas que regulam o tratamento de dados, como a proteção dos segredos comerciais;
- Quando o pedido puder expor dados de terceiros, o que muitas vezes ocorre no contexto de apurações investigativas; ou
- Quando o titular, em exercício do direito de acesso, solicita informações específicas sobre quais as medidas técnicas e administrativas que são adotadas no controlador. Essas questões envolvem segredos de negócios dos controladores, expressamente ressalvados no artigo 19 inciso II da LGPD e estarão desobrigados a fornecê-las.

⁴⁶ A “*nightmare letter*” foi criada por um advogado canadense que buscava testar e melhorar os processos relacionados ao exercício do direito de acesso das empresas. O referido modelo foi copiado e desvirtuado, ao ser replicado em diversos países como exemplo de pedido de direito de acesso feito pelos titulares a controladores de dados. O próprio autor escreve em seu LinkedIn o propósito da carta e pede que não seja copiada para fins de exercício de direito de acesso, eis que a carta, por tão extensa, dificilmente poderá ser respondida a contento e ainda minará a credibilidade do titular-requerente. Disponível em: <https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis>

⁴⁷ V. precedentes mencionados acima da Corte de Justiça de Amsterdã e da Corte de Justiça da Alemanha;

⁴⁸ V. precedente da Corte de Justiça de Amsterdã citado;

⁴⁹ V. *CIPL White Paper*.

⁵⁰ Sugestão da autoridade de dados espanhola.

⁵¹ Noord-Nederland Court, 23/04/2019, ECLI:NL:RBNNE:2019:3761: “*Insofar as it must be established that the plaintiff is ultimately not concerned with the accuracy of factual personal data relating to him that appear on those data carriers, but the plaintiff can do to obtain information that he wishes to use in any other procedure, the court is of the opinion that this constitutes an abuse of the law (...)* It appeared at the hearing that all documents, including an inspection report, are already in the possession of the plaintiff. The court has not shown that any other personal data has been processed by the defendant. The court declares the appeal inadmissible.” Disponível em: <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBNNE:2019:3761>

- vii) A recusa do controlador nos casos acima deve ser devidamente justificada ao titular de dados que, igualmente, deve ser informado sobre seu direito de formular uma reclamação perante a ANPD⁵²;
- viii) Pedidos feitos por terceiros são permitidos desde que acompanhados de documento idôneo que comprove a legitimidade do pedido, como procuração com firma reconhecida, seja em sua representação física, seja em versão eletrônica com assinatura digital que possa ter sua autenticidade verificada, além de documentos que comprovem as identidades do requerente e do titular representado. Já a resposta deve ser encaminhada ao titular diretamente para evitar riscos de incidentes de segurança, exceto se previsto expressamente na procuração o direito de receber a resposta por parte do procurador⁵³;
- ix) O tempo para a resposta deve poder ser suspenso se o controlador dos dados precisar esclarecer aspectos importantes quanto ao pedido formulado pelo titular⁵⁴;
- x) Se o pedido de acesso envolver outros indivíduos, cujas informações são inseparáveis, é justificável a recusa em fornecer tais dados⁵⁵. O titular deve ser informado sobre essa questão;
- xi) A recusa igualmente pode ocorrer em casos de sigilo de dados determinado por lei, assim como se os dados pessoais envolverem segredo comercial ou industrial do controlador; e
- xii) Pedido de acesso com relação a dados pessoais de crianças ou a dados pessoais sensíveis demanda um requerimento específico e por escrito, devidamente formulado por um dos pais, ou representante legal, ou pelo titular, respectivamente. Referida cautela atende o rigor da lei com relação a esses dados e prestigia o princípio da responsabilização e prestação de contas. O controlador deve manter o registro desse pedido de acesso, de sua resposta, assim como de seu destinatário (requerente).

4.2. DOS DIREITOS À ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS

A LGPD confere ao titular de dados, no inciso IV do artigo 19, o direito à anonimização, ao bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados de forma ilegal.

O inciso delimita o exercício desses direitos, de forma alternativa e com relação a dados pessoais que não encontram base legal para tratamento, porque são desnecessários, excessivos ou sujeitos a tratamento ilegal. Entretanto, os titulares de dados confundem sua aplicabilidade e solicitam

⁵² A ANPD inclusive atualizou em dezembro de 2021 um guia sobre “Petição de Titular”, no qual esclareceu a necessidade de o titular exercer antes seu direito perante o controlador de dados, para, caso não atendido, apresentar requerimento na ANPD. Nesse sentido vide: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contr-controlador-de-dados

⁵³ V. *CIPL, White Paper*.

⁵⁴ V. *CIPL White Paper and ICO*.

⁵⁵ V. *Recital 63 e artigo 15 (4) do GDPR*.

muitas vezes a anonimização de dados que ainda necessitam ser tratados pelo controlador, os quais ainda possuem base legal adequada para tanto, logo não caberia, nessa circunstância, atender ao pedido do titular, já que com a anonimização, os dados deixam de ser pessoais e o titular não poderá mais ser identificado por aquele controlador específico.

Portanto, é importante que a ANPD esclareça aos titulares de dados que a anonimização, bloqueio ou eliminação não deve ter lugar se o controlador estiver realizando o tratamento dos dados pessoais devidamente pautado em qualquer base legal pelo que os dados ainda serão necessários e legal a sua utilização razão pela qual não haveria de se falar em anonimização, bloqueio ou eliminação a pedido de titular.

Deste modo, como Recomendação da ANPD, nesse tema poderia ser no seguinte sentido: o direito à anonimização, bloqueio e eliminação pressupõe um tratamento ilegítimo, ou ilegal de dados pessoais e que não deve ser atendido se o controlador ainda precisar tratar os dados, para uma finalidade legítima e devidamente pautado em uma base legal, a exemplo do cumprimento de obrigações legais e regulamentares, ou para exercício regular de direitos.

4.4. DO DIREITO À PORTABILIDADE

A criação do direito à portabilidade para os titulares de dados pessoais, conforme previsão do artigo 18 inciso V, é uma novidade positiva trazida pela LGPD ao estimular a concorrência e a inovação, favorecendo o desenvolvimento econômico e tecnológico com o surgimento de novos players no mercado. Por consequência, amplia a possibilidade de escolha por parte dos titulares e, principalmente, permite um maior controle sobre seus dados pessoais.

É, porém, uma questão complexa que merece um maior aprofundamento pelo regulador antes de recomendações serem sugeridas. Nesse sentido, é fundamental que esta r. Autoridade Nacional promova espaço para uma discussão ampla com os diversos setores envolvidos através de tomadas de subsídios ou consultas públicas. Ademais, um conhecimento mais aprofundado do cenário internacional e de diretrizes, padrões e boas práticas adotadas a respeito do tema⁵⁶ podem fornecer substrato extremamente rico para endereçar diversos aspectos que emergem do tema.

A título de contribuição para uma melhor percepção da problemática, apresentamos alguns questionamentos que vêm sendo levantados por agentes de tratamento e precisam ser esclarecidos. São eles, em especial:

⁵⁶ Article 29 Guidelines on the right to "data portability": <https://ec.europa.eu/newsroom/article29/items/611233/en>; the Data Transfer Project: <https://datatransferproject.dev>.

- i) a definição de conceitos fundamentais, como o que seja portabilidade e, nos termos do artigo 40 da LGPD, interoperabilidade para fins de portabilidade;
- ii) quais dados pessoais devem ser objeto da portabilidade;
- iii) quais os limites da portabilidade, incluindo limites técnicos, para que seu exercício não viole direitos de terceiros, titulares de dados, ou os segredos industrial e comercial;
- iv) quando houver envolvimento de terceiros, o atendimento ao pedido de portabilidade deveria ser condicionado ao consentimento deles? Isso representaria a criação de um obstáculo ao pedido do titular?
- v) a transferência de dados será feita diretamente ao destinatário indicado pelo titular-requerente, ou este receberá seus dados e os repassará aos destinatários por ele escolhidos?
- vi) como se pode proteger a privacidade ao mesmo tempo que se permite a portabilidade? Como assegurar, por exemplo, que o provedor de destino indicado para a portabilidade garanta um mesmo nível de proteção que o provedor de origem (especialmente quando sujeitos a diferentes regimes regulatórios)?
- vii) o tratamento dos dados pelos destinatários, em quaisquer das situações indicadas deve ser condicionado a certos limites ou será ilimitado?
- viii) como delimitar a responsabilidade dos agentes de tratamento, ou seja, daquele que fornece os dados e daquele que os recebe antes, durante e depois de concluída a portabilidade?
- ix) como garantir a segurança entre os sistemas interoperáveis quando do cumprimento do pedido de portabilidade? Haverá exigência de padrões mínimos de segurança?

Portanto, para que os controladores tenham segurança jurídica suficiente para atender a um pedido de portabilidade e para que o titular de dados tenha seu direito atendido de forma adequada, tais questões devem ser endereçadas pela ANPD. Diante da complexidade relacionada a esse direito, aqui apenas brevemente demonstrada, sugerimos um estudo aprofundado no tema antes da emissão de qualquer orientação na matéria.

Recomendação sobre direito de portabilidade:

No tocante ao direito de portabilidade dos dados, sugerimos que, de plano, esta r. Autoridade Nacional determine a instituição de um grupo de trabalho nesta ANPD que possa coordenar estudos sobre o cenário internacional, e propor medidas de consulta à sociedade e ao mercado sobre o tema da portabilidade de dados através de consultas públicas e tomadas de subsídios para o enfrentamento das questões postas acima, preservada a prerrogativa do controlador de eleger a

forma que mais se adequa ao seu modelo de negócios, desde que atendidos os critérios estabelecidos por esta r. Autoridade.

5. DOS LIMITES PARA GRATUIDADE DOS PEDIDOS REALIZADOS PELOS TITULARES

Mais um tema que merece atenção da ANPD quando da normatização dos direitos dos titulares diz respeito às situações nas quais os direitos dos titulares serão atendidos gratuitamente e aquelas em que haverá possibilidade de cobrança para seu atendimento. A LGPD dá margem para a ANPD estabelecer em regulamento os prazos e as condições nas quais o exercício de direitos será atendido sem custos para os titulares⁵⁷.

Nesse sentido, é fundamental a ANPD trazer os parâmetros razoáveis para que isso possa ocorrer. Novamente trazendo a referência do GDPR⁵⁸, todos os direitos garantidos aos titulares de dados pessoais serão, em princípio, atendidos de forma gratuita, no entanto, quando forem manifestamente infundados ou excessivos, particularmente quando forem repetitivos, o controlador pode cobrar do titular uma tarifa para seu cumprimento em virtude dos custos administrativos despendidos para prover a informação solicitada ou realizar a ação requerida⁵⁹.

Logo, a ANPD deveria estabelecer em seu regulamento sobre o tema que o atendimento a pedidos dos titulares será em um primeiro momento gratuito, no entanto, em caso de pedidos manifestamente infundados ou excessivos, de pedidos repetitivos, de situações abusivas, o controlador poderá optar por realizar cobrança de um valor do titular para seu atendimento⁶⁰.

⁵⁷ V. artigo 18, parágrafo 5o da LGPD

⁵⁸ V. artigo 12 (5) do GDPR

⁵⁹ O White Paper da CIPL sobre direito dos titulares dá exemplo de inúmeros pedidos abusivos como pedidos de titulares repetidos, feitos numa periodicidade muito curta entre eles, como dias, semanas ou meses e menciona que algumas organizações consideram como abusivo pedidos consecutivos realizados em menos de 3 meses ou em menos de 6 meses. Outro exemplo se refere a pedidos coletivos que são realizados sem propósito legítimo, mas como retaliação ao controlador ou para perturbar suas operações comerciais, entupir seus sistemas pois sabem que o controlador pode enfrentar multas altas caso não cumpra o pedido de forma adequada. (<https://boingboing.net/2019/10/08/ddos-gdpr.html>) Mais um exemplo se refere a pedido de titulares que buscam informações perante o controlador para coletar provas visando mover uma ação judicial contra ele, dentre outros (v. p. 18).

⁶⁰ V. *GDPR e CIPL, White Paper and ICO*

Anexo I

Tabela sugerida pela autoridade de dados espanhola (AEPD) para a resposta a pedidos dos titulares “em camadas”⁶¹ (tradução livre)

<u>Epígrafe</u>	<u>Informação básica</u> <u>(1ª camada, resumida)</u>	<u>Informação adicional</u> <u>(2ª camada, detalhada)</u>
Responsável (pelo tratamento)	Identificação do responsável pelo tratamento	Informação de contato do responsável; Identidade e detalhes de contato do representante; Detalhes de contato do Encarregado de Dados
Finalidade (do tratamento)	Descrição simples dos fins do tratamento, incluindo elaboração de perfis	Descrição ampliada dos objetivos do tratamento; Prazos ou critérios para a conservação de dados; Decisões automatizadas, perfis e lógica aplicada
Legitimação (do tratamento)	Base legal para o tratamento	Detalhe da base legal do tratamento, em casos de obrigação legal, interesse público ou legítimo interesse; Obrigação, ou não, de fornecer dados e as consequências de não fazê-lo.
Destinatários (de compartilhamento ou transferências)	Previsão ou não de compartilhamento; Previsão, ou não, de transferência internacional a terceiros países	Destinatários ou categorias de destinatários; Decisões de adequação, garantias, normas corporativas vinculantes ou situações específicas aplicáveis
Direitos das pessoas interessadas	Referência ao exercício dos direitos	Como exercer direitos de acesso, retificação, exclusão e portabilidade de seus dados e a limitação ou oposição de seu tratamento;

⁶¹ A tabela da Autoridade Espanhola é apresentada como uma referência no tocante à possibilidade de resposta aos titulares em camadas quando do atendimento do direito de acesso, entretanto, é preciso fazer sua adaptação e contextualização à realidade da legislação brasileira sobre as informações que devem constar nas respectivas camadas.

		Direito de retirar o consentimento dado; Direito de reclamar perante a Autoridade de Controle
Procedência (dos Dados)	Fonte dos dados (quando não provenientes do interessado)	Informações detalhadas sobre a origem dos dados, mesmo se vierem de fontes de acesso público; Categorias de dados que são processados

prorrogação por mais 60 (sessenta) dias, caso necessário, devendo o termo inicial ser a data de autenticação do titular. Alternativamente, caso a Autoridade opte por não seguir tal recomendação, sugere-se que o prazo aplicável seja de 30 (trinta) dias úteis, com termo inicial da data da autenticação do titular.

b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

Compreende-se que a lógica utilizada para diferenciar os prazos previstos incisos I e II do artigo 19 é o nível de detalhamento das informações fornecidas, visto que o inciso I fala da confirmação de existência ou do acesso a dados pessoais em formato simplificado, enquanto o inciso II fala de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento. Porém, como a própria LGPD já estabelece os prazos para atendimento aos direitos previstos em tais incisos, entende-se que a presente questão se refere ao §4º do artigo 19, que dispõe sobre a possibilidade da Autoridade dispor, de forma diferenciada, acerca dos prazos previstos nos incisos I e II do *caput* no caso de setores específicos.

Nesses casos, para setores que precisam de tempo adicional para atender aos direitos previstos nos incisos I e II do artigo 19 da LGPD, uma alternativa seria seguir o prazo previsto pelo GDPR, em seu artigo 12.1.: os direitos dos titulares deverão ser atendidos em um mês a partir do requerimento, podendo esse período ser estendido por mais dois meses, se necessário, levando em consideração a complexidade e o número de pedidos. Para definir quais setores poderiam se beneficiar de um prazo diferenciado, a ANPD pode considerar uma série de critérios, por exemplo: o volume dos pedidos recebidos, os tipos de requisições recebidas por aquele setor especificado, a complexidade de tais requerimentos e dos sistemas nos quais os dados são tratados, dentre outros, dados esses que a ANPD já tem conhecimento pela atividade de sua Ouvidoria e os relatórios que produz.

c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Para garantir a efetividade da comunicação entre o titular dos dados e o agente de tratamento, algumas medidas são essenciais:

- (i) É fundamental que as informações sobre os direitos dos titulares e os procedimentos para exercê-los sejam divulgadas de maneira clara e simplificada.
- (ii) Importante disponibilizar ao titular meios de exercer todos os direitos conferidos pela LGPD.
- (iii) Antes de atender aos direitos do titular, é necessário autenticar sua identidade de acordo com os padrões estabelecidos pelo controlador.
- (iv) O atendimento ao requerimento deve ser realizado de forma gratuita, porém, a ANPD deve coibir o exercício de direitos de forma abusiva, indicando exemplos de requerimentos que poderiam ser configurados como tal.

Contudo, ao se debruçar sobre as características dos canais de atendimento disponibilizados aos titulares, a Autoridade deve levar em conta a diversidade dos agentes de tratamento, levando em

consideração aspectos como tamanho e estrutura organizacional. Da mesma forma, a ANPD precisa reconhecer que as organizações lidam com o exercício dos direitos dos titulares de maneiras diversas, adaptando-se à realidade específica de cada uma e sendo elas as mais hábeis a determinar as características daquele canal. Nesse contexto, destaca-se um estudo realizado pela International Association of Privacy Professionals (The State of Data Rights, 2020, p. 46-57, disponível em: <https://iapp.org/resources/article/the-state-of-data-rights/>).

Além disso, é preciso que se considere que os titulares podem apresentar desafios adicionais à comunicação. Por exemplo, um pedido genérico de dados por parte do titular pode resultar em um atendimento falho devido à imprecisão da solicitação, exigindo esclarecimentos adicionais. Em complemento, a tendência dos titulares em utilizar outros meios de comunicação ao invés daqueles indicados pelo controlador e sua recusa em fornecer informações necessárias podem complicar o processo de atendimento, mesmo quando o canal de comunicação está disponível e acessível. Assim, é fundamental que se reconheça que a efetividade da comunicação entre as partes não está exclusivamente sob a responsabilidade do controlador.

d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

Inicialmente, é preciso que se considere que o atendimento, pelo operador, às suas obrigações legais é essencial para a concretização dos direitos dos titulares. Nesse sentido, destaca-se o dever de manter registros de operações de tratamento de dados pessoais (artigo 37) e realizar o tratamento segundo as instruções fornecidas pelo controlador (artigo 39). No que tange às obrigações específicas que deverão ser impostas ao operador para permitir o atendimento adequado dos direitos dos titulares por parte do controlador, é preciso que essas sejam estabelecidas contratualmente de acordo com negociações a serem feitas entre as partes, podendo incluir: assistência técnica e operacional; notificação em prazo adequado sobre o recebimento de requerimento de exercício de direito; dentre outras.

e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

A abordagem semelhante ao SAC para atender aos direitos dos titulares é inviável por diversos motivos:

- 1) Múltiplos canais: A disponibilização de vários canais pode gerar complexidade operacional, custos adicionais e fragmentação de recursos.
- 2) Disponibilidade 24/7: Manter disponibilidade ininterrupta é impraticável para muitas organizações, especialmente as de menor porte, e pode comprometer a qualidade do atendimento devido à necessidade de análises cuidadosas e consultas legais.

- 3) Atendimento telefônico obrigatório: Impor o atendimento telefônico restringe a flexibilidade dos controladores, ignorando as preferências dos titulares e limitando a acessibilidade e a comodidade.
- 4) Acesso não condicionado aos dados: Embora a autenticação seja crucial, exigir acesso não condicionado pode comprometer a privacidade e a segurança dos dados.
- 5) Condições mínimas para atendimento telefônico: Estabelecer condições mínimas pode gerar burocracia e custos adicionais, sem necessariamente melhorar o atendimento.
- 6) Opções de acesso em documentos impressos: A obrigação de incluir opções de acesso em documentos impressos pode ser excessiva, especialmente em um mundo digitalizado.
- 7) Parâmetros pormenorizados para acompanhamento: Definir parâmetros rígidos pode ser inadequado, não considerando a diversidade das organizações e das demandas dos titulares.
- 8) Prazo de resposta: O prazo estabelecido pode ser exíguo e inviável para muitas organizações, diferentemente do GDPR, que prevê um prazo mais realista.

f. Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

Não há um modelo ideal. As organizações devem ter liberdade para estabelecer o formato de atendimento mais adequado às suas particularidades e às necessidades dos titulares. Isso é crucial, pois muitas empresas já investiram recursos significativos em sistemas de atendimento aos titulares, e a implementação de um novo modelo poderia representar desafios estruturais e desperdício de investimentos anteriores. Essa liberdade também se alinha à lógica de gestão de riscos da LGPD.

Assim, é fundamental que as organizações mantenham a flexibilidade para determinar o formato de atendimento mais adequado às suas particularidades e às exigências dos titulares dos dados. Essa abordagem é justificada por diversos motivos:

- Flexibilidade: As empresas possuem estruturas, processos e sistemas variados, não havendo uma solução única. Permitir que elas determinem seus próprios formatos de atendimento possibilita uma adaptação mais eficaz às suas realidades individuais e às demandas dos titulares.
- Inovação: Ao conceder às organizações a liberdade de definir seus formatos de atendimento, incentiva-se a inovação e o surgimento de novas soluções e tecnologias que aprimoram a experiência do titular e a eficiência do processo.
- Personalização: Cada empresa tem uma compreensão única das necessidades e preferências de seus titulares. Conceder a elas autonomia para determinar seus formatos de atendimento viabiliza a personalização das soluções para melhor atender às expectativas dos usuários.
- Eficiência econômica: Permitir que as empresas estabeleçam seus próprios formatos de atendimento abre espaço para a busca por soluções mais econômicas e eficientes, considerando suas capacidades financeiras e operacionais.

Portanto, embora seja importante que a ANPD forneça orientações claras e elucidativas, é igualmente crucial que as organizações tenham autonomia para determinar como implementar essas diretrizes de forma a melhor atender às necessidades dos titulares e garantir a conformidade com a legislação de proteção de dados.

II. INFORMAÇÕES SOBRE O TRATAMENTO (ART. 18, INCISOS I, II, VII E VIII):

a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Inicialmente, para fins de uma resposta mais completa à presente questão, a Brasscom gostaria de remeter esta Autoridade ao item 4 da contribuição submetida via e-mail que trata sobre os limites do direito de acesso. Além disso, apesar da resposta ter sido incluída na seção dedicada ao direito de acesso e do tópico do documento submetido por e-mail também se referir especificamente a esse direito, a reflexão se aplica a todos os direitos previstos na LGPD. De forma resumida, a presente associação gostaria de destacar que nenhum direito individual deve ser tido por absoluto, devendo a ANPD estar atenta e coibir o exercício abusivo de direitos. Esse raciocínio não deve ser diferente na interpretação da LGPD quanto aos direitos conferidos aos titulares de dados pessoais.

No que se refere ao direito de confirmação da existência de tratamento, são exemplos de hipóteses que justificam a negativa da confirmação: i) o solicitante não confirmou a identidade do titular de dados; ii) a solicitação tem intenções maliciosas e está sendo evidentemente usada para assediar, de forma recorrente, uma organização sem nenhum propósito real a não ser causar transtorno; (iii) quando o controlador indica o canal correto para o exercício dos direitos (ex: OneTrust, e-mail específico) e o titular insiste reiteradamente em realizar o exercício por canal diverso ; (iv) quando um titular de dados evidentemente formula o pedido de acesso com um intuito diverso daquele que justifica o próprio direito e (v) quando formula pedidos idênticos e repetidos após já ter sido atendido pelo controlador.

b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

A informação individualizada sobre todos os destinatários dos dados pessoais, além de possivelmente revelar dados de outras pessoas físicas que eventualmente não permitiram essa revelação, pode expor dados comercialmente estratégicos do controlador, tutelados pelos segredos comercial e industrial. Assim, a divulgação nominal pode ensejar um problema concorrencial, o que violaria um dos princípios da LGPD. Por essa razão, entendemos que a obrigação de prestar as informações sobre o compartilhamento de dados poderia se limitar à indicação das categorias de destinatários e à finalidade para os quais são tratados, o que atenderia ao princípio da transparência e o pedido de acesso do titular dos dados. Eventual fornecimento de dados mais específicos sobre entidades com as quais o compartilhamento é realizado poderia ser realizado caso o titular não ficasse satisfeito com os dados fornecidos, seguindo a lógica do repasse de informações em camadas, como sugere a Agencia Española de Protección de Datos ("AEPD") (mais detalhes podem ser encontrados no seguinte link: <<https://www.aepd.es/en/rights-and->

[duties/know-your-rights/right-information](#)>; bem como na submissão feita pela Brasscom por e-mail) ou a critério do controlador, respeitada a legislação vigente.

c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?

Inicialmente, é preciso que se considere que o atendimento, pelo operador, às suas obrigações legais é essencial para a concretização dos direitos dos titulares. Nesse sentido, destaca-se o dever de manter registros de operações de tratamento de dados pessoais (artigo 37) e realizar o tratamento segundo as instruções fornecidas pelo controlador (artigo 39). No que tange às obrigações específicas que deverão ser impostas ao operador para permitir o atendimento adequado dos direitos dos titulares por parte do controlador, é preciso que essas sejam estabelecidas contratualmente de acordo com negociações a serem feitas entre as partes, podendo incluir: assistência técnica e operacional; notificação em prazo adequado sobre o recebimento de requerimento de exercício de direito; dentre outras.

d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

O *caput* do artigo 19 regula a possibilidade de exercício de dois direitos distintos, o direito de confirmação da existência do tratamento (artigo 18 I da LGPD) e o direito de acesso aos dados pessoais tratados (artigo 18 II da LGPD). Partindo da premissa que o titular de dados exerceu o direito de acesso, solicitando uma declaração simplificada, para atender ao requisito do inciso I do artigo 19 da LGPD, que estabelece a necessidade de uma declaração em formato simplificado sobre o tratamento de dados pessoais, é crucial que o controlador forneça as informações essenciais que permitam aos titulares entenderem como seus dados estão sendo tratados. Assim, conforme estabelecido no *caput* do artigo 19, deve-se garantir o acesso dos titulares aos dados pessoais que estão sendo tratados, nos limites do que foi solicitado.

e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

As informações que devem ser disponibilizadas ao titular sobre o tratamento de seus dados, independentemente de requerimento, encontram-se previstas pelo artigo 9º da LGPD (finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei), as quais estarão previstas na Política de Privacidade e Proteção de Dados do agente de tratamento. Para além disso, no que tange às informações objeto de requerimento pelos titulares, a Brasscom gostaria de citar novamente como um bom exemplo aquele recomendado pela Agencia Española de Protección de Datos, que sugere que recomenda que as informações sejam repassada

"em camadas" aos titulares (mais detalhes podem ser encontrados no seguinte link: <<https://www.aepd.es/en/rights-and-duties/know-your-rights/right-information>>; bem como na submissão feita pela Brasscom por e-mail).

f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

A questão apresenta certa ambiguidade em relação ao seu objetivo, mas parece indagar se o direito de acesso seria considerado atendido quando o agente de tratamento disponibiliza os dados pessoais em formato digital ou em papel, de acordo com a escolha do titular. Nesse sentido, o §2º do artigo 19 da LGPD estabelece que o controlador deve atender ao direito de acesso conforme requerido pelo titular, devendo sempre ser considerada a razoabilidade do pedido. Isso significa que, se o titular especificar sua preferência por um formato específico (digital ou papel), o controlador deve fornecer no formato solicitado, desde que não demande um esforço desproporcional, caso em que poderá o controlador preferir o formato digital. Nesse sentido, é importante considerar que os formatos podem variar dependendo dos próprios dados pessoais a serem fornecidos e da forma de contato normalmente mantida entre titular e controlador. Por exemplo, para relações usualmente mantidas em ambiente virtual, o formato digital via portal de privacidade, e-mails ou área logada pode ser preferível. Por fim, cabe também observar que prazos diferenciados poderão ser estabelecidos a depender do formato escolhido pelo titular.

Um aspecto que não diz respeito especificamente ao questionamento apresentado pela Autoridade, mas que a Brasscom considera relevante trazer à atenção da ANPD, envolve situações em que é feito um pedido de acesso a um controlador que detém um grande volume de dados do titular. Nesses casos, como destacado pelo guia sobre direito de acesso do European Data Protection Board ("EDPB", disponível no seguinte link: <https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf>), é importante que se considere que: (i) diante de um conjunto extenso de dados de um indivíduo, pode ser desafiador determinar se um pedido de acesso abrangente deve buscar todas as informações ou apenas dados específicos, o que pode ser mitigado ao solicitar que o indivíduo especifique sua requisição antes da disponibilização das informações; e (ii) ainda na hipótese do controlador ter muitas informações sobre o titular, uma solução é responder o pedido de acesso usando uma abordagem em camadas, pela qual as informações são fornecidas em etapas, que dependem do interesse do titular em aprofundar as informações a seu respeito.

III. PORTABILIDADE DOS DADOS (ART. 18, INCISO V):

a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

O tema da portabilidade demanda uma análise mais pormenorizada antes de recomendações serem feitas, na medida em que se apresenta como um tema complexo e transversal, havendo maior ou menor aplicabilidade a depender do setor econômico e/ou atividade desenvolvida pelo controlador. Assim, é crucial que a Autoridade promova um debate mais amplo com os setores envolvidos, dada a variabilidade na maturidade para implementar o direito à portabilidade. Ademais, um conhecimento mais aprofundado do cenário internacional e de diretrizes, padrões e boas práticas adotadas a respeito do tema pode fornecer substrato extremamente rico para endereçar diversos aspectos que emergem do tema.

A complexidade de tal tema pode ser demonstrada, por exemplo, no setor de telecomunicações, no qual é garantia aos consumidores a portabilidade numérica (mais informações sobre sua configuração podem ser encontradas no Código de Boas Práticas do setor disponível neste link: <<https://conexis.org.br/wp-content/uploads/2022/08/Co%CC%81digo-de-Boas-Pra%CC%81ticas-de-Protec%CC%A7a%CC%83o-de-Dados-para-o-Sector-de-Telecomunicac%CC%A7o%CC%83es.pdf>>). Pela portabilidade específica deste setor, permite-se a migração de um contrato de prestação de serviço de uma prestadora de serviço de telecomunicações para a outra por meio do “Código de Acesso” (número de telefone do titular). Nesse sentido, o anexo (disponível aqui: <<https://informacoes.anatel.gov.br/legislacao/resolucoes/1998/34-resolucao-73#AnexoI>>) que atualmente dispõem sobre tal portabilidade aborda detalhadamente diversos temas, são exemplos: abrangência e objetivos da portabilidade; definições; características da portabilidade; direitos e deveres dos usuários; direitos e deveres das prestadoras; preços cobrados; modelo de portabilidade; etc.

Nessa toada, levantamos alguns temas meramente exemplificativos que precisam ser elucidados por esta Autoridade antes de regulamentar o direito de portabilidade:

- i) definição de portabilidade e interoperabilidade;
- ii) quais dados devem ser portáveis;
- iii) limites técnicos e legais da portabilidade para proteger direitos de terceiros;
- iv) consentimento de terceiros para portabilidade;
- v) transferência direta de dados ou através do titular;
- vi) equilíbrio entre portabilidade e privacidade;
- vii) limites ao tratamento dos dados pelos destinatários;
- viii) responsabilidade dos agentes de tratamento antes, durante e após a portabilidade;
- ix) garantia de segurança nos sistemas interoperáveis;
- x) os limites do direito de portabilidade em face do segredo de negócio e de direitos de propriedade intelectual.

Para que os controladores tenham segurança jurídica suficiente para responder se teriam maturidade para atender a um pedido de portabilidade, tais questões devem ser endereçadas pela ANPD. Assim, recomenda-se a instituição de um grupo de trabalho que possa coordenar estudos sobre o cenário internacional, e propor medidas de consulta à sociedade e ao mercado sobre o tema da portabilidade de dados através de consultas públicas e tomadas de subsídios para o

enfrentamento das questões postas acima, preservada a prerrogativa do controlador de eleger a forma que mais se adequa ao seu modelo de negócios, desde que atendidos os critérios estabelecidos por esta Autoridade.

b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

Os desafios tecnológicos para implementação de um padrão de interoperabilidade para o direito de portabilidade são diversos e abrangentes. Eles envolvem a complexidade das operações, a diversidade de formatos de dados e metadados, bem como as ferramentas e protocolos de comunicação adotados pelo mercado de cada setor e indústria.

Além da complexidade sistêmica envolvida, existe também uma diversidade de práticas entre os diferentes agentes econômicos, o que dificulta ainda mais uma harmonização entre os diferentes interesses e ações.

Dessa maneira, uma abordagem que estimule a discussão entre setores, a fim de promover uma maior flexibilidade por meio da autorregulação, é uma opção para que sejam adotadas soluções condizentes com as necessidades individuais das organizações.

c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?

Sim, é adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibiliza para o titular todos os seus dados pessoais em formato interoperável, caso esse tenha sido o pedido feito pelo titular. Os Guidelines do Working Party 29 (disponível aqui: < https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-right-data-portability-under-regulation-2016679_en>) sobre portabilidade elucidam que esse direito também pode abranger a transmissão de dados pessoais de um controlador para outro, caso essa tenha sido a solicitação do titular. No entanto, é importante observar que esse aspecto do direito de portabilidade não:

- 1) implica na obrigação para os controladores adotarem e manterem sistemas de processamento que sejam tecnicamente compatíveis;
- 2) os torna responsáveis pelo tratamento realizado pelo próprio titular dos dados ou por outra empresa que receba os dados pessoais;
- 3) gera uma obrigação específica de verificar a qualidade dos dados antes de transmiti-los; e
- 4) impõe uma obrigação ao controlador de reter os dados pessoais por mais tempo do que o necessário ou além de qualquer período de retenção especificado.

e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

Sim, é razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas no contexto da portabilidade de dados. Isso se justifica pelo fato de que diferentes setores podem ter necessidades e características específicas em relação à transferência de dados entre diferentes sistemas e plataformas. Permitir que o setor privado participe ativamente no estabelecimento desses padrões pode levar a soluções mais adequadas e eficientes para as empresas e os consumidores dentro de cada setor.

No entanto, é importante ressaltar que esses padrões de interoperabilidade não deveriam ser obrigatórios. Embora possam ser úteis como referências ou guias para as empresas, a imposição de padrões específicos poderia restringir a flexibilidade das organizações para encontrar soluções que melhor atendam às suas necessidades individuais. Além disso, a definição de prazos para a implementação desses padrões deve levar em consideração a complexidade das atividades econômicas envolvidas, bem como o tempo necessário para que as empresas se adaptem e implementem as mudanças necessárias.

IV. CORREÇÃO DOS DADOS TRATADOS (ART. 18, INCISO III):

a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

Para qualificar um dado como incompleto, inexato ou desatualizado, a situação concreta deve ser considerada à luz dos princípios da qualidade e finalidade estabelecidos pela LGPD. Embora o princípio da qualidade exija a exatidão dos dados, é importante reconhecer que essa exigência pode variar de acordo com a finalidade do tratamento. Por exemplo, em situações como o cadastro em um e-commerce, pode ser aceitável que o titular forneça apenas um dos seus sobrenomes, enquanto em contextos mais formais, como o preenchimento de uma escritura de imóvel, a precisão dos dados é crucial.

O Information Commissioner's Office ("ICO", a posição pode ser encontrada no seguinte link: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/#ib5>>) defende que ao receber uma solicitação de retificação, o controlador deve tomar medidas razoáveis para verificar a precisão dos dados e retificá-los, se necessário. Essas medidas devem levar em consideração a natureza dos dados pessoais e sua utilização. Quanto maior for a necessidade de precisão dos dados, maior deve ser o esforço para verificar sua exatidão e retificá-los, especialmente se os dados forem utilizados para tomar decisões significativas que afetem o indivíduo ou terceiros.

Além disso, é fundamental que se estabeleça claramente os limites desse direito, garantindo que ele se aplique apenas a dados genuinamente incompletos, inexatos ou desatualizados. Esse direito não deve ser usado para revisar eventos passados, e os controladores devem ter a possibilidade de solicitar aos indivíduos evidências específicas que comprovem a incorreção das informações

retidas. É crucial ainda que tais aspectos se refiram apenas a fatos, excluindo opiniões. Isso é essencial para proteger a liberdade de expressão. A ANPD deve deixar claro que a retificação deve se aplicar exclusivamente a dados que são factualmente incompletos, inexatos ou desatualizados e não a dados com os quais o indivíduo simplesmente discorda.

b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

É preciso considerar que o direito de correção está estreitamente relacionado com o princípio da qualidade dos dados que garante, aos titulares, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Nesse sentido, o controlador deve ter a possibilidade de requerer aos titulares comprovação de que os dados estariam incompletos, inexatos e desatualizados. O Information Commissioner's Office ("ICO", mais informações podem ser encontradas aqui: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/>>), por exemplo, pontua que, ao receber um pedido de correção, o controlador deve adotar medidas razoáveis para se certificar da qualidade dos dados e para retificá-los, se necessário, levando em consideração os argumentos e as provas fornecidas pelo titular. Nesse sentido, são exemplos específicos em que a simples declaração do titular não seria suficiente para o exercício do direito à correção: situação em que haja dúvida sobre a veracidade dos dados; ausência de documentação comprobatória; eventual alteração em bases públicas; impossibilidade de confirmação de tratamento de dados do titular e/ou de confirmação da sua identidade; dentre outras.

c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.

Para avaliar a impossibilidade ou o esforço desproporcional conforme o art. 18, § 6º, da LGPD, é crucial considerar cada situação de forma concreta e individualizada. Isso significa que não há uma lista definitiva de critérios objetivos que se apliquem uniformemente a todas as circunstâncias. Em vez disso, é necessário analisar cuidadosamente os detalhes específicos de cada pedido de correção, eliminação, anonimização ou bloqueio de dados pessoais.

Essa abordagem personalizada permite que se leve em conta uma série de fatores contextuais que podem influenciar a viabilidade de atender à solicitação. Por exemplo, o volume de solicitações, o tamanho e recursos disponíveis do controlador, o número de agentes envolvidos no tratamento dos dados e os eventuais prejuízos à atividade do controlador são considerações importantes a serem ponderadas.

Dessa forma, ao lidar com pedidos de acesso aos dados pessoais, é essencial que o controlador avalie cada caso individualmente, levando em conta os diversos aspectos que podem afetar a capacidade de atender à solicitação de forma adequada e dentro dos parâmetros estabelecidos pela LGPD. Isso assegura que os direitos dos titulares de dados sejam respeitados de maneira efetiva, ao mesmo tempo em que reconhece as limitações e desafios enfrentados pelos controladores na gestão e proteção desses dados.

d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

Considerando o princípio da qualidade dos dados e a própria disposição do inciso III do artigo 18, o controlador poderá se recusar a atender ao pedido do titular caso entenda, primeiramente, que os dados estão completos, exatos e atualizados. Além disso, caso o titular não forneça os documentos necessários para o atendimento a tal direito, o controlador também poderá negá-lo. Em complemento, a ANPD também deverá elucidar que o direito de correção: (i) não equivale a uma revisão do passado (por exemplo, uma mudança de nome ou de estado civil não deverá ter efeitos retroativos), o que poderia inclusive afetar o cumprimento a eventual obrigação legal;; e (ii) deve se aplicar apenas a fatos e não a opiniões, de forma a salvaguardar a liberdade de expressão (essas opiniões são defendidas pelos Centre for Information Policy Leadership no seguinte documento: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world_8_july_2020.pdf >). Por fim, reitera-se os pontos trazidos em relação aos limites do exercício abusivo de direito, nos termos da resposta à questão II.a desta Tomada de Subsídios e do item 4 do documento submetido por essa Associação por e-mail.

V. ANONIMIZAÇÃO, BLOQUEIO, ELIMINAÇÃO E OPOSIÇÃO NO CASO DE TRATAMENTO IRREGULAR (ART. 18, IV E § 2º):

a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Sim, nos termos do inciso IV do artigo 18, é preciso que o titular fundamente e comprove que os dados são desnecessários, excessivos ou que estão sendo tratados em desconformidade legal para fins de exercício dos direitos de anonimização, bloqueio ou eliminação. Portanto, é importante que a ANPD esclareça aos titulares de dados que a anonimização, bloqueio ou eliminação não são direitos irrestritos, sendo necessário, para seu atendimento, a existência de dados considerados desnecessários, excessivos ou a ocorrência de tratamento em desconformidade legal. Além disso, é importante ressaltar ainda que a anonimização, bloqueio ou eliminação não devem ser realizados se o controlador estiver tratando os dados pessoais de acordo com uma base legal válida, pois nesse caso os dados continuarão sendo necessários e seu uso será legalmente justificado.

Além disso, os dados também poderão ser mantidos nos casos previstos no artigo 16 da LGPD. Isto é, os dados poderão ser armazenados para: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

Sim, tanto a anonimização quanto à eliminação é medidas que podem ser adotadas de forma alternativa, dependendo das circunstâncias específicas, sendo ambas reconhecidas pela Lei Geral de Proteção de Dados Pessoais.

O artigo 12 da LGPD estabelece que os dados anonimizados não são considerados como dados pessoais. Isso significa que, ao anonimizar os dados de acordo com os critérios definidos pela legislação, eles perdem sua natureza de identificadores pessoais, proporcionando uma alternativa viável à eliminação completa dos dados.

Além disso, o inciso IV do artigo 16 da LGPD autoriza a conservação dos dados pessoais exclusivamente para uso do controlador, desde que os dados sejam anonimizados. Essa disposição legal reconhece que a anonimização dos dados oferece um nível adequado de proteção à privacidade, permitindo que o controlador mantenha os dados para fins específicos, desde que não possam ser acessados por terceiros.

Portanto, a LGPD reconhece tanto a anonimização quanto à eliminação como medidas equivalentes para garantir a proteção dos dados pessoais, proporcionando às organizações a flexibilidade necessária para escolher a abordagem mais adequada às suas necessidades e à natureza dos dados em questão.

c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

Caso o titular se oponha ao tratamento de dados realizado com base em uma das hipóteses de dispensa de consentimento, e essa oposição seja considerada legítima, o controlador deverá interromper a operação de tratamento, a menos que consiga justificá-la com base em outra fundamentação legal.

No entanto, mesmo diante da possibilidade de que a oposição legítima estaria fundada em tratamento de dados em descumprimento da LGPD, isso não deveria, por si só, configurar infração para fins de aplicação de sanções administrativas perante a ANPD.

Isso porque o nível de exigência, comprovação e apuração deve ser mais elevado, devendo ser respeitado o trâmite de apuração da ocorrência garantindo a ampla defesa do agente de tratamento.

Ademais, espera-se que a ANPD possa auxiliar os agentes de tratamento na tarefa de adequar suas atividades de tratamento, abrindo prazo para essa adequação no caso concreto - e promover, assim, o incremento de maturidade da cultura de proteção de dados no Brasil e a atuação responsiva da

autoridade - e não que aplique sanções a partir de situações isoladas e que podem ser absolutamente pontuais.

Assim, o efeito de considerar o pedido realizado pelo titular nos termos do §2º do artigo 18 legítimo seria a necessidade de atendimento ao pedido e, conseqüentemente, a indução à conformidade legal. Com o atendimento de tal pedido, o direito de oposição, nos termos do referido dispositivo, perde seu fundamento.

VI. REVOGAÇÃO DO CONSENTIMENTO (ART. 18, VI E IX):

a. A revogação do consentimento prevista no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular? Explique

A revogação do consentimento, conforme prevista no art. 18, IX, da LGPD, não necessariamente implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular. Isso porque pode haver outra base legal que justifique o tratamento desses dados, por exemplo, quando os dados são necessários para o cumprimento de um contrato entre o controlador e o titular dos dados ou para o adimplemento a uma obrigação legal.

Assim, destaca-se que, muitas vezes, as empresas precisam dos dados pessoais para diversos propósitos, e o tratamento pode ser baseado em mais de uma base legal. Portanto, a revogação do consentimento não significa automaticamente que o controlador deva apagar os dados, especialmente se houver outra base legal que justifique o tratamento para certo fim (esse é o entendimento defendido nos Guidelines on consent under Regulation 2016/679 do Working Party 29, disponível aqui: <<https://ec.europa.eu/newsroom/article29/items/623051>>). Outra circunstância que pode exigir que o controlador mantenha os dados é a necessidade de saber como agir em determinada situação (por exemplo: no caso do titular que não quer receber propagandas, é preciso guardar os dados para garantir que o direcionamento não será feito).

Por fim, é importante que se considere que a revogação do consentimento não deve gerar efeitos retroativos. Isso significa que, se o consentimento foi concedido para uma determinada operação de tratamento - como um processo de autenticação para a execução de uma transação (operação X) - a sua revogação não deve afetar retroativamente a operação já realizada. Em outras palavras, uma vez que uma operação foi concluída com base no consentimento válido naquele momento, a revogação subsequente do consentimento não deve invalidar a legalidade dessa operação.

b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

Na ausência de outra base legal, os dados devem ser eliminados. Caso tenham sido compartilhados, é necessário notificar os entes com quem foram compartilhados. No entanto, em determinadas circunstâncias, é essencial que o controlador mantenha os dados para orientar suas ações em situações específicas. Por exemplo, se um titular expressar o desejo de não receber mais propagandas, é necessário manter os dados para garantir que o direcionamento não ocorra.

Contudo, é fundamental ressaltar que o tratamento realizado com base no consentimento anteriormente à revogação permanece legal.

VII. DECISÕES BASEADAS EM TRATAMENTO AUTOMATIZADO (ART. 20, CAPUT):

a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

Uma decisão tomada unicamente com base em tratamento automatizado é aquela em que não há envolvimento humano no processo de tomada de decisão. Isso significa que a decisão é tomada inteiramente por tratamento automatizado, sem qualquer intervenção ou influência direta de seres humanos. Além disso, é preciso que se considere que, ao tratar da LGPD e especificamente do artigo 20, necessariamente está a se tratar de decisões automatizadas que envolvam o tratamento de dados pessoais.

b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

A implementação do direito de revisão de decisões, conforme previsto no art. 20 da LGPD, enfrenta uma série de desafios práticos significativos. Um dos principais desafios reside na complexidade dos sistemas que utilizam aprendizado de máquina e inteligência artificial. Esses sistemas muitas vezes tomam decisões automatizadas com base em algoritmos complexos, tornando difícil explicar de forma clara aos titulares os motivos por trás de uma decisão específica.

Além disso, a potencial exigência de intervenção humana para revisar e explicar as decisões automatizadas pode gerar gastos adicionais de recursos para as organizações, isso porque, a necessidade de envolvimento humano para revisar e explicar essas decisões pode aumentar os custos operacionais e administrativos.

Outro desafio é fornecer explicações claras e acessíveis aos titulares sem comprometer os direitos de propriedade intelectual e segredos comerciais das organizações. O fornecimento das informações exigidas pelos §1º do artigo 20 pode entrar em conflito com a necessidade de proteger informações confidenciais e estratégicas da empresa, criando um desafio adicional na implementação desse direito.

Além disso, a manutenção de registros detalhados sobre as decisões tomadas e os processos envolvidos pode exigir investimentos significativos em sistemas de registro e armazenamento de dados. Isso pode representar um desafio especialmente para organizações que lidam com grandes volumes de dados e decisões automatizadas em escala.

Ainda, a implementação efetiva do direito de revisão de decisões também está sujeita a custos financeiros relacionados à atualização e adaptação dos sistemas de informação e processos organizacionais para garantir a conformidade com os requisitos da LGPD. Esses custos podem ser substanciais, especialmente para pequenas e médias empresas.

Por fim, apesar de não tratar dos desafios práticos para implementar o direito de revisão de decisões, a Brasscom gostaria de pontuar à ANPD que entende essencial assegurar que o procedimento de revisão seja conduzido de acordo com critérios estabelecidos pelo próprio controlador dos dados. O controlador, por deter o conhecimento especializado necessário para compreender as suas operações de tratamento, bem como os resultados produzidos, é o agente apto a avaliar a pertinência de revisar os critérios empregados, quando o titular exerce o direito em questão. Assim, é sua expertise que permitirá uma análise adequada, garantindo que a revisão seja conduzida de maneira adequada.

d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

Sim, quando: não há enquadramento nos termos do artigo 20 ("decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade"); a resposta possa revelar algoritmo ou lógica de programação, bem como violar direitos de propriedade intelectual e segredo comercial; e caso a revisão seja impossível, pela técnica ou pela prática.



público, mantido pela Administração com esta finalidade, compartilhem documentos já produzidos com requerentes interessados em acessá-los.

O atendimento a titulares de dados pessoais coloca os agentes de tratamento privados diante de situação diversa. Vasta é a gama de possíveis pedidos, alguns a demandar providências adicionais, que vão além do simples compartilhamento de informações consolidadas em documentos já existentes ou previamente elaborados. Muitas das vezes os agentes de tratamento terão de se debruçar sobre cada pedido para compreendê-lo e poder atendê-lo satisfatoriamente, além de terem de recuperar informações nem sempre mantidas de forma consolidada e que correspondam exatamente ao pedido formulado pelo titular dos dados. Noutras tantas vezes o atendimento aos titulares implicará na tomada de ações concretas, que em nada se assemelham ao simples compartilhamento de informações ou documentos. Nesse contexto, a LAI não parece um bom ponto de aproximação para a regulação dirigida ao atendimento dos pedidos formulados pelos titulares aos agentes de tratamento atuantes no setor privado. Uma proposta alternativa segue na resposta da ABERT à pergunta seguinte (I.b).

b. Na definição de prazos, quais critérios deveriam ser levados em consideração para dispor de forma diferenciada como previstos nos incisos I e II do caput do art. 19 da LGPD?

Idealmente o prazo, na visão da ABERT, deve ser de no mínimo 30 (trinta) dias úteis, em linha com o que dispõe o artigo 12, 3, do GDPR. Esse prazo deve poder ser prorrogado (mediante aviso ao Titular de forma clara e formal), por igual período, ante a complexidade do processo de cada companhia para análise e atendimento das solicitações.

A complexidade envolvida para o pleno atendimento de solicitações de titulares varia conforme os setores de atuação de cada empresa, o volume de dados envolvidos e a natureza das atividades de tratamento, entre outros elementos.

A ausência de um prazo adequado somado a essa pluralidade de complexidades, volumes e especificidades para atendimento pelos diferentes controladores impacta diretamente o titular. A depender do relacionamento entre o titular e o controlador, é possível que o histórico de dados seja bastante extenso, logo, envolvendo um volume de dados relevante.

Neste contexto, sem prazos adequados (e sua possível prorrogação), a ABERT enxerga, além de um risco de inviabilidade de verificação e atendimento adequado pelo controlador, um risco associado ao titular, no que se refere à qualidade dos dados recebidos. Prazos excessivamente curtos possivelmente resultarão em dificuldades operacionais que levarão os controladores a deixarem de atender por completo as solicitações recebidas.





Por fim, é importante mencionar que há um risco relevante a respeito dos limites da solicitação de confirmação ou de acesso, com efeitos tanto para o controlador quanto para o titular: o potencial excesso de informações solicitadas ou encaminhadas. A ABERT entende que esse excesso pode se configurar de duas formas:

- (i) Para o controlador: na exigência de apresentação de dados que foram produzidos a partir de análises ou de aplicação de inteligência sobre dados pessoais, e que carregam consigo informações que representam segredo de negócio. Vale recordar que a LGPD menciona múltiplas vezes a necessidade de proteção de segredos comerciais e industriais;
- (ii) Para o titular: a exigência de dados historicamente muito antigos, que podem causar uma demora adicional no atendimento do titular e que – na prática – sequer seriam úteis, já que o excesso de informações pode ser prejudicial, no sentido de criar confusão ao titular.

c. Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Na perspectiva da ABERT, as características fundamentais de um canal de atendimento para garantir efetividade na comunicação entre o titular e o agente de tratamento são a disponibilidade e a usabilidade.

Nesse sentido, é essencial que este canal de atendimento esteja publicamente disponível e facilmente localizável em *sites* ou redes oficiais dos agentes de tratamento, priorizando a praticidade na construção de meios para que o titular possa exercer seus direitos. É igualmente essencial que o canal seja de fácil usabilidade – especialmente considerando a diversidade social e cultural dos titulares do nosso país – contendo o mínimo possível de etapas a serem percorridas, mas não sem o mínimo necessário para a adequada identificação da necessidade ou demanda do Titular.

d. Há responsabilidade dos operadores na concretização dos direitos dos titulares? De que maneira eles devem cooperar com os controladores para o atendimento aos direitos dos titulares?

A ABERT entende que sim, há responsabilidade dos operadores, na medida das atividades de tratamento de dados que conduzirem. A cooperação dos operadores no atendimento aos direitos dos titulares pelos controladores está diretamente relacionada ao papel central que assumem em diversas atividades de tratamento, uma vez que os operadores são frequentemente responsáveis por sua realização direta. Por exemplo: uma empresa que presta serviços de processamento de folha de pagamento, atuando como operadora, detém acesso imediato e organizado a informações relevantes sobre os empregados do





controlador; e não poderia se furtar a colaborar com o controlador com vistas ao exercício dos direitos desses empregados. Assim sendo, independentemente da existência de cláusula contratual nesse sentido, deve-se presumir a existência de um dever de colaboração dos operadores em relação aos controladores para análise e atendimento às solicitações de titulares.

Na visão da Abert, não caberia à própria regulação fazer recair apenas sobre os controladores ônus regulatórios e responsabilidades em casos como o mencionado logo acima, no qual um operador de grande porte e com alta capacidade operacional é contratado por vários controladores. Caminhar no sentido contrário representaria transferir parte significativa dos custos impostos pela LGPD – no caso concreto, aqueles relacionados ao não atendimento a requisições de titulares de dados pessoais, como o pagamento de multas administrativas – aos controladores, como se os operadores, que se valem tanto ou mais que os controladores do tratamento de dados para impulsionar suas atividades econômicas, não tivessem que os suportar. Estar-se-ia, portanto, diante de uma má escolha regulatória, que induziria controladores a internalizar os custos das atividades dos operadores, e, por consequência, reduziria os incentivos para que os próprios operadores – que em muitos casos são elementos centrais às cadeias de tratamento de dados – realizassem investimentos para assegurar um pronto atendimento às solicitações que lhes fossem encaminhadas, relacionadas ao exercício de direitos por titulares.

Nesse sentido, imagine-se que a ANPD possa reputar razoáveis os casos em que um controlador informar ao titular ser necessário um prazo adicional para atendimento a um pedido que não seja trivial (art. 18, §4º da LGPD) e no qual ficar evidente a necessidade de colaboração de um operador. Ainda no mesmo sentido, parece razoável que operadores possam figurar em processos administrativos voltados à apuração de descumprimentos ao dever de suportar o exercício dos direitos de titulares de dados pessoais. Do contrário, como dito, criar-se-á uma distorção regulatória e uma ineficiência alocativa no que diz respeito à repartição dos custos associados ao atendimento aos titulares. Esperar que apenas por meio de ajustes contratuais os controladores tenham condições de pressionar os operadores a adotarem bons SLAs (*service level agreements*) para solução de pedidos dos titulares não é plausível, na medida em que há vários casos em que os atores com maior poder de barganha e com controle sobre meios indispensáveis ao pronto atendimento a solicitações de titulares restam enquadrados como operadores; e não controladores.

Além disso, a ABERT entende que as ações executadas pelos operadores, especialmente aquelas que são tomadas com liberdade (considerando conhecimento técnico, ferramentas, governança ou tecnologia a serem utilizadas na atividade dos operadores), serão de sua responsabilidade e devem ser esclarecidas ao controlador sempre que necessário para a análise e atendimento de solicitações de titulares.





Por fim, importante ressaltar que é sempre do controlador o dever de analisar e responder aos titulares, de modo que o dever de cooperação do operador não lhe confere autonomia nem independência para prestar atendimento ou esclarecimentos diretamente aos titulares, sem a devida supervisão ou autorização do controlador.

e. Seria viável a adoção de diretrizes e procedimentos análogos aos do Serviço de Atendimento ao Consumidor, estabelecido pelo Decreto nº 11.034, de 5 de abril de 2022, para o exercício dos direitos do titular de dados pessoais? Em caso negativo, quais diretrizes não deveriam ser adotadas e por qual motivo?

O Decreto do SAC (Decreto nº 11.034/2022) foi desenhado para lidar com atendimento a consumidores de “*serviços regulados pelo poder público federal*”, leia-se: setores de água, energia, telecomunicações, saúde, seguros, financeiro e aviação. O Decreto tem em vista a solução de reclamações, a abertura e cancelamento de contratos de consumo, exercício do direito de arrependimento, discussões sobre cobranças indevidas e restituição de valores a partir de uma estrutura de atendimento criada na década de 1990 e início dos anos 2000, marcada pelo surgimento dos grandes *players* em setores de infraestrutura após as privatizações, como as companhias de energia e telecomunicações. O esforço da Senacon/MJ, ator importante na construção do Decreto do SAC, foi reduzir os altos índices de insatisfação com as empresas mais reclamadas, novamente: companhias aéreas, concessionárias de água e energia, prestadoras de serviços de telecomunicação, entre outras. Nesse contexto é que pareceu adequado impor aos grandes *players* desses setores as obrigações que constavam na primeira versão Decreto (2008) e que foram parcialmente mantidas no texto atualmente em vigor.

Ainda que importantes lições possam ser retiradas do próprio Decreto do SAC e dos vários regulamentos setoriais dirigidos à regulação de direitos dos consumidores, pensar na adoção dos procedimentos ali previstos, pela ANPD, como solução para a regulamentação de aspectos das LGPD, não parece uma solução adequada.

Na visão da ABERT, a *regulação por analogia* tende a ser mais negativa do que positiva do ponto de vista econômico e operacional, tendo em vista:

- A complexidade adicionada aos negócios, especialmente aos setores já regulados;
- A alta probabilidade de controvérsias entre mais de uma norma reguladora, ocasionando a impossibilidade de implementação prática de determinadas etapas ou obrigações, gerando insegurança jurídica; e
- O aumento na complexidade operacional dos negócios e, naturalmente, na qualidade e tempo demandado no próprio processo de atendimento ao Titular.

Um caminho produtor e equilibrado passa pela construção de um regime que permita, sempre tendo atenção à efetiva resolução das demandas dos titulares, diferentes formas





de atendimento, de acordo com as características de cada indústria ou de cada setor de atividade econômica e das formas de relacionamento existentes entre empresas e seus clientes em cada um deles.

f. Existe um modelo de atendimento adotado por agentes privados ou pelo setor público que poderia servir como paradigma, considerando principalmente a capacidade de se tratar grandes volumes de demandas com economicidade? Exemplifique.

Na visão da ABERT, não há no setor privado um modelo de atendimento que possa ser considerado como padrão. Considerando os diferentes perfis e portes de agentes de tratamento – todos eles sujeitos ao atendimento dos direitos do titular – é importante que não existam modelos de atendimento padronizados obrigatórios, ainda que exemplos específicos possam ser vistos como boas práticas.

A complexidade e o volume das solicitações podem variar consideravelmente de um setor para outro, mesmo considerando apenas empresas de grande porte. Utilizar como modelo a realidade de uma empresa com alta complexidade e alto volume de solicitações pode distorcer os parâmetros e prejudicar a implementação de um modelo realmente eficiente por empresas com estruturas menores ou volumes de solicitação reduzidos.

Portanto, a sugestão da ABERT é que não exista um padrão obrigatório a ser implementado por agentes de tratamento.

II. Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII)

a. Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Sim. A ABERT apresenta abaixo rol exemplificativo, com algumas hipóteses em que, a seu ver, o direito de confirmação poderá ser negado pelo agente de tratamento. A saber:

- i. **Quando o titular não realiza a validação da sua identidade conforme solicitado pelo controlador:** como se sabe, para o atendimento de solicitações de titulares, é imprescindível que o controlador realize a validação de identidade como medida de segurança, de modo a assegurar que a resposta seja enviada ao verdadeiro titular ou a seu representante legal devidamente autorizado, inclusive em obediência ao artigo 46 da LGPD²;

² Art. 46, caput, da LGPD: “Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”





- ii. **Segredo de negócio e confidencialidade:** quando o titular solicitar a disponibilidade de informações desenvolvidas ou inferidas pelo controlador a partir dos seus dados que contenham informações relativas à estratégia de negócio, posicionamento de mercado ou relacionamento com seus clientes pelo controlador – todas consideradas segredo de negócio. Nestes casos, a ABERT entende que o cumprimento da solicitação não deve se sobrepor ao segredo comercial e industrial;
- iii. **Requisições massivas em curto período:** quando houver múltiplas requisições em um pequeno espaço de tempo que demandem esforço desproporcional do agente de tratamento para atendê-las, considerando os aspectos técnicos e operacionais envolvidos; neste contexto, cabe ressaltar que a ANPD e os próprios agentes de tratamento têm atuado para levar aos titulares cada vez mais conhecimento a respeito dos seus direitos, de modo que se torna possível que o volume inicial seja elevado, até que se caminhe em direção a patamares normais.
- iv. **Má-fé:** deve ser autorizada a recusa de atendimento pelo agente de tratamento em casos de suspeita de que as solicitações recebidas tenham sido enviadas de má-fé por pretensos titulares. Dessa forma devem ser tomadas as solicitações de titulares que representem empresas que possam estar interessados nos segredos de negócio de agentes concorrentes ou, ainda, os casos em que determinado titular ou conjunto de titulares solicitar providências com o flagrante intuito de importunar e onerar, insistentemente, determinado agente de tratamento a partir da realização de múltiplas e repetidas requisições (idênticas ou não).

Sendo assim, nos contextos específicos mencionados acima, a ABERT considera possível a recusa, que deverá ser informada ao titular por meio de resposta fundamentada, respeitado o art. 18, §4º, II da LGPD. Não obstante, a ABERT reforça que rol acima é meramente exemplificativo, dado não ser possível antever todas as diversas situações em que o agente de tratamento poderá se ver inserido e que poderão levá-lo a ter de negar o atendimento a uma dada solicitação.

Ante o exposto, a ABERT entende ser salutar que a futura regulamentação preveja que o agente de tratamento poderá negar o direito de confirmação da existência do tratamento, mesmo em hipóteses não previstas específica e expressamente na letra da norma, desde que sempre por razões fundamentadas e informadas aos titulares.

b. Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?





No entendimento da ABERT, a menção, na Política de Privacidade publicamente disponível das categorias de destinatários com os quais o Controlador realiza o compartilhamento de dados pessoais já deve ser considerada suficiente para cumprir a disposição do artigo 9º da LGPD, que visa a promover o acesso facilitado a informações sobre tratamento de dados pessoais.

A perspectiva adotada se baseia na premissa de que o excesso de informação, considerando a assimetria de conhecimento entre titulares e agentes de tratamento, pode mais facilmente confundir do que esclarecer os titulares. É de pouca utilidade para a esmagadora maioria dos titulares saber exatamente quais são as empresas específicas (CNPJ a CNPJ) com quem o controlador compartilha dados, além de essa informação poder representar, em alguns cenários, segredo de negócio (por exemplo, quais empresas realizam validação de identidade e verificação antifraude).

Deste modo, a ABERT entende que o objetivo de proporcionar transparência e clareza ao titular de dados seja plenamente alcançado de forma adequada, ostensiva e razoável por meio da menção, na Política de Privacidade do agente de tratamento, das principais categorias dos destinatários, como provedores de nuvem, de pagamento e autoridades competentes.

Caso o titular manifeste interesse em obter mais detalhes acerca das entidades públicas e privadas com as quais o controlador compartilha seus dados pessoais, incluindo detalhes como nome e CNPJ das respectivas empresas, estes esclarecimentos poderão ser obtidos mediante o exercício de direito garantido pela legislação, ocasião em que o controlador poderá especificar e prover mais detalhes, apenas quando requisitado pelo titular.

Por outro lado, especificamente no que diz respeito ao controlador, a ABERT entende, de igual modo, bastar a menção, na sua Política de Privacidade, do seu nome, CNPJ e respectivos canais oficiais de comunicação, cujos dados satisfarão quaisquer eventuais necessidades dos titulares, lhes permitindo o pleno gozo de seus direitos.

c. Qual a responsabilidade dos operadores no que se refere ao direito do titular de obter informações sobre o tratamento de dados pessoais?

Em linha com a resposta dirigida à questão “I.d”, a ABERT entende que sim, há responsabilidade dos operadores, na medida das atividades de tratamento de dados que conduzirem. A cooperação dos operadores no atendimento aos direitos dos titulares pelos controladores está diretamente relacionada ao papel central que assumem em diversas atividades de tratamento, uma vez que os operadores são frequentemente responsáveis por sua realização direta. Como mencionado anteriormente, uma empresa que presta serviços de processamento de folha de pagamento, atuando como operadora, detém acesso imediato e organizado a informações relevantes sobre os empregados do





controlador; e não poderia se furtar a colaborar com o controlador com vistas ao exercício dos direitos desses empregados. Assim sendo, independentemente da existência de cláusula contratual nesse sentido, deve-se presumir a existência de um dever de colaboração dos operadores em relação aos controladores para análise e atendimento às solicitações de titulares.

Na visão da Abert, como exposto acima, não caberia à própria regulação fazer recair apenas sobre os controladores ônus regulatórios e responsabilidades em casos como o mencionado logo acima, no qual um operador de grande porte e com alta capacidade operacional é contratado por vários controladores. Caminhar no sentido contrário representaria transferir parte significativa dos custos impostos pela LGPD – no caso concreto, aqueles relacionados ao não atendimento a requisições de titulares de dados pessoais, como o pagamento de multas administrativas – aos controladores, como se os operadores, que se valem tanto ou mais que os controladores do tratamento de dados para impulsionar suas atividades econômicas, não tivessem que os suportar. Estar-se-ia, portanto, diante de uma má escolha regulatória, que induziria controladores a internalizar os custos das atividades dos operadores, e, por consequência, reduziria os incentivos para que os próprios operadores – que em muitos casos são elementos centrais às cadeias de tratamento de dados – realizassem investimentos para assegurar um pronto atendimento às solicitações relacionadas ao exercício de direitos por titulares que lhes fossem encaminhadas.

Nesse sentido, imagine-se que a ANPD possa reputar razoáveis os casos em que um controlador informar ao titular ser necessário um prazo adicional para atendimento a um pedido que não seja trivial (art. 18, §4º da LGPD) e no qual ficar evidente a necessidade de colaboração de um operador. Ainda no mesmo sentido, parece razoável que operadores possam figurar em processos administrativos voltados à apuração de descumprimentos ao dever de suportar o exercício dos direitos de titulares de dados pessoais. Do contrário, como dito, criar-se-á uma distorção regulatória e uma ineficiência alocativa no que diz respeito à repartição dos custos associados ao atendimento aos titulares. Esperar que apenas por meio de ajustes contratuais os controladores poderão pressionar os operadores a adotarem bons SLAs (*service level agreements*) para solução de pedidos dos titulares não é plausível, à medida em que há vários casos em que os atores com maior poder de barganha e com controle sobre meios indispensáveis ao pronto atendimento a solicitações de titulares restam enquadrados como operadores; e não controladores.

Além disso, a ABERT entende que as ações executadas pelos operadores, especialmente aquelas que são tomadas com liberdade (considerando conhecimento técnico, ferramentas, governança ou tecnologia a serem utilizadas na atividade dos operadores), serão de sua responsabilidade e devem ser esclarecidas ao controlador sempre que necessário para a análise e atendimento de solicitações de Titulares.





Por fim, importante ressaltar que é sempre do controlador o dever de analisar e responder aos Titulares, de modo que o dever de cooperação do operador não lhe confere autonomia nem independência para prestar atendimento ou esclarecimentos diretamente aos titulares, sem a devida supervisão ou autorização do controlador.

d. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam constar da declaração em formato simplificado prevista no art. 19, inciso I, da LGPD?

Na visão da ABERT, entendemos que na declaração em formato simplificado, os dados constantes no atendimento pelo controlador serão dados cadastrais básicos. Por exemplo: nome completo, RG ou CPF, endereço, e-mail, telefone ou outros da mesma natureza.

Ainda, no caso dos serviços ou fornecedores que tenham sites disponíveis com área logada pelo cliente-titular, a lista de dados habitualmente visíveis nos menus comumente denominados "Meu Perfil", "Sua Conta", "Seus Dados" ou semelhantes já devem servir como a própria declaração simplificada, a qual estará, portanto, disponível ao titular em tempo integral.

Naturalmente, para as empresas que não ofereçam essa possibilidade, o processo de atendimento deve ser realizado por meio da geração de um relatório pelo controlador e encaminhado ao titular em formato de fácil acesso e considerando mecanismos de segurança.

e. Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

Sob a perspectiva da ABERT, para garantir a transparência e o direito à informação, o controlador deve prover informações mínimas e essenciais referentes à finalidade do tratamento de dados, descrição das categorias dos dados pessoais coletados, informações genéricas referentes ao compartilhamento de dados com terceiros (como melhor exposto na resposta à pergunta "II.b"), bem como os direitos que poderão ser exercidos pelos titulares, além da disponibilização de canais oficiais de comunicação com o agente de tratamento – que deve dispor de equipes multidisciplinares adequadas (internas ou terceirizadas) para gerir e analisar as solicitações dos titulares de dados pessoais – bastando que as informações supracitadas constem na sua Política de Privacidade.

Não obstante, a ABERT entende que as informações acerca dos critérios e procedimentos utilizados em decisões automatizadas não devem figurar entre as informações mínimas a serem fornecidas ao titular, sem que haja requerimento específico. Pensamos que tal divisão esteja em linha com a LGPD, que separa o pedido relacionado a critérios e





procedimentos utilizados para decisões automatizadas (art. 20, §1º) das demais obrigações relacionadas ao fornecimento de informações aos titulares.

f. Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

Conforme estabelecido no artigo 19, § 2º da LGPD, o titular dos dados possui a prerrogativa de escolher o formato de recebimento dos dados pessoais relacionados ao direito de acesso, seja em formato físico ou digital. Não obstante, é importante também observar o disposto no § 1º deste mesmo dispositivo, que estipula que os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso.

Considerando o avanço tecnológico contínuo no cenário atual, é inegável afirmar que o armazenamento de dados em formato físico, tanto por pessoas físicas quanto jurídicas, tornou-se obsoleto. A ABERT entende que a disponibilização dos dados pessoais em formato eletrônico deve ser priorizada.

Este posicionamento não apenas está em conformidade com a LGPD, mas também proporciona um ambiente mais seguro e idôneo para a finalidade pretendida: disponibilização de documentos ao titular de dados pessoais, sem as desvantagens e riscos inerentes à documentação em papel (extravio, sigilo, transporte, custos, entre outros).

Em outras palavras, embora a LGPD contenha disposições específicas a respeito, a ABERT reforça o seu entendimento de que a disponibilização dos dados pessoais em formato eletrônico deve ser preferível por conferir maior segurança aos documentos, além de maior praticidade e economicidade aos controladores que, atualmente, possuem a quase totalidade de seus dados armazenados de forma digital.

III. Portabilidade dos dados (art. 18, inciso V)

a. Em quais setores haveria maturidade nos processos de negócio e tecnologia para implementar o direito à portabilidade dos dados diretamente entre agentes de tratamento, a pedido do titular?

A instituição de portabilidade, tomada como um instrumento regulatório, tem em vista reduzir custos de mudança suportados por usuários de serviços concorrentes, que possuam a mesma utilidade para o consumidor final. No setor de telecomunicações, com a portabilidade (instituída já há alguns anos), os consumidores deixaram de suportar a perda de seu número de contato telefônico ao “mudar” de operadora e passaram a poder mantê-lo, levando-o consigo para a nova operadora de sua escolha. Nesse contexto, mais apenas do que uma mera praticidade para os consumidores, a instituição da portabilidade





representa uma verdadeira ferramenta de fomento à competição, já que os consumidores deixam de ser desencorajados pelo custo de mudança antes suportado e se veem em condições de seguir adiante, trocando de operadora, com maior facilidade. Considerado esse efeito habilitador da competição a portabilidade passou a ser exigida no setor de telecomunicações, sendo levada a outros setores, como o de serviços financeiros.

Tratar da criação de um direito à portabilidade, de forma ampla, a todos os setores de atividade econômica, é obviamente um enorme desafio. Em primeiro lugar, porque não se sabe ao certo qual seria o objeto dessa portabilidade, isto é, quais dados pessoais seriam levados de um agente de tratamento a outro. Em segundo lugar, porque não se sabe se seria necessária a criação de sistema intermediário, ou alguma solução tecnológica para que haja uma interconexão entre o agente de origem e de destino. Em terceiro lugar, porque não estão claros quais seriam os reais benefícios da aplicação do direito à portabilidade a cada ramo de atividade econômica, de modo que se possa determinar até que ponto seria justificável criar obstáculos operacionais e econômicos ao funcionamento de empresas.

Sem resposta a essas e a outras questões a serem levantadas, qualquer avaliação mais detalhada da ABERT sobre quais setores estariam em condições de implementar medidas tendentes à portabilidade de dados seria precipitada. Não por acaso a implementação do direito à portabilidade tem representado um enorme desafio aos reguladores europeus, sob o GDPR, que até o presente momento não atingiram evolução significativa.

b. Quais são os desafios tecnológicos que devem ser enfrentados para implementar um padrão de interoperabilidade?

Como mencionado na questão anterior, temos um cenário de absoluta incerteza, no qual não se sabe ao certo quais dados seriam objeto de interoperabilidade ou em que termos essa interoperabilidade seria implementada. Somente após o preenchimento dessas lacunas parece, à ABERT, possível que se possa pensar em quais sistemas operacionais serviriam de ponto de contato entre agentes e, então, pensar nos desafios tecnológicos relacionados.

De toda sorte, parece evidente que a vasta gama de diferentes sistemas desenvolvidos e implementados pelos respectivos times de TI das empresas representam um desafio importante – ainda que se esteja tratando de um mesmo setor de atividade econômica. Vale lembrar que mesmo nos casos em que diferentes agentes de tratamento contratarem um dado sistema, provido por um mesmo fornecedor, é comum que esses sistemas passem por processos de customização. Sistemas customizados dificilmente utilizam os mesmos campos e parâmetros e podem apresentar dificuldades significativas para simples exportação e importação dados com a equivalência esperada, ainda que em formato interoperável.





Ainda é necessário considerar que a interoperabilidade pode acabar representando uma ameaça aos direitos dos titulares. Uma falha na identificação da pessoa natural que solicita acesso ou outras providências relacionadas a seus dados pessoais podem resultar em um incidente de segurança, com impacto para o real titular dos dados. Outro desafio trazido pela interoperabilidade é gestão do tempo de guarda dos dados armazenados. Chegando o momento da exclusão, os agentes que tiveram acesso aos dados por meio do mecanismo de interoperabilidade deverão ter claro qual a data inicial a ser considerada para fins de contagem do prazo de guarda.

Esses são, ao que parece à ABERT, apenas alguns exemplos dos desafios tecnológicos que deverão ser superados para que se alcance um padrão de interoperabilidade eficaz e abrangente.

c. Quais aspectos devem ser objeto de padronização para garantir a interoperabilidade (ferramentas, formato dos arquivos de dados portáteis etc.)?

A partir da perspectiva da ABERT, destacamos a importância de uma discussão técnica com especialistas capacitados neste tema para identificar os aspectos que devem ser padronizados para garantir a interoperabilidade.

É fundamental abordar questões como a estrutura dos dados, protocolos de comunicação e segurança da informação para garantir uma interoperabilidade eficaz entre os diferentes agentes de tratamento de dados. E evitar que se crie o risco de compartilhamento indevido e não desejável de dados entre diferentes agentes de tratamento que passem a operar de forma interconectada.

Esses são apenas alguns dos aspectos que devem ser considerados na padronização para promover uma interoperabilidade consistente e abrangente. Uma colaboração técnica e especializada será essencial para identificar e implementar os padrões necessários nesse processo.

d. É adequado considerar satisfeito o direito à portabilidade quando o agente de tratamento disponibilizar para o titular todos os seus dados pessoais em formato interoperável, conforme for estabelecido no regulamento previsto pelo art. 40 da LGPD?

Sem contribuições.

e. É razoável permitir que o setor privado defina padrões de interoperabilidade específicos para certas atividades econômicas para fins de portabilidade? Qual prazo seria razoável?

Como mencionado na questão anterior, temos um cenário incerto, no qual não se sabe quais dados seriam objeto de interoperabilidade ou em que termos essa





interoperabilidade seria implementada. Somente após o preenchimento dessa lacuna parece, à ABERT, possível que se possa pensar em quais sistemas operacionais serviriam de ponto de contato entre agentes e daí pensar nos desafios tecnológicos relacionados. A partir desse ponto seria, sim, razoável permitir que as empresas de um mesmo setor se reúnam para debater padrões de interoperabilidade específicos para suas atividades.

IV. Correção dos dados tratados (art. 18, inciso III)

a. Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

A ABERT entende que um dado é considerado incompleto quando faltam informações que estariam diretamente associadas a ele (por exemplo, somente o sobrenome em um cadastro que depende do nome completo para poder alcançar sua finalidade). Um dado inexato seria aquele que parece estar correto, porém algum erro no momento da coleta ou posteriormente levou à inexatidão (exemplos são anos de nascimento errados ou grafias equivocadas no nome ou endereço do titular). Já o dado desatualizado é aquele que estava completo e correto no passado, mas não mais reflete a realidade do titular (por exemplo, endereço ou telefone antigos cadastrados em vez dos atuais). Vale observar, porém, que dados desatualizados nem por isso deixam de ser úteis, como por exemplo nos cenários de combate à fraude, em que o histórico de endereços ou telefones anteriores é crucial para a atividade.

b. Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

Para que o pedido possa ser atendido, é imprescindível que o titular demonstre por quais motivos os dados existentes estão incompletos, inexatos ou desatualizados, bem como confirme a veracidade dos dados por ele apresentados como corretos, não bastando, portanto, na grande maioria das situações, a simples declaração do titular para o exercício do direito à correção. Infelizmente, um dos principais vetores de fraudes nas empresas é a falsa correção de informações por quem se passa por um titular – o exemplo mais conhecido é a alteração de endereço de entrega em um *e-commerce*, para que o produto seja enviado ao fraudador e não para o titular.

Na visão da ABERT, solicitações de correção devem ser revisadas com cuidado antes que as alterações pretendidas sejam implementadas, tendo em vista que seu atendimento implica na substituição de informações no banco de dados dos agentes de tratamento envolvidos. Por esse motivo, essas solicitações só devem ser atendidas após conferência dos dados apontados como incompletos, inexatos ou desatualizados e confirmação da veracidade dos dados apontados pelo titular como corretos, evitando-se com isso a prática de fraudes e a eliminação de dados originais verídicos.





c. Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.

No entendimento da ABERT, a impossibilidade ou o esforço desproporcional devem ser considerados de acordo com os aspectos técnicos e operacionais envolvidos.

Além disso, como se sabe, os direitos dos titulares não são absolutos. Certos direitos, por exemplo, podem ser eventualmente restringidos pelos direitos dos agentes de tratamento sobre seus segredos empresariais, situação em que caberá ao controlador explicar ao titular as razões pelas quais algumas de suas solicitações não serão atendidas.

Nesse sentido, vale conferir as orientações e exemplos do Information Commissioner's Office (ICO)³ sobre requisições infundadas:

"Uma requisição pode ser manifestamente infundada se:

- *O titular claramente não tem a intenção de exercer seu direito de correção. Por exemplo, um titular faz um pedido, mas depois se oferece para retirá-lo em troca de algum tipo de benefício da organização; ou*
- *O pedido é malicioso e tem a intenção de prejudicar a reputação de uma organização sem ter reais propósitos além de causar tumulto. Por exemplo:*
 1. *o titular declarou explicitamente, no próprio pedido ou em outras comunicações, que pretende causar tumulto;*
 2. *o pedido faz acusações não fundamentadas contra o responsável ou funcionários específicos;*
 3. *o titular está mirando um funcionário específico contra quem ele tenha alguma rixa pessoal; ou*
 4. *o titular envia sistematicamente diferentes pedidos para o responsável como parte de uma campanha, por exemplo, uma vez por semana, com a intenção de causar tumulto".*

Em situações como essas, caberá ao controlador, entretanto, explicar ao titular as razões da negativa de atendimento de sua requisição, de acordo com as razões fáticas apresentadas.

Outra situação que pode impactar a comunicação imediata aos demais agentes é o recebimento de grande volumetria de requisições de titulares, quando um controlador recebe temporariamente uma grande quantidade de requisições devido, por exemplo, a uma procura extraordinária por seus serviços ou produtos, o que poderia ser considerado

³ Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-rectification/#ib14>





como um motivo legítimo que justifique a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD.

Haverá também dificuldades causadas para a atualização de cadastros quando os dados obtidos tiverem sido objeto de um *compartilhamento unidirecional* e em que apenas um dos agentes envolvidos se mantenha responsável pela atualização dos dados relacionados a um determinado titular. Em exemplo: o agente de destino recebe os dados e, então, passa a proceder atualizações. Em casos como este, parece desproporcional exigir que os dois agentes envolvidos tenham condições de atender de forma coordenada a uma solicitação do titular, já que o agente de origem não possui informações atualizadas a seu respeito, inclusive para que possa verificar se há algum problema com a solicitação, como eventual tentativa de fraude.

d. Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique.

Sim, a ABERT entende que o direito de correção poderá ser negado pelo controlador sempre que a requisição do titular se mostrar infundada ou manifestamente abusiva, o que deverá ser avaliado no caso concreto, com base nos parâmetros mencionados na resposta à questão anterior (“IV.c”), bem como nos casos em que não houver validação de identidade do titular, ou, ainda, se houver dúvidas razoáveis sobre as informações apresentadas pelo titular.

V. Anonimização, bloqueio, eliminação e oposição no caso de tratamento irregular (art. 18, IV e § 2º)

a. É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Sim. Na visão da ABERT, é fundamental que solicitações de anonimização, bloqueio ou eliminação apenas devam ser atendidas em casos especiais, após rigorosa análise interna dos dados pessoais indicados pelo titular e revisão das atividades de tratamento, tendo em vista que o atendimento ao pedido do titular implica reconhecer que o controlador não está cumprindo com as exigências da LGPD.

A qualificação aqui é extremamente importante: dados desnecessários referem-se àqueles que não são úteis nem pertinentes para a finalidade que justifica o seu tratamento; dados excessivos são considerados àqueles supervenientes aos necessários para atingir a finalidade que justifica o seu tratamento e dados tratados em desconformidade com a LGPD são aqueles cujo tratamento é ilegal.





Consequentemente, é essencial que o titular, ao formular esta modalidade de requerimento relacionado à anonimização, bloqueio ou eliminação de dados pessoais, forneça justificativas claras que respaldem a sua solicitação, além de especificar a quais dados pessoais a solicitação se refere. Isto porque o requerimento do titular não deverá ser acolhido pelo controlador apenas por uma mera e simples alegação. Além do mais, ao fornecer fundamentos claros e expor detalhadamente os motivos da solicitação, o titular facilita o entendimento por parte do controlador sobre os motivos pelos quais o pedido está sendo feito.

A relevância deste entendimento se justifica dado que as medidas propostas que, uma vez acolhidas, extinguem o tratamento de dados pessoais, seja por meio da anonimização ou eliminação de dados. Deste modo, a ABERT entende que o requerimento de anonimização, bloqueio ou eliminação de dados pessoais, quando fundamentado pelo titular, não apenas facilita a análise por parte do controlador, mas também possibilita que este justifique de maneira mais clara e substancial a decisão de acolher ou recusar a solicitação.

Necessário frisar, ainda, que eventual **atendimento ao pedido do titular não implica reconhecer que o controlador está descumprindo a LGPD**. É possível que haja indícios de um possível tratamento irregular, que leve o titular a solicitar providências, e que o agente de tratamento, seja por não chegar a uma análise conclusiva, seja por atuar de forma conservadora, decida atender ao pedido. Sendo assim a ABERT entende ser relevante que a futura regulamentação preveja, de forma expressa, por uma questão de segurança jurídica, que o atendimento pelo agente de tratamento ao pleito do titular não implicará em reconhecimento de que, de fato, havia tratamento desnecessário, excessivo, desconforme ou que importe violação à LGPD.

b. A anonimização e a eliminação podem ser adotadas alternativamente, considerando situações específicas? Explique.

No entendimento da ABERT, a anonimização e a eliminação de dados pessoais podem ser adotadas de forma alternativa, considerando situações específicas, já que o que realmente importa é o resultado prático, ou seja, a impossibilidade de reutilização dos dados pessoais.

Ademais, a escolha específica entre anonimização e eliminação pode depender de circunstâncias particulares, as quais um titular de dados, considerando uma pessoa média, pode não conseguir diferenciar com clareza. Na esmagadora maioria dos casos, os titulares exercem seu direito solicitando a exclusão das informações sem, no entanto, compreender que, segundo a legislação, há uma distinção entre os direitos relacionados à anonimização e à eliminação de dados, bem como que a eliminação completa de dados muitas vezes não poderá ser realizada, inclusive para o cumprimento de obrigações legais e regulatórias ou o exercício regular de direitos.





A anonimização de dados, por exemplo, é um benefício de alto valor, pois permite implementar como estratégia a exclusão da aplicação da LGPD a certas atividades e amenizar riscos inerentes a titulares dos dados, trazendo também maior versatilidade ao desenvolvimento de produtos e serviços. Já a eliminação de dados consiste na remoção integral do dado pessoal da base de dados do agente do tratamento. O dado não passa por nenhum processo técnico, é simplesmente excluído da base de dados de forma completa.

É relevante ressaltar, neste contexto, que ambos os métodos proporcionam resultados práticos equivalentes ao titular dos dados, considerando que tanto a eliminação quanto a anonimização resultam no término do tratamento dos dados pessoais. Deste modo, a ABERT sustenta que a decisão quanto ao método a ser utilizado para a concretização deste direito não deve depender exclusivamente de uma escolha do titular, mas, sim, do controlador.

c. Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

O artigo 18, § 2º da LGPD estabelece a possibilidade de o titular dos dados pessoais se opor a um tratamento específico realizado por um controlador quando a base legal para o tratamento dos dados pessoais não for o consentimento e quando, no seu entendimento, houver descumprimento da legislação.

Segundo a visão da ABERT, se a alegação do titular for considerada legítima pelo controlador, o resultado prático desta ação consiste na interrupção do tratamento de dados pessoais do titular que vinha sendo realizado até então, bem como a suspensão de novas atividades de tratamento, paralisando quaisquer novos usos dos dados pessoais desse titular.

Isso indica, inclusive, que o controlador talvez necessite realizar a eliminação de dados pessoais, a depender da atividade de tratamento questionada. A eliminação, todavia, pode não ser a medida mais adequada caso a organização também utilize os dados para outras finalidades que não tenham sido objeto de oposição do titular. Nestes casos, o controlador deve se certificar de que os dados não serão utilizados para as finalidades às quais o titular se opôs, podendo prosseguir com outras atividades de tratamento realizadas com os mesmos dados e que tenham outras finalidades.

Necessário frisar, ainda, que eventual **atendimento ao pedido do titular não implica reconhecer que o controlador está descumprindo a LGPD.** É possível que haja indícios de um possível tratamento irregular, que leve o titular a solicitar providências, e que o agente de tratamento, seja por não chegar a uma análise conclusiva, seja por atuar de forma conservadora, decida atender ao pedido. Sendo assim a ABERT entende ser relevante que





a futura regulamentação preveja, de forma expressa, por uma questão de segurança jurídica, que o atendimento pelo agente de tratamento ao pleito do titular não implicará em reconhecimento de que, de fato, haja violação à LGPD.

VI. Revogação do consentimento (art. 18, VI e IX)

a. A revogação do consentimento prevista no art. 18, IX, da LGPD, implica na obrigação de eliminar os dados pessoais tratados com base no consentimento do titular? Explique.

Não. A ABERT entende não haver um direito absoluto que implique na eliminação automática dos dados pessoais tratados pelos agentes de tratamento, ainda que com base na revogação do consentimento do titular.

Como se sabe, quando o titular revoga seu consentimento para o tratamento de dados pessoais, pode também solicitar a eliminação desses dados, com algumas exceções. No entanto a LGPD nos parece clara ao prever que a eliminação e a revogação do consentimento são direitos distintos e que a realização deste não implicará, automaticamente, na execução daquele (vide, por exemplo, art. 8º, §5º, da LGPD).

A revogação do consentimento pelo titular possui efeitos não retroativos, mas, sim prospectivos (*ex-nunc*), não gerando, portanto, automaticamente, o dever de eliminação dos dados pessoais tratados com base nesse consentimento. É sempre necessária solicitação expressa do titular, a qual será avaliada, e que, eventualmente, poderá não ser atendida.

Isso porque o atendimento a uma solicitação de eliminação dos dados pessoais tratados com o consentimento do titular implica na exclusão de tais informações de banco de dados ou sistemas, o que pode gerar consequências gravosas caso não seja avaliada a pertinência de manutenção desses mesmos dados pessoais por outros motivos, particularmente em razão de obrigações legais, cumprimento de contratos, exercício regular de direitos ou outras razões. Em muitos cenários, o consentimento se refere apenas a finalidades determinadas, e não se aplica para todos os tratamentos realizados pelo controlador, justificando-se assim a manutenção desses dados para outras finalidades vinculadas a esses outros tratamentos.

b. Considerando o art. 8º, quais são os efeitos do requerimento de eliminação sobre os tratamentos realizados sob o amparo do consentimento anteriormente manifestado?

Na visão da ABERT, a requisição de eliminação de dados pessoais tratados sob o amparo de consentimento anteriormente manifestado não deve afetar os tratamentos realizados até a revogação do consentimento, os quais ficam ratificados de acordo com o art. 8º, §5º. Ainda que o titular requeira expressamente a eliminação de seus dados pessoais tratados com base em consentimento fornecido para finalidade específica, há de ser avaliado pelo





controlador eventual dever de retenção dos dados por obrigação legal ou regulatória, outras finalidades previstas no artigo 16 da LGPD, ou, ainda a utilização dos dados afetados com base em outras hipóteses legais.

VII. Decisões baseadas em tratamento automatizado (art. 20, caput)

a. O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

No entendimento da ABERT, decisão automatizada consiste no tratamento de determinado conjunto de dados por um software, o qual identifica, correlaciona e analisa certas informações sobre determinado indivíduo sem intervenção humana. A partir destas informações, esse mesmo software toma uma decisão acerca do (ou associa um determinado predicado ao) indivíduo em questão.

Evidentemente, pode haver cenários em que uma decisão seja tomada por humanos a partir de tratamento automatizado (por exemplo, criação automática de score de crédito utilizado para manualmente se decidir pela concessão de empréstimo ou não). Nesse caso, estaríamos falando de uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais, mas não de uma decisão automatizada.

b. Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado? Fundamente.

Quando há consequências relevantes para o titular de dados pessoais, notadamente impossibilidade de contratar produtos ou serviços, ter acesso negado a serviços essenciais, bem como em cenários de análise de sua situação de saúde e crédito. A simples existência de perfis, por exemplo, não deve ser interpretada como uma atividade que afeta significativamente o interesse do titular; é preciso compreender a finalidade da criação desse perfil.

c. Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

Para a ABERT, os desafios práticos incluem a compreensão do conceito de “direito à revisão”. Esse direito não significa que os titulares possam forçar a mudança de uma decisão automatizada, mas sim de solicitar que esta seja revista. Ou seja, não é o direito de obrigar que uma decisão diferente seja tomada, senão de solicitar que a decisão automatizada original seja avaliada e, caso erros sejam efetivamente constatados, que ela possa ser modificada. Deste modo, em diversos cenários, não haverá nada a ser modificado na decisão original.





Em outras palavras, o direito à revisão não implica o direito de obter um resultado diferente nem de controlar o resultado do tratamento e a decisão tomada; trata-se do direito de compreender os motivos pelos quais uma determinada decisão foi tomada, sem que isso implique obrigar o controlador a alterar a decisão.

Por fim, a ABERT ressalta que o direito à revisão de decisões automatizadas não poderá ser exercido quando a automatização for acompanhada por supervisão humana, caso em que já conta, ao longo do seu processo, com algum tipo de curadoria. Nestes casos, sequer há de se falar em direito à revisão, dado que, conforme o art. 20 da LGPD, o titular *“tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais”*.

d. Existem situações em que o controlador pode negar o direito de revisão sobre decisões automatizadas? Fundamente.

Sim, para que o titular possa solicitar a revisão mencionada no caput do artigo 20 da LGPD, a ABERT entende que ele deve ter condições de demonstrar que a decisão automatizada afeta, de modo significativo, seus interesses. Caberá aqui, portanto, que o titular justifique o pedido de revisão, explicitando o porquê de a decisão afetar significativamente seus interesses e qual é alteração pretendida. Evidentemente, quanto maior for a importância dos direitos em jogo relativos à decisão automatizada, mais simples será ao titular fazer essa demonstração.

Não parece razoável imaginar que o controlador tenha como atender bem à solicitação do titular se não souber ao certo de qual revisão está se tratando. Em primeiro lugar, é possível que decisão cuja revisão esteja sendo solicitada não seja resultante de tratamento automatizado. Em segundo, o controlador precisa entender qual a revisão pretendida. Em alguns casos pode ser evidente que o titular deseja que uma negativa de crédito seja revertida em concessão de crédito, mas essa é uma situação simples que nem sempre se repetirá. Em suma, parece necessário que todo pedido conte com alguma descrição de seu objeto para que se possa respondê-lo adequadamente. Pedidos de revisão do tipo *“solicito revisão da decisão automatizada destinada a definir meu perfil pessoal”* tendem a levar a uma resposta do mesmo calibre. Essa é uma situação de *‘perde-perde’*, que leva à ineficiência, na qual o controlador será impelido a uma resposta padrão, o titular não conseguirá alterar a situação em que se encontra e tampouco a ANPD terá bases sólidas para intervir se assim for necessário.



CONSIDERAÇÕES SOBRE A MINUTA DO GUIA DE ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DA ANPD

1. Glossário

Inicialmente, observa-se que o parágrafo 8 do Estudo Preliminar busca apresentar um glossário com conceitos básicos em matéria de privacidade, proteção de dados e anonimização, a fim de auxiliar o leitor na compreensão das orientações da ANPD. Apesar de essa ideia ser interessante para fins de padronizar e de proporcionar um melhor entendimento dos significados dos termos técnicos utilizados ao longo do documento, a ANBC sugere que a Autoridade centre a definição de conceitos no seu Glossário de Proteção de Dados Pessoais e Privacidade.³

O Glossário tem por objetivo justamente apresentar o significado dos principais conceitos, termos e expressões usados na Lei Geral de Proteção de Dados Pessoais (Lei Federal n.º 13.709/2018, ou “LGPD”) e nos documentos da ANPD, motivo pelo qual se entende que uma atualização constante desse documento garantiria maior uniformidade no entendimento conceitual e técnico da Autoridade. Assim, a ANBC acredita que os termos contidos no parágrafo 8 do Estudo Preliminar poderiam ser apresentados diretamente no Glossário de Proteção de Dados Pessoais e Privacidade da ANPD, reunindo em um único documento o entendimento conceitual e técnico da Autoridade na matéria.

2. Anonimização e os princípios de proteção de dados pessoais

a. Anonimização como atividade de tratamento de dados pessoais

A partir do parágrafo 27 do Estudo Preliminar, especificamente no parágrafo 30, a ANPD parece indicar que a anonimização de dados pessoais seria uma atividade de tratamento (artigo 5º, X, LGPD) em si mesma, com o intuito de desassociar os identificadores que se referem aos titulares dos dados. Ainda que a ANBC compreenda o raciocínio utilizado pela Autoridade, fato é que a anonimização não pode ser entendida meramente como um tratamento, haja vista que a legislação define anonimização como a utilização de meios

³ ANPD. “ANPD lança Glossário de Proteção de Dados Pessoais”. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-glossario-de-protecao-de-dados-pessoais>>. Acesso em: 26.02.2024.

técnicos razoáveis e disponíveis no momento de um tratamento específico – que não se trata da anonimização em si –, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (artigo 5º, XI, LGPD), sem que haja qualquer referência a uma operação posterior com dados. Ao mesmo tempo, a definição de tratamento apresentada pela LGPD indica uma série de atividades, como coleta, utilização, acesso, processamento, armazenamento e eliminação (artigo 5º, X, LGPD), sem qualquer menção à anonimização.

Nesse sentido, a ANBC entende que a anonimização não contrariaria a finalidade inicial do tratamento realizado pelo controlador (conforme disposto no artigo 5º, XI, da LGPD). Isso porque a anonimização ocorreria no momento imediatamente anterior à perda da associação de um dado a um titular, sendo, por esse motivo, plenamente compatível com operações lícitas anteriores. Logo, infere-se que não seria necessário um fundamento jurídico distinto do que permitiu o tratamento inicial dos dados pessoais, como consagra a experiência internacional na matéria: à luz do considerando 50 do Regulamento Geral sobre a Proteção de Dados 2016/679 da Europa (“GDPR”), o tratamento de dados pessoais para outros fins que não aqueles para os quais inicialmente coletados será autorizado quando compatível com as finalidades originais de tratamento, não sendo necessária uma hipótese legal distinta da que permitiu a operação prévia com os dados pessoais. Sob essa lógica, a ANBC defende que a anonimização não dependeria de fundamentação em nova hipótese legal prevista nos artigos 7º ou 11 da LGPD, uma vez que essa obrigatoriedade poderia, em última instância, inviabilizar a anonimização.

No ponto, considerando que **(i)** dentre outros objetivos, a LGPD visa proteger as liberdades e os direitos fundamentais dos titulares de dados pessoais; e **(ii)** a anonimização consiste na remoção de qualquer possibilidade de identificação de titulares, impedindo a ocorrência de danos e violações aos seus direitos, é possível concluir que dificultar ou inviabilizar a anonimização é, no limite, ir contra um dos objetivos centrais da legislação de proteção de dados. Com efeito, limitar a anonimização e o uso de dados anonimizados não confere aos titulares ou à sociedade qualquer proteção adicional, mas pode representar uma interpretação extensiva da lei, que foi clara ao afastar a aplicabilidade da LGPD aos dados anonimizados.

Com isso em mente, defende-se que a ANPD indique expressamente que a anonimização corresponde a uma medida de segurança a ser implementada pelo controlador, não

significando uma nova atividade que dependa de uma base legal ou que contemple uma finalidade incompatível com o tratamento inicial dos dados pessoais.

b. Utilização posterior de dados anonimizados e princípio da finalidade

A Autoridade afirma, no parágrafo 54 de seu Estudo Preliminar, que os agentes de tratamento podem utilizar dados anonimizados para outras finalidades – desde que compatíveis – além daquelas para as quais as informações tenham sido originalmente coletadas. Todavia, a ANBC entende que a utilização de dados anonimizados não deve atender ao princípio da finalidade, segundo o qual a operação com dados deve se voltar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (artigo 6º, I, LGPD).

De fato, após a anonimização, o controlador não precisa garantir a aplicação dos princípios previstos no artigo 6º da LGPD, em relação a qualquer operação realizada com dados anonimizados, uma vez que eles não mais são considerados dados pessoais (artigo 12, LGPD). Esse entendimento é, inclusive, referendado pelo Guidance on Anonymisation and Pseudonymisation,⁴ da autoridade de proteção de dados da Irlanda, segundo o qual dados irreversíveis e eficazmente anonimizados não são dados pessoais e os princípios de proteção de dados não precisam ser cumpridos em relação a essas informações. A autoridade da Irlanda indica que o controlador pode, conseqüentemente, utilizar dados anonimizados para outros fins além daqueles que inicialmente justificaram a coleta das informações.

Nessa linha, o controlador brasileiro é também livre para operar as informações sobre as quais a LGPD não é aplicável, inclusive para finalidades que não sejam compatíveis com o tratamento anterior indicado ao titular, motivo pelo qual a ANBC sugere a revisão do parágrafo 54 do Estudo Preliminar para retirar o trecho, por exemplo, “desde que compatíveis”.

c. Princípio da necessidade e dados anonimizados

⁴ Data Protection Commission. “Guidance on Anonymisation and Pseudonymisation”. Disponível em: <<https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf>>. Acesso em: 26.02.2024.

Outro ponto de atenção constante no Estudo Preliminar da ANPD é a argumentação de que, uma vez cumprida a finalidade de tratamento, a retenção das informações para uso exclusivo do controlador só seria possível desde que os dados fossem anonimizados (parágrafo 39 do Estudo Preliminar), observando o princípio da necessidade.

Ocorre que a LGPD, em seu artigo 16, IV, autoriza a conservação de dados pessoais após o término do seu tratamento para o uso exclusivo do controlador, vedado o seu acesso por terceiros e desde que anonimizados os dados. No entanto, considerando os demais e anteriores incisos⁵, fato é que a LGPD não condiciona a conservação de dados anonimizados, após o término do tratamento dos dados pessoais, ao cumprimento do princípio da necessidade (artigo 6º, III, LGPD), nem cria quaisquer obrigações aplicáveis aos dados anonimizados. Com efeito, a indicação prevista no parágrafo 39 do Estudo Preliminar parece criar uma obrigação adicional não prevista na legislação de proteção de dados pessoais, ao atribuir uma interpretação mais restritiva do que aquela determinada inicialmente pelo legislador.

Além disso, cumpre ressaltar que os dados anonimizados não estão sujeitos à normativa consagrada pela LGPD, inclusive ao princípio da necessidade, sendo certo que os dados anonimizados não serão considerados dados pessoais (artigo 12, LGPD). Nesse sentido, o controlador pode utilizá-los para a realização de suas finalidades, sem que haja a obrigação de limitar as suas operações ao mínimo necessário para a concretização dos seus propósitos ou de abranger somente dados pertinentes, proporcionais e não excessivos em relação às finalidades iniciais do tratamento dos dados pessoais não anonimizados (artigo 6º, III, LGPD). Em outras palavras, a partir da anonimização das informações, o controlador tem a liberdade de empregá-las a partir de parâmetros próprios para quais finalidades lícitas preferir, sem que a LGPD lhe seja aplicável, de sorte que a ANBC recomenda a exclusão da menção ao princípio da necessidade no parágrafo 39 do Estudo Preliminar.

3. Riscos de reidentificação de dados anonimizados

⁵ Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

- I - cumprimento de obrigação legal ou regulatória pelo controlador;
- II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

a. Responsabilidade do controlador pela reidentificação do titular

A ANPD sustenta no parágrafo 31 do Estudo Preliminar que a anonimização não seria um processo capaz de transformar em legítima a irregular atividade de tratamento de dados, sem fundamentação legal. À luz dessa afirmação, haveria um risco de responsabilização do controlador pela reidentificação posterior do titular dos dados pessoais conduzida por terceiros, na hipótese de reversão do processo de anonimização.

Assim, a ANBC considera importante a revisão do Estudo Preliminar, de modo que se indique expressamente que eventual reversão do processo de anonimização, levando à reidentificação do titular por terceiros, não configura tratamento irregular de dados pessoais pelo agente que anonimizou as informações. Além disso, não haveria violação de qualquer dispositivo da LGPD por parte do agente, tendo em vista que, segundo a legislação, a reversão do processo de anonimização somente é capaz de responsabilizar o agente quando ocorrer a partir da utilização de meios próprios, na forma do artigo 12 da LGPD. Desse modo, o agente que não realizou o tratamento irregular de dados pessoais (artigo 43, I, LGPD), não pode ser considerado responsável pela reidentificação de titulares realizada por terceiros.

Com isso, a ANPD poderia indicar diretamente em seu Estudo Preliminar, mais especificamente no parágrafo 61, que entenderá pelo não descumprimento da LGPD, e que não aplicará sanções específicas ao controlador, quando o processo de reidentificação do titular for realizado por terceiros, sem que haja culpa do agente que anonimizou os dados. Em outras palavras, caso o controlador adote todas as medidas de segurança e demais requisitos previstos na LGPD, não poderá ser penalizado pela reidentificação realizada por terceiros, tendo em vista que nenhum processo de anonimização é perpétuo (Apêndice I, alínea “c”, do Estudo Preliminar).

Além disso, como a LGPD indica que a anonimização corresponde à utilização de meios técnicos razoáveis e disponíveis no momento do tratamento (artigo 5º, XI, LGPD), a ANPD também poderia esclarecer em seu guia orientativo que, caso novas tecnologias sejam capazes de reverter o processo de anonimização anteriormente conduzido pelo agente de tratamento, este último não poderá ser responsabilizado pela reidentificação possibilitada pelo surgimento dessas novas técnicas. Na mesma linha descrita no ponto anterior, a reidentificação posterior do titular realizada por terceiros a partir de nova tecnologia não

disponível quando da anonimização não deve levar à responsabilização do agente, que teria cumprido com as obrigações dispostas na LGPD no momento da condução da anonimização.

Em outras palavras, a Autoridade pode indicar que a responsabilidade do agente que anonimizou os dados deve se limitar às técnicas disponíveis no momento da anonimização. Assim, os agentes devem estar vinculados à tecnologia disponível em seu tempo, devendo adotar as medidas razoáveis e disponíveis para condução dos processos de anonimização.

A ANBC compreende que uma delimitação específica da Autoridade a esse respeito garantirá maior segurança jurídica aos agentes regulados, além de auxiliá-los na avaliação de seus processos de anonimização sob uma lógica de responsabilização pelas técnicas disponíveis no momento da anonimização, sem possibilidade de penalização por novas tecnologias posteriores que superem os meios técnicos razoáveis e disponíveis naquele cenário inicial.

b. Avaliação de robustez dos processos de anonimização

A ANPD indica no parágrafo 43 do Estudo Preliminar que a adoção de modelos baseados em riscos relacionados à identificabilidade de dados mostra-se pertinente na avaliação da robustez do processo de anonimização, desde que referida avaliação não seja episódica ou pontual, mas iterativa e contínua. Apesar de a ANBC concordar que novos riscos de reidentificação possam advir ao longo do tempo, a partir dos avanços tecnológicos e da quantidade de dados auxiliares que se tornam disponíveis, compreende-se que a Autoridade poderia definir com maior precisão o que entende por “avaliação de robustez dos processos de anonimização” por meios iterativos e contínuos.

A título de exemplo, e como sugestão, a ANBC entende que poderiam ser considerados robustos, e indicados diretamente pela ANPD, os processos de anonimização conduzidos por algoritmos, cuja chave criptográfica não seja de conhecimento público – em outras palavras, cuja chave seja de conhecimento exclusivo do agente de tratamento que realiza tal ação – e de forma que se repute razoavelmente complexo, à luz das medidas técnicas de segurança da informação disponíveis a terceiros, realizar a quebra da criptografia dessa chave. Ademais, a ANPD poderia indicar quais questões deveriam ser consideradas pelo controlador em sua análise de risco. Busca-se, portanto, facilitar a definição de critérios no contexto dos processos de anonimização.

Deve-se considerar ‘robustos’ os processos de anonimização que tiverem passado por algoritmos cuja chave não seja de conhecimento público, ou seja, cuja chave de anonimização seja de conhecimento exclusivo da empresa que realiza tal ação e com nível de quebra de dificuldade razoável.

O desenvolvimento de raciocínio específico da Autoridade na matéria (conforme parágrafo 43) facilitaria o estabelecimento dos critérios de iteratividade e continuidade aplicáveis no contexto de processos de anonimização delimitados, além de garantir maior segurança jurídica aos agentes de tratamento regulados.

c. Gestão do risco de reidentificação

Ao contrário do indicado no parágrafo 62 do Estudo Preliminar, a ANBC entende que não seria possível ao agente de tratamento conduzir a gestão de risco de reidentificação durante o tratamento de dados pessoais, mas somente após o término do processo de anonimização. Nessa etapa final, efetivamente, seria possível avaliar a eficiência das técnicas utilizadas, a fim de afastar a possibilidade de identificação do titular.

Isso porque, em casos concretos, a gestão de riscos apenas pode ser efetivada quando o processo de anonimização tenha se concluído e as informações deixem de referir-se a uma pessoa natural identificada ou identificável – assim, a avaliação da medida de segurança e a análise de riscos teria relação direta com um processo finalizado passível de ser examinado pelo agente –, razão pela qual sugere-se a revisão do parágrafo 62 do Estudo Preliminar.

d. Risco de reidentificação aceitável

Dentre as etapas do processo de anonimização baseado em riscos, a ANPD indica ao agente de tratamento a determinação do Risco de Reidentificação Aceitável para um certo conjunto de dados, com o objetivo de estipular um limite superior para o risco. Essa definição, que seria estipulada somente pelo próprio agente de tratamento, consoante o parágrafo 65 do Estudo Preliminar, pode colidir com os entendimentos fiscalizatórios posteriores da ANPD. Em outras palavras, o agente de tratamento pode identificar um Risco de Reidentificação Aceitável que seja diferente do analisado futuramente pela Autoridade.

Nesse sentido, a definição do Risco de Reidentificação Aceitável pelo próprio agente de tratamento pode gerar insegurança jurídica em eventuais processos de anonimização, motivo pelo qual a ANBC sugere que a Autoridade indique um rol exemplificativo de quais seriam os parâmetros adequados para que o agente procedesse com a ponderação do Risco de Reidentificação Aceitável nesses cenários.

4. As noções de esforços razoáveis e meios próprios

a. Esforços razoáveis para reversão da anonimização

A ANBC entende que a razoabilidade dos esforços para a reversão do processo de anonimização (artigo 12, LGPD) não seria um conceito jurídico indeterminado, como sustenta a ANPD no parágrafo 48 do Estudo Preliminar, ao indicar que a própria Autoridade, como intérprete e aplicadora da LGPD, deveria preencher, com elementos e critérios pertinentes com o caso concreto, a noção de esforços razoáveis.

A bem da verdade, o artigo 12, § 1º, da LGPD, apresenta exemplos de fatores específicos que devem ser utilizados para a definição dos esforços razoáveis empregados em um determinado caso concreto. Logo, a determinação do que é razoável leva em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (artigo 12, § 1º, LGPD).

Dessa forma, a ANPD pode auxiliar os agentes de tratamento na identificação e na análise dos fatores descritos no artigo 12, § 1º, da LGPD, desde que a Autoridade esteja adstrita ao que dispõe a legislação – notadamente, a previsão de que a reidentificação do titular tem que ser possível pela utilização exclusiva de meios próprios. Com isso, sugere-se a exclusão da menção à teoria do conceito jurídico indeterminado presente no parágrafo 48 do Estudo Preliminar, a fim de não conferir uma competência não prevista na LGPD à Autoridade.

b. Utilização de meios próprios na anonimização

De acordo com o parágrafo 52 do Estudo Preliminar, a avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização deve considerar não apenas o uso de meios próprios do agente de tratamento responsável pela anonimização,

mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, possam reidentificar os dados anonimizados.

Contudo, a LGPD indica expressamente em seu artigo 12 que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização puder ser revertido, utilizando exclusivamente meios próprios. Por isso, não seria possível sustentar que a análise de reidentificação deve levar em conta os meios de terceiros, visto que essa previsão não encontra respaldo na lei. Logo, para que não seja criada uma nova obrigação de avaliação ao agente de tratamento, relativa à possibilidade de reidentificação do titular e de reversão do processo de anonimização por terceiros, recomenda-se a modificação do parágrafo 52 do Estudo Preliminar para excluir a referência a meios de terceiros .

5. Os processos de anonimização e pseudonimização

a. Técnicas de anonimização e pseudonimização

A ANPD identifica a substituição de dados, ofuscação de dados, tokenização e mascaramento de dados como técnicas de pseudonimização de informações, conforme o parágrafo 81 do Estudo Preliminar. Todavia, essas técnicas igualmente podem ser aplicadas para fins de anonimização de dados pessoais, à luz do Guide to Basic Anonymisation, da autoridade de proteção de dados de Singapura,⁶ bem como do Anonymization Code of Practice, da autoridade de proteção de dados do Reino Unido.⁷

A depender do Risco de Reidentificação Aceitável, o agente de tratamento pode adotar diferentes técnicas para garantir que o processo de anonimização esteja em conformidade com a LGPD e com as orientações da ANPD. Justamente por isso, a ANBC sugere que o Estudo Preliminar indique diretamente, para além de seu Apêndice II, que as técnicas de pseudonimização também podem ser adotadas para processos de anonimização, à exceção das hipóteses de criptografia típica, sobre as quais a Autoridade já se manifestou no parágrafo 81 do Estudo Preliminar.

b. Metodologia eficaz de pseudonimização

⁶ PDPC. “Guide to Basic Anonymisation”. Disponível em:<<https://www.pdpc.gov.sg/news-and-events/announcements/2022/03/guide-to-basic-anonymisation-now-available>>. Acesso em: 26.02.2024.

⁷ ICO. “Anonymization Code of Practice”. Disponível em:<<https://ico.org.uk/media/1061/anonymisation-code.pdf>>. Acesso em: 26.02.2024.

No âmbito dos parágrafos 83 e 84 do Estudo Preliminar, a ANPD parece referenciar diferentes etapas a serem observadas pelos agentes de tratamento no que se relaciona à condução de processos de pseudonimização. Ao adotar uma linguagem que parece indicar novas obrigações aos agentes regulados, sem qualquer correspondente na LGPD que indique esses deveres adicionais e específicos aos controladores, pode-se criar uma insegurança jurídica indesejável para um documento que visa orientar os agentes a respeito de metodologias eficazes para a pseudonimização.

A Autoridade estabelece, por exemplo, que os controladores devem fornecer treinamentos regulares aos seus colaboradores que realizem o tratamento de dados pessoais – obrigação essa que não se encontra especificamente na LGPD e que poderia ser prejudicial para agentes de tratamento de pequeno porte que não possuem condições de garantir esse tipo de atividade de adequação à legislação de proteção de dados pessoais.

Por isso, a ANBC recomenda que o posterior guia orientativo sobre anonimização e pseudonimização adote uma linguagem mais voltada à recomendação de metodologias a serem implementadas pelos agentes de tratamento regulados, a fim de garantir-lhes maior segurança jurídica, sem que haja a criação ou indicação de obrigações adicionais para a adequação à LGPD.

c. Meios automatizados no processo de anonimização

O Apêndice I, alínea “k”, do Estudo Preliminar, indica que a anonimização não deve ser totalmente automatizada, dada a importância do contexto e da avaliação geral do processo de anonimização. Para esse raciocínio, a ANPD parece ter se inspirado em documento da autoridade de proteção de dados da Espanha,⁸ tendo em vista que os “10 Misunderstanding Related to Anonymisation” apresentam a mesma orientação em seu item 7 (“anonymisation can be fully automated”).

Contudo, o título da alínea “k” (“a anonimização não deve ser totalmente automatizada”) parece estar em dissonância com o conteúdo remanescente da alínea (“ferramentas

⁸ AEPD. “10 Misunderstanding Related to Anonymisation”. Disponível em: <https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf>. Acesso em: 26.02.2024.

automatizadas podem ser usadas durante o processo de anonimização, no entanto, dada a importância do contexto e a avaliação geral do processo, poderá ser necessária a intervenção de um especialista humano”) e com a própria LGPD.

Isso porque, ao contrário da experiência europeia na matéria, é perfeitamente possível que o processo de anonimização no Brasil ocorra apenas por meios automatizados e sem a participação ou intervenção de humanos. Essa afirmação alinha-se diretamente ao artigo 5º, III, da LGPD, o qual prevê que um dado será considerado anonimizado à luz da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Assim, não se recomenda à Autoridade indicar que a anonimização não possa ser “totalmente automatizada”, tendo em vista que a LGPD não proíbe a utilização de sistemas automatizados para o processo de anonimização. Na verdade, a lei autoriza que o agente de tratamento utilize os meios disponíveis para garantir o processo, ainda que esses meios compreendam apenas a utilização de sistemas automatizados, motivo pelo qual sugere-se a modificação do Apêndice I, alínea “k”, do Estudo Preliminar.

d. Fiscalização dos processos de anonimização

Ao contrário do recente Guia Orientativo sobre Legítimo Interesse,⁹ que apresentou indicação específica de elaboração de teste de balanceamento, o Estudo Preliminar não informa aos agentes regulados como a Autoridade poderá analisar os processos de anonimização e pseudonimização. Dessa forma, recomenda-se maior especificação a esse respeito por parte da ANPD, principalmente a fim de garantir mais segurança jurídica nos projetos de adequação constante à LGPD dos agentes de tratamento.

Após essa especificação, a ANBC entende que poderia ser indicado um prazo para que os agentes de tratamento opinem e dialoguem com a Autoridade acerca de como documentar o processo de anonimização, especialmente tendo em vista eventuais processos administrativos fiscalizatórios da ANPD em face das operações conduzidas pelos agentes de tratamento.

6. Uso compartilhado de dados anonimizados e pseudonimizados

⁹ ANPD. “ANPD lança Guia Orientativo sobre Legítimo Interesse”. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse>>. Acesso em: 26.02.2024.

A ANBC compreende que o compartilhamento de dados pseudonimizados, sem os seus identificadores, configura para o destinatário dessas informações a coleta de dados anonimizados, uma vez que o terceiro não seria capaz de identificar o titular das informações. Essa é a mesma conclusão da autoridade de proteção de dados do Reino Unido,¹⁰ segundo a qual as mesmas informações podem ser dados pessoais para um agente de tratamento (dados pseudonimizados), e , ao mesmo tempo, consistirem em dados anonimizados para terceiros, a depender das circunstâncias e do contexto do uso compartilhado.

Diante desse racional, recomenda-se que a ANPD inclua semelhante esclarecimento no posterior guia orientativo sobre anonimização e pseudonimização, especialmente para que o destinatário, isto é, o agente para quem os dados estarão anonimizados, não seja responsabilizado pelos riscos relativos ao processo inicial de pseudonimização.

Ademais, a ANBC entende que o uso compartilhado de dados anonimizados, para ambas as partes que operam as informações, não poderia gerar responsabilização do destinatário pelos riscos relativos ao processo de anonimização previamente realizado a esse compartilhamento – uma vez que não seria o destinatário o agente de tratamento responsável por garantir um processo de anonimização em conformidade com a LGPD. Assim, recomenda-se que a ANPD também preveja esse raciocínio específico em seu guia orientativo, especialmente para garantir maior segurança jurídica aos destinatários dessas informações.

* * *

¹⁰ ICO. “Introduction to Anonymisation”. Disponível em:<<https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>>. Acesso em: 26.02.2024.

1. Relacionamento entre o controlador e o titular

Quais características de um canal de atendimento são essenciais para assegurar a efetividade na comunicação entre o titular e o agente de tratamento?

Resumo da recomendação: Um canal de atendimento ao titular deve levar em conta critérios de efetividade, acessibilidade e redução de barreiras de acesso.

Em relação a efetividade, é fundamental a **demonstração** por parte dos controladores que os canais de atendimento estão sendo efetivos e acessados pelos titulares. Ainda, é essencial a **clareza nos mecanismos de resolução de problemas**

Em relação a acessibilidade, **além de informações claras e compreensíveis**, é grande importância que sejam consideradas medidas de acessibilidade como, por exemplo, descrições nas imagens, plugin de acessibilidade em Libras; legendas e janelas de Libras, fontes com boa legibilidade e adoção de layouts com cores em alto contraste, plugins de busca por comando de voz.

Por fim, em relação a redução das barreiras de acesso, os canais de atendimento devem ser **gratuitos e indicados no momento de início da relação entre o titular e o controlador**. Ainda, a **diversificação dos pontos de atendimento** é fundamental para que os titulares consigam exercer seus direitos em sites, aplicativos, email, telefone e pontos físicos de atendimento (caso a organização possua instalações físicas). Por fim, é essencial garantir que **sempre exista um canal de atendimento e exercício de direitos dos titulares em todos os pontos de coleta de dados entre o controlador e o titular**.

Um bom canal de atendimento deve estar orientado em todo momento pelo fortalecimento do poder de autodeterminação informativa que corresponde ao titular dos dados pessoais. É indispensável o estabelecimento de parâmetros básicos unificados que garantam a efetividade na comunicação entre o titular e o agente de tratamento, a redução de barreiras simbólicas e materiais para o exercício do direito

e o cumprimento dos requisitos de acessibilidade, inclusão para pessoas com deficiência, idosos e aqueles com dificuldades tecnológicas.

A redução de barreiras que limitem a concretização efetiva de direitos implica tomar como ponto de partida para a regulamentação a realidade socioeconômica da população brasileira, onde desigualdades estruturais, assimetrias de poder e assimetrias no acesso à informação representam entraves.

Alguns aspectos que devem orientar o funcionamento do canal de atendimento para garantir o acesso efetivo aos direitos dos titulares. Em relação a **efetividade**, é fundamental que o controlador, em observância ao princípio da responsabilização e prestação de contas, **demonstre** que os canais disponibilizados estão sendo efetivos, seja por meio de relatórios públicos, campanhas de conscientização ou auditorias. Ainda, a efetividade só se concretizará caso exista **clareza nos mecanismos de resolução de problemas** por meio de, por exemplo, minimização das etapas para o atendimento; possibilidade de resgate do diálogo por meio de protocolo ou gravação; presença de ferramenta de pesquisa de conteúdo; garantia da autenticidade e integridade das informações disponíveis para acesso; manutenção atualizada das informações disponíveis para acesso; possibilidade de acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina; garantia de ininterruptibilidade no atendimento.

Em relação a acessibilidade, é essencial que o titular tenha acesso às informações suficientes e necessárias para o exercício dos direitos dos titulares: **garantir a transparência e informações claras e compreensíveis acerca** dos direitos do titular, da política de privacidade da organização nos locais físicos ou virtuais em que o titular de fato acessa o serviço; **orientar-se pelos princípios de transparência, responsabilização e prestação de contas**, nesse sentido, todas as informações sobre tratamento de dados pessoais, inclusive as informações de identificação e contato do controlador, uso compartilhado de dados e sobre as responsabilidades dos agentes de tratamento deve ser disponibilizada para crivo público, inclusive nos canais de atendimento; **orientar-se pelo dever de informar** acerca da extensão e operacionalização dos direitos dos titulares, inclusive sobre os meios de acesso, oposição e retificação dos dados pessoais; garantir o livre acesso aos dados por parte do titular. Ainda, medidas de acessibilidade como descrições nas imagens, plugin de acessibilidade em Libras; legendas e janelas de Libras, fontes com boa legibilidade e adoção de layouts com cores em alto contraste, plugins de busca por

comando de voz são essenciais para que titulares com algum tipo de deficiência consigam exercer plenamente seus direitos.

Em relação a **redução das barreiras de acesso** do canal de atendimento é indispensável garantir a **gratuidade** do serviço; **a indicação, prévia à prestação do serviço, do canal de atendimento** e instruções que permitam ao titular se comunicar, por via eletrônica ou telefônica, com o órgão ou entidade a quem vai permitir a coleta de dados ou o pedido de consentimento do titular; a **diversificação dos pontos de atendimento** (telefone, e-mail, mensageria instantânea, etc.), garantindo sempre a opção por atendimento em meio físico por pessoa humana quando o controlador possuir instalações físicas. Por fim, como atividades de tratamento de dados regulamentadas pela LGPD podem se dar em diferentes formas e meios, é essencial garantir que **sempre exista um canal de atendimento e exercício de direitos dos titulares em todos os pontos de coleta de dados entre o controlador e o titular**. Isso significa que se o controlador coleta dados de um titular em uma loja física, essa loja física necessariamente deve contar com algum canal de acesso aos mecanismos de exercício de direitos dos titulares, seja por meio de um funcionário ou disponibilização de ferramentas como telefone e internet para que o titular possa exercer seus direitos naquele instante. Esse ponto é essencial para evitar que controladores dificultem o exercício dos direitos dos titulares.

2. Informações sobre o tratamento (art. 18, incisos I, II, VII e VIII):

Quais as informações mínimas sobre o tratamento de dados pessoais deveriam ser evidenciadas pelo controlador, independentemente de requerimento – inclusive a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada – para garantir a transparência e o direito à informação?

2.1. Direito à informação e transparência ativa

Resumo da recomendação: A ANPD deve considerar o previsto pela LGPD em seu art. 9º e dar regulamentação concreta acerca dos parâmetros mínimos de transparência ali descritos, tendo como norte a efetividade da comunicação entre controlador e titular. É necessário que o titular de fato compreenda como se dá a atividade de tratamento de dados para que possa exercer sua autodeterminação informativa. Portanto, informações genéricas, confusas, em linguagem hermética e prolixa não são suficientes para o atendimento do dever de transparência.

Ainda, além do previsto no art. 9º, a ANPD tem a oportunidade de estabelecer um novo requisito: **o dever de os controladores informarem as fontes dos dados tratados**. Essa informação, no contexto da transparência ativa, não exige o grau mais elevado de granularidade acerca das fontes, bastando que o controlador informe de quais meios vem os dados (coleta direta do titular, observação, inferência, coleta de bases de dados públicas, compartilhamento de dados com parceiros comerciais, etc.).

Por fim, seria de grande importância para o fortalecimento da cultura de proteção de dados no Brasil que a ANPD incentivasse medidas de transparência inovadoras, como **“tabelas nutricionais de proteção de dados”** e selos que indiquem atividades de tratamento de dados que apresentem alto risco para os titulares.

Os direitos dos titulares, assim como outros temas de proteção de dados, devem ser interpretados a partir dos princípios enunciados pela lei. Dessa forma, o primeiro passo para se compreender a extensão e operacionalização dos direitos dos titulares é entender o seu diálogo com os princípios especificamente enunciados no art. 6º, da LGPD. Os princípios da transparência e do livre acesso, previstos no art. 6º, IV e VI, são a origem do direito à informação na LGPD, eles garantem ao titular o

acesso a uma série de informações sobre o tratamento de dados realizado. Essa informação, por sua vez, é a base para o exercício de todos os direitos previstos pela LGPD e pelo ordenamento jurídico como um todo, e pressuposto para o exercício da autodeterminação informativa.

A partir de um esforço para diferenciar esses princípios, a ANPD entende que o princípio da transparência indica para um dever de “dever de disponibilizar as informações exigidas pela lei, independentemente de solicitação do titular”. Já o livre acesso “ênfatisa a necessidade de o agente de tratamento disponibilizar mecanismos efetivos para que o titular possa solicitar e ter acesso facilitado e gratuito a determinadas informações”.¹

Esses princípios concretizam um dos pilares da proteção de dados pessoais, já que a lei não busca criar barreiras para o fluxo de dados, mas determina parâmetros concretos para que esse fluxo ocorra em observância aos direitos fundamentais dos titulares e grupos afetados. Nesse sentido, para além do titular concordar ou não com o tratamento de dados que está sujeito, ele deve ser informado sobre esse tratamento. A partir de informações sobre o tratamento de dados, o agente de tratamento atende o dever de justificar a atividade que realiza, adotar medidas de contenção de dados e, sobretudo, colocar-se sob escrutínio público, em observância ao princípio da prestação de contas.² Esses princípios apresentam as balizas para a concretização do dever de informar.

A LGPD prevê parâmetros mínimos desta obrigação de transparência ativa em seu art. 9º:

- Finalidade específica: o titular deve saber para quais finalidades os dados dele estão sendo tratados, não sendo suficiente indicar propósito genérico como “aprimorar os serviços”, “informar o sistema”. **A pergunta que deve ser respondida é: para quê o meu dado pessoal está sendo tratado?**
- Identificação e contato do controlador: o titular deve saber nome completo, se for pessoa natural, ou nome empresarial ou título do estabelecimento, se pessoa jurídica, ainda deve saber os meios de comunicação que viabilizem o exercício dos direitos dos titulares junto ao controlador e possibilitem o recebimento de comunicações da ANPD. **As perguntas que devem ser respondidas são: qual o nome do controlador de dados? Qual meio de comunicação posso usar para entrar em contato com o controlador?;**
- Informações sobre o uso compartilhado e as responsabilidades entre esses controladores: o titular deve saber com quem o controlador compartilha o seu dado pessoal e para quais finalidades. **As perguntas que devem ser respondidas são: qual o nome do outro controlador de dados que o**

¹ BRASIL. Autoridade Nacional de Proteção de dados. Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público. 2022, p. 15. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico_defeso_eleitoral.pdf. Acesso em: 12 fev. 2024.

² BIONI, Bruno. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. Universidade de São Paulo, Faculdade de Direito (Tese), 2021. p. 36

controlador compartilha os meus dados? De acordo com cada compartilhamento que o primeiro controlador faz, para qual finalidade ele realiza esse compartilhamento? Quais as obrigações que o novo agente de tratamento terá em relação ao tratamento que ele realizará?;

- **Forma e duração do tratamento:** o titular deve saber informações que impactam o tratamento, ou seja, se o tratamento é automatizado ou não, quanto tempo o dado é tratado até sua eliminação e qual a origem dos dados. **As perguntas que devem ser respondidas são: por quanto tempo meu dado pessoal está sendo tratado para atender as finalidades acima? Qual a origem dos dados que o controlador trata? O tratamento, em alguma das suas fases, é automatizado? Qual outra informação sobre o tratamento pode me impactar?;**

O termo “forma do tratamento” tem um caráter residual, ele é preenchido pelos casos em que o titular já sabe (i) a finalidade do tratamento, (ii) o controlador responsável pelo tratamento, (iii) o uso compartilhado que é feito, (iv) e a duração do tratamento, e ainda precisa de mais informações que impactam seus direitos.

Além dos elementos previstos no art 9º da LGPD, é de grande importância que a ANPD estabeleça também o dever de os controladores informarem as fontes dos dados tratados. Essa informação, no contexto da transparência ativa, não exige o grau mais elevado de granularidade acerca das fontes, **bastando que o controlador informe de quais meios vem os dados (coleta direta do titular, observação, inferência, coleta de bases de dados públicas, compartilhamento de dados com parceiros comerciais, etc.)**. Somente a partir dessas informações iniciais acerca da origem dos dados tratados o titular poderá iniciar um processo de tomada de decisão autônomo acerca de sua autodeterminação informativa.

Outro elemento que pode ser incentivado pela ANPD é a disposição de “tabelas nutricionais” de proteção de dados. Assim como alimentos que possuem alto teor de nutrientes maléficos à saúde devem informar isso em sua embalagem, os controladores devem informar os titulares de forma facilitada acerca de práticas que podem gerar alto risco, como perfilamento, cruzamento de informações de terceiros, transferência internacional de dados, etc.

É possível depreender que essa necessidade adicional surge do contexto regulatório da LGPD, tendo em vista que a lei, ao entrelaçar o princípio da boa-fé e o da prestação de contas, cria um direito-dever de prestação e julgamento de contas maximizada pelo dever de informar e cooperar para a garantia de direitos fundamentais.³ Dessa forma, o caso concreto pode lançar luz sobre quais informações compõem a forma do tratamento para que seja possível uma prestação de contas adequada e proporcional ao impacto do tratamento para o titular.

Assim, conhecer a origem dos dados pessoais deve ser entendido como uma das formas de tratar dados, tendo em vista a centralidade dessa informação para o titular

³ BIONI, Bruno. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. Universidade de São Paulo, Faculdade de Direito (Tese), 2021. p. 221.

se autodeterminar, além de já ser um parâmetro para a concretização do direito de acesso a dados pessoais, previsto no art. 19. Ainda, saber se o tratamento a que o titular está submetido é composto por processos automatizados é um dos pressupostos para concretização de outros direitos e demonstra o processo do tratamento, de forma a também ser entendido como aspecto que compõe a forma do tratamento.

2.2. Direitos de requisição de informações sobre o tratamento quando requisita

Ao mesmo tempo que a LGPD impõe ao agente de tratamento obrigações de, a partir de uma postura ativa, disponibilizar informação de maneira geral sobre os parâmetros do art. 9º no tratamento de dados, independente de solicitação do titular, há também uma série de direitos ligados ao acesso a informações acerca do tratamento de dados prevista no art. 18.

Ao regulamentar os direitos de acesso do art. 18 a ANPD deve considerar a progressão e a razão de existir dessas duas frentes - transparência ativa e acesso à informação por meio de pedido específico. Nesse sentido, parece lógico afirmar que as informações fornecidas ao titular, no contexto de um exercício de direito de acesso específico, devem contar com maior detalhamento e informações do que um direito geral de transparência.

Existe hipótese excepcional para negar o direito de confirmação da existência do tratamento? Cite e exemplifique.

Resumo da recomendação: A Lei Geral de Proteção de Dados não prevê qualquer hipótese de exceção do direito de confirmação da existência do tratamento de dados, motivo pelo qual tal hipótese deve ser analisada de forma restritiva e excepcional.

Contudo, vislumbra-se a hipótese em que a confirmação da existência da atividade de tratamento de dados coloca em risco outro bem jurídico de grande importância, e que, naquela situação específica, poderia sobrepor o direito do titular de ter este direito exercido.

Excepcionalmente, situações em que um controlador realiza atividades de tratamento de dados **única e exclusivamente** no contexto de investigações sigilosas e prevenção a fraudes, que, pela mera confirmação da existência do tratamento de dado de um titular revelaria a esta informação que traria prejuízo à investigação ou ao combate à fraude, vislumbra-se a hipótese de negar este exercício de direito. **Contudo, tal negativa deverá ser devidamente**

fundamentada e o titular deve ser informado ostensivamente acerca de peticionar à ANPD caso entenda que a negativa se mostra abusiva ou em desacordo com a disposição legal.

Poderia ser considerado satisfeito o direito de acesso quando o agente de tratamento disponibilizar os dados pessoais para conhecimento do titular em formato digital e em papel, conforme escolhido pelo titular?

Resumo da recomendação: O direito de acesso se consolida mediante a disponibilização das informações e dos dados ao titular, seja por meio eletrônico ou físico, em conformidade com os incisos I e II, § 2º do art. 19 da LGPD. Tal disponibilização deve contemplar elementos de acessibilidade, garantindo ao titular acesso completo às suas informações. No meio eletrônico, é essencial assegurar uma diagramação adequada para permitir a leitura por pessoas que utilizam leitores de tela e outras tecnologias assistivas. Já em meio físico, deve-se considerar a impressão em Braille para possibilitar a leitura por pessoas cegas ou com baixa visão.

Quais informações devem ser fornecidas para os titulares para a identificação dos controladores, inclusive no caso de uso compartilhado dos dados pessoais?

Resumo da recomendação:

O direito de o titular receber informações sobre o uso compartilhado de dados de forma passiva é consequência do direito à informação ativa (art. 9º, V). No entanto, eles não se confundem entre si. Como evidenciado acima, o direito previsto no art. 9º não depende de qualquer requerimento do titular, ao passo que os direitos do art. 18 ganham concretude a partir do pedido do titular. **Como consequência, quando solicitado, o titular tem direito de saber informações sobre o uso compartilhado de seus dados pessoais de forma específica, não genérica, ou aplicável a qualquer titular de dados pessoais que o controlador solicitado realize.**

Ainda, o art. 18 destaca que o controlador deve informar não apenas as entidades privadas com quem realizou uso compartilhado de dados de determinado titular, mas também as entidades públicas. Isso reforça o princípio da transparência e livre acesso da LGPD aplicável a qualquer tipo de controlador de dados.

Cumpramos ressaltar que, assim como no art. 9º, V, considera-se informações sobre o uso compartilhado aquelas necessárias para que o titular possa exercer sua autodeterminação frente ao tratamento a que está submetido. **Assim, o titular deve, no mínimo, ser informado sobre o nome do controlador que recebeu os dados e a finalidade do uso compartilhado no caso específico para que possa exercer seus direitos também perante a esse controlador.**

Esta entre o acesso pelo titular de toda cadeia de controladores que tem acesso a seus dados é comumente associada a preocupações relacionadas a proteção do segredo industrial. Várias das disposições da LGPD, inclusive a concretização de direitos, traz o sopesamento do segredo de negócio como um dos filtros para divulgação de informações. Ao mesmo tempo, a lei não oferece uma definição clara do que é um segredo comercial ou industrial, de forma a tornar esses conceitos fluídos no âmbito da proteção de dados. Conforme as diretrizes do Grupo de Trabalho do Artigo 29, os controladores não podem usar o segredo comercial como justificativa para negar acesso a dados ou recusar fornecer informações ao titular dos dados.⁴

Portanto, o argumento do segredo de negócio só é válido em circunstâncias excepcionais e não pode ser invocado de maneira indiscriminada. Em vez de adotar uma abordagem de "tudo ou nada", é necessário buscar um nível de transparência adequado tanto para o titular dos dados quanto para a empresa que detém o direito de manter seus segredos comerciais.

Por fim, a exceção do segredo industrial deve ser devidamente fundamentada pelo controlador, de forma específica para cada caso, e ser passível de questionamento pelo titular perante à ANPD e demais órgãos competentes.

⁴ UNIÃO EUROPEIA. Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Bruxelas: European Commission, 2017, p. 17. Disponível em: <https://ec.europa.eu/newsroom/article29/redirection/document/49826>. Acesso em: 08 dez. 2022.

3. Portabilidade

Resumo da recomendação: A ANPD deve iniciar e impulsionar a implementação de soluções de portabilidade por meio de regulamentação específica sobre esse direito. É comum que, uma regulamentação sobre o tema ocorra de forma setorial, porém a interoperabilidade é um dos pilares para o desenvolvimento de uma infraestrutura pública digital, tema chave para a agenda digital do Brasil. Com isso, a portabilidade assume perspectiva geral, para além das implicações setoriais do tema.

Nesse sentido, a ANPD é o órgão regulador que possui a competência legal definida para estabelecer **parâmetros mínimos** acerca desse direito e dialogar com **órgãos setoriais para que as regulamentações setoriais possuam um mesmo nível adequado de proteção aos titulares de dados.**

A portabilidade de dados permite ao titular solicitar que seus dados sejam enviados a um outro prestador de serviço, de forma a mover, copiar e transferir seus dados pessoais de um sistema para outro.⁵ Ou seja, a portabilidade engloba o direito de acesso, já que, além do titular ter acesso aos seus dados, ele passa a transmiti-los para que outro prestador de serviço possa tratá-los. O art. 40 da LGPD não dispõe que o direito de portabilidade é apenas o agente de tratamento disponibilizar os dados ao titular, mas sim permitir que esses sejam transmitidos de forma segura e em acordo com a LGPD. Para que seja possível portar dados, os sistemas que armazenam essa informação devem ser interoperáveis, ou seja, devem ser capazes de se comunicarem com outros sistemas, dispositivos e aplicações.

Sistemas interoperáveis surgem a partir da definição de padrões e, em regra, o esforço de delimitar esses modelos e estruturas comuns é feito setorialmente. Isso porque entidades que atuam em setores parecidos possuem peculiaridades e desafios em comum, que podem ser solucionados com o uso de ferramentas semelhantes ou mesmo idênticas. Assim, os setores especificamente considerados possuem maior conhecimento para avançar internamente na definição de padrões que permitirá a comunicação entre sistemas diferentes, mas com produtos parecidos.

O direito de portabilidade possui uma faceta concorrencial na medida em que a inexistência de sistemas interoperáveis é meio para o estabelecimento de nichos de mercado. Isso porque, se não há interoperabilidade, não é possível que o consumidor flua entre empresas que fornecem o mesmo serviço e uma empresa concentre o maior número de clientes.

⁵ ICO. Right to portability. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/>. Acesso em: 12 fev. 2024.

Ao passo que a interoperabilidade é uma solução de interesse setorial, podem haver barreiras entre as empresas de um mesmo setor no desenvolvimento desses sistemas a fim de se preservar esses silos e evitar a ampliação da concorrência. Nessa medida, é provável que o CADE assuma papel relevante sobre a forma de concretização do direito de portabilidade.

Ao mesmo tempo que é razoável que os setores sejam responsáveis por definirem os padrões de interoperabilidade, em regra não é dessa forma que as ferramentas de interoperabilidade são implementadas. Para a portabilidade de serviços ser feita, por exemplo, é comum que haja uma norma exarada pela agência reguladora competente indicando as diretrizes para tanto.

- Lei Complementar nº 109, de 2001: determina a portabilidade do direito acumulado pelo participante para outro plano de previdência privada.
- Resolução nº 460, de 2007, da Agência Nacional de Telecomunicações: estabelece as condições para a implementação da Portabilidade de Código de Acesso pelas empresas prestadoras de serviços de telecomunicações de interesse coletivo.
- Resolução nº 4.292, de 2013, do Banco Central do Brasil: determina a portabilidade de operações de crédito realizadas com pessoas naturais.
- Resolução Normativa nº 438, de 2018, da Agência Nacional de Saúde Suplementar: dispõe sobre a regulamentação da portabilidade de carências para beneficiários de planos privados de assistência à saúde.
- Resolução Conjunta nº 5, de 2022, do Banco Central do Brasil e Superintendência de Seguros Privados: dispõe sobre a interoperabilidade no Open Finance.

Dessa forma, nota-se que, para a construção de soluções de portabilidade, existe um diálogo entre as organizações que compõem o setor, bem como o Poder Público, que interage com o setor e regulamenta a solução. Com isso, o período de tempo relevante para se estruturar a portabilidade está relacionado com o início das discussões sobre o tema inclusive nas entidades da administração pública.

Para além do desenvolvimento setorial de soluções de portabilidade, outras formas de se pensar a interoperabilidade ganham espaço. Em um contexto de desenvolvimento de infraestrutura pública digital (DPI), sistemas interoperáveis são um dos pilares para que seja possível formar esse arcabouço digital comum.

Diante da potencialidade de uma DPI, o G20, especialmente durante a presidência da Índia, encampou o tema como ferramenta fundamental para a prestação de serviços públicos em escala. Nesse contexto, sabe-se que a infraestrutura deve ser desenhada em protocolos e padrões comuns para que outras funcionalidades possam ser adicionadas a ela e essas possam interagir entre si. O ecossistema

deve ser construído com base em princípios de abertura, interoperabilidade e escalabilidade, de forma que módulos independentes possam ser adicionados e aprimorados conforme desenvolvimento da infraestrutura.

É por isso que o desenvolvimento de sistemas interoperáveis para se garantir direito à portabilidade ganha outra dimensão para além dos silos formados por setores econômicos. Por mais que não seja uma necessidade iminente, a implementação de iniciativas de DPI está se tornando ponto de atenção para fóruns internacionais, como a OCDE, o Banco Mundial, e nacionais, com a presidência do Brasil no G20.

4. Revogação, oposição e correção - O poder do titular face ao controlador

Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?

Resumo da recomendação: O maior ponto de controvérsia acerca do direito de correção de dados incompletos, inexatos ou desatualizados se dá em dados que não podem ter sua validade/veracidade verificados objetivamente.

EX: Um birô de crédito atribui uma baixa avaliação de crédito a um titular, implicando que este possui altas chances de não pagar dívidas contraídas. Essa atribuição foi baseada no histórico de pagamentos e de recebimentos deste titular nos últimos 5 anos.

Nesse caso, o score de crédito final é um dado que não garante, por si só, elementos suficientes para ter sua veracidade apurada. Contudo, a análise dos dados de histórico de pagamentos e recebimentos, por sua vez, pode ser apurada. Portanto, se o score de crédito foi calculado com base em informações desatualizadas, ele passa a ser objeto de correção na medida em que os elementos objetivos que o embasam estão incorretos.

Por este motivo, o direito à correção está intimamente ligado ao direito de acesso às informações. Caso o titular não tenha acesso aos dados que embasam alguma análise feita sobre ele pelo controlador, torna-se impossível o exercício de um direito previsto em lei.

Além disso, recai sobre o controlador o ônus de demonstrar que análises e inferências feitas possuem algum lastro na realidade e podem ter sua acurácia mensurada em algum parâmetro. Essa discussão se relaciona ao chamado “direito a inferências razoáveis”⁶ e se mostra como uma importante janela de oportunidade para a ANPD fixar parâmetros mínimos para atividades de tratamento de dados que atribuem características ou comportamentos a titulares que não podem ser diretamente observados ou mensurados objetivamente.

⁶ WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and IA. Columbia Business Law Review, 2019.

Em quais situações a simples declaração do titular não seria suficiente para o exercício do direito à correção? Fundamente.

Resumo da recomendação: Em primeiro lugar, é importante que o titular consiga demonstrar minimamente qual a informação que está imprecisa. Quando o pedido é ininteligível, não sendo possível compreender qual dado está incorreto e o que deve ser corrigido, o direito de correção fica prejudicado.

Contudo, situações em que o erro envolve informações sobre crédito, registro criminal, situação familiar e outras informações que dizem respeito aos seus direitos fundamentais é preciso contar com documentos capazes de demonstrar o erro.

Aliado a isso, ressaltamos que é papel do controlador esclarecer quais documentos servem de justificativa nesses casos e do porque somente a declaração do titular não é suficiente para que a correção ocorra. Ao mesmo tempo, é preciso que o controlador tenha cautela e respeite a proporcionalidade da documentação exigida.

Ou seja, a solicitação de mais informações para proceder à correção deve versar somente para o necessário da comprovação, não sendo admitida solicitações de documentos que só trariam maiores dificuldades de acesso ao direito do titular.

Ex: O titular mudou de nome e quer que o novo nome conste na base de dados do controlador. Para tanto, ele faz a solicitação de correção e o controlador informa que a correção depende de uma documentação que mostre o nome atual como o RG, a documentação que comprove a mudança de nome, a certidão de nascimento ou casamento e comprovante de residência.

No caso em questão, é possível ver que o comprovante de residência é uma solicitação excessiva tendo em vista que não é adequada para averiguar a inexatidão do dado a ser corrigido.

Quais critérios objetivos devem ser considerados para avaliar a impossibilidade ou o esforço desproporcional para os efeitos do art. 18, § 6º, da LGPD? Exemplifique.

Resumo da recomendação: Cabe ressaltar que o dever de comunicar a correção a terceiros de quem o controlador compartilha dados é um dever legal previsto expressamente aliado a um dos princípios basilares da proteção de dados no Brasil. Tal obrigação tem como decorrência a exigência de que o controlador tenha medidas técnicas e organizacionais para poder informar parceiros de que um dado foi corrigido.

Todavia, sabemos que as múltiplas atividades de tratamento e as tecnologias envolvidas podem ser um fator relevante na hora de informar com clareza e qualidade que um dado foi corrigido.

Dito isso, ressaltamos alguns critérios objetivos:

1. **A quantidade de parceiros em que se compartilha os dados**
2. **A complexidade técnica da correção.**

A quantidade de parceiros é um critério seguro pois quantificável e avaliável como elemento que dificulta a comunicação imediata da correção. Já o segundo elemento, diz respeito a impossibilidade de comunicação imediata da correção por conta do tempo de execução da própria correção, de modo que uma correção mais demorada, atrase o momento da comunicação imediata, bem como da qualidade dessa comunicação haja vista a complexidade com que foi executada.

Ex: um plano de saúde compartilha informações triviais de cadastro como nome, telefone e endereço de seus pacientes para centenas de clínicas e hospitais parceiros no país todo com a finalidade de proporcionar o atendimento facilitado nessas instituições. Tais clínicas e hospitais são controladores na medida em que decidem sobre o tratamento dado às informações fornecidas pelo plano de saúde. Tal plano de saúde recebe uma solicitação de correção dos nomes de um grupo familiar como um todo. Em resposta, o plano informa um prazo de 30 dias para que a correção seja feita e que todas as instituições parceiras sejam informadas da mudança. Explicam também que o tempo de espera se dá por conta das inúmeras instituições em que a comunicação precisa ser feita de modo eficaz em todas as cadeias de informação do plano.

Nesse caso, a quantidade de agentes com a qual o plano de saúde precisa comunicar a mudança cadastral é tamanha que se exige um tempo para que ela possa acontecer com qualidade.

Reforça-se que esses critérios podem ser utilizados para justificar um prazo estendido para a correção ou eliminação dos dados, ou apresentação de solução

alternativa (ex: controlador apresentar anonimização como solução quando a eliminação é inviável) **mas jamais o descumprimento da solicitação do titular.**

Existe situação excepcional em que o direito de correção pode ser negado pelo controlador? Exemplifique

Resumo da recomendação: Existe uma certa dificuldade em exceções na qual o controlador pode se recusar a realizar a correção dos dados, tendo em vista que a correção colabora com o princípio da qualidade dos dados e seus fluxos em nossa sociedade. Contudo, existem dois elementos que podem ser utilizados para negar um pedido de correção::

- Pedidos ininteligíveis
- Pedidos excessivos ou infundados⁷

Pedidos ininteligíveis são aqueles em que o pedido do titular não consegue esclarecer qual dado está inexato e precisa ser corrigido ou quando o titular não apresenta a documentação necessária para tanto.

Já os **pedidos excessivos** ou infundados são aqueles em que o titular solicita múltiplas vezes sobre o mesmo assunto em um período de tempo curto, de forma que a resposta de um, responde a todos. Nesse caso, o controlador pode responder a uma solicitação e se recusar a responder as repetidas, alegando que a correção solicitada já foi realizada.

Em qualquer dos casos, a recusa pela correção dos dados deve vir com uma justificativa, que deve conter:

- os **motivos pelos quais a correção não foi feita;**
- o **direito de fazer uma reclamação à ANPD e**
- a **possibilidade do titular de buscar a seara judicial para a resolução do problema.**

Por fim, ressalta-se que esta pergunta possui íntima conexão com a pergunta anterior "Quais critérios objetivos devem ser considerados para qualificar um dado como incompleto, inexato ou desatualizado?", **motivo pelo qual é de grande importância uma regulamentação que garanta aos titulares o máximo de informações possíveis acerca de seus dados tratados pelo controlador para que controvérsias sobre a correção de um dado sejam mitigadas.**

Considerando que a oposição prevista no art. 18, § 2º, da LGPD, seria aplicável em caso de descumprimento ao disposto na Lei, qual o seu efeito se a alegação do titular for considerada legítima? Explique.

⁷ ICO. [Right to rectification](#)

Resumo da recomendação: Diante de tal pergunta, duas respostas podem ser possíveis:

Resposta 1: encerrar o tratamento de dados pessoais do titular que se opôs.

Resposta 2: proceder à conformidade do tratamento.

Como a proposição legal do art. 16 §2º estabelece que o direito à oposição deve ser exercido em caso de desconformidade com a lei, caso seja legítimo, o controlador precisa tomar medidas para que o tratamento esteja de acordo com a LGPD. Portanto, a resposta 2 parece ser a mais adequada.

Opor-se ao tratamento de um dado também pode levar ao encerramento do tratamento no caso do legítimo interesse, onde a irregularidade do tratamento está na violação das legítimas expectativas do titular. Contudo, mesmo nesses casos, o encerramento do tratamento dos dados do titular é uma forma de conformidade.

EX: Uma Instituição de Ensino Superior (IES) particular oferece formação de ensino superior e pós-graduações e com base no legítimo interesse de terceiro e buscando potencializar a formação do corpo discente, a instituição divulgou para os seus alunos uma campanha promocional que consiste em um cupom que habilita um desconto de 10% nas mensalidades de cursos de inglês e espanhol em todas as escolas do município. A ação foi realizada apenas uma vez. Nesse contexto, muitos alunos formularam pedidos de oposição àquele tipo de tratamento de dados pois isso violava as legítimas expectativas deles. Para atender aos pedidos, a instituição excluiu os dados destes alunos do banco de dados utilizados para ações dessa natureza, restabelecendo a conformidade no uso da base legal do legítimo interesse (ANPD, 2024).⁸

Vale lembrar que é uma boa prática que as comunicações com titulares de dados como as do exemplo venham acompanhadas de uma interface que forneça um canal de atendimento e um canal de exercício ao direito à oposição no mesmo ambiente. Ex: o email tem que vir acompanhado com alguma opção de “fale conosco” e “quero me opor a esse tratamento de dados”

Algo distinto é o pedido de eliminação, anonimização ou bloqueio dos dados, que visa impedir tratamentos de dados excessivos, desnecessários ou em desconformidade. Nesses casos, o pedido visa o encerramento do tratamento de dados pessoais do titular, razão pela qual essa deve ser a consequência caso ele seja legítimo nas hipóteses de tratamento excessivo ou desnecessário. No caso da desconformidade à lei, o agente de tratamento precisa adequar a atividade de

⁸ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. [Guia orientativo Hipóteses legais de tratamento de dados pessoais: legítimo interesse](#). Brasília 2024.p. 20

tratamento ao mesmo tempo que exclui, anonimiza ou bloqueia o tratamento dos dados do titular.

É necessário que o titular fundamente o seu requerimento e comprove a desnecessidade dos dados, a excessividade do tratamento, a desconformidade ou o descumprimento legal verificado? Fundamente.

Resumo da recomendação:

Os direitos dos titulares previstos na LGPD existem a partir do pressuposto da assimetria de poder e informações na relação entre titular e controlador. Desta forma, nenhum exercício de direitos deve se basear na capacidade técnica do titular de formular um pedido, mas sim na forma como o controlador fornece informações suficientes para que o titular possa compreender o tratamento de dados e se seu pedido tem legitimidade ou não. Nesse sentido, é desproporcional que o titular saiba avaliar a conformidade do tratamento para poder exercer tais direitos, pois trata-se de uma hipótese clara de inversão do ônus da prova.

A LGPD prevê em dois momentos a inversão do ônus da prova, inicialmente em seu art.8º §2 da LGPD, ao dispor que o controlador precisa comprovar que cumpriu com os requisitos do consentimento, e no art. 42 §2º, em que se autoriza em processo judicial a inversão do ônus da prova quando “for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa”.

Tal disposição se assemelha a dos art.6, VIII;51, VI CDC e art 373, §1º CPC. que dispõem que a inversão do ônus da prova deve ocorrer quando for muito oneroso a comprovação pela parte. No caso em questão, a informação sobre o tratamento está de posse do controlador, razão pela qual é do controlador o dever demonstrar que cumpriu a lei após a manifestação do titular.

5. Decisões automatizadas e contestabilidade

O que caracterizaria uma decisão automatizada e uma decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Fundamente.

Resumo da recomendação:

Há uma grande dificuldade de se caracterizar uma decisão tomada “unicamente” com base em decisões automatizadas, na medida em que o elemento central trazido pela LGPD é a automação dos elementos que levam ao **embasamento** da decisão, e **não da decisão em si**.

Nesse contexto, a palavra “unicamente” não deve ser interpretada de forma restritiva para descaracterizar a decisão como automatizada em qualquer envolvimento humano na tomada de decisão, mas apenas nos casos em que esse envolvimento é significativo, isto é, quando pode alterar ou influenciar o resultado da decisão. Essa interpretação afasta a tentativa de fabricação de interferência humana na tomada de decisão para afastar a aplicação do art. 20, o que confere maior carga protetiva aos titulares de dados.

Tal interpretação é corroborada no contexto europeu, em que o Grupo de Trabalho do Artigo 29 (corroborado pelo EDPB) se manifestou pelo entendimento de que, para ser qualificado como participação humana, esta deve ser significativa para a tomada de decisão, ou seja, envolver pessoa com autoridade e competência para interferir no resultado – não meramente um ato simbólico.⁹

Nesse sentido, a Autoridade Espanhola de Proteção de Dados faz uma complexificação necessária da análise sobre a interferência humana significativa. Esta pode ser entendida quando a pessoa que participa da decisão: (i) tem competência ou autoridade para mudar o resultado; (ii) tem conhecimento e preparo para mudar o resultado da decisão automatizada; (iii) tem independência e diligência no exercício de sua competência, ou seja, quando não há pressões da organização ou externas que impeçam o agir pela pessoa, assim como a ausência do pré-condicionamento de aceitar a decisão automatizada como certa (viés da automação); (iv) pode exercer sua competência e qualificação, pois pode exercer a jurisdição no caso concreto, além de ter informações, recursos e tempo para exercer sua função de interferir na decisão.¹⁰

Portanto, é essencial que a análise da decisão automatizada e a participação humana significativa considere não apenas a decisão final, mas também

⁹ Article 29 Data Protection Working Party. Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679.p. 21.

¹⁰

<https://www.aepd.es/prensa-y-comunicacion/blog/evaluacion-de-la-intervencion-humana-en-las-decisiones-automatizadas>

eventuais decisões intermediárias [*upstream*] que possam também ter impactos potencialmente distribuídos ou observados com atraso em decisões posteriores [*downstream*]¹¹ que afetarão os interesses dos titulares.

Quais são os critérios para determinar quando um interesse está sendo efetivamente afetado?

Resumo da recomendação:

De acordo com o Grupo de Trabalho do Artigo 29, no contexto do art. 22 do RGPD da União Europeia, a afetação de um interesse jurídico no âmbito de decisões automatizadas ocorre sempre que houver afetação em direitos ou no seu estatuto jurídico, como no caso de impactos na liberdade de reunião, recebimento de benefício social ou até mesmo participar de processos democráticos.¹²

Porém, diferentemente do acontece no âmbito do RGPD, o art. 20 da LGPD não define que a afetação de interesses deve ser meramente jurídica, assim como não prevê a possibilidade de afetar “significativamente de forma similar”.

Consequentemente, a afetação de interesses pela lei brasileira pode ser entendida de forma mais ampla, não havendo necessidade da verificação de violação de um direito específico para que o art. 20 e seus direitos correlatos possam ser invocados. Como exemplo de afetação de interesses, podemos citar o caso de decisões que neguem eficácia ou deixem de promover direitos do titular de dados, negando ou limitando alguma perspectiva de promoção da pessoa humana,¹³ inclusive apenas por meio de ameaça de afetação de direitos.¹⁴ Em outras palavras, a tutela dada pelo art. 20 pode ter natureza preventiva, antes da concretização em dano efetivo.¹⁵

¹¹ MARTINS, Pedro. Profiling na Lei Geral de Proteção de Dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. Indaiatuba: Editora Foco, 2022.

¹² <https://www.aepd.es/documento/wp251rev01-es.pdf>

¹³ KORKMAZ, Maria Regina Rigolon. Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial. Thomson Reuters, Revista dos Tribunais; 1ª edição, 2023.

¹⁴ MARTINS, Pedro B. Lobo; HOSNI, David Salim S. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. *Internet e Sociedade*, Vol. 1, nº 2, dez. 2020, pp. 77-101.

¹⁵ Ibid.

Quais são os desafios práticos para implementar o direito de revisão de decisões previsto no art. 20 da LGPD?

Resumo da recomendação:

Os desafios práticos para implementação do direito de revisão de decisões previsto no art. 20 da LGPD no Brasil giram em torno, principalmente, de três elementos: (i) concretizar o entendimento a respeito dos critérios para exercício do art. 20; (ii) a possibilidade (ou não) de a revisão ser realizada por pessoa humana e, em caso positivo, em quais situações (delimitação dos critérios); (iii) como garantir o direito de revisão nos casos em que o sistema é mais opaco em função da complexidade do algoritmo e, em caso de impossibilidade, como garantir medidas alternativas para o titular; (iv) como compatibilizar o direito de revisão do art. 20 da LGPD com a possível futura regulação de inteligência artificial que pode trazer um rol de direitos com a previsão de um novo direito de contestação, inclusive com participação humana (exemplo do que já acontece no Projeto de Lei 2338/2023).

6. Direitos de crianças e adolescentes

Resumo da recomendação:

Considerando que a LGPD estabelece **direitos específicos dos titulares crianças e adolescentes no artigo 14**, é fundamental que a ANPD, ao regulamentar o tópico de direitos dos titulares, também inclua previsões específicas sobre crianças e adolescentes.

Além disso, é importante ressaltar que, enquanto sujeitos de direitos, os mais jovens **dispõem não apenas de todos os direitos elencados no artigo 18, mas também direitos específicos** como, por exemplo, **o direito de transparência duplamente qualificado e um direito à minimização/necessidade qualificado**, que serão abordados a seguir.

Sendo assim, **como recomendações gerais para a discussão**, sugerimos:

- Que seja destinada uma seção específica do Guia sobre Direito dos Titulares para tratar exclusivamente sobre os direitos dos titulares crianças e adolescentes e suas especificidades.
- Que a ANPD construa um código de design apropriado para idade para produtos e serviços online, na toada do quanto prelecionado pelo artigo 14, de forma também a construir uma paridade regulatória com a tendência global de construção de diretrizes do tipo.

Compreendendo que o espaço da tomada de subsídios também abre margem para que sejam mapeados tópicos centrais da discussão que porventura não tenham sido incluídos, destacamos aqui a omissão relacionada aos direitos específicos dos titulares crianças e adolescentes.

Enquanto sujeitos de direitos, crianças e adolescentes possuem todos os direitos estabelecidos no artigo 18 da LGPD. No entanto, devido a sua condição peculiar de pessoas em desenvolvimento que detém proteção integral conferida pela Constituição Federal, **foram estabelecidos direitos específicos a esses titulares pelo artigo 14 da LGPD.** Tais direitos precisam ser tratados com a devida seriedade, além de terem como lastro central o princípio do melhor interesse, que é mencionado no caput deste artigo.

Isso porque, essa proteção integral:

“desempenha papel estruturante no sistema na medida em que o reconhece sob a ótica da integralidade, ou seja, o reconhecimento de todos

os direitos fundamentais inerentes à pessoa humana e, ainda, direitos especiais decorrentes da condição peculiar de pessoa em desenvolvimento, que se articulam, produzem e reproduzem de forma recíproca”¹⁶

Sendo assim, a partir da gramática da proteção integral oriunda da Convenção sobre os Direitos da Criança, que foi ratificada no contexto brasileiro e também abraçada pela Constituição Federal no artigo 227¹⁷, um regime de tutela “regular” não é suficiente. **Para que a referida proteção integral seja colocada em prática, é necessária a adoção de medidas de proteção complementares, específicas e qualificadas, se comparadas à de outros sujeitos menos vulneráveis.** Esse é o racional adotado por todo o ordenamento jurídico brasileiro quando se trata dos direitos dos mais jovens, que, por consequência, foi absorvido no texto do artigo 14 da LGPD. **Portanto, existem direitos específicos e qualificados previstos na legislação que se harmonizam com o arcabouço de proteção da infância e adolescência do país.**

Desse modo, o seu reconhecimento e identificação decorre de mera leitura da letra da lei, o que torna imprescindível que a Autoridade dê o tratamento adequado sobre o tema na regulamentação que se pretende dispor sobre os direitos dos Titulares.

→ Dever de Transparência Qualificado

Resumo da recomendação:

No caso de tratamento de dados pessoais de crianças e adolescentes, pela interpretação conjunta do parágrafo 2^a e 6^a do artigo 14, a LGPD **estabelece um dever de transparência qualificado que deve ser adotado desde o design do produto ou serviço.**

São deveres previstos na legislação que não demandam orientações complementares para sua exigibilidade imediata, mas que precisam ter uma abordagem adequada e destacada pela Autoridade, especialmente em relação ao direito de transparência ativa, de forma a diferenciar a obrigação de transparência geral da obrigação qualificada direcionada a crianças e adolescentes.

¹⁶ CUSTÓDIO, André Viana. Teoria da proteção integral: pressuposto para compreensão do direito da criança e do adolescente, p. 11.

¹⁷ Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Sendo assim, recomendamos que sejam aprofundadas no Guia sobre Direitos dos Titulares as diretrizes propostas:

- **No art. 14 §2º com o reforço da necessidade de transparência ativa:** “os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos
- **No art.14 §6ª com a necessidade de adequar o conteúdo para o entendimento das crianças:** “ deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Conforme destacado anteriormente, o princípio da transparência é estabelecido pelo artigo 6º, inciso VI, bem como as diretrizes para garantia do livre acesso, na sua dimensão ativa e passiva, estabelecidos no artigo 9º da LGPD. Nesse mesmo sentido, no artigo 18 da mesma lei são elencados os direitos dos titulares, dentre os quais, estão diferentes direitos relacionados à transparência, como o direito ao acesso e direito à informação.

Importante iniciar reforçando que as crianças e adolescentes, enquanto sujeitos de direitos, são titulares dos mesmos direitos que qualquer titular adulto, englobando, portanto, todos os acima apontados. No entanto, é importante salientar que o artigo 14 da LGPD, especialmente através dos parágrafos §2º e §6º, estabelece um direito à **transparência qualificado para esses titulares**.

Isso porque, o parágrafo 2º determina que, mesmo sem necessitar uma ação direta do titular criança ou adolescente, por exemplo, através de um pedido de acesso aos dados, **os controladores devem manter pública previamente, desde o design, as informações sobre os tipos de dados coletados e a forma de sua utilização, bem como os procedimentos para o exercício dos direitos do artigo 18.** Tal dispositivo, portanto, reforça e traz primeira qualificação sobre o dever de transparência ativa relacionado à crianças e adolescentes: **de que o mesmo deve ser implementado desde o design.**

Como forma de ilustrar a necessidade de transparência ativa e qualificada para o tratamento de dados de crianças e adolescentes, é interessante mencionar um

exemplo que ocorreu no contexto da Holanda. A Autoridade Holandesa de Proteção de Dados Pessoais (DPA) aplicou uma **multa de 750.000 euros ao TikTok** por violações à privacidade e proteção de dados pessoais de crianças e adolescentes¹⁸.

Dentre as principais justificativas, foi apontado o fato de que várias partes da instalação e utilização da aplicação, bem como sua política de privacidade estavam disponibilizadas apenas no idioma inglês. Desse modo, **ao não oferecer uma tradução para o holandês, língua nativa dos jovens em questão, a DPA considerou que o TikTok não forneceu uma explicação adequada sobre como a aplicação recolhe, processa e utiliza dados pessoais de crianças e adolescentes, incorrendo em patente violação dos seus direitos.**

É importante destacar também **que a própria ANPD já se pronunciou a respeito da necessidade dessa transparência qualificada para o tratamento de dados de crianças e adolescentes, através da Nota Técnica 6/2023/CGF/ANPD¹⁹.** Na oportunidade, a Autoridade analisou que durante o cadastro na plataforma do aplicativo TikTok (Bytedance Brasil Tecnologia Ltd), a finalidade para o tratamento que foi informada e colocada publicamente, em cumprimento ao §2º do artigo 14, foi considerada “genérica”. Portanto, segundo a própria autoridade, essa disposição legal preza por uma transparência ativa efetiva e qualificada e não apenas meramente protocolar:

“As finalidades, para menores de 18 anos, seriam as de “informar os algoritmos da Plataforma”, “realizar análise de dados e testar a Plataforma, visando garantir a sua estabilidade”, “para ajudar o TikTok a detectar e combater abusos, atividades prejudiciais, fraudes, spam e atividades ilegais na Plataforma; e para garantir e aprimorar a segurança e estabilidade da Plataforma”. **Primeiramente entende-se que a finalidade de “informar os algoritmos da Plataforma” é demasiadamente genérica.** Os algoritmos, na verdade, são os meios pelos quais os dados são tratados. **Dessa forma, tal finalidade não está de acordo com o art. 10, § 2º, que prevê a obrigatoriedade de transparência no tratamento de dados baseado em seu legítimo interesse.**”

Entendemos também que o dever de transparência ativa estabelecido pelo supramencionado parágrafo deve ser interpretado conjuntamente com o parágrafo

¹⁸https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en

¹⁹https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf

§6º do mesmo artigo 14. Sendo assim, todas as informações sobre o tratamento de dados de crianças e adolescentes **devem ser disponibilizados de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário**, sendo utilizadas, inclusive, recursos audiovisuais quando cabível, **para o adequado entendimento da criança**. O referido parágrafo, portanto, determina a dupla qualificação do dever de transparência para o tratamento de dados pessoais dos mais jovens.

O fundamento para essa dupla qualificação é pautado justamente pela doutrina da proteção integral e todo o arcabouço de proteção de crianças e adolescentes estabelecido pelo ordenamento jurídico brasileiro. Tais sujeitos estão em fase específica de desenvolvimento, o que justifica a necessidade de proporcionar-lhes cuidados especiais distintos dos concedidos aos adultos. Nesse sentido, essa atenção especial deve considerar a evolução gradual das suas habilidades ao longo do seu crescimento, fundamentada pela noção de autonomia progressiva²⁰.

Dependendo da faixa etária do público-alvo de um produto ou serviço online, as adequações a serem feitas serão diferentes, levando em consideração cada etapa peculiar de desenvolvimento dos usuários em questão. As adequações feitas para um usuário criança de 05 (cinco) anos, por exemplo, não vão ser as mesmas que para um usuário de adolescentes de 16 (dezesseis).

Na já mencionada Nota Técnica 6/2023/CGF/ANPD²¹, a Autoridade se pronunciou também sobre a diferença de tratamento não apenas entre crianças e adultos, mas também entre sujeitos com diferentes faixas etárias:

“As diferenças entre o tratamento de dados pessoais de crianças e adolescentes e o de adultos devem estar informadas na Política de Privacidade do TikTok, a fim de dar maior transparência e informação quanto ao processo de tratamento de dados pessoais, que varia de acordo com a faixa etária do titular.”

É importante ratificar que **as adequações atreladas à transparência qualificada desde o design é direito expressamente estabelecido pela legislação, ou seja,**

²⁰ <https://www.dataprivacybr.org/wp-content/uploads/2022/12/tomada-subsidios-infancia.pdf>

²¹ https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/tiktok-nota_tecnica_6_versao_publica_ret-1.pdf

já possui aplicabilidade prática e imediata. No entanto, recomendamos que a ANPD adote uma postura de **dar destaque e fornecer maiores diretrizes para que o assunto seja tratado com a seriedade necessária.**

Para tanto, urge que a Autoridade acompanhe a importante tendência mundial da elaboração de Códigos de Design apropriados para a idade, com o objetivo de produzir orientações voltadas para produtos e serviços online. Isso porque, apesar das crianças representarem 1 a cada 3 usuários da internet²², a mesma não foi pensada e desenhada para os mais jovens, o que acaba perpetuando características adultocêntricas que muitas vezes não respeitam sua autonomia e desenvolvimento progressivo.

Por isso, vários países vêm construindo, a partir de uma reflexão conjunta com base na Convenção sobre os Direitos da Criança²³ e na já mencionada doutrina da proteção integral, padrões protetivos de design para produtos e serviços online, especialmente ligados à privacidade e proteção de dados pessoais. Entre os seus principais objetivos, estão o de construir um ambiente mais seguro e protetivo para os jovens, no lugar de simplesmente fomentar afastamento das crianças e adolescentes do mundo digital como solução para os riscos envolvidos²⁴.

É nessa toada que o Information Commissioner's Office (ICO) do Reino Unido foi pioneiro ao lançar em 2020, o Age Appropriate Design Code²⁵. Esse código **estabelece 15 padrões de design apropriados à idade, adotando uma abordagem proporcional e baseada no risco, para serem implementados em serviços e produtos online que processem dados pessoais e possam ser acessados por crianças.** Dentre os pontos principais abordados, estão disposições específicas sobre transparência, que coadunam com a importância da transparência duplamente qualificada estabelecida na LGPD:

²² <https://criancaeconsumo.org.br/wp-content/uploads/2021/11/sowc-2017-eng.pdf>

²³ https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm

²⁴

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-co-de-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/>

²⁵

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-co-de-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/>

“Transparência: é a garantia dada aos(às) titulares de que terão **informações claras, precisas e facilmente acessíveis sobre a realização do tratamento** e os respectivos agentes de tratamento, observados os segredos comercial e industrial;”²⁶

Cenário semelhante é o perpetrado pela Data Protection Commission (DPC) da Irlanda. O seu Código de Design denominado “**Fundamentals for a child-oriented approach to data processing**”, também estabelece diretrizes específicas sobre transparência:

“As informações de privacidade devem **ser fornecidas de forma concisa, transparente, compreensível e acessível, utilizando linguagem clara e simples que seja compreensível e adequada à idade da criança**. Além de considerar a adequação da linguagem em si, **as crianças podem precisar de informações em diferentes formatos e em momentos diferentes na jornada do usuário** (por exemplo, aviso imediato e funções de bate-papo instantâneo) para cumprir esse requisito”.

Merece menção também o “California Age-Appropriate Design Code”²⁷, aprovado no legislativo do estado que entrou em vigor recentemente, em 2024, e foi fruto de uma intensa campanha e incidência realizada pelas organizações da sociedade civil²⁸ de proteção da infância no país. O texto, apresentado através do Assembly Bill No. 2273 também apresenta várias diretrizes específicas de proteção que vão desde a obrigatoriedade de elaboração de Relatório de Impacto para casos do tratamento de dados de crianças e adolescentes, até orientações sobre mais específicas sobre transparência ativa e passiva.

Por fim, além dos exemplos de códigos mencionados e atualmente em vigor em vários países do mundo, destaque-se também que, no âmbito da Estratégia “Better Internet for Kids” (BIK+)²⁹, estão ocorrendo diversas movimentações sobre o tema na União Europeia. Mais recentemente, inclusive, foi designado um grupo de trabalho para a construção de um “Código de conduta abrangente da UE sobre design adequado à idade”³⁰, de aplicabilidade conjunta para todos os países membros.

²⁶

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/4-transparency/>

²⁷ https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

²⁸ <https://californiaaadcd.com/>

²⁹ <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>

³⁰ <https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design>

Diante dos pontos expostos, é importante que na seção específica sobre crianças e adolescentes do Guia de Direitos dos Titulares, a ANPD ressalte que independentemente de qualquer orientação complementar, o direito à transparência duplamente qualificado é expresso na LGPD, devendo ser implementados, desde o design, para qualquer tratamento de dados pessoais de crianças ou adolescentes. Como forma de dar destaque e detalhamento à essa interpretação, recomendamos também que sejam fornecidos diretrizes mais robustas

Aliado a isso, recomenda-se que a ANPD deve colocar dentro das suas prioridades o desenvolvimento de uma agenda que regule o tema de maneira mais específica, incluindo aqui a paridade regulatória com outros países, a partir do desenvolvimento de um Código de Design apropriado à idade direcionado a produtos e serviços online.

→ Direito à Minimização Qualificado

Resumo da recomendação:

No caso de tratamento de dados pessoais de crianças e adolescentes, pela interpretação do parágrafo 4^a do artigo 14, a LGPD estabelece **um direito à minimização qualificado**:

Sendo assim, recomendamos que sejam aprofundadas no Guia sobre Direitos dos Titulares as diretrizes propostas:

- **No art. 14 §4^a com a necessidade de um dever de minimização qualificado:** “Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.”

O inciso III do artigo 6º da LGPD apresenta o princípio da necessidade como sendo a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”. Ou seja, a não realização da coleta de dados é a regra, sendo excetuada quando existir uma finalidade evidente e proporcional que justifique a operação de tratamento, condição consubstanciada pelo dever de minimização.

Com base em tal raciocínio, enquanto sujeitos de direitos, as crianças e adolescentes também devem ter seus dados tratados respaldados pelo princípio da necessidade, mas não apenas. Por serem indivíduos detentores de proteção integral garantida pela Constituição Federal, além de cumprir com a disposição acima mencionada, o §4^a do artigo 14, **estabelece um direito qualificado à minimização de dados para titulares crianças e adolescentes.**

Isso porque, tal dispositivo determina expressamente que a participação dos mais jovens em jogos, aplicações de internet ou quaisquer outras atividades **não pode ser condicionada ao fornecimento de informações que não sejam estritamente necessárias à atividade.**

Dessa forma, por exemplo, uma criança ou adolescente que for acessar uma plataforma de jogos online de “corrida”, não pode ser perguntado informações sobre sua religião como condição para o seu acesso à plataforma. Isso porque, não há qualquer relação contextual entre a atividade em questão e as informações solicitadas. O “contexto”, portanto, é um dos elementos centrais de análise para entender o direito à minimização qualificado para o tratamento de dados de crianças e adolescentes.

Nessa mesma toada, **e aqui reforçando a importância de que a ANPD desenvolva um Código de Design Adequado à idade**, o já mencionado Age Appropriate Design Code do ICO, também estabelece premissas sobre esse tema:

“Colete e retenha apenas a quantidade mínima de dados pessoais necessários para fornecer os elementos do seu serviço nos quais uma criança está ativamente e conscientemente envolvida.”³¹

Adicionalmente, o código ainda estabelece **a possibilidade da própria criança escolher os elementos que deseja ativar, de forma consciente e granulada**, apontando a necessidade de dar “às crianças escolhas separadas sobre quais elementos elas desejam ativar.”³²

³¹

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-of-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/8-data-minimisation/>

³²

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-co>

É importante mencionar que essa disposição, assim como todas as diretrizes impostas pelo artigo 14 da LGPD, também independe de qualquer complementação adicional para sua exigibilidade. É um direito dos titulares crianças e adolescentes estabelecido em lei e, por conseguinte, deve, desde já, estar sendo cumprido.

No entanto, reforçamos a importância de que a ANPD trate especificamente sobre o assunto em um Guia sobre Direitos dos Titulares para não apenas trazer caminhos mais concretos e robustos para a sua aplicabilidade, mas também destacar a importância do seu cumprimento.