Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Coordenação de Normatização 1

Nota Técnica nº 12/2025/CON1/CGN/ANPD

1. INTERESSADO

1.1. COORDENAÇÃO-GERAL DE NORMATIZAÇÃO

2. ASSUNTO

2.1. Consolidação das contribuições recebidas na Tomada de Subsídios.

3. REFERÊNCIAS

3.1. Processo SEI/ANPD nº 00261.006920/2024-46.

4. RELATÓRIO

4.1. Trata-se do projeto que visa à Regulamentação do Item 7 da Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2025-2026, aprovada pela Resolução nº 23, de 09 de dezembro de 2024 (SEI/ANPD nº 0160131) - Inteligência Artificial.

4.2. Conforme Termo de Abertura de Projeto (TAP) (SEI/ANPD nº 0118175),

> para além da determinação legal de regulamentar o disposto na LGPD, em especial o disposto no art. 20 da Lei, que trata do direito do titular de solicitar revisão de decisões automatizadas, a ANPD pode endereçar melhor o tema por meio de documentos orientativos, como guias e estudos técnicos, uma vez que o assunto está sendo bastante utilizado pelos agentes de tratamento, frente à vulnerabilidade do titular que não possui conhecimento avançado sobre o tema.

4.3. Assim é que, a fim de verificar a perspectiva da sociedade sobre o tema – incluindo aí titulares, agentes de tratamento e diferente setores e modelos de negócio, esta Coordenação-Geral optou por realizar Tomada de Subsídios, nos termos dos arts. 18 a 22 da Portaria nº 16, de 8 de julho de

2021, que aprova o processo de regulamentação no âmbito da Autoridade. *In verbis*:

> Art. 18. A Tomada de Subsídios visa obter insumos para o processo de regulamentação e pode ser realizada a qualquer momento, a critério da Equipe de Projeto. § 1º A Tomada de Subsídios não representa o posicionamento final da ANPD.

4.4. Nesse contexto, foi comunicada a referida Tomada, por meio do Despacho SEI/ANPD º0154149, a ser realizada entre os dias 6 de novembro e 5 de dezembro de 2024, com prorrogação por meio de novo Despacho (SEI/ANPD nº 0157773) até o dia 24 de janeiro de 2025.

4.5. Foram elaboradas 15 perguntas, divididas em 5 (cinco) blocos, da seguinte forma (SEI/ANPD nº 0154546):

a) Bloco 1 - Princípios da LGPD
b) Bloco 2 - Hipóteses Legais
c) Bloco 3 - Direitos dos Titulares
d) Bloco 4 - Boas Práticas e Governança

4.6. Foi, então, publicada a Consulta à Sociedade em formato de Tomada de Subsídios e disponibilizada para contribuições por meio da Plataforma Participa Mais Brasil.

4.7. É o Relatório.

5. ANÁLISE

Das Contribuições Recebidas

5.1. No âmbito da Plataforma foram recebidas 99 (noventa e nove) contribuições e 25 (vinte e cinco) contribuições em formato .pdf por meio do correio eletrônico institucional normatizacao@anpd.gov.br. Estas se deram pela justificativa que o espaço para preenchimento disponível no Opine Aqui da Plataforma Participa Mais Brasil não era disponível para submissão do conteúdo integral da contribuição. Tais considerações foram devidamente analisadas pela Equipe de Projeto e juntadas ao processo, conforme Certidão (SEI/ANPD nº 0178829). Ressalte-se que as contribuições em formato PDF foram anexadas ao processo em epígrafe (SEI/ANPD nº 0173508), assim como as contribuições provenientes da Plataforma Participa Mais Brasil (SEI/ANPD nº 0173510).

5.2. Assim, de um total de 124 (cento e vinte e quatro) participantes, aproximadamente 56% (70 participantes) declararam ter respondido em nome de algum agente de tratamento. Por outro lado, 44% (54 participantes) não se

identificaram como representantes de qualquer agente, conforme ilustrado no Gráfico 01:

Gráfico 01 - Pessoas que responderam ao questionário em nome de algum agente de tratamento de dados pessoais.

5.3. Em relação à origem das contribuições, houve 9 (7%) contribuições de origem internacional, enquanto outras 115 (93%) foram de origem nacional, vide Gráfico 02. Os participantes nacionais representaram as 5 (cinco) regiões do Brasil havendo maior expressividade na região Sudeste (61%), seguida pela região Centro-oeste (16%), região Sul (4%) e região Nordeste (4%), 15% dos participantes não identificaram sua região de origem, conforme pode ser visto no Gráfico 03. da seguinte forma:

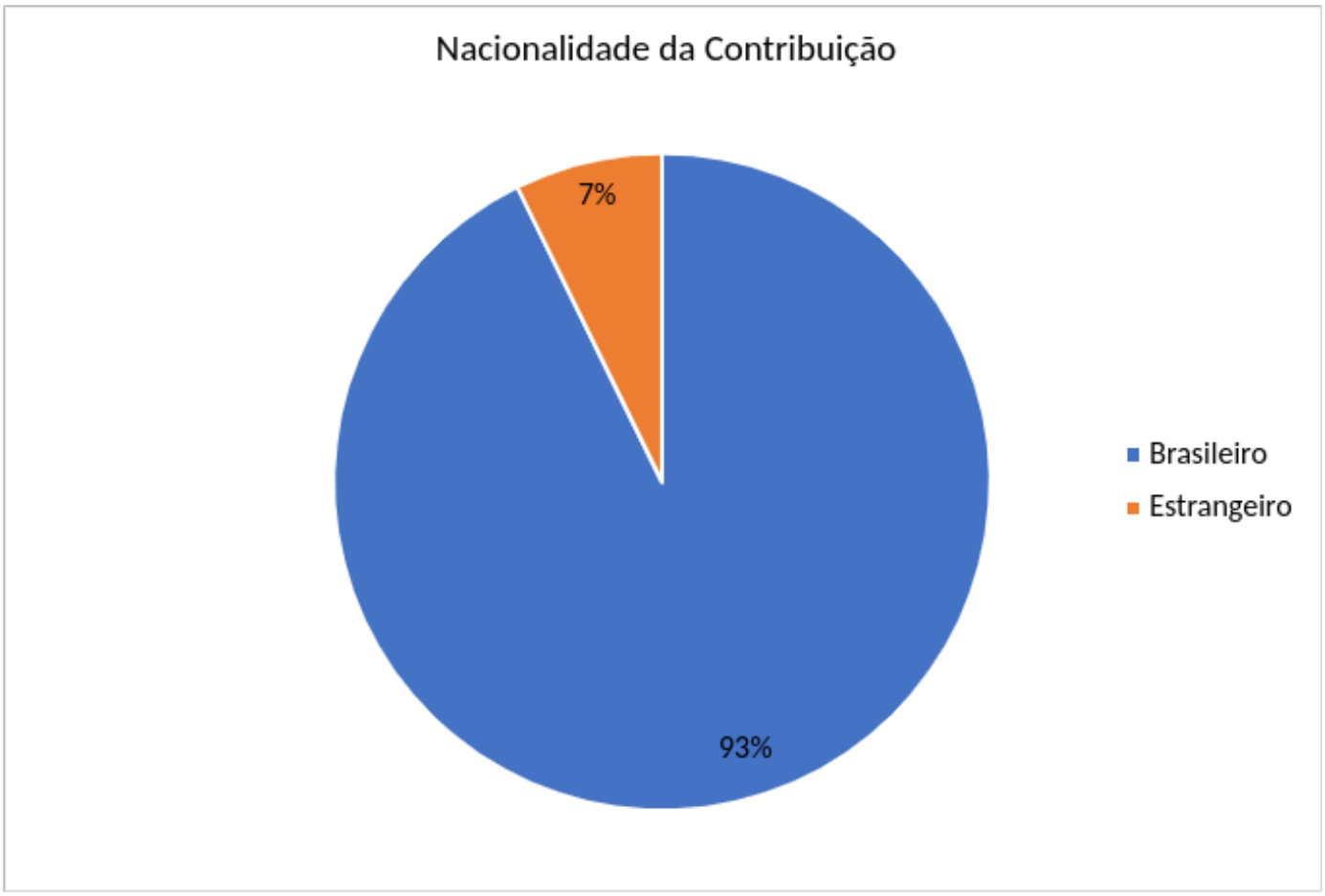

Gráfico 02 - Contribuições por nacionalidade

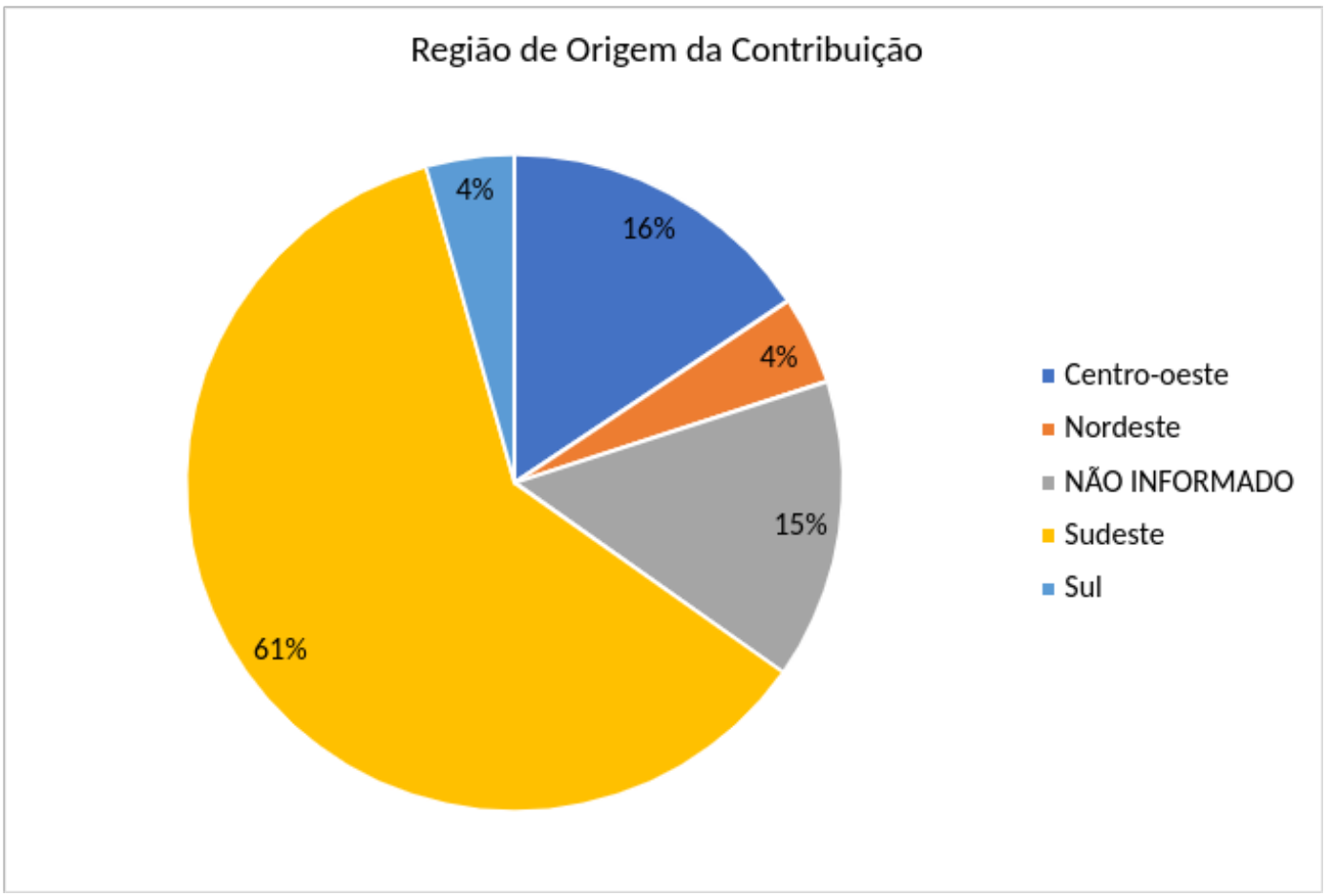

Gráfico 03 - Contribuições por região do Brasil

5.4. Essa tomada de subsídios contou com contribuições de pessoas físicas (50%), empresas da iniciativa privada (25%), organizações do terceiro setor (22%) e instituições públicas (3%), vide Gráfico 4. Dentre as pessoas físicas há 18 advogados (33%), 3 professores (6%), 3 designers (6%), e 2 analistas e desenvolvedores de sistemas (4%), 5 participantes (9%) informaram outras profissões, e 23 participantes não informaram (42%), conforme pode ser visto no Gráfico 5.

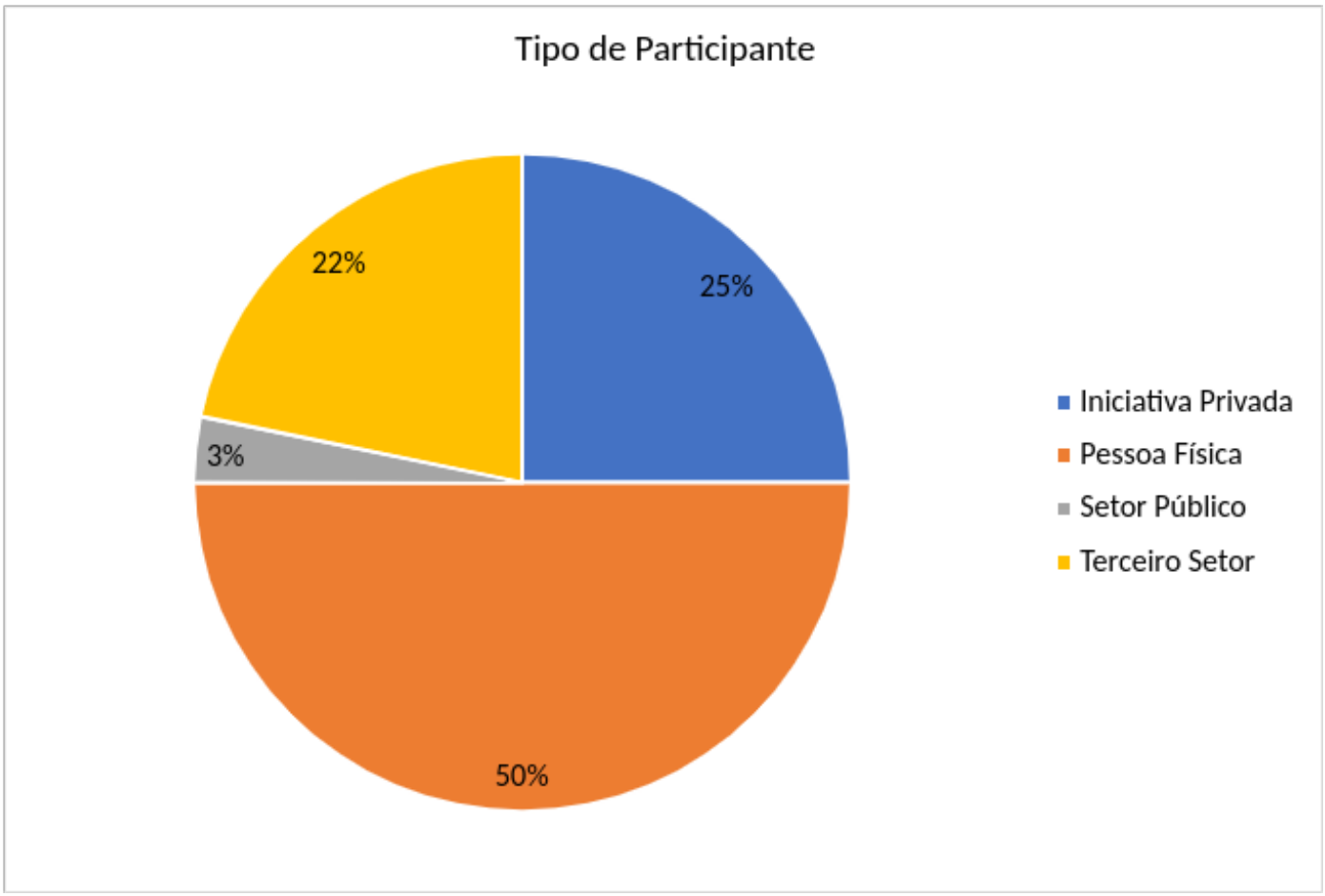

Gráfico 04 – Tipo do Participante

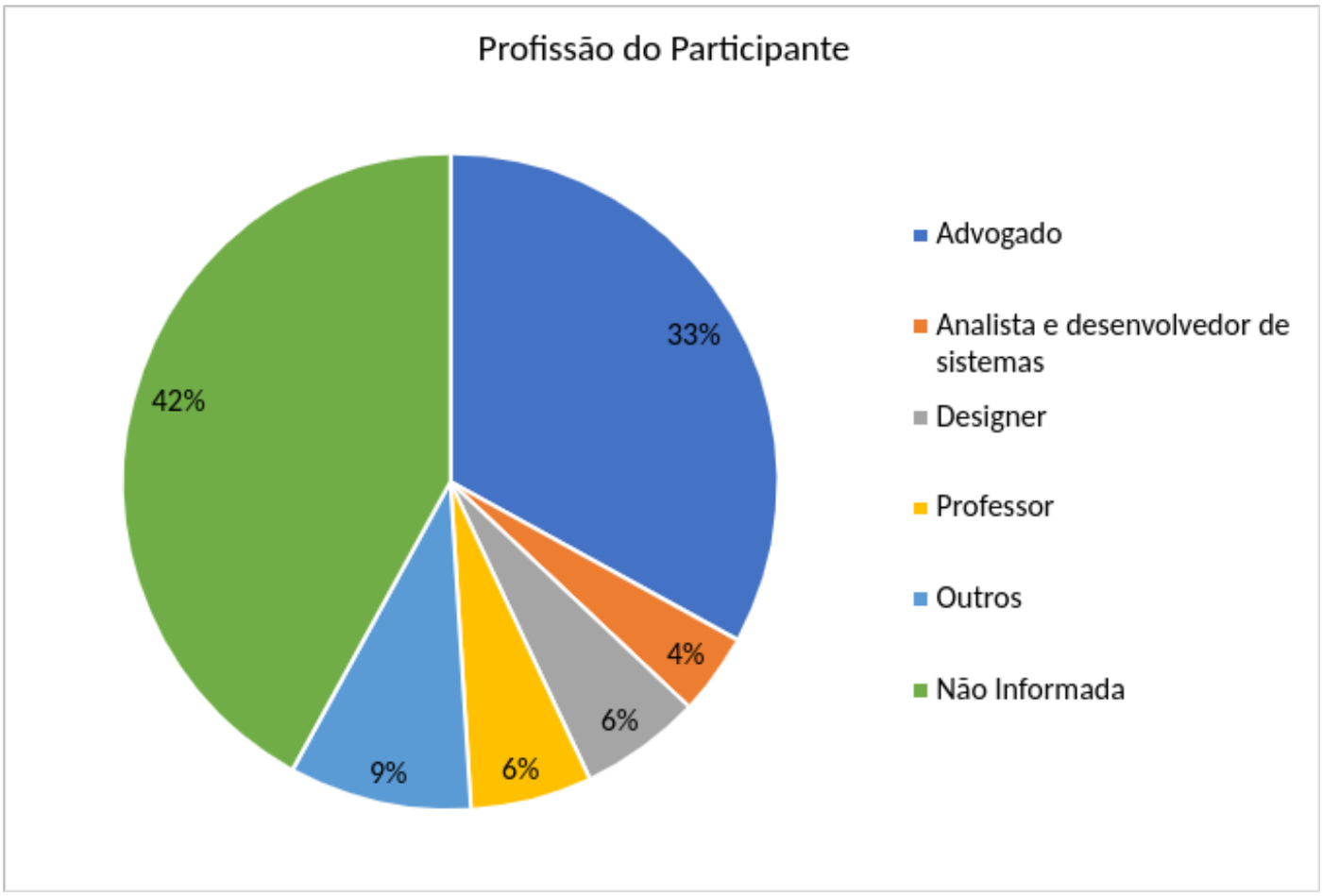

Gráfico 05 - Profissão do participante

Metodologis da Análise

5.5. As análises foram realizadas, mesmo não se tratando de Consulta Pública de normativo, nos termos da legislação aplicável, procedendo-se de forma similar com objetivo de favorecer a transparência e a participação social.

5.6. Nesse sentido, foi realizada a eliminação das contribuições repetitivas, em conformidade com o parágrafo único do art. 19 do Decreto nº 10.411/2020 e com o § 6º do art. 62, do Regimento Interno da ANPD (RIANPD), estabelecido pela Portaria nº 1, de 8 de março de 2021.

5.7. Neste ensejo, cabe destacar que o juízo de admissibilidade de tais contribuições levou em consideração a pertinência com o escopo Projeto – Item 7 da Agenda Regulatória - e o teor duplicado com as outrora analisadas.

5.8. As contribuições foram consolidadas em 15 (quinze) arquivos, que correspondem a cada questão submetida à Tomada de Subsídios. Tanto as contribuições submetidas por e-mail, em formato .pdf, quanto as contribuições submetidas no âmbito da Plataforma foram consolidadas nos mesmos documentos.

Consolidação das contribuições: convergências e divergências

5.9. Conforme se verá a seguir, a análise das contribuições nesta

Nota Técnica foram consolidadas de modo a delinear um cenário no qual se verificam pontos de consenso entre as diversas contribuições, mas, também, divergências. Assim, optou-se aqui por destacar tais questões em formato de *bullets*, a fim de facilitar à equipe de projeto a análise de mérito das contribuições e, com isso, eventualmente utilizá-las como parâmetros na elaboração dos produtos relativos ao projeto de regulamentação.

5.10. As contribuições provenientes da Plataforma Participa+Brasil também estão disponíveis e podem ser acessadas pelo SEI/ANPD nº 0173510.

5.11. Sublinha-se, ainda, que as contribuições encaminhadas por e-mail foram anexadas ao Processo em epígrafe; contudo, algumas não foram disponibilizadas em formato público, a pedido dos contribuintes, em razão de segredos de ordem comercial ou industrial. Os eventuais pedidos de acesso a tais documentos serão analisados individualmente por esta Autoridade.

5.12. A seguir, tem-se cada uma das 15 (quinze) questões, com as respectivas convergências e divergências.

BLOCO I - PRINCÍPIOS DA LGPD

Pergunta 1 - Como compatibilizar o treinamento de sistemas de IA com o princípio da necessidade, haja vista se tratar de atividade que, muitas vezes, demanda o tratamento de quantidades massivas de dados pessoais? Quais salvaguardas podem ser adotadas de modo a assegurar a observância desse princípio e viabilizar o desenvolvimento adequado de sistemas de IA, considerando, ainda, a importância da qualidade e diversidade dos dados utilizados?

5.13. As contribuições relativas ao primeiro questionamento trataram dos meios sobre como compatibilizar o treinamento de sistemas de IA com o princípio da necessidade, considerando a demanda por grandes volumes de dados pessoais. As contribuições convergem em alguns pontos principais, ao mesmo tempo que apresentam divergências em relação à interpretação e à aplicação do princípio da necessidade.

<u>Pontos de convergência</u>

5.14. Dentre os pontos que convergem a semelhante análise do princípio da necessidade estão os seguintes:

- **Necessidade de equilibrar o uso de dados e a proteção da privacidade:** há um consenso de que é importante encontrar um ponto de equilíbrio entre a utilização de dados, muitas vezes em grande volume, para o treinamento eficaz de sistemas de IA, e a necessidade de proteger a privacidade e os dados pessoais dos indivíduos. A exemplo, tem-se contribuição que afirma que os conceitos de minimização de dados e proporcionalidade, em especial no contexto de Inteligência Artificial Generativa, não significam que apenas pequenos volumes de dados

sejam legítimos para o treinamento de sistemas. Em vez disso, a minimização de dados nesse contexto deve ser entendida como a limitação da quantidade de dados pessoais utilizados ao que é necessário, permitindo, ao mesmo tempo, o volume adequado de dados para o desenvolvimento de um sistema de alta qualidade e uma experiência satisfatória para o usuário. Em outras palavras, "minimização de dados" não pode significar usar menos dados do que o necessário e adequado para garantir a qualidade de um sistema de IA Generativa.

- **Importância da qualidade e diversidade dos dados:** as contribuições convergiram para o fato de que a eficácia dos sistemas de IA depende da qualidade e da diversidade das informações utilizadas no treinamento. Assim, um conjunto de dados diversificado pode ser fundamental para mitigar vieses e garantir que o sistema seja suficientemente treinado e testado. Contudo, há contribuições que ressaltam a importância de finalidades legais e claras. Nesse sentido, propõe-se evitar excessos de volume, promover a identificação de dados sensíveis, priorizar o uso de dados anonimizados e garantir a legitimidade da origem dos dados. Nesses termos, há contribuição que assevera que a mera possibilidade de dados serem usados no futuro para o treinamento de sistemas de IA não se caracteriza como situação compatível com o princípio da necessidade para justificar o armazenamento de dados pessoais, e da mesma forma não pode ser usado para legitimar de forma retroativa tratamentos de dados ilicitamente mantidos.

- **Adoção de salvaguardas para a mitigação de riscos:** são diversas as salvaguardas sugeridas a fim de garantir a conformidade com o princípio da necessidade e, assim, evitar o uso excessivo ou inadequado de dados pessoais. Tais salvaguardas incluem:

  a) Anonimização, pseudonimização e dados sintéticos: a utilização dessas técnicas é fundamental, nos termos das contribuições analisadas, para reduzir a dependência de dados pessoais, em especial nas fases de desenvolvimento e treinamento.

  b) *Privacy by design:* a incorporação de medidas de proteção de dados desde a concepção do sistema e assim identificar as informações que serão realmente necessárias para o atingimento da finalidade, nos termos de alguns frameworks de respaldo, tais como o NIST Privacy Framework e a ISO/IEC 27701.

  c) Avaliação de impacto: as contribuições apontam para a

realização de análises de impacto à proteção de dados pessoais para a identificação de riscos e mitigação de dados à privacidade, nos termos do art. 38 da LGPD, mencionando, ainda, a necessidade específica de avaliação de impacto algorítmico.

d) Também foi apontada a necessidade de relatórios de avaliação de impacto especificamente para os casos em que há tratamento de dados pessoais de crianças e adolescentes.

e) Governança de dados: a definição de políticas claras para a coleta, uso, retenção e descarte de dados pessoais. Houve, ainda, contribuição que reputou como fundamental que algumas tecnologias, como modelos de *machine learning* com potencial de ocasionar risco ao titular nas decisões tomadas devem ser monitoradas e acompanhadas por um Comitê de Governança de IA definindo *guardrails* diferentes para cada nível de risco, controles esses que podem implicar na deliberação da não aprovação de uso da referida IA.

f) Transparência: o titular deve ser informado sobre a origem, forma de coleta, finalidade e procedimentos de tratamento de seus dados pessoais. Nesse sentido, as contribuições apontam o seguinte, em resumo:

g) Modelos e conjunto de dados devem ser acompanhados de documentação que tenha informação detalhada sobre: estrutura, manutenção e finalidade de uso. Isso proporciona transparência, facilita fiscalização e auxilia na conformidade regulatória.

h) Transparência e explicabilidade devem ser promovidas a partir de meios de comunicação acessíveis ao titular.

i) Controle de acesso: implementação de medidas para restringir o acesso aos dados de treinamento. Há contribuição que sugere o uso de dados anonimizados ou sintéticos para experimentação inicial, serviços de redução de dados pessoais (*PII redaction services*), revisões éticas e controle de acesso. Também ressalta que as salvaguardas devem ser concentradas nas fases de coleta e aplicação do sistema, e não nas etapas de desenvolvimento, embora mencione o controle de acesso a base de dados de treino.

- **Necessidade de uma finalidade clara e justificada:** a coleta e a retenção de dados devem ser justificadas com base em finalidades legais e claramente definidas. Assim, a mera possibilidade de uso futuro dos dados não é suficiente para justificar o armazenamento. Ou seja, segundo uma contribuição, tal situação não é compatível com o

princípio da necessidade para justificar o armazenamento de dados pessoais, e da mesma forma, não pode ser utilizado para legitimar de forma retroativa tratamentos de dados ilicitamente mantidos.

- **Revisões periódicas e monitoramento:** realização de revisões periódicas dos dados tratados e monitoramento do acesso e utilização dos dados em tempo real, principalmente para fins de rastreabilidade.

Pontos de divergência

5.15. Acerca dos pontos divergentes, podem ser mencionados os seguintes:

- Interpretação do princípio da necessidade: há distintas interpretações sobre como o princípio da necessidade se aplica ao treinamento de IA.

Visão restritiva: alguns defendem uma interpretação mais estrita, enfatizando a minimização do uso de dados pessoais e a necessidade de limitar a coleta ao mínimo necessário. Argumentam que o princípio da necessidade não é compatível com o tratamento em larga escala para o treinamento de soluções de IA.

Visão pragmática: outros defendem uma interpretação mais flexível, reconhecendo que o treinamento de IA muitas vezes demanda grandes volumes de dados para garantir a qualidade e eficácia dos sistemas. Argumentam que o princípio da necessidade não proíbe o uso de grandes volumes de dados, desde que haja salvaguardas adequadas e uma finalidade legítima. Alguns propõem uma reinterpretação do princípio da necessidade para permitir a coleta de mais dados em determinadas circunstâncias. Assim, segundo uma variedade de contribuições, o princípio da necessidade acaba por esbarrar no contexto de treinamento de IA de larga escala, no qual se pressupõe quantidades massivas de dados para treinamento. Ainda, uma das contribuições afirma que *o princípio não é incompatível com o tratamento em larga escala para o treinamento de soluções de IA. A limitação deve ser guiada por uma análise criteriosa dos dados realmente necessários e pelo uso de medidas técnicas que restrinjam a coleta a dados pertinentes*. Finalmente, outra contribuição ressalta que o princípio da necessidade não se confunde com volumetria de dados, ou seja, como salvaguarda é importante garantir o uso de dados mínimos necessários, o que não se confunde com baixa volumetria, mas, que haja finalidade definida, afastando, assim, o uso excessivo de dados.

- **Obrigatoriedade de certas salvaguardas:** há divergências sobre se certas salvaguardas, como o uso de dados anonimizados ou sintéticos, devem

ser obrigatórias. Algumas contribuições defendem que a decisão sobre quais salvaguardas adotar deve ser deixada a critério de cada controlador, de acordo com sua atividade e os riscos envolvidos. Além da anonimização, são mencionadas outras salvaguardas, como a (i) criptografia; a sobrescrição de identificadores individuais, substituindo-os por valores fictícios ou irreversíveis, impossibilitando a recuperação dos dados originais; iii) a remoção de identificadores diretos, retirando informações que possibilitam a identificação de um indivíduo ou até a tokenização, substituindo dados identificáveis por tokens únicos e gerados aleatoriamente; iv) a utilização de dados sintéticos; v) ruídos e vi) avaliações de impacto a serem realizadas quando presente o alto risco. Finalmente, pode-se citar as contribuições que afirmam serem as boas práticas e as salvaguardas já implementadas pelos agentes de tratamento suficientes e aplicáveis aos sistemas de IA.

- **Foco das salvaguardas:** algumas contribuições argumentam que as salvaguardas devem ser concentradas nas fases de coleta e aplicação do sistema, e não nas etapas de desenvolvimento. Ressaltam que a implementação de salvaguardas pode ser desafiadora para startups e pequenas empresas no cenário nacional, que frequentemente possuem recursos limitados.

- **Âmbito da LGPD:** há contribuições que apontam para que as diretrizes da LGPD sejam observadas no desenvolvimento de sistemas de IA somente quando envolver dados pessoais, pois em alguns modelos sequer há o tratamento desses dados. Afirmam, ainda, que acomodar satisfatoriamente o treinamento de sistemas de IA que demandam grande quantidade de dados no bojo normativo da LGPD em sua forma corrente é impraticável. Por outro lado, há contribuições que defendem que previamente ao tratamento de grandes quantidades de dados pessoais, as organizações devem realizar uma avaliação de impacto à proteção de dados, nos termos do art. 38 da LGPD. Além disso, é importante demonstrar que o volume de dados é tecnicamente justificável em função das especificidades do projeto. A organização, assim, deve documentar essa justificativa, conforme o princípio da prestação de contas previsto no art. 6, X, da LGPD.

5.16. Assim, em resumo, verifica-se que as contribuições refletem a complexidade de compatibilizar o desenvolvimento de sistemas de IA com a proteção de dados pessoais. Embora haja um consenso sobre a necessidade de encontrar um equilíbrio e adotar salvaguardas, existem diferentes visões sobre como interpretar e aplicar o princípio da necessidade, bem como sobre quais medidas de proteção devem ser obrigatórias.

Pergunta 2 - Quais boas práticas e salvaguardas devem ser observadas visando

à definição de finalidades específicas e à divulgação de informações claras e adequadas e facilmente acessíveis aos titulares a respeito do tratamento de dados pessoais realizado durante o desenvolvimento e uso de sistemas de IA?

5.17. As contribuições à pergunta 2 apresentam diversos pontos sobre as boas práticas e as salvaguardas a serem observadas na definição de finalidades específicas e na divulgação de informações claras sobre o tratamento de dados pessoais no contexto dos sistemas de IA.

Pontos de convergência

5.18. Dentre os pontos que convergem a semelhante análise do princípio da necessidade estão os seguintes:

- **Transparência e informação clara:** há um consenso sobre a importância da transparência e da necessidade de fornecer informações claras, acessíveis e compreensíveis aos titulares dos dados sobre como seus dados são coletados, usados e processados por sistemas de IA. Isso inclui o uso de linguagem simples, formatos multimodais (como infográficos) e a contextualização das informações. A transparência deve garantir que os indivíduos compreendam como seus dados estão sendo utilizados e assegurar que possam exercer seus direitos. Por sua vez, há contribuição que propõe clareza e especificidade no propósito detalhado, com finalidades previamente definidas. Sugere a delimitação temporal para retenção de dados conforme a finalidade, o uso de linguagem clara e acessível nas políticas de privacidade e o mapeamento dos riscos através de relatórios de impacto. Finalmente, ressalta a importância de auditoria e monitoramento, bem como a comunicação através de informações nas políticas de privacidade e canais de comunicação.
- **Definição clara de finalidades:** a definição clara e específica das finalidades do tratamento de dados desde o início do desenvolvimento de sistemas de IA é essencial. As finalidades devem ser legítimas, específicas, transparentes e alinhadas com a LGPD. Em sistemas de IA de propósito geral, é importante mapear as capacidades do sistema que geram maiores riscos e descrever propósitos excluídos e condições de uso no design do sistema.
- **Avaliação de riscos:** a implementação de um sistema abrangente de avaliação de riscos é crucial para identificar riscos potenciais e determinar se os insumos ou resultados de IA constituem dados pessoais. O Relatório de Impacto à Proteção de Dados (RIPD) é frequentemente mencionado como um instrumento importante para essa avaliação.
- **Governança e monitoramento:** protocolos robustos de governança de

dados, monitoramento e avaliações contínuas são necessários para garantir a conformidade e a eficácia das medidas de proteção. Auditorias regulares também são recomendadas, sendo sugeridas: (i) a implementação de medidas baseadas na metodologia PDCA, de forma que haja auditoria periódica nos processos adotados; (ii) manutenção de logs de tratamento de dados para registrar operações realizadas, assegurando rastreabilidade e facilitando auditorias regulares.

- **Canais de atendimento:** a implementação de canais de atendimento acessíveis e eficientes é fundamental para garantir que os titulares possam exercer seus direitos, como acesso, correção, exclusão e portabilidade dos dados. A transparência deve ser promovida por meio de avisos de privacidade claros, acessíveis e disponibilizados em canais apropriados.

- **Políticas de privacidade:** As políticas de privacidade são um meio importante de comunicar informações sobre o tratamento de dados em sistemas de IA. As informações devem ser claras, acessíveis e adaptadas a diferentes públicos.

- ***Privacy by design e default:*** A aplicação dos princípios de *privacy by design* e *privacy by default* desde a concepção dos sistemas é amplamente recomendada.

<u>Pontos de divergência</u>

5.19. Sobre os principais pontos de divergência, têm-se:

- **Nível de especificidade da informação:** há divergências sobre o nível de detalhe que deve ser divulgado aos titulares. Algumas contribuições enfatizam a importância de fornecer informações "em camadas", adaptadas ao nível de interesse do titular. Outras ressaltam que a divulgação excessiva de detalhes técnicos pode comprometer as medidas de proteção. Nos termos das contribuições, a ANPD deve valorizar a boa-fé dos agentes de tratamento ao delinearem suas medidas de transparência, considerando as técnicas razoáveis disponíveis e os recursos do controlador para não onerar excessivamente a utilização responsável de IA.

- **Obrigatoriedade de informar sobre o uso de IA:** existe uma divergência sobre se a LGPD exige explicitamente que os titulares sejam informados sobre o uso de sistemas de IA. Algumas contribuições argumentam que o foco deve estar na transparência sobre as finalidades e efeitos do tratamento dos dados pessoais, e não nos meios tecnológicos utilizados. A mesma contribuição afirma que a transparência deve ser balanceada com a necessidade de proteger informações sensíveis sobre mecanismos

de segurança e proteção de conteúdo, especialmente considerando que a divulgação excessiva de detalhes técnicos pode comprometer a eficácia das medidas de proteção à propriedade intelectual.

- **Necessidade de documentação específica:** há opiniões divergentes sobre a necessidade de criar documentação específica para comunicar o tratamento de dados em sistemas de IA. Algumas contribuições sugerem que as políticas de privacidade existentes podem ser suficientes, com o uso de links para informações adicionais. Outras defendem a criação de uma "Política de Inteligência Artificial" específica. Há contribuição, por exemplo, que recomenda incluir informações obre o tratamento de dados pessoais em sistemas de IA nas políticas de privacidade, usando links para informações adicionais. Contudo, defende que as finalidades de IA sejam descritas nas políticas de privacidade já existentes, evitando obrigatoriedades de documentações específicas.

- **Transparência em projetos de pesquisa:** nesse sentido, uma contribuição menciona o CNIL, que identifica três cenários para o tratamento de dados em IA: soluções especialistas, pesquisa científica e soluções de propósito geral1. em projetos de pesquisa, há um consenso de que a transparência pode ser progressiva, começando com informações gerais e evoluindo conforme os objetivos se concretizam. No entanto, há diferentes visões sobre como equilibrar a necessidade de transparência com a natureza exploratória da pesquisa.

- **Padrões e normas:** há diferentes visões sobre quais padrões e normas devem ser seguidos. Algumas contribuições sugerem o uso de frameworks como os do NIST ou ISO sobre governança de sistemas de IA. Outras mencionam a aplicação de normas como a ISO/IEC 27701, que complementam os requisitos da LGPD. Há, ainda, contribuições que afirmam que as boas práticas e salvaguardas não precisam diferir dos padrões previamente adotados, pois seriam igualmente aplicáveis aos sistemas de IA. Por outro lado, há contribuições que recomendam o uso de documentos explicativos, como relatórios técnicos, para fornecer maior clareza sobre os modelos de IA, incluindo informações sobre sua construção, avaliação, limitações, tipos de dados usados no treinamento e medidas de mitigação de riscos.

Pergunta 3 - Como compatibilizar os princípios da finalidade e da transparência com o uso de sistemas de IA de propósito geral, isto é, sistemas que possam realizar uma ampla variedade de tarefas distintas e servir a diferentes finalidades?

5.20. As respostas à Pergunta 3 trouxeram luz a questões sobre os princípios da finalidade e da transparência relacionadas à aplicação de IA de propósito geral, abordando temas como avaliação de risco, definição de

finalidade, medidas de salvaguarda e transparência, etc. Como segue, foram identificados os seguintes pontos de convergência e divergência:

Pontos de convergência

- **Avaliação de risco:** Foi ressaltada a mitigação de riscos e a proteção de direitos, sem restringir a inovação. Citadas, ainda, as avaliações de impacto ético e algorítmico.

- **Revisão periódica:** Há contribuições convergindo para a necessidade de revisão periódica e contínua, além de governança adaptativa, estabelecendo processos de revisão contínua das finalidades e mecanismos de atualização das informações dos titulares.

- **Flexibilidade:** Algumas contribuições mencionam documentos de referência da ICO e da CNIL, que defendem uma abordagem flexível e orientada pelo contexto; um equilíbrio entre flexibilidade técnica e conformidade legal.

- **Medidas de salvaguarda:** as contribuições convergem para a adoção de medidas de salvaguardada no tratamento de dados pessoais para treinamento de IA de propósito geral, e apontam que novos dados pessoais criados por sistemas de IA estão sujeitos às mesmas salvaguardas garantidas pela LGPD para os dados de entrada. Há uma contribuição que afirma que desenvolvedores de IA devem implementar medidas de accountability e salvaguardas como avaliação de nível de risco.

- **Explicabilidade:** deve ser promovida a partir de meios de comunicação acessíveis ao titular. Ainda, ressalta-se a importância de mecanismos de explicabilidade e interpretabilidade, de modo a permitir que os usuários e reguladores compreendam os critérios de decisão utilizados pelo sistema.

- **Transparência:** divulgação clara de informações e políticas de privacidade. Deve ser implementada em diversos níveis: no desenvolvimento do modelo base, na integração com aplicações específicas e no uso final. Há desafios, contudo, incluindo a sua difícil operacionalização para fins de documentação e explicabilidade do algoritmo.

- **Governança colaborativa:** as contribuições convergem para a colaboração entre governos, indústria e academia na formulação de diretrizes. Ainda, afirmam que a governança colaborativa entre desenvolvedores, operadores e reguladores é essencial para o alinhamento de práticas éticas e legais.

- **Transparência e finalidade:** os sistemas de IA devem seguir os mesmos princípios de finalidade e transparência que os demais sistemas seguem, a partir de abordagem estruturada e multifacetada e deve incluir explicações sobre a coleta, uso e atividades de processamento de dados.

- **Avisos de privacidade:** uma das contribuições sublinhou o ponto de que em sistemas de IA de propósito geral, uma abordagem em camadas para os avisos de privacidade é altamente recomendada, garantindo a transparência mesmo em sistemas complexos. A divulgação de informações em meios de comunicação variados também pode ser de extrema utilidade para a consecução da transparência.

Pontos de divergência

5.21. Sobre os pontos de divergência, destacam-se:

- **Base legal para GPAI:** enquanto há diversas contribuições que afirmam que a hipótese legal do legítimo interesse é a base legal adequada no tratamento de dados no âmbito da GPAI, há contribuições que, embota não descartem essa base legal, destacam a possibilidade de utilização do consentimento, inclusive de forma progressiva e contextual.

- **Nível de especificidade da finalidade:** Há contribuição que defende que a finalidade deve ser suficientemente específica, referindo-se ao tipo de sistema desenvolvido e às funcionalidades tecnicamente viáveis, outra afirma que a finalidade pode abranger tarefas e casos de uso distintos, mas convergentes e complementares. Outra contribuição, de forma similar, defende a possibilidade de finalidades mais amplas e abrangentes, descritas de forma mais geral e exemplificativa. Ainda, determinada contribuição defende que a comunicação com os titulares deve ser individualizada, incluindo dados utilizados, tratamentos realizados, finalidades específicas e bases legais. Por fim, cabe citar a contribuição que sugere a implementação de uma estrutura em camadas, estabelecendo finalidades macro para o sistema e subfinalidades específicas para cada uso.

- **Transparência:** há contribuições que sugerem que o princípio da transparência seja aplicado de forma diferente a depender da fase do tratamento nos sistemas de IA. Por seu turno, há contribuições que afirma que os sistemas de IA devem seguir os mesmos princípios de finalidade e transparência que os demais sistemas seguem.

- **Responsabilidade pela definição da finalidade:** há divergência sobre quem deve ser o responsável pela definição da finalidade. Algumas contribuições indicam que a responsabilidade deve ser compartilhada entre o desenvolvedor e a organização que implementa o sistema,

enquanto outras defendem que a responsabilidade deve recair sobre o aplicador de IA ou que os desenvolvedores são os responsáveis para indicar a finalidade do tratamento. Há divergência, mais específica sobre a responsabilidade dos desenvolvedores pelas aplicações de seus sistemas de IA. Algumas contribuições defendem que os desenvolvedores não são responsáveis por toda e qualquer aplicação, enquanto outras enfatizam a obrigação legal de que os desenvolvedores orientem sobre sua utilização.

- **Momento da avaliação da limitação de propósito:** há contribuições que defendem que o juízo de admissibilidade da limitação de propósito/finalidade somente deve ser obrigatório na aplicação do Sistema de IA em si, após a conclusão da fase de testagem, enquanto outras enfatizam que o tratamento de dados pessoais permanece específico à finalidade e dependente do contexto

5.22. Assim é que as contribuições convergem na importância da transparência, da definição clara de finalidades, da avaliação de riscos, da governança e do monitoramento, da implementação de canais de atendimento e do uso de políticas de privacidade. No entanto, há divergências sobre a base legal para GPAI, o nível de especificidade da finalidade, a responsabilidade pela definição da finalidade, o momento da avaliação da limitação de propósito e a responsabilidade dos desenvolvedores.

Pergunta 4 - Quais boas práticas e salvaguardas, bem como parâmetros ou critérios, devem ser considerados ao longo de todo o ciclo de vida de sistemas de IA para prevenir discriminações ilícitas ou abusivas?

5.23. As contribuições responderam ao questionamento da pergunta 4 sobre boas práticas e salvaguardas para a prevenção de discriminações ilícitas ou abusivas, versando sobre monitoramento, auditorias, supervisão humana, flexibilização da LGPD, dentre outros aspectos. A seguir, nota-se áreas de convergência e divergência.

<u>Pontos de convergência</u>

- **Monitoramento contínuo e auditorias:** Há uma convergência para a realização de auditorias regulares, a fim de assegurar que os sistemas operem de forma justa e de modo a garantir a conformidade, ressaltando, ainda, a proficuidade de auditoria retrospectiva após o término da relação contratual, pois os impactos de uma tecnologia nos direitos humanos podem ser retardados.

- **Qualidade e diversidade dos dados:** as contribuições apontam para a necessidade de assegurar a diversidade e qualidade dos dados para resultados representativos.

- **Avaliação de impacto:** diversas contribuições apontam para a necessidade de avaliação de impacto a fim de identificar e mitigar riscos à privacidade, em especial quando houver alto risco. Determinada contribuição defende, ainda, a avaliação de impacto em direitos humanos (HRIA).

- **Supervisão humana:** Há um consenso em algumas contribuições sobre a implementação de supervisão humana para a mitigação de riscos de discriminação ilícitca ou abusiva.

- **Equipes multidisciplinares e diversas:** várias contribuições destacam a importância da inclusão de equipes multidisciplinares na estruturação dos sistemas e com diversidade social, a fim de identificar e mitigar vieses inconscientes.

- **Canais de feedback e mecanismos de correção:** algumas contribuições apontam para a utilização de canais de feedback e atendimento como meio para que os titulares consigam exercer seus direitos, dentro das limitações técnicas.

- **Dados sensíveis:** há uma convergência em determinadas contribuições para a possibilidade de tratamento de dados pessoais sensíveis nas fases de teste e validação e com a utilização da hipótese legal de cumprimento de obrigação legal ou regulatória.

5.24. Por sua vez, foram os seguintes os pontos de divergência relativos à Questão 4:

<u>Pontos de divergência</u>

- **Dados sensíveis:** existe discussão sobre o uso de dados sensíveis, com algumas contribuições defendendo que sejam usados apenas quando estritamente necessário, enquanto outras apontam para uma maior flexibilidade com os dados pessoais sensíveis para treinamento dos sistemas de IA e a consequente redução de discriminação.

- **Flexibilização da LGPD:** Há uma divergência sobre a necessidade de flexibilizar a aplicação dos princípios da LGPD para viabilizar o combate aos vieses discriminatórios.

- **Necessidade de requisitos adicionais:** Há divergência sobre se são necessários requisitos adicionais e específicos para os sistemas de IA para combate à discriminação, ou se bastam os já existentes. Nesse aspecto, colaciona-se a contribuição, que traz, em resumo, o seguinte:

> Enfatiza-se a necessidade de seguir rigorosas práticas e salvaguardas ao longo do ciclo de vida de sistemas de IA, com foco em uma

estrutura robusta de governança para gestão integrada de riscos, incluindo a avaliação de vieses e análises de impacto quando o tratamento de dados pessoais for de alto risco.

Destaca a importância de definir claramente as finalidades dos sistemas para minimizar vieses, de executar testes contínuos e documentar todo o processo.

Propõe determinar antecipadamente as categorias de dados pessoais aceitáveis e assegurar a efetividade do exercício dos direitos dos titulares desde o desenvolvimento.

Boas Práticas:

1. Definição clara das finalidades dos sistemas para minimizar vieses;

2. Execução de testes contínuos e documentação para transparência e responsabilidade;

3. Monitoramento contínuo e auditorias independentes para garantir a conformidade;

4. Engajamento das partes interessadas e educação contínua das equipes.

Salvaguardas:

Realização de bias assessments and ethical reviews em cenários de alto risco;

Implementação do RIPD;

Desenvolvimento de estratégias de mitigação junto aos times de negócios;

Adaptação das normas para equilibrar inovação, proteção de dados e requisitos de natureza prudencial.

Parâmetros:

1. Assegurar diversidade e qualidade dos dados para resultados representativos;

2. Determinar de forma antecipada as categorias de dados pessoais aceitáveis, conforme o caso de uso;

3. Assegurar efetividade do exercício dos direitos dos titulares desde o desenvolvimento.

- **Adoção de boas práticas e salvaguardas:** a adoção de práticas e salvaguardas deve considerar a viabilidade de sua implementação em modelos, tendo em vista a realidade operacional. As medidas adotadas devem ser proporcionais aos riscos decorrentes de possíveis vieses ilícitos nos sistemas de IA, de modo a não inviabilizar o nascimento de novas empresas e mitigar o ciclo competitivo. Por sua vez, há contribuições que defendem uma estrutura robusta de salvaguardas ao longo de todo o ciclo de vida do sistema de IA.

5.25. Em síntese, as contribuições convergem sobre a necessidade de monitoramento contínuo e auditorias, avaliações de impacto, implantação de supervisão humana, qualidade e diversidade dos dados, formação de equipes

multidisciplinares e diversas, e utilização de canais de feedback e mecanismos de correção. Entretanto, há diferentes ponderações a respeito da flexibilização da LGPD, necessidade de requisitos adicionais para combate à discriminação e a forma de adoção de boas práticas e salvaguardas. Houve ainda convergência parcial sobre o tratamento de dados pessoais sensíveis.

BLOCO II - HIPÓTESES LEGAIS

Pergunta 5 - O tratamento de dados pessoais no contexto de sistemas de IA pode ser amparado pela hipótese legal do consentimento? Em quais circunstâncias? Quais as limitações para a utilização dessa hipótese legal nesses contextos e quais salvaguardas devem ser observadas?

5.26. A pergunta 5 foi respondida com perspectivas sobre a viabilidade de uso da hipótese legal do consentimento, considerando os meios necessários para sua operacionalização em face da escalabilidade necessária e a garantia de direitos dos titulares como o direito de revogação, bem como salvaguardas necessárias e hipóteses legais alternativas. Na sequência, são descritos pontos de divergência e convergência.

Pontos de convergência

- **Limitações e desafios:** A maioria das contribuições converge que o uso do consentimento como única base legal para o tratamento de dados em sistemas de IA enfrenta desafios e limitações significativas. Gerenciar consentimentos e revogações individuais é considerado logisticamente inviável e oneroso. A complexidade dos sistemas de IA dificulta a clareza na explicação das finalidades do tratamento de dados e a possibilidade de retirada do consentimento. Nesse sentido, cita-se o seguinte excerto de uma das contribuições:

> Em alguns casos, dependendo do propósito do sistema de IA, basear-se no consentimento pode levar a conjuntos de dados de treinamento incompletos ou não representativos, o que pode gerar efeitos negativos subsequentes. Essas limitações não apenas sobrecarregam a autonomia do usuário, mas também podem diminuir a eficiência e a eficácia do ecossistema digital. Além disso, pode não ser tecnicamente viável ou ser excessivamente oneroso atender a solicitações de retirada de consentimento ou exclusão de dados por parte dos indivíduos. Isso ocorre porque rastrear os dados de volta aos indivíduos específicos é, não apenas intensivo em recursos e quase impossível no caso de dados de terceiros, mas também representa riscos à privacidade dos indivíduos e pode até comprometer estruturalmente os sistemas de IA, impactando significativamente seu funcionamento.

- **Dificuldade de revogação:** a revogação do consentimento é vista como um desafio crítico. Após os dados serem utilizados no modelo de IA,

reverter seu impacto é extremamente difícil. Em alguns casos, "destreinar" um modelo pode ser tecnicamente inviável. Assim, os requisitos de validação do consentimento e possibilidade de revogação podem inviabilizar a aplicação da hipótese legal.

- **Necessidade de transparência e informação:** quando o consentimento é considerado, enfatiza-se a necessidade de transparência e informações detalhadas. Os titulares devem ser claramente informados sobre as finalidades do uso de seus dados, o funcionamento do sistema de IA e seus possíveis impactos.

- **Consentimento específico e informado:** O consentimento, quando aplicável, deve ser livre, informado e específico. As autorizações genéricas para o tratamento de dados pessoais são consideradas nulas. Ademais, há contribuições que atentam para a necessidade de relacionamento prévio entre o agente de tratamento e o titular de dados pessoais. Há contribuições que dizem ser de difícil obtenção o consentimento informado. Outrossim, um sistema que não pode ser adequadamente explicado, também não pode ser objeto de consentimento válido.

- **Alternativas ao consentimento:** Muitos defendem que bases legais como o legítimo interesse, a execução de contrato e o cumprimento de obrigação legal podem ser mais adequadas em certos contextos de IA.

- **Avaliação criteriosa:** A utilização do consentimento como base legal deve ser avaliada de forma criteriosa no contexto de sistemas de IA, devido à dificuldade de obtenção de um consentimento prévio e específico.

- **Salvaguardas:** Caso o consentimento seja utilizado, são necessárias salvaguardas específicas, como transparência, "accountability", documentação, auditorias, mecanismos de revogação, limite de reutilização, medidas de segurança robustas, consentimento granular, linguagem acessível nos termos do art. 9º da LGPD, minimização e anonimização. Além disso, aponta-se para a necessidade de salvaguardas adicionais quando o tratamento de dados estiver relacionado à oferta de serviços personalizados, como recomendações baseadas em preferências dos usuários ou funcionalidades específicas de um sistema de IA. Há ainda contribuição que ressalta a necessidade de salvaguardas adicionais para grupos vulneráveis.

<u>Pontos divergentes</u>

- **Viabilidade do consentimento:** embora a maioria das contribuições aponte para as limitações do consentimento, algumas consideram que

pode ser uma hipótese legal apropriada em situações específicas. Isso ocorre especialmente quando o tratamento de dados tem finalidade claramente definida, há um relacionamento direto com os titulares, e o consentimento pode ser obtido de forma livre, informada e inequívoca. Contudo, outras contribuições apontam que a utilização do consentimento para alguns casos, como tratamento de grande base de dados, pode inviabilizar o desenvolvimento de tecnologias. Da mesma sorte, os requisitos de validação do consentimento e a possibilidade de revogação podem inviabilizar a aplicação desta hipótese legal, especialmente para casos em que sistemas são extremamente úteis para a sociedade, como os de detecção de fraude.

- **Finalidades específicas vs. Secundárias:** Há discussão sobre se é necessário falar em finalidades específicas para o treinamento de IA ou se esse treinamento já está implícito em qualquer atividade de tratamento de dados pessoais. Alguns defendem a possibilidade de finalidades secundárias, desde que conectadas à finalidade original, que os titulares tenham expectativa e que medidas de segurança adequadas sejam implementadas.

- **Escalabilidade do consentimento:** Algumas contribuições mencionam que o consentimento não deve ser escalável.

- **Necessidade de renovação do consentimento:** Há quem defenda que o consentimento deve ser renovado a cada atualização significativa do sistema).

- **Dados públicos:** Há divergência sobre a possibilidade de utilizar o consentimento para tratamento de dados públicos, como raspagem de dados.

5.27. Assim, as contribuições são convergentes sobre as limitações e desafios do uso da hipótese legal do consentimento e procedimentos operacionais relacionados, dificuldade de revogação, a necessidade de transparência e salvaguardas. Por outro lado, não houve consenso a respeito da viabilidade do consentimento e sua escalabilidade, necessidade de renovação de consentimento, e o tratamento de dados públicos para raspagem de dados.

Pergunta 6 - O tratamento de dados pessoais, no contexto de sistemas de IA, pode ser amparado pela hipótese legal do legítimo interesse? Em quais circuntâncias? Em caso afirmativo, quais salvaguardas devem ser adotadas nessas situações com vistas à proteção de direitos dos titulares, especialmente considerando a vedação de tratamento de dados pessoais sensíveis com base na

hipótese legal do legítimo interesse? Em particular, a coleta de dados pessoais para o treinamento de sistemas de IA, especialmente mediante técnicas de raspagem de dados, pode ser fundamentada na hipótese legal do legítimo interesse?

5.28. Sobre a hipótese legal do legítimo interesse, as contribuições discutiram tópicos como a aplicabilidade da hipótese legal, teste de balanceamento, transparência, medidas de mitigação e salvaguarda, dados sensíveis e raspagem de dados. Adiante, são mostrados pontos de convergência e divergência.

Pontos de convergência

- **Aplicabilidade do legítimo interesse:** a maioria das contribuições converge que o legítimo interesse pode ser uma base legal válida para o tratamento de dados pessoais em sistemas de IA. Isso inclui o treinamento de modelos de IA, especialmente quando envolve grandes volumes de dados e validação de processos. Ainda, mostra-se uma base legal apropriada quando se trata de dados tornados manifestamente públicos pelo titular.

- **Necessidade de teste de balanceamento:** é amplamente aceito que, para utilizar o legítimo interesse, é imprescindível realizar um teste de balanceamento. Esse teste visa equilibrar os interesses legítimos do controlador com os direitos e liberdades fundamentais dos titulares. O teste de balanceamento deve considerar a finalidade e a necessidade do tratamento, bem como as salvaguardas implementadas.

- **Transparência:** a transparência é apontada como elemento crucial. É necessário informar os titulares sobre o tratamento de seus dados de forma clara e acessível, utilizando uma linguagem compreensível.

- **Salvaguardas e medidas de mitigação:** existe um consenso sobre a necessidade de implementar salvaguardas para proteger os direitos dos titulares. Essas salvaguardas incluem:

    a) Anonimização e pseudonimização;

    b) Minimização de dados;

    c) Implementação de medidas de segurança;

    d) Possibilidade de oposição ao tratamento;

    e) Relatórios de Impacto à Proteção de Dados (RIPD).

- **Raspagem de dados:** o legítimo interesse pode ser utilizado para raspagem de dados (*scraping*), desde que os dados sejam acessíveis

publicamente, o impacto sobre os titulares seja minimizado, e não haja expectativa de privacidade. Ainda, há contribuição atentando para o fato de que a raspagem de dados não deve coletar dados pessoais sensíveis ou de crianças e adolescentes e que a inclusão de salvaguardas desde o início é necessária para limitar a coleta de dados pessoais sensíveis.

- **Dados sensíveis:** há uma forte convergência de que o legítimo interesse não deve ser utilizado para o tratamento de dados pessoais sensíveis. A LGPD proíbe o uso do legítimo interesse como base legal para o tratamento de dados pessoais sensíveis. No entanto, algumas contribuições mencionam que, se o tratamento de dados sensíveis for acidental e medidas de mitigação adequadas forem adotadas, o uso do legítimo interesse pode ser considerado. Assim, sugerem a filtragem, na medida do possível, de dados pessoais e sensíveis desnecessários, inadequados e irrelevantes antes de usar conjuntos de dados para treinar sistemas de genAI; e quando a filtragem prévia não for prática, anotação de dados para identificar dados pessoais e sensíveis inseridos no treinamento da IA, com medidas técnicas para impedir que esses dados sejam reproduzidos ou extraídos nos resultados do sistema. Há contribuições que sugerem medidas para mitigar o risco associado, tais como: definir critérios que evitem a coleta de dados sensíveis durante o processo de captura; e higienizar as bases de dados, eliminando eventuais informações sensíveis coletadas incidentalmente.

<u>Pontos de divergência</u>

- **Dados sensíveis:** Há divergências sobre o tratamento de dados sensíveis, mesmo que de forma não intencional. Alguns argumentam que o tratamento de dados sensíveis, mesmo que não intencional, impede o uso do legítimo interesse. Nesse sentido, necessário se faz a adoção de salvaguardas no contexto de IA, como a exclusão de dados sensíveis e inferências das bases de dados. Outros defendem que, se o tratamento não tiver por objetivo classificar ou segmentar pessoas com base em atributos protegidos por lei, o legítimo interesse pode ser aplicado, desde que medidas de segurança sejam adotadas e que a vedação ao uso de dados sensíveis pode, inclusive, dificultar a mitigação de vieses. Por fim, algumas contribuições citam o documento em formado de diretrizes do EDPB, que afirma que a coleta não intencional de dados sensíveis não inviabiliza o uso do legítimo interesse, desde que medidas apropriadas de mitigação sejam adotadas.

- **Raspagem de dados:** Algumas contribuições expressam cautela em relação ao uso do legítimo interesse para raspagem de dados, especialmente quando a finalidade é diversa da original ou quando há

risco de violação dos direitos dos titulares. Há quem defenda que a raspagem de dados não pode usar o legítimo interesse como justificativa. Outros afirmam que a raspagem de dados pode ser fundamentada no legítimo se: os dados estiverem acessíveis publicamente; não houver expectativa de privacidade por parte do titular; e o impacto sobre os titulares for minimizado. Finalmente, há contribuição que assevera ser a raspagem de dados antiética e impede o consentimento do titular, a fiscalização da adequação, o controle sobre quais dados são utilizados e a aplicação de penalidades.

- **Abrangência do legítimo interesse:** Há diferentes interpretações sobre a abrangência do legítimo interesse, com algumas contribuições defendendo uma aplicabilidade limitada, enquanto outras defendem uma aplicabilidade mais ampla. Há contribuição que afirma ser o interesse comercial de uma organização um legítimo interesse, desde que lícito e atenda ao teste do legítimo interesse. Outras contribuições afirmam que o legítimo interesse pode ser usado em casos em que a finalidade seja para a melhoria do sistema e para proteger direitos do controlador e do operador, como em sistemas de segurança. Nesse sentido, cabe citar uma das contribuições:

> A concepção da base legal dos legítimos interesses na LGPD, única base legal sem uma finalidade prévia e objetiva quando ausente o consentimento do titular, decorre, dentre outros: do reconhecimento da essencialidade da circulação de dados pessoais; da necessidade de tolerar limitações ao exercício informacional; para atender exigências dos agentes de tratamento do setor privado que tratam dados pessoais em larga escala, garantindo maior flexibilidade para o ecossistema de tratamento de dados pessoais.

- **Hierarquia entre as bases legais:** A LGPD não estabelece hierarquia entre as bases legais. Os controladores devem ter flexibilidade para determinar a hipótese legal para o tratamento de dados pessoais. Nesse ponto, há contribuição que discute a base legal de execução do contrato, afirmando que atividades acessórias não podem ser amparadas por essa base legal, sendo necessário outras bases como o legítimo interesse e o consentimento. Ainda, que o legítimo interesse tem aplicabilidade limitada. Pode ser uma base legal flexível que permite novos usos para dados já coletados, ela requer um alto grau de accountability e observância de princípios fundamentais de proteção de dados. Outra contribuição trata da base legal do exercício regular de direitos

- **Interesse da sociedade vs. Fins privados:** há quem defenda que o tratamento de dados, quando baseado no legítimo interesse, deve ocorrer somente se alinhado com o interesse da sociedade e quando

não houver outras alternativas. O uso do legítimo interesse não deve servir a fins privados, devido aos riscos à privacidade e possibilidade de abusos. Assim, há contribuições que defendem que o legítimo interesse não pode ser uma solução universal para as empresas procederem ao tratamento de dados e que muitas empresas de IA que coletam indiscriminadamente dados da internet para treinar seus modelos não estão atendendo aos requisitos do teste de balanceamento. Por fim, afirma-se que quando a IA não consegue ser compatível com as leis existentes de proteção de dados, deve-se considerar a possibilidade de que o problema esteja na tecnologia e não na legislação, que foi projetada para proteger os indivíduos.

- **Necessidade de consentimento:** em algumas situações, pode ser difícil ou impossível obter o consentimento do titular, tornando o legítimo interesse a hipótese legal mais apropriada. Outros defendem que agentes de IA podem utilizar o consentimento gradual para especificidades e finalidades diversificadas ao longo da interação com o sistema de IA, ou que o uso do consentimento deve ser determinado caso a caso. Outros, ainda, defendem o consentimento para o tratamento de dados pessoais sensíveis.

5.29. De modo geral, as contribuições concordam sobre a aplicabilidade do legítimo interesse, a necessidade de teste de balanceamento e transparência, salvaguarda e medidas de mitigação. Porém, há discordância sobre a abrangência do legítimo interesse, a hierarquia entre as bases legais, a oposição de interesses da sociedade e fins privados, e a necessidade de consentimento. Houve, ainda, convergência parcial sobre o tratamento de dados sensíveis e a raspagem de dados.

BLOCO III - DIREITOS DOS TITULARES

Pergunta 7 - De que maneira os direitos do titular, previstos na LGPD, se aplicam a sistemas de IA?

5.30. As contribuições recebidas a partir da pergunta 7 exploram temas inerentes aos direitos do titular, como a aplicabilidade da LGPD, transparência, governança e accountability, exclusão de dados e direitos de acesso, oposição e retificação. A seguir, são evidenciados os pontos de vistas trazidos pelas contribuições, destacando áreas de conflito e consenso.

Pontos de convergência

- **Aplicabilidade da LGPD:** A maioria das contribuições converge no entendimento de que a LGPD se aplica ao tratamento de dados pessoais realizado por sistemas de IA. A lei não se aplica aos sistemas de IA em si, mas sim ao tratamento de dados pessoais que eles realizam. Isso inclui as fases de treinamento, desenvolvimento e aplicação dos modelos. Há contribuições que defendem a aplicação integral dos direitos, mas

alertam para que sua implementação seja feita de forma pragmática e proporcional.

- **Necessidade de transparência:** Há um consenso sobre a importância da transparência no uso de IA, garantindo que os titulares sejam informados sobre como seus dados são coletados, utilizados e tratados. Essa transparência deve ser equilibrada com a proteção de segredos comerciais e informações confidenciais. Também se fala em transparência algorítmica.

- **Atenção ao contexto:** Existe um entendimento comum de que o exercício dos direitos dos titulares deve observar o contexto dos sistemas de IA. Isso significa considerar as limitações técnicas, a complexidade dos algoritmos e a necessidade de equilibrar a proteção da privacidade com outros interesses legítimos, como a gestão de riscos financeiros.

- **Governança e *accountability*:** As contribuições ressaltam a importância de implementar programas de governança em IA, privacidade e proteção de dados. Esses programas devem incluir a documentação do tratamento de dados, o monitoramento do acesso e uso de dados, e a criação de mecanismos de atendimento aos titulares.

5.31. Sobre as divergências, destacam-se:

<u>Pontos de divergência</u>

- **Exclusão dos dados:** Há divergências sobre a possibilidade de exclusão de dados pessoais utilizados no treinamento de sistemas de IA. Algumas contribuições apontam que a exclusão é tecnicamente inviável, enquanto outras defendem a necessidade de implementar mecanismos que permitam ajustes nos dados sem comprometer a integridade do sistema. Há contribuições que afirmam que a exclusão de dados específicos pode ser economicamente inviável. Houve ainda uma contribuição que afirmou que o direito de exclusão é mitigado pela onerosidade do *machine unlearning*. Nesse sentido, há contribuição que argumenta:

> Dados utilizados durante o treinamento, mas que não foram catalogados ou filtrados para identificar dados pessoais, pode ser irracional ou tecnicamente inviável para um desenvolvedor atender a solicitações de exclusão, especialmente após os dados terem sido utilizados para o treinamento. Podem existir situações em que as organizações não consigam atender a solicitações de exclusão porque os dados associados estão sujeitos a requisitos de retenção previstos por outras normas legais (lavagem de dinheiro, processos judiciais).

Por seu turno, em sentido contrário, há documentos que defendem a aplicação dos direitos dos titulares como os de retificação e exclusão aplicados em sistemas de IA, propondo a implementação de mecanismos que permitam ajustes nos dados pessoais sem comprometer a integridade do sistema e, ainda, técnicas como a anonimização e minimização de dados. Menciona-se também que os sistemas de IA devem oferecer mecanismos de acesso, oposição e revisão de decisões automatizadas, e que os canais de atendimento devem garantir o pleno exercício desses direitos. Ainda, contribuições argumentam que os direitos de retificação, exclusão e anonimização devem ter implicações diretas na governança de sistemas de IA.

- **Direito de acesso:** deve ser traduzido em termos concretos. Outras contribuições defendem que os agentes de IA devem monitorar e registrar o acesso e o uso de dados em tempo real para fins de rastreabilidade ou que o direito de acesso deve se limitar a informações compreensíveis pelo titular, e não a todos os dados internos do sistema, a fim de proteger segredos comerciais. Há contribuição que reconhece sua importância, mas considera que, como o conjunto de dados não é estruturado, não há métodos para vincular informações específicas a um titular. Assim, empresas de IA podem não conseguir fornecer acesso à informação de dados pessoais contidas incidentalmente em sua fase de pré-treinamento se não estiverem associadas a pessoa identificável. Nesses termos, resta impossibilitada a determinação de quais informações antes e depois desse identificador pertencem a determinado indivíduo. Finalmente, há contribuição que afirma que, quanto ao direito de acesso, muitos dados tratados por soluções de IA não possuem significado fora do contexto em que são utilizados. Assim, não parece razoável exigir que esse direito abranja todos os atributos individuais tratados pela solução.

- **Direito de oposição:** a contribuição afirma que tal direito deve ser traduzido em termos concretos. Por outro lado, há contribuições que defendem ser o direito de oposição um direito a ser gozado apenas para futuras versões do sistema, a menos que a organização demonstre que seus interesses continuem a prevalecer, ocasião em que, segundo a contribuição, não cabe o exercício desse direito. Ainda, há contribuição que afirma que direitos como oposição e deleção podem sofrer restrições como decorrência de um exercício de balanceamento entre os direitos de privacidade e o interesse público na gestão adequada do risco financeiro sistêmico:

> Os direitos dos titulares são aplicáveis, mas podem sofrer restrições e limitações a depender da natureza e do contexto do tratamento de dados pessoais em sistemas de IA. Por exemplo, um modelo de crédito precisa, por regulação, tratar os dados pessoais relevantes para a proteção do crédito.

Por sua vez, há contribuição em sentido contrário, que menciona que s sistemas de IA devem oferecer mecanismos de acesso, oposição e revisão de decisões automatizadas, e que os canais de atendimento devem garantir o pleno exercício desses direitos. Ainda, afirma-se que o direito à oposição ao tratamento torna-se um elemento essencial no uso da IA para atividades como segmentação de anúncios ou análise de crédito.

- **Direitos dos titulares:** As contribuições convergem na importância de garantir aos titulares os direitos previstos na LGPD, como acesso, correção, exclusão, oposição, revogação do consentimento e revisão de decisões automatizadas. No entanto, a forma como esses direitos são exercidos pode variar dependendo das características do sistema de IA e da finalidade do tratamento de dados. Ou seja, os direitos aplicam-se integralmente, mas sua implementação deve ser feita de forma proporcional e pragmática. Para uma das contribuições, oposição, revogação e eliminação devem ser aplicados de forma que equilibrem a proteção do titular e a viabilidade técnica. Muitas contribuições afirmam que o exercício de direitos não pode ser implementado por inviabilidade técnica. Há contribuição que afirma que os direitos dos titulares são aplicáveis ao tratamento de dados pessoais em bases de dados utilizadas para treinamento, desenvolvimento e aplicação de modelos de IA, bem como em hipóteses de geração de dados e nos resultados (outputs) quando houver tratamento de dados pessoais (direitos são aplicáveis aos resultados - outputs - nas hipóteses em que permaneça um tratamento de dados pessoais. Nesta última hipótese, a responsabilidade será do desenvolvedor quando o resultado for proveniente de dados integrados à memória do modelo). Cabe ainda citar a contribuição que afirma que a LGPD, assim como os direitos dos titulares, não se plica aos sistemas de IA em si, mas sim ao tratamento de dados pessoais realizado por eles. Nesse esteio, as limitações aos direitos dos titulares de dados não levam a riscos para os titulares de dados onde os modelos de IA não estão sendo usados para identificar titulares de dados específicos ou administrar tratamento diferente. Em suma, defende-se que os direitos de oposição, revogação e eliminação não devem exigir que o sistema "esqueça" totalmente as informações, o que pode inviabilizar a IA. Outras contribuições afirmam o seguinte:

> - Os direitos previstos na LGPD deverão ser aplicados somente a sistemas de IA que utilizem dados pessoais em seus modelos ou resultados.
>
> - A ANPD não deve exigir requisitos excessivamente específicos sobre as formas de exercício dos direitos do titular; pois as melhores formas de comunicação podem variar de acordo com as especificidades de produtos e serviços.
>
> - Os direitos do titular previstos pela LGPD devem ser integralmente aplicados aos sistemas de IA.

- Os direitos dos titulares de dados pessoais aplicam-se ao tratamento realizado por sistemas de inteligência artificial (IA), abrangendo a coleta, geração e resultados (outputs), desde que haja efetivo tratamento de dados pessoais.

Os direitos dos titulares aplicam-se ao tratamento de dados pessoais em bases de dados utilizadas para treinamento, desenvolvimento e aplicação de modelos de IA.

- **Âmbito de aplicação:** Existe debate sobre o âmbito de aplicação da LGPD em relação aos sistemas de IA. Algumas contribuições defendem que a LGPD se restringe às fases de treinamento e output do modelo, enquanto outras argumentam que a lei se aplica a todo o ciclo de vida das aplicações de IA que tratam dados pessoais.

- **Direito de retificação:** há divergências sobre a aplicabilidade do direito de retificação em sistemas de IA. Algumas contribuições defendem que o direito deve ser aplicado apenas a fatos verificáveis, e não a soluções de IA com resultados probabilísticos, enquanto outras propõem a implementação de mecanismos que permitam ajustes nos dados pessoais sem comprometer a integridade do sistema. Há contribuição que afirma ser impossível implementar o direito de retificação de dados, incluídos no modelo treinado, pois exigiria um retreinamento completo do modelo. Ainda, algumas contribuições defendem que o direito de retificação só deve ser aplicado em casos de prejuízo razoável ao titular. Outras sugerem sua aplicabilidade apenas para dados factuais verificáveis e não inferências probabilísticas, e apenas quando houver prejuízo razoável ao titular.

- **Requisitos excessivos:** Algumas contribuições alertam para o risco de a ANPD criar requisitos excessivamente específicos sobre os métodos pelos quais um titular de dados exerce seus direitos. Defende-se que a ANPD deve evitar criar exigências que não considerem a ampla variedade de controladores e as diferentes tecnologias existentes.

- **Necessidade de legislação específica:** Há quem defenda que o PL 2338/2023 já estabelece um marco regulatório abrangente para sistemas de IA, incluindo requisitos específicos sobre transparência e direitos dos usuários, não havendo necessidade de criar obrigações adicionais com base no tratamento de dados pessoais.

5.32. Assim é que as contribuições à pergunta 7 foram largamente abrangentes sobre a relação dos direitos dos titulares e sistemas de IA. Em síntese, houve alinhamento a respeito da aplicabilidade da LGPD, a necessidade de transparência, a atenção ao contexto de IA para exercício dos direitos do titular e governança e accountability. Todavia, há divergência em relação à exclusão de dados, direitos de acesso, oposição, e retificação, o

âmbito de aplicação da LGPD em relação a sistemas de IA, a necessidade de legislação específica, e o risco de criação de requisitos excessivos.

Pergunta 8 - Quais as boas práticas e as salvaguardas a serem observadas na disponibilização de canais de atendimento ao titular para exercício dos seus direitos, a exemplo dos direitos de acesso, de oposição e de revisão de decisões automatizadas, no contexto do tratamento de dados pessoais por sistemas de IA? Se possível, descreva as ferramentas utilizadas para implementação de tais canais de atendimento, com os respectivos parâmetros utilizados.

5.33. As respostas direcionadas à pergunta 8 se dedicaram a explorar temas a respeito de boas práticas e salvaguardas na disponibilização de canais de atendimento ao titular. Assim, foram discutidos a importância sobre questões como obrigatoriedade, acessibilidade, usabilidade, transparência, boas práticas, salvaguardas, rastreabilidade, formatos e padrões dos canais de atendimento. A seguir, os pontos de convergência e divergência.

Pontos de convergência

- **Importância dos Canais de Atendimento:** Há um consenso sobre a necessidade de canais de atendimento para que os titulares de dados possam exercer seus direitos, como acesso, oposição e revisão de decisões automatizadas.

- **Acessibilidade e Facilidade de Uso:** As contribuições convergem na importância de que os canais de atendimento sejam de fácil acesso e possuam uma interface intuitiva e simples, com informações claras sobre como exercer cada um dos direitos. A linguagem utilizada deve ser clara e livre de termos técnicos e deve-se garantir que os canais estejam sempre disponíveis.

- **Transparência:** A transparência é apontada como um princípio fundamental. Os canais devem oferecer informações claras e detalhadas sobre como o titular pode exercer seus direitos e oferecer políticas que ofereçam transparência aos titulares em relação aos modelos e tecnologias adotados. Além disso, é necessário informar os titulares sobre o uso de IA no tratamento de seus dados e os impactos em suas decisões. Ainda, sugere-se que os canais de atendimento sejam acessíveis a todos os titulares, incluindo pessoas com deficiência de diferentes níveis de letramento digital. Por fim, pode-se destacar a contribuição que afirma que os canais de atendimento devem incluir mecanismos que possibilitem ao titular obter informações detalhadas sobre as inferências realizadas, bem como os critérios, dados e modelos utilizados para gerá-las.

- **Necessidade de salvaguardas e boas práticas:** Existe um acordo sobre a

importância de implementar salvaguardas para garantir a segurança e a proteção dos dados nos canais de atendimento. Isso inclui a utilização de tecnologia segura, autenticação robusta e a implementação de métodos de verificação de identidade. Nesses termos, há contribuição que traz uma lista de boas práticas para o exercício dos direitos por parte dos titulares:

> Boas práticas para o exercício dos direitos: Estabelecimento de período prévio mínimo para que os titulares sejam comunicados e possam se opor ao tratamento de seus dados para treinamento de sistemas de IA; ● Facilidade no direito de oposição, sem exigir dos titulares qualquer justificativa ou ônus injustificado; ● Granularidade no exercício do direito de oposição, podendo o titular se opor ou vetar o uso de dados de determinada fonte (ex: indiciar a URL de um blog que mantém com relatos de viagens contendo dados pessoais) ou alguma categoria de dado que se opõe ao tratamento para o treinamento de algum sistema de IA; ● Garantir o direito de acesso aos titulares acerca de seus dados pessoais tratados por sistemas de IA, incluindo as anotações e metadados; ● Garantir o direito de informação acerca de tratamento compartilhado e compartilhamento de dados pessoais com terceiros, incluindo se esses terceiros são fontes de dados pessoais sobre o titular para o uso e treinamento de sistemas de IA; e ● Em cumprimento ao dever de transparência, sempre informar ao titular quando ele estiver interagindo com um sistema de IA e informar de forma específica os direitos que ele pode exercer frente a esse sistemas, como por exemplo, direito de revisão de decisão automatizada ou o direito à informação previsto no art. 20 §1º.

Além disso, há contribuições que trazem listagem de medidas de salvaguarda, dentre as quais podem ser citadas a exclusão de informações indesejadas dos dados coletados online; de duplicação: remoção de trechos de texto idênticos; técnicas pós-treinamento; filtragem (As empresas podem manter os direitos dos titulares de dados filtrando os dados pessoais verificados das pessoas para que não apareçam nos resultados do modelo e garantindo que sejam excluídos de futuras execuções de treinamento do modelo); medidas de proteção de privacidade devem ser abordadas de forma holística, abrangendo todas as etapas do tratamento de dados, em vez de serem limitadas a uma única fase. Essa visão holística permite que as empresas abordem os riscos potenciais de privacidade de maneira mais abrangente, ao mesmo tempo em que mantêm a eficácia dos sistemas de IA.

- **Registro e Rastreabilidade:** As contribuições convergem na necessidade de manter registros de atendimento para assegurar a rastreabilidade e a responsabilização. Os sistemas de atendimento devem permitir o rastreamento de solicitações.

- **Prazos:** Os prazos para atendimento devem ser claros e alinhados aos previstos na LGPD.

Pontos de divergência:

- **Obrigatoriedade de Canais Específicos para IA:** Uma das principais divergências reside na obrigatoriedade de criação de canais de atendimento específicos para sistemas de IA. Algumas contribuições defendem que a LGPD não exige a criação de canais específicos, enquanto outras recomendam que os controladores avaliem a necessidade de mecanismos especializados em casos de tratamentos complexos ou de alto impacto sobre os titulares:

> Embora a LGPD não obrigue a criação de canais específicos para tratamentos realizados por IA, é recomendável que controladores avaliem mecanismos especializados em casos em que a complexidade do tratamento ou o impacto sobre os titulares o justifique. Por exemplo, sistemas de IA utilizados para análise de crédito ou prevenção a fraudes poderiam contar com canais dedicados para esclarecer dúvidas específicas sobre esses tratamentos. Contudo, tais mecanismos devem ser vistos como boas práticas para aprimorar a governança e a transparência, e não como exigências legais.

- **Padronização dos Canais de Atendimento:** Há divergências quanto à padronização dos canais de atendimento. Algumas contribuições defendem que a ANPD deve se limitar a apontar diretrizes sobre o tema, prestigiando a autonomia do controlador. Outras sugerem que a ANPD defina diretrizes sobre o tema.

- **Formato dos Canais de Atendimento:** Existe uma divergência sobre qual o formato de canal de atendimento deve ser priorizado. Há quem defenda que o controlador define o canal (formulário, e-mail, etc.) conforme suas possibilidades e critérios. Outros defendem que o atendimento humano deve ser priorizado.

- **Necessidade de Revisão Humana:** Há divergências sobre a necessidade de revisão humana nas decisões automatizadas. Algumas contribuições defendem a possibilidade de escalonamento para revisão humana em casos complexos ou de contestação de decisões automatizadas.

5.34. Resumidamente, as contribuições expressaram o mesmo entendimento sobre a importância dos canais de atendimento, acessibilidade e facilidade de uso, transparência como princípio fundamental, necessidade de salvaguardas e boas práticas, registro e rastreabilidade e estabelecimento de prazos de atendimento. No entanto, houve diferentes entendimentos sobre obrigatoriedade de canais específicos para IA, padronização e formato

dos canais de atendimento, e necessidade de revisão humana.

Pergunta 9 - Deve haver salvaguardas e limites específicos para o tratamento de dados pessoais sensíveis e para o tratamento de dados pessoais de crianças, adolescentes e idosos durante as etapas do ciclo de vida de sistemas de IA?

5.35. A partir das contribuições direcionadas à pergunta 9, foi possível receber variados pontos de vistas sobre aspectos referentes ao tratamento de dados pessoais de crianças, adolescentes, e idosos nas diversas etapas do ciclo de vida de sistemas de IA. Assim, foram considerados o princípio do melhor interesse, teste de proporcionalidade, consentimento, classificação de dados de idosos como sensíveis, tratamento de dados sensíveis, transparência, segurança e salvaguardas. Foram notadas similaridades e diferenças de perspectivas, reunidas a seguir.

Pontos de convergência

- **Necessidade de Salvaguardas:** A maioria das contribuições converge na necessidade de salvaguardas adicionais ao tratar dados pessoais sensíveis e dados de grupos vulneráveis como crianças, adolescentes e idosos. Essas salvaguardas visam minimizar danos e proteger os direitos desses grupos. Dados e riscos associados exigem salvaguardas que considerem as particularidades de cada grupo vulnerável. Isso inclui técnicas de PETs/PPTs (anonimização, dados sintéticos, técnicas de anotação de dados e privacidade diferencial, criptografia), além de ferramentas de privacy by design. Ainda sugerem a minimização do uso de dados pessoais, o monitoramento contínuo e a obtenção do consentimento de forma destacada e com comunicação compatível com o nível de compreensão do titular ou responsável legal. Algumas ainda defendem a acessibilidade e linguagem simples dos sistemas de IA.

- **Princípio do Melhor Interesse da Criança:** Há um forte consenso de que o tratamento de dados de crianças e adolescentes deve observar o princípio do melhor interesse do menor, conforme previsto na LGPD e na Convenção das Nações Unidas. Em especial, há contribuição que defende que o melhor interesse deve ser prévio ao desenvolvimento ou implementação de um sistema de IA que trate dados pessoais e/ou seja direcionado a estes grupos. Sugerem também a minimização da coleta de dados e a restrição de seu uso para fins de publicidade infantil. Há ainda contribuição que sugere que empresas que desenvolvem produtos de IA para menores devem investir em educação e alfabetização em IA.

- **Transparência:** A transparência no tratamento de dados, especialmente de idosos, é apontada como fundamental. É importante garantir que o consentimento seja compreendido e informado.

- **Medidas de Segurança:** Há convergência na necessidade de medidas de segurança reforçadas para o tratamento de dados sensíveis e de grupos vulneráveis. Há contribuição que foca bastante na minimização de dados e que alega a remoção de dados com conteúdo impróprio, como conteúdo sexual, ilegal ou abuso sexual infantil. Algumas medidas sugeridas incluem criação de perfis de risco para vulneráveis, treinamento de modelos com dados balanceados para evitar vieses, desenvolvimento de interfaces intuitivas e criação de canais de atendimento especializados.

- **Avaliação de Risco e Impacto:** A realização de avaliações de risco e Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) é amplamente recomendada, especialmente em casos que envolvem dados sensíveis ou grupos vulneráveis.

Pontos de divergência

- **Necessidade de Requisitos Distintos para Idosos:** Algumas contribuições defendem que o tratamento de dados de idosos não deve atender a requisitos distintos dos de outros adultos. Argumenta-se que exigir tratamento diferenciado pode ser discriminatório, considerando a presunção de plena capacidade cognitiva desses titulares. Outras contribuições apontam que idosos requerem atenção devido ao risco de exclusão digital e dificuldade em compreender os impactos do uso de IA. Ainda, afirmam que a linguagem deve ser clara, verificando, inclusive, se há curador ou necessidade de decisão apoiada, de modo que as decisões respeitem suas funções cognitivas. Afirma-se que os idosos são vulneráveis a riscos específicos, como fraudes digitais e explorações financeiras. Finalmente, há contribuição que sugere que as salvaguardas específicas sejam restritas a idosos maiores de 80 anos.

- **Classificação de Dados de Idosos como Sensíveis:** Existe discordância sobre a classificação de dados de idosos como dados sensíveis. Algumas contribuições argumentam que equiparar idosos a crianças e adolescentes ou classificar seus dados como sensíveis extrapola os limites estabelecidos pela legislação. Outras apontam que dados de pessoas idosas podem ser sensíveis em determinados contextos. Atentam para o risco de etarismo.

- **Amplitude das Salvaguardas:** Há divergências sobre se limitações adicionais devem ser impostas além das já previstas na legislação. Algumas contribuições defendem que não devem ser impostas limitações específicas ao tratamento de dados no contexto da IA que não estejam expressamente previstas na LGPD. Outras argumentam que salvaguardas e limites restritivos são mandatórios, sendo importante

haver medidas de governança que possibilitem a mitigação de riscos para dados pessoais sensíveis, de crianças, adolescentes e idosos.

- **Resolução 245/2024 do CONANDA:** Há divergências sobre o conteúdo da Resolução 245/2024 do CONANDA, que proíbe a perfilização de dados pessoais de crianças e adolescentes para fins comerciais. Algumas contribuições apontam que a resolução pode excluir tais indivíduos do acesso a produtos que poderiam estar alinhados com seu melhor interesse.

- **Consentimento:** há contribuição que destaca que a hipótese legal do consentimento deve ser reconsiderada, devido à opacidade intencional que permeia o desenvolvimento da IA. Assim, os titulares não conseguem avaliar os riscos associados à anuência com o tratamento de dados.

- **Teste de Proporcionalidade:** Uma contribuição menciona a suficiência do teste de proporcionalidade como limitação quando o tratamento de dados em sistemas de IA é fundamentado no legítimo interesse e usa dados pessoais de crianças, adolescentes e/ou idosos.

- **Dados sensíveis:** há contribuições que afirmam que o tratamento de dados pessoais sensíveis ocorre somente quando a finalidade é identificar aspectos específicos descritos no artigo 5º, II, da LGPD, e associá-los a um indivíduo em particular. Os documentos ressaltam, ainda, que o mero potencial de inferir tais informações não qualifica os dados pessoais como sensíveis. Ainda há contribuição que afirma que requisitos normativos podem levar desenvolvedores a excluir dados sensíveis do conjunto de treinamento em detrimento do desempenho do sistema de IA. Por outro lado, há contribuições que sugere que, para dados sensíveis, é recomendável que as operações sejam guiadas pelo princípio da necessidade estrita.

5.36. Algumas contribuições afirmam, ainda, que os limites sobre o tratamento de dados pessoais sensíveis, de crianças e adolescentes e de idosos já estão bem delineados na LGPD (arts. 11, 14 e 55-J, XIX), cabendo ao legislador a tarefa de impor as restrições de tratamento, não à ANPD. Ainda, afirmam que questões relacionadas a eventuais salvaguardas e limites ao tratamento no contexto dos sistemas de IA estão sendo debatidas no âmbito do PL nº 2338/2023, **sendo recomendável que se aguarde o avanço da discussão legislativa, a fim de não causar insegurança jurídica**.

5.37. Há, ainda, uma contribuição que sugere o uso restrito de decisões automatizadas para tais dados, de modo a proibir decisões

exclusivamente automatizadas nesses casos, exceto em situações em que haja supervisão humana clara e benefícios comprovados. Ainda, a mesma contribuição afirma que deve ser estruturada classificação de risco para sistemas de IA, sendo que os que realizam o tratamento de dados de grupos vulneráveis sejam classificados como alto risco, devendo tais sistemas serem submetidos a obrigações mais rigorosas, como auditorias, documentação e transparência. Deve-se, ainda, proibir sistemas de IA projetados para manipular o comportamento de crianças de forma exploratória ou prejudicial, incluindo práticas de publicidade subliminares.

5.38. Cabe destacar contribuição que sugere o amplo diálogo com agências reguladoras como a ANS, Anvisa, além do Ministério da Saúde, quando do estabelecimento de regulação setorial sobre o tema.

5.39. O tema de tratamento de dados pessoais sensíveis de crianças, adolescentes e idosos foi discutido de forma ampla nas contribuições recebidas. O tema tem discurso uniforme sobre a necessidade, a observação do princípio do melhor interesse, medidas de transparência e de segurança, e recomendação de avaliação de risco e impacto. Porém, há abordagens discordantes ao se tratar da necessidade de requisitos distintos para idosos, classificação de dados de idosos como sensíveis, aplicação da resolução 245/2024 do CONANDA, viabilidade do uso de hipótese legal do consentimento, suficiência do teste de proporcionalidade e ocorrência de tratamento de dados pessoais sensíveis. Apesar de haver concordância sobre a necessidade de medidas de salvaguardas, há divergência sobre limitações que excedam aquelas já previstas em legislação.

5.40. Por fim, contribuições individuais abordaram outros temas de forma isolada, como a restrição do uso de decisões automatizadas, amplo diálogo com agências reguladoras e a classificação do tratamento de dados pessoais de grupo vulneráveis como de alto risco.

Pergunta 10 - Quais os requisitos a serem observados para a garantia e a aplicação do direito à revisão de decisões automatizadas (art. 20 da LGPD)? O que pode ser considerado como decisão tomada unicamente com base em tratamento automatizado de dados pessoais? Quais interesses poderiam ser afetados?

5.41. As respostas à pergunta 10 formam extensa discussão sobre os requisitos para aplicação do direito à revisão de decisões automatizadas. Assim, foram observadas opiniões sobre o direito à revisão e seus requisitos, afetação de interesses, conceito de decisão unicamente automatizada, necessidade de revisão humana, transparência, necessidade de salvaguardas, decisões de alto risco e a oposição da transparência e segredos comerciais. Na

sequência, são descritos os pontos de convergência e divergência conforme as contribuições recebidas.

Pontos de convergência

- **Direito à Revisão:** Há um consenso de que o artigo 20 da LGPD garante ao titular o direito de solicitar a revisão de decisões tomadas exclusivamente por meio de tratamento automatizado de dados que afetem seus interesses. Há citações de exemplos de decisões automatizadas, como análises de crédito, seleção de candidatos em processos seletivos, anúncios personalizados (afetando a liberdade de escolha do usuário), sistemas de recomendação. As contribuições afirmam que as decisões automatizadas podem afetar direitos de liberdade e privacidade, levar à discriminação e desigualdade de oportunidades.

- **Requisitos para a Revisão:** As contribuições convergem em alguns requisitos essenciais para a garantia do direito à revisão:

  a) Possibilidade de Revisão Humana: Necessidade de revisão por pessoa qualificada.

  b) Transparência: Transparência no processo decisório.

  c) Explicabilidade: Explicabilidade do algoritmo.

  d) Canais de Comunicação: Canais de comunicação adequados.

  e) Documentação: Documentação dos processos de tomada de decisão automatizada e seus critérios.

- **Afetação de Interesses:** A aplicação do direito à revisão está condicionada à afetação dos interesses do titular. A afetação não exige a constatação de violação material de um direito, mas uma ameaça ou risco aos direitos já é suficiente.

- **Decisão Unicamente Automatizada:** A decisão deve ser tomada unicamente com base em tratamento automatizado de dados pessoais. A participação humana no processo de tomada de decisão precisa ser significativa para que a decisão não seja considerada totalmente automatizada. Ainda, o "human in the loop" não pode apenas atuar apenas para referendar o resultado apresentado pelo algoritmo como forma de evadir a disposição normativa, mas deve ter a capacidade de considerar todos os dados de entrada e saída disponíveis).

- **Interesses Afetados:** As decisões automatizadas podem afetar diversos interesses do titular, incluindo direitos de liberdade e privacidade,

discriminação e desigualdade de oportunidades, acesso a bens e serviços, direitos econômicos e financeiros, direitos trabalhistas, questões relacionadas à saúde, reputação e autonomia.

- **Transparência e Acesso à Informação:** É necessário garantir que o titular tenha acesso claro à lógica envolvida na tomada de decisão automatizada, incluindo informações sobre os critérios utilizados.

- **Necessidade de Salvaguardas:** Há um reconhecimento da necessidade de salvaguardas robustas para proteger os usuários de danos e apoiar o uso responsável da IA.

5.42. Os pontos de divergência identificados, por seu turno, foram os seguintes:

Pontos de divergência

- **Decisões de Alto Risco:** Algumas contribuições defendem que a revisão deve se aplicar apenas a decisões automatizadas de alto risco, que produzem efeitos jurídicos ou similares. No entanto, outras argumentam que a revisão não depende de efeito legal ou significativamente equivalente.

- **Abrangência da Afetação de Interesses:** Há divergências sobre a amplitude da afetação de interesses. Algumas contribuições sugerem não ampliar o alcance do direito à revisão para situações como perfilizações para publicidade direcionada, que geram impactos menos significativos. Outras afirmam que os interesses do titular envolvem aspectos referentes à sua personalidade e que as decisões devem afetar os interesses dos titulares de forma significativa ou negativa. Há contribuição que afirma que os interesses podem envolver interesses contratuais, financeiros e de direitos e liberdades fundamentais dos titulares. Assim, os agentes de tratamento devem assegurar que as decisões automatizadas sejam corretas, legais e éticas, bem como permitir que os titulares entendam e contestem as decisões, quando necessário, a fim de evitar vieses e discriminação nessas decisões. Alguns exemplos dados por contribuições são: acesso a serviços, oportunidades de emprego, reputação e autonomia dos indivíduos. Por fim, cabe apontar para a contribuição que afirma que os principais interesses afetados por decisões puramente automatizadas são aqueles que interferem nos preceitos morais de uma sociedade, interesses jurídicos, econômicos, políticos, de privacidade, reputação, e direitos públicos, além do viés algorítmico (discriminação algorítmica).

- **Necessidade de Revisão Humana:** A obrigatoriedade da revisão humana é um ponto de divergência. São apontados problemas na revisão

humana, como: vieses mentais, como confiança na lógica automatizada e o argumento de que a automatização traz objetividade e rapidez. Há apontamentos de que a revisão humana somente é necessária quando o tratamento é exclusivamente automatizado. Outros apontam sua necessidade somente se houver efeito legal ou significativamente equivalente. A LGPD não exige revisão humana, mas os argumentos do titular devem ser analisados. A revisão pode ser feita por humanos ou máquinas. Destacam, ainda, que há desafios substanciais na implementação de um processo de revisão humana, como custos elevados e a complexidade de adaptação de processos empresariais muitas vezes projetados para operar de maneira inteiramente automatizada. Há contribuição que afirma que a revisão humana e a transparência são essenciais para evitar discriminações, vieses ou erros que comprometam esses direitos e traz como requisitos para garantia do direito à revisão os seguintes: transparência sobre o processo automatizado, garantia de revisão humana, clareza explicativa e justificação, mitigação de vieses, salvaguardas e boas práticas, auditorias regulares, interface de atendimento ao titular, monitoramento contínuo de impactos. Por fim, destaca-se a contribuição que sugere que a revisão humana, quando necessária e requerida, deve ser implementada de forma eficiente e escalável, utilizando equipes com capacitação técnica e que sejam imparciais.

- **Conceito de Decisão Unicamente Automatizada:** Há diferentes interpretações sobre o que configura uma decisão tomada unicamente com base em tratamento automatizado. A necessidade de intervenção humana "significativa" é um ponto central. Ainda, há contribuição que destaca 3 aspectos a serem considerados para aplicação do art. 20: existência de uma decisão com impacto material, tratamento exclusivamente automatizado e que afete materialmente a vida do titular. Ainda, aponta a necessidade de distinguir entre sistemas com impacto mínimo e sistemas usados na tomada de decisões que afetam a prestação de serviços essenciais. Cabe citar também contribuição que traz uma definição de decisão automatizada: aquela destinada a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade - aspectos que podem ser afetados por meio desse tipo de automação. Outra contribuição afirma que uma decisão é caracterizada como automatizada se: não houver interferência humana significativa e gerar impacto jurídico ou prático significativo ao titular. Ainda, afirma-se em contribuição que modelos de IA que fornecem dados de saída, revisado por um humano habilitado, que é o decisor final, não se enquadrariam no contexto de decisão automatizada. Cabe citar contribuição que aponta a necessidade de 3 critérios cumulativos para que o titular tenha direito de solicitar a revisão de decisão automatizada: autenticação do titular para validação

da identidade; a decisão ter sido tomada unicamente com base em tratamento automatizado de dados pessoais; o titular demonstrar que os impactos da decisão afetaram seus interesses. Por fim, cabe citar a contribuição que afirma que uma decisão que se reverta em insumo para um sistema ou uma atividade mais ampla de avaliação não deve ser considerada como uma decisão automatizada.

- **Extensão do Direito à Revisão:** Existe divergência se a noção de decisão baseada em tratamento totalmente automatizado deve se estender às decisões intermediárias de um processo decisório que possam influenciar e impactar as decisões posteriores. Duas contribuições afirmam que a noção de decisão baseada em tratamento totalmente automatizada também se estenda às decisões intermediárias de um processo decisório que possam influenciar e impactar a decisões posteriores. Esse tipo de análise deve ser feito de forma casuística e contextual, cabendo ao controlador a responsabilidade de identificar esses nódulos da árvore decisória que têm o potencial de impactar os interesses dos titulares, e por consequência garantir o direito previsto no art. 20 da LGPD. Outras, por outro lado, afirmam que decisões intermediárias não lançam efeito a qualquer titular.

- **Transparência vs. Segredos Comerciais:** É apontado o desafio de equilibrar o direito dos titulares à transparência e revisão com a necessidade de preservar a propriedade intelectual e proteger os interesses comerciais das empresas. Destacam que a transparência deve considerar o contexto regulatório sem comprometer segredos comerciais, oferecendo informações claras e relevantes, como os critérios utilizados na avaliação, sem detalhar fórmulas específicas. Assim, o controlador deve adotar medidas adequadas de transparência, para que, resguardados os seus segredos comercial e industrial (art. 20, §1º, LGPD), informar, de modo simples e direto, a lógica do processo decisório.

- **Modelos de IA Generativa:** Há divergências se modelos de IA generativa tomam decisões que se encaixam nos critérios do artigo 20 da LGPD e afirmam que modelos generativos apenas preveem a próxima palavra ou frase, não configurando uma decisão no sentido da lei.

5.43. Em síntese, as contribuições mostraram opiniões semelhantes quanto ao direito à revisão e seus respectivos requisitos, a necessidade de salvaguardas, a transparência e o acesso à informação. Por outro lado, as opiniões são discrepantes ao tratar sobre a aplicação de revisão a decisões que não sejam classificadas como de alto risco, a abrangência da afetação de interesses, necessidade de revisão humana, equilíbrio entre transparência e segredos comerciais, e o conceito de decisão unicamente automatizada.

Também não há consenso sobre a aplicação do artigo 20 da LGPD sobre as decisões de modelos de IA generativa.

Pergunta 11 - Em que hipóteses e sob quais condições pode ser necessária a revisão humana de decisões automatizadas com vistas à adequada garantia de direitos dos titulares?

5.44. No que se refere à necessidade à necessidade de revisões automatizadas, os participantes discutiram temáticas que permeiam o tema, como a sua necessidade e obrigatoriedade, seus efeitos jurídicos, alto risco, e impactos nos direitos do titular, abordando discriminação, vieses, transparência, e o direito à contestação de informação. Também foram debatidos aspectos de efeito operacional como a qualificação de revisores, custos e viabilidade. Adiante, podem ser observados os aspectos que tiveram pontos de vista unânimes e discordantes.

Pontos de convergência

- **Efeitos Jurídicos ou Similares:** Existe concordância de que a revisão humana é necessária quando decisões automatizadas produzem efeitos jurídicos ou efeitos significativamente similares, além de efeitos adversos significativos decorrentes de fatores como a falta de transparência e explicabilidade, desconformidade com a legislação e discriminação ou viés abusivo ou ilícito.

- **Impacto nos Direitos do Titular:** A revisão humana é vista como necessária quando a decisão automatizada tem um impacto significativo nos direitos do titular. Isso inclui situações que envolvem discriminação, vieses, tratamento de dados sensíveis, ou falta de explicações satisfatórias por parte do sistema automatizado. Ainda, há contribuição que afirma que qualquer decisão automatizada que tenha impacto na vida de um indivíduo, mesmo que mínimo, deve ser significativamente revisada e aprovada por um ser humano. Outras sugerem que apenas as decisões de alto impacto devem ser revisadas, como a concessão de crédito, a aprovação de um empréstimo, a definição de um perfil de risco ou a seleção de um emprego.

- **Discriminação e Vieses:** A necessidade de revisão humana é enfatizada em casos de suspeita de discriminação ou vieses nas decisões automatizadas.

- **Transparência e Explicabilidade:** A revisão humana está diretamente ligada aos princípios de transparência e explicabilidade. A falta de transparência no processo automatizado justifica a necessidade de revisão humana para que o titular compreenda os critérios e dados que fundamentaram a decisão.

- **Alto Risco:** A utilização do alto risco no tratamento de dados pessoais nos sistemas de IA é apontada como um fator determinante para a revisão humana.

- **Qualificação dos Revisores:** A revisão humana deve ser conduzida por profissionais qualificados e capazes de identificar erros ou vieses nos algoritmos.

- **Direito à Contestação e Informação:** O titular deve ter o direito de contestar a decisão automatizada de maneira eficiente. É fundamental que o titular tenha acesso a informações claras e adequadas sobre os critérios e dados utilizados no processo de decisão.

- **Revisão como Boa Prática:** Mesmo não sendo legalmente obrigatória, a revisão humana é amplamente recomendada como uma boa prática, podendo ser uma boa prática para evitar danos em larga escala. A adoção de políticas de revisão humana pode ser considerada uma circunstância atenuante em fiscalizações. Também pode ser considerada uma boa prática para revisão de outputs de IA Generativa, como forma de controle de qualidade e ação de prevenção à discriminação.

- **Necessidade de Mecanismos de Supervisão:** Há um consenso sobre a importância de mecanismos de supervisão incorporados aos sistemas de IA.

5.45. Ainda, cabe destacar a contribuição que sugere que a ANPD **não se concentre em algo que não esteja previsto na lei, pois discutir a supervisão humana corre o risco de criar uma expectativa regulatória paralela sem fundamento na LGPD.**

<u>Pontos de divergência</u>

- **Obrigatoriedade da Revisão Humana:** A principal divergência reside na obrigatoriedade da revisão humana. A LGPD não deixa claro se as revisões das decisões devem ser realizadas por humanos, permitindo a revisão automatizada. Algumas contribuições defendem que a revisão humana não é um requisito legal obrigatório. Por outro lado, há contribuição que afirma que decisões tomadas por sistemas de IA envolvidas com o Poder Judiciário devem ser obrigatoriamente revisadas.

- **Revisão Automatizada vs. Humana:** Algumas contribuições argumentam que a revisão automatizada pode ser suficiente, desde que seja eficaz e que a LGPD não deixa claro que as revisões sejam realizadas por humanos. Priorizar mecanismos de supervisão integrados aos sistemas de IA é visto como mais eficiente.

- **Interpretação do Artigo 20 da LGPD:**Há diferentes interpretações sobre o artigo 20 da LGPD, que trata do direito do titular à revisão de decisões automatizadas. Algumas contribuições ressaltam que o legislador excluiu deliberadamente a previsão de revisão humana.

- **Custos e Viabilidade:** A obrigatoriedade da revisão humana pode inviabilizar negócios e elevar custos operacionais. A intervenção humana também pode ser influenciada por vieses inconscientes, não garantindo necessariamente decisões mais justas.

- **Amplitude do Impacto:** Há divergências sobre qual nível de impacto justifica a revisão humana. Algumas contribuições defendem que a revisão deve ser proporcional e aplicada apenas em situações onde as decisões impactam significativamente os direitos ou interesses dos titulares. Outras defendem que qualquer decisão automatizada que tenha impacto na vida de um indivíduo deve ser revisada.

- **Setores Específicos:** Algumas contribuições mencionam setores específicos onde a revisão humana seria mais importante, como saúde, justiça e segurança pública. No setor financeiro, a revisão humana deve observar os requisitos regulatórios.

- **IA Generativa:** Não há consenso se os modelos de IA generativa se encaixam nos critérios de revisão do artigo 20 da LGPD.

5.46. Destaca-se a contribuição que afirma que impactos significativos são aquelas com consequências graves, como negação de crédito ou perda de emprego, com indícios de erro ou vieses (erros nos dados ou suspeitas de viés algorítmico), que possa trazer violações a normas legais ou contratuais, em que há falta de transparência (quando o titular não compreende os motivos da decisão) e que geram impactos em direitos fundamentais. Assim, prossegue afirmando que as condições para uma revisão eficaz incluem independência do revisor (deve ser imparcial); acesso à informação (o revisor deve ter acesso a todas as informações relevantes); prazo para revisão (estabelecimento de prazos para a revisão e comunicação dos resultados). Ainda, há que ter-se confidencialidade e mecanismos de recurso para o titular.

5.47. É de bom alvitre ressaltar, ainda, a contribuição que afirma ser a revisão humana necessária quando, a decisão impacta significativamente o titular, há suspeita de viés, erro ou discriminação no sistema de IA, o titular solicita formalmente a decisão e é exigida por leis setoriais ou regulamentos específicos.

5.48. Sumariamente, há consenso quanto à necessidade de revisão

humana para os casos de efeitos jurídicos ou impacto significativo nos direitos do titular. As contribuições também concordaram sobre a qualificação dos revisores e a necessidade de mecanismos de supervisão. Porém, houve discordância na interpretação do artigo 20 da LGPD, havendo diferentes manifestações acerca da IA Generativa, e da obrigatoriedade de revisão humana e sua real necessidade em havendo revisão automatizada eficiente.

Pergunta 12 - Quais os parâmetros a serem observados para o fornecimento de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, nos termos do §1º do art. 20 da LGPD? QUais limites e parâmetros de segredo comercial e industrial que justificam a não observância do fornecimento de informações, conforme disposto no mesmo dispositivo legal?

5.49. Os temais centrais tratados pelas contribuições em resposta à pergunta 9 versaram sobre a transparência, acessibilidade e explicabilidade, ponderando o equilíbrio com a preservação de segredos comerciais do controlador. Também houve atenção à necessidade de auditoria, à elaboração de diretrizes por parte da ANPD, às formas de explicação de decisões automatizadas e nível de detalhamento das informações, e ao equilíbrio entre transparência e segurança.

5.50. A seguir, os pontos de convergência e divergência:

<u>Pontos de convergência</u>

- **Transparência e Acessibilidade:** Há um consenso de que as informações sobre decisões automatizadas devem ser acessíveis, compreensíveis e transparentes, permitindo que o titular entenda como e por que a decisão foi tomada. A linguagem utilizada deve ser clara, evitando termos técnicos complexos.

- **Finalidade da Explicabilidade:** A finalidade principal da explicabilidade da IA é permitir que as pessoas afetadas por uma decisão possam questioná-la.

- **Equilíbrio entre Transparência e Segredo Comercial:** Existe um reconhecimento da necessidade de equilibrar a transparência com a proteção de segredos comerciais e industriais. A divulgação excessiva pode levar à manipulação e uso malicioso das informações.

- **Flexibilidade e Contexto:** As regulamentações devem ser flexíveis para acomodar diferentes contextos, sem exigir que as empresas divulguem segredos comerciais, propriedade intelectual ou mecanismos internos de segurança e proteção.

- **Diretrizes da ANPD:**Muitos defendem que a Autoridade Nacional de

Proteção de Dados (ANPD) deve elaborar diretrizes para auxiliar os agentes de IA a fornecer respostas claras sobre as decisões, considerando as particularidades dos diversos setores da economia.

- **Necessidade de Acesso e Compreensão:** Os titulares devem ter acesso e poder compreender a lógica normativa por trás das decisões automatizadas, e não necessariamente a lógica técnica.

- **Duas Abordagens de Explicação:** Há duas abordagens principais para explicar as decisões: baseada no raciocínio lógico ou baseada nos dados utilizados.

- **Parâmetros para o Fornecimento de Informações:**

  a) Clareza e Compreensão: Usar linguagem acessível e evitar termos técnicos complexos.

  b) Objetividade: Informar apenas os critérios relevantes para a decisão.

  c) Proporcionalidade: Fornecer informações proporcionais à necessidade do titular, garantindo que apenas detalhes relevantes e não confidenciais sejam fornecidos.

  d) Finalidade e Base Legal: Indicar a finalidade da decisão automatizada e a base legal que a sustenta.

  e) Acessibilidade: Promover a transparência e a explicabilidade por meio de meios de comunicação acessíveis ao titular.

  f) Documentação: Elaborar um documento explicativo durante o desenvolvimento do sistema de IA, que pode ser fornecido quando necessário.

- **Limites e Parâmetros Relacionados ao Segredo Comercial:**

  g) Restrições Justificadas: O segredo comercial e industrial pode justificar a não divulgação de informações que revelem metodologias de tratamento, dados confidenciais da empresa e informações estratégicas.

  h) Balanceamento: Buscar um equilíbrio entre a transparência e a proteção dos segredos comerciais, garantindo que o titular receba informações úteis sem expor elementos sensíveis.

  i) Compliance com a LGPD: Assegurar que a proteção dos segredos comerciais não impeça a observância dos direitos do usuário, permitindo que ele compreenda os critérios

utilizados e conteste resultados.

Pontos de divergência

- **Nível de Detalhamento das Informações:** Há divergência sobre o nível de detalhamento técnico que deve ser fornecido. Alguns defendem que não é necessário revelar algoritmos ou fórmulas complexas, bastando a transparência quanto aos dados coletados e as finalidades do tratamento automatizado. Outros enfatizam a importância de informações completas e abrangentes.

- **Definição de Segredo Comercial e Industrial:** Existe insegurança jurídica sobre o que seriam informações "claras e adequadas" e como conceituar "segredos comercial e industrial". Informações eminentemente técnicas, como fórmulas, não devem ser abarcadas pelo princípio da transparência.

- **Abrangência do Segredo Comercial:** Há diferentes visões sobre o que abrange o segredo comercial e industrial. Alguns incluem a metodologia do tratamento, dados confidenciais da empresa e informações estratégicas, enquanto outros restringem a divulgação apenas aos elementos essenciais para garantir a transparência, sem comprometer a inovação ou a posição no mercado.

- **Transparência vs. Segurança:** Alguns argumentam que a transparência excessiva pode comprometer a segurança dos sistemas, levando à manipulação e uso malicioso das informações.

- **Auditoria:** Em caso de alegação de sigilo, alguns sugerem que auditorias poderão ser feitas para verificar a veracidade das alegações.

5.51. A análise das ontribuições revela um debate sobre como fornecer informações claras e adequadas sobre decisões automatizadas, equilibrando a transparência com a proteção de segredos comerciais e industriais. Há um consenso sobre a necessidade de informações acessíveis e compreensíveis, mas divergências sobre o nível de detalhamento técnico e a definição do que constitui um segredo comercial. A implementação das diretrizes do art. 20 da LGPD deve considerar o contexto específico de cada caso, buscando um equilíbrio entre a proteção dos direitos dos titulares e a promoção da inovação e do desenvolvimento tecnológico.

BLOCO IV - BOAS PRÁTICAS E GOVERNANÇA

Pergunta 13 - De que forma programas de governança em privacidade podem ser utilizados como um mecanismo de promoção da conformidade do desenvolvimento e uso dos sistemas de IA com a LGPD? Quais requisitos,

especificamente relacionados ao desenvolvimento e uso de sistemas de IA, devem ser observados nesses casos?

5.52. A pauta das contribuições dirigidas à pergunta 13 discutiram a necessidade de programas de governança em privacidade e o Privacy by Design, incluindo questões de transparência, RIPD e avaliação de impacto, e capacitação de colaboradores. Além disso, também foram discutidos a adoção de padrões internacionais e o nível de detalhe a ser empregado em eventual regulamentação pela ANPD.

Pontos de convergência

- **Necessidade de programas de governança em privacidade:** Existe um consenso de que programas de governança em privacidade são fundamentais para assegurar a conformidade com a LGPD no desenvolvimento e uso de sistemas de IA.

- **Privacidade desde a concepção (Privacy by Design):** A abordagem de "Privacy by Design" é amplamente defendida como um princípio essencial na criação de sistemas de IA, garantindo que a privacidade seja considerada desde o início do processo de desenvolvimento.

- **Transparência e comunicação:** A importância da transparência e da comunicação com os titulares de dados é enfatizada, garantindo que os indivíduos compreendam como seus dados estão sendo utilizados e tenham seus direitos respeitados.

- **Relatório de Impacto à Proteção de Dados (RIPD):** O RIPD é citado como um instrumento indispensável para identificar e mitigar riscos relacionados ao tratamento de dados em sistemas de IA.

- **Monitoramento contínuo:** A necessidade de monitoramento contínuo e auditorias é destacada para garantir a conformidade e a eficácia das medidas de proteção de dados ao longo do tempo. Também sugerem auditorias de software com revisão periódica dos algoritmos com potencial de discriminação ou violações da privacidade.

- **Treinamento e capacitação:** A importância de investir em treinamento e capacitação das equipes envolvidas no desenvolvimento e operação de sistemas de IA é ressaltada, abordando princípios da LGPD, ética e prevenção de riscos.

- **Adoção de políticas de privacidade adaptáveis:** Há incentivo à adoção de políticas de privacidade adaptáveis às evoluções de segurança e proteção de dados em sistemas de IA.

- **Segurança e proteção de dados:** A segurança da informação e a proteção

de dados são mencionadas como elementos cruciais dos programas de governança.

Pontos de divergência

- **Obrigatoriedade de algumas práticas:** Enquanto algumas contribuições defendem a aplicação de princípios de governança de dados aos sistemas de IA, como os de qualidade e não discriminação e mesmo os princípios gerais da LGPD, outras consideram que nem todos devem ser obrigatórios. Outras contribuições ressaltam que princípios como privacy by design, avaliação de riscos e boas práticas de anonimização são relevantes, mas é essencial reconhecer que a maioria dos riscos relacionados à IA não envolve dados pessoais e exigem análises de risco muito diferentes daquelas relacionadas a dados pessoais.

- **Âmbito da regulamentação:** Existe debate sobre a necessidade de estabelecer novos requisitos e obrigações para sistemas de IA fora dos limites legislativos existentes. Há contribuições que afirmam não ser possível estabelecer novas obrigações e requisitos ao desenvolvimento e uso de sistemas de IA fora dos limites legislativos. Outras afirmam que a governança de sistemas de IA pode ser considerada uma boa prática, mas inexiste obrigação legal.

- **Nível de detalhe na regulamentação pela ANPD:**Há discussão sobre se a ANPD deve estabelecer requisitos específicos no contexto da IA, com alguns defendendo maior flexibilidade e outros buscando maior clareza e diretrizes. Assim, há contribuição que sugere que a ANPD não se antecipe em estabelecer requisitos específicos no contexto de IA, a fim de não ocasionar insegurança jurídica, devendo aguardar o desenrolar do PL 2338/23. Ainda, a contribuição que afirma que a ANPD não possui competência para emitir regulamentações específicas ou estabelecer requisitos relacionados a programas de governança voltados ao desenvolvimento e uso de inteligência artificial. Assim, a implementação de normas de governança de sistemas de IA pode ser considerada uma boa prática, mas inexiste obrigação legal. Por sua vez, há contribuições que afirmam que a ANPD deve trazer diretrizes de governança de dados pessoais para uso no treinamento e suso de sistemas e modelos de IA, podendo emitir orientações e diretrizes para a governança de dados pessoais usados no treinamento e uso de sistemas de IA.

- **Necessidade de avaliação de impacto para todos os sistemas:** Há divergência sobre se todas as organizações que utilizam sistemas de IA de alto risco devem preparar avaliação de impacto à proteção de dados, ou se organizações que lidam com aplicações de baixíssimo risco não necessitam de avaliação. Assim, há contribuições que sugerem avaliação

de impacto apenas para as organizações que desenvolvam sistemas de IA de alto risco. Outras não fazem distinção. Há contribuições que sugerem a avaliação de impacto algorítmico.

- **Adoção de padrões internacionais:** Enquanto alguns defendem o alinhamento com melhores práticas e padrões internacionais, como o AI Risk Management Framework do NIST e ISO 42001 e 23894, outros podem não exigir essa adoção.

5.53. Assim, verificou-se a convergência sobre a necessidade de programas de governança e privacidade e adoção do Privacy by Design, a importância da transparência e do RIPD; além de pontos como segurança, monitoramento contínuo e capacitação das equipes envolvidas com o tratamento de dados pessoais. Em contrapartida, houve discordância sobre a obrigatoriedade de algumas práticas, a necessidade de regulamentação e o nível de detalhe e flexibilidade de requisitos a serem estabelecidos. A necessidade de avaliação de impacto e a adoção de padrões internacionais também foram temas de contraste.

Pergunta 14 - Considerando o princípio da responsabilização e prestação de contas, quais informações devem ser documentadas durante o ciclo de vida de um sistema de IA? Em quais contextos específicos relacionados a sistemas de IA é recomendada a elaboração de RIPD? Neste caso, é possível estabelecer requisitos específicos a serem observados na elaboração do RIPD?

5.54. Sobre a pergunta 14, foram identificados os seguintes pontos de convergência e divergência:

<u>Pontos de convergência</u>

- **Necessidade de documentação no ciclo de vida da IA:** Várias contribuições concordam que é fundamental documentar todas as etapas do tratamento de dados em sistemas de IA. Isso inclui desde a concepção e planejamento, desenvolvimento, implementação e monitoramento contínuo até a desativação do sistema.

- **Risco como fator determinante para o RIPD:** Há um consenso de que o Relatório de Impacto à Proteção de Dados (RIPD) é mais necessário em contextos de alto risco. A avaliação de risco deve considerar a probabilidade e a severidade dos impactos nos direitos e liberdades dos titulares.

- **Transparência e explicabilidade:** A transparência nos algoritmos e nas decisões automatizadas é amplamente defendida. A documentação deve incluir as justificativas para as decisões automatizadas e os métodos utilizados no treinamento dos algoritmos.

- **Atenção aos direitos dos titulares:** As contribuições enfatizam a importância de garantir os direitos dos titulares de dados, como o direito à informação, acesso, retificação, oposição e portabilidade. Os agentes de IA devem implementar mecanismos para lidar com incidentes de segurança e violações de dados.

- **Governança e responsabilidade:** A necessidade de estabelecer uma cadeia de governança coletiva entre os desenvolvedores e aplicadores de IA é reconhecida. A documentação deve demonstrar a conformidade com os princípios da LGPD e a responsabilização dos agentes.

Pontos de divergência

- **Obrigatoriedade do RIPD:**Algumas contribuições indicam que o RIPD é exigível em todas as circunstâncias previstas na LGPD, independentemente do sistema de IA. Outras sugerem que a necessidade do RIPD deve ser avaliada caso a caso, considerando fatores como o risco e a inovação da IA. Há também quem defenda que a ANPD não deveria estabelecer requisitos específicos para o RIPD envolvendo sistemas de IA, pois a LGPD já é um marco legal suficiente.

- **Especificidade dos requisitos da ANPD:** Existe uma divergência sobre se a ANPD deve ou não estabelecer requisitos específicos para a elaboração de RIPD). Alguns argumentam que a LGPD já fornece as diretrizes necessárias, enquanto outros defendem que a ANPD pode detalhar os requisitos para garantir a conformidade e a proteção de dados. Há contribuições que sugerem uma lista de exemplos de informações a serem documentadas.

- **Conceito de "ciclo de vida" nos sistemas de IA:** Algumas contribuições mencionam a importância de documentar todas as etapas do ciclo de vida da IA, enquanto outras afirmam que o conceito de "ciclo de vida" não se aplica aos sistemas de IA.

- **Âmbito do RIPD:**Há diferentes visões sobre o que deve ser incluído no RIPD. Algumas contribuições detalham os elementos essenciais, como a descrição do tratamento, a avaliação da necessidade e os riscos para os indivíduos. Outras enfatizam a importância de analisar os impactos sociais e éticos e de documentar as medidas de segurança adotadas.

- **Interpretação do "alto risco":** Algumas contribuições afirmam que o RIPD é necessário somente em contextos de alto risco. A interpretação do conceito de "alto risco" é outro ponto de divergência. Algumas contribuições sugerem que critérios específicos devem ser aplicados para evitar a classificação indevida de atividades de baixo impacto como

de alto risco.

5.55. Nesse último ponto, cabe destacar a contribuição que indica que os critérios para identificar situações de alto risco no tratamento de dados são mais específicos quando comparados aos aplicados a sistemas de IA, e que em contextos sem IA, a análise foca nos impactos à privacidade (por exemplo, EDPB adota uma abordagem mais ampla, considerando decisões automatizadas e impactos significativos sobre direitos e liberdades individuais). Afirma que antes de implementar sistemas de IA, é imprescindível realizar avaliação prévia de riscos, além da publicação de uma versão pública do RIPD e a participação de grupos afetados e especialistas na identificação de impactos, especialmente em atividades de alto risco. Recomenda documentar o propósito e o escopo do sistema de IA, incluindo os critérios e métodos usados no treinamento do modelo, objetivos, casos de uso previstos, limitações técnicas e potenciais impactos sociais e éticos, registrando as fontes de dados, métodos de coleta e base legal para o tratamento. A contribuições afirma também que o RIPD deve identificar riscos como discriminação algorítmica, impactos na privacidade e segurança, e descrever estratégias de mitigação para cada risco identificado. Finalmente, indica que a documentação completa do ciclo de vida do sistema, incluindo entradas, saídas, funcionamento dos algoritmos e justificativas para decisões automatizadas, é indispensável para garantir rastreabilidade e transparência.

5.56. Também importa mencionar contribuição que afirma que o RIPD deverá existir sempre quando houver tratamento de dados sensíveis, dados de grupos de vulneráveis, tratamento de alto risco ou quando for utilizada a hipótese legal do legítimo interesse.

Pergunta 15 - Considerando o ciclo de vida de um sistema de IA, em que momento e contexto do tratamento seria viável ou necessária a anonimização? Qual a técnica utilizada? Quais outras medidas de segurança poderiam ser eventualmente utilizadas visando à proteção da privacidade de titulares de dados?

5.57. Destacam-se as seguintes temáticas em relação ao questionamento:

<u>Pontos de convergência</u>

- **A anonimização como boa prática:** Várias contribuições convergem que a anonimização é uma boa prática.

- **A anonimização como medida de segurança:** A anonimização é vista como uma medida acessória de segurança que está vinculada à finalidade inicial dos tratamentos.

- **Anonimização em diferentes fases do ciclo de vida da IA:** A anonimização pode ser necessária e viável em diferentes momentos e contextos no ciclo de vida de um sistema de IA. A anonimização é recomendada especialmente, nos termos de algumas contribuições, nas fases de coleta, armazenamento e compartilhamento de dados.

- **Técnicas de anonimização:** Há várias técnicas de anonimização como criptografia, supressão, generalização, perturbação, pseudonimização, agregação e hashing.

Pontos de divergência

- **Obrigatoriedade da anonimização:** Algumas contribuições indicam que a anonimização é uma boa prática, mas não há obrigação legal expressa de seu uso.

- **A anonimização não é recomendável para alguns sistemas de IA.**

- **Dados anonimizados não configuram tratamento.**

- **A anonimização não implica em consequências para o titular de dados.**

- **Sistemas de IA que apresentem riscos aos direitos fundamentais de titulares de dados devem cumprir com as obrigações da LGPD, ainda que se utilizem de dados inicialmente anonimizados.**

- **A anonimização deve ser feita de forma anterior ao ingresso nos sistemas de IA:** É recomendável que a anonimização seja feita de forma anterior ao ingresso nos sistemas de IA.

- **A anonimização pode ser aplicada em momento posterior ao tratamento nos sistemas de IA, como a tokenização ou generalização:** As técnicas de anonimização podem ser aplicadas em momento posterior ao tratamento nos sistemas de IA.

5.58. Destaca-se a contribuição que afirma que a anonimização, assim como outras opções, como o uso de dados sintéticos e a pseudonimização, deve ser priorizada, mas não deve ser considerada como uma “bala de prata”. Com efeito, ela não reduz o risco a zero de reidentificação e exige monitoramento e avaliação constante para que atenda aos parâmetros mínimos de segurança. Especialmente em sistemas de IA, esse monitoramento constante pode se tornar mais complexo, ou até mesmo impossível. Pelas diferentes lógicas de funcionamento desses sistemas, muitas vezes os desenvolvedores não terão condições técnicas de avaliar com confiança e

precisão tudo que ocorre com um dado entre o “input” e o “output” do sistema. A mesma lógica se aplica para os desenvolvedores de sistema. Assim, a partir da lógica da “caixa preta” não se pode ter certeza de que um sistema de IA não interagiu com um banco de dados a ponto de possibilitar a reidentificação de dados antes anonimizados. **Nesses termos, sistemas de IA que apresentem riscos aos direitos fundamentais de titulares de dados devem cumprir com as obrigações da LGPD, ainda que se utilizem de dados inicialmente anonimizados para seu treinamento ou operação.**

5.59. Assim, percebe-se que, nos termos das contribuições, a **anonimização é vista como uma prática recomendada e, em alguns casos, essencial para proteger a privacidade dos titulares de dados e garantir a conformidade com a legislação, especialmente a LGPD** . No entanto, a anonimização não é isenta de desafios e pode afetar a utilidade dos dados e a capacidade dos modelos de IA.

5.60. As contribuições enfatizam que **o momento ideal para identificar a necessidade de anonimização é no período de desenvolvimento do sistema de IA**. As técnicas de anonimização devem ser proporcionais ao contexto e ao propósito do tratamento dos dados. Além disso, a anonimização deve ser vista como parte de um conjunto de medidas de segurança, incluindo criptografia, controle de acesso e auditorias. **A escolha da técnica de anonimização depende da natureza e organização dos dados**.

5.61. Por sua vez, verificou-se a existência de alguns pontos divergentes, como a recomendação ou não da anonimização para alguns sistemas de IA, a obrigatoridade ou facultatividade de seu uso, o momento ideal para realizar a anonimização (antes do treinamento do modelo ou em diferentes etapas e contextos), e a visão geral sobre a medida, vez que algumas contribuições a consideram como uma medida essencial de segurança, enquanto outras a enxergam como uma das várias medidas de segurança a serem implementadas.

6. DOCUMENTOS RELACIONADOS

6.1. Anexo Contribuição (SEI/ANPD nº0173307);

6.2. Anexo Contribuição (SEI/ANPD nº0173308);

6.3. Anexo Contribuição (SEI/ANPD nº0173310);

6.4. Anexo Contribuição (SEI/ANPD nº0173311);

6.5. Anexo Contribuição (SEI/ANPD nº0173312);

6.6. Anexo Contribuição (SEI/ANPD nº0173313);

6.7. Anexo Contribuição (SEI/ANPD nº0173315);

6.8. Anexo Contribuição (SEI/ANPD nº0173314);

6.9. Anexo Contribuição (SEI/ANPD nº0173316);

6.10. Anexo Contribuição (SEI/ANPD nº0173317);

6.11. Anexo Contribuição (SEI/ANPD nº0173318);

6.12. Anexo Contribuição (SEI/ANPD nº0173319);

6.13. Anexo Contribuição (SEI/ANPD nº0173320);

6.14. Anexo Contribuição (SEI/ANPD nº0173321);

6.15. Anexo Contribuição (SEI/ANPD nº0173322);

6.16. Anexo Contribuição (SEI/ANPD nº0173323);

6.17. Anexo Contribuição (SEI/ANPD nº0173324);

6.18. Anexo Contribuição (SEI/ANPD nº0173325);

6.19. Anexo Contribuição (SEI/ANPD nº0173326);

6.20. Anexo Contribuição (SEI/ANPD nº0173327);

6.21. Anexo Contribuição (SEI/ANPD nº0173328);

6.22. Anexo Contribuição (SEI/ANPD nº0173329);

6.23. Anexo Contribuição (SEI/ANPD nº0173330);

6.24. Anexo Contribuição (SEI/ANPD nº0173331);

6.25. Anexo contribuições OPINEAQUI (SEI/ANPD nº 0173510);

6.26. Consolidação Questões 1 a 15 (SEI/ANPD nº 0178837).

7. CONCLUSÃO

7.1. Tendo em vista todos os pontos aqui destacados, sugere-se que a presente Nota Técnica conste como insumo para os trabalhos e atividades a serem realizados no âmbito do Projeto - Item 7 da Agenda Regulatória para o biênio 2025-2026 da ANPD e, ainda, sirva para o robustecimento da instrução processual referente ao citado projeto regulatório.

7.2. Nesses termos, sugere-se, ainda, encaminhar a presente Nota, junto com seus anexos, à Secretaria-Geral do Conselho Diretor, para conhecimento dos membros deste Colegiado.

À consideração superior.

Brasília-DF, 3 de abril de 2025.

GABRIELA NATACHA BECHARA
Servidora Pública em exercício na CGN

FÁBIO SILVEIRA VIDAL
Servidor Público em exercício na CGN

MARIANA TALOUKI
Coordenadora de Normatização

De acordo. Encaminha-se.

Brasília-DF, 3 de abril de 2025.

RODRIGO SANTANA DOS SANTOS
Coordenador-Geral de Normatização

Documento assinado eletronicamente por **Mariana Almeida de Sousa Talouki**, **Coordenador(a)**, em 03/04/2025, às 15:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Gabriela Natacha Bechara**, **Professor do Magistério Superior**, em 03/04/2025, às 15:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fábio Silveira Vidal**, **Servidor(a) Requisitado(a)-ANPD**, em 03/04/2025, às 15:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral de Normatização**, em 03/04/2025, às 15:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0173345** e o código CRC **18F035F4**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900
Telefone: - https://www.gov.br/anpd/pt-br