2° PRÊMIO
DANILO
DONEDA
DE ARTIGOS CIENTÍFICOS

Artigos científicos vencedores

ANPD

II Concurso de Artigos Científicos da ANPD

— Prêmio Danilo Doneda 2024 —

Artigos científicos vencedores

ANPD
Brasília, DF
2025

Autoridade Nacional de Proteção de Dados

Diretor-Presidente
Waldemar Gonçalves Ortunho Junior

Diretores
Arthur Pereira Sabbat
Miriam Wimmer

Comissão julgadora
Diego Carvalho Machado
Joacil Basílio Rael
Kátia Adriana Cardoso de Oliveira
Lucas Borges de Carvalho
Lucas Costa dos Anjos
Miriam Wimmer

Comissão organizadora
Albert França Josuá Costa
Edgard Costa Oliveira
Fabiana S. P. Faraco Cebrian
Marcus Vinícius Rossi da Rocha
Priscilla Madalena Duarte da Mata

Revisão e organização textual
Albert França Josuá Costa
Edgard Costa Oliveira
Fabiana S. P. Faraco Cebrian
Marcus Vinícius Rossi da Rocha

Projeto gráfico, editoração eletrônica e capa
André Scofano Maia Porto

1ª edição
Publicação digital – PDF (janeiro / 2025)

ANPD · Autoridade Nacional de Proteção de Dados
SCN, Qd. 6, Conj. A
Ed. Venâncio 3000, Bl. A, 9º andar
Brasília, DF · Brasil · 70716-900
www.gov.br/anpd

Sumário

Prefácio

Vivemos em um contexto histórico marcado pela aceleração contínua dos avanços tecnológicos e pela progressiva digitalização das interações sociais, econômicas e políticas. Nesse ambiente dinâmico, o debate acerca da proteção de dados, da privacidade e do uso ético de tecnologias coloca-se como tema central no campo acadêmico, regulatório e prático, não apenas no Brasil, mas também no âmbito global.

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, configura um marco regulatório fundamental, estabelecendo os parâmetros para a governança e o tratamento responsável de dados pessoais em um ambiente digital cada vez mais complexo e conectado. A LGPD contribui para consolidar princípios essenciais, como transparência, responsabilidade, segurança, respeito à privacidade e o fortalecimento dos direitos dos titulares de dados.

A implementação progressiva da agenda regulatória e do mapa de temas prioritários estabelecidos pela Autoridade Nacional de Proteção de Dados (ANPD) torna-se, assim, um elemento essencial para o alcance de um ambiente digital mais seguro, ético e resiliente diante das inovações tecnológicas. Ao evidenciar o ser humano e seus direitos fundamentais como elementos centrais, a LGPD não apenas estimula a confiança no tratamento de dados pessoais, mas também promove a construção de uma sociedade em que o tratamento de dados pessoais seja realizado de forma justa, equilibrada e orientado pelo bem comum.

Desde sua criação, em 2023, o Prêmio Danilo Doneda vem se afirmando como uma iniciativa para o fortalecimento da produção acadêmica nacional sobre proteção de dados, demonstrando o compromisso contínuo da ANPD com a ampliação do debate e a construção de uma cultura de conscientização sobre a relevância dos dados pessoais. O engajamento da ANPD com o meio acadêmico, refletido na realização deste concurso, não apenas incentiva os pesquisadores e a renovação de ideias sobre o tema, mas também reforça a importância da pesquisa científica como ferramenta para o aperfeiçoamento dos marcos regulatórios e das práticas sociais.

É nesse contexto que se insere a presente coletânea de artigos científicos vencedores do II Concurso de Artigos Científicos – Prêmio Danilo Doneda, promovido pela ANPD. Instituído em homenagem ao jurista e professor Danilo Doneda, figura central na construção do arcabouço jurídico e acadêmico da proteção de dados pessoais no Brasil, o prêmio desempenha um papel significativo na promoção do conhecimento e no incentivo à pesquisa, consolidando-se como uma ação que permite a reflexão crítica no campo da privacidade e proteção de dados por jovens pesquisadores.

Nessa segunda edição do Prêmio Danilo Doneda, recebemos artigos provenientes de todas as regiões do País, assim como a abordagem de temas diversificados. Isso revela não apenas o aumento do interesse acadêmico pelo assunto, mas também o amadurecimento de um ecossistema de pesquisadores comprometidos com a consolidação dos pilares da LGPD e com o diálogo entre teoria e prática.

Esta coletânea, que engloba os artigos premiados, não se limita a ser um registro do pensamento sobre a proteção de dados, mas reflete a multiplicidade de desafios e oportunidades apresentados pela era digital, como pode ser observado pelos temas abordados.

O primeiro artigo, "Entre Riscos e Obrigações: A Atuação do Controlador em Incidentes de Segurança", aborda a responsabilidade do controlador diante de incidentes de segurança, evidenciando a necessidade de posturas proativas frente aos riscos crescentes de vazamento de dados. A análise, fundamentada na LGPD, destaca não apenas o arcabouço normativo, mas também as implicações reputacionais e jurídicas, convidando o leitor a refletir sobre as melhores práticas de *compliance* e gestão de incidentes.

Já o segundo artigo, "Diga-me o que Você Curte, que eu lhe Direi Quem Você é: O Direito à Explicação na Lei Geral de Proteção de Dados", adentra o debate sobre o direito à explicação diante de decisões automatizadas, examinando a autodeterminação informativa dos titulares e as consequências éticas, legais e técnicas da automatização de processos decisórios. Esse estudo conecta-se diretamente com questões atuais no campo da regulação da inteligência artificial, colocando em evidência a tensão entre inovação

tecnológica e garantias fundamentais de transparência sobre o tratamento de dados pessoais.

Por fim, o artigo "Entre a Transparência e a Proteção: A Compatibilização da Lei de Acesso à Informação à Lei Geral de Proteção de Dados na Divulgação de Dados Públicos" trata do equilíbrio entre o direito de acesso à informação e o direito à proteção de dados pessoais no contexto da Administração Pública. A análise propõe soluções interpretativas e legislativas que viabilizem uma harmonização entre esses direitos, assegurando a coexistência construtiva entre a transparência e o respeito à privacidade.

Agradecemos aos autores, à Comissão Julgadora, à Comissão Organizadora e a todos os envolvidos nesta iniciativa pela dedicação e excelência demonstradas. Esperamos que esta coletânea sirva não apenas como fonte de informação e inspiração para pesquisadores, gestores, formuladores de políticas e a sociedade em geral, mas também como um convite ao aprofundamento dos debates e à busca de soluções inovadoras e responsáveis para os desafios que permeiam a proteção de dados na era digital.

Que a leitura deste volume seja instigante, produtiva e formadora de novas perspectivas, contribuindo para o fortalecimento de uma cultura nacional de proteção de dados fundamentada na responsabilidade, na transparência e na inovação, em consonância com a missão da Autoridade Nacional de Proteção de Dados.

Waldemar Gonçalves Ortunho Junior
Diretor-Presidente da Autoridade Nacional de Proteção de Dados – ANPD

Miriam Wimmer
Diretora da Autoridade Nacional de Proteção de Dados – ANPD

Arthur Pereira Sabbat
Diretor da Autoridade Nacional de Proteção de Dados – ANPD

Sobre os premiados

1º lugar

Bruno Junqueira Meirelles Marcolini

Bacharel em direito pela Universidade Federal do Paraná e pós-graduando em direito digital pela Fundação Getúlio Vargas – São Paulo. É especialista nas áreas de direito digital e propriedade intelectual.

2º lugar

Eduarda Costa Almeida

Mestranda no programa "Digital humanities: political ideas in a digital age". Pesquisadora em Infraestrutura Pública Digital na Data Privacy Brasil. Bacharel em Direito pela Universidade de Brasília (UnB). Monitora da pós-graduação em Direito Digital e Proteção de Dados do Instituto Brasiliense de Direito Público (IDP). Pesquisadora do Privacy Lab-CEDIS/IDP. Coordenadora de Estudos do Observatório da LGPD/UnB. Advogada.

3º lugar

Fernanda Magni Berthier

Pós-Graduanda em Direito Empresarial pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Bacharela e laureada em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Realizou período de mobilidade acadêmica na Universidade de Lund – Suécia. Experiência em diversas competições acadêmicas e em coaching das equipes da UFRGS.

Artigos científicos vencedores

1º lugar

Entre riscos e obrigações: a atuação do controlador em incidentes de segurança

Bruno Junqueira Meirelles Marcolini

Resumo

Este trabalho tem por objetivo analisar as responsabilidades atinentes ao controlador em casos de incidentes de segurança e seus riscos perante a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados, LGPD), tendo como parâmetro principal os princípios da segurança, prevenção e responsabilização e prestação de contas. A LGPD conferiu um novo grau de atenção sobre a proteção de dados e a segurança da informação, obrigando os agentes de tratamento a observar variadas questões relacionadas ao risco e ao dano relevante aos titulares. Entretanto, com a alta constante de incidentes, a dúvida sobre quais procedimentos adotar para mitigar efeitos e evitar responsabilizações ainda paira, provando que os conceitos da LGPD ainda não são amplamente compreendidos. Assim, por meio de revisão bibliográfica, análise literária-científica, legislativa, jurisprudencial e doutrinária, assim como por meio da interpretação de notícias, utilizou-se o método hipotético-dedutivo para alcançar o objetivo supracitado. O estudo se baseou no disposto na LGPD, enfrentando: (i) contexto e definições da lei para incidentes; (ii) princípios legais; (iii) modalidades de incidentes segundo o Grupo de Trabalho do Artigo 29; (iv) publicações da Autoridade Nacional de

Proteção de Dados (ANPD); (v) obrigações e procedimentos decorrentes do texto legal; e (vi) casos de incidentes nacionais e internacionais. Desta forma, o trabalho resulta na indicação das obrigações e dos procedimentos a serem adotados pelo controlador frente ao incidente, concluindo que a inércia em relação às obrigações previstas na LGPD resultará em responsabilização, mesmo que se entenda que o controlador é também uma das vítimas do incidente.

Palavras-chave: *Incidente; LGPD; Segurança; Prevenção; Responsabilização.*

Introdução

Especialmente no mundo digital, a proteção de dados emergiu como uma das maiores prioridades para empresas e indivíduos. Com a proliferação de tecnologias da informação e a crescente dependência de sistemas digitais para a realização de atividades cotidianas, o volume de dados gerados, armazenados e processados atingiu níveis sem precedentes. Esses dados, que incluem informações pessoais, financeiras e corporativas, são frequentemente alvo de cibercriminosos, tornando os incidentes um risco de alta criticidade.

Tais incidentes, como ataques de *ransomware* e acessos não autorizados, podem ter consequências devastadoras. Além das perdas financeiras diretas, as empresas podem sofrer danos reputacionais, perda de confiança dos clientes e, em alguns casos, enfrentar sanções legais. O prejuízo é igualmente avistado para os indivíduos, cuja exposição dos dados pessoais pode levar a fraudes, roubo de identidade e outros impactos negativos nas vidas privada e profissional.

O mundo contemporâneo vem enfrentando a chamada "Epidemia de Vazamento de Dados", situação em que, ano após ano, verifica-se o aumento do número de incidentes globalmente (Hartzog; Solove, 2022). Ainda que tal aumento tenha impulsionado uma maior preocupação das organizações com a segurança da informação, o ápice dessa epidemia ainda não foi alcançado, com a curva de incidentes em ascendência e sem sinais de mudança.

Esse cenário pode ser confirmado ao analisarmos o histórico de incidentes em um país continental como os Estados Unidos, que passou de um total estimado de cinquenta e cinco milhões de dados comprometidos em incidentes (conforme apuração realizada em 2005), para um bilhão, trezentos e sessenta e nove milhões de dados comprometidos em incidentes (conforme apuração realizada em 2018) segundo dados do Privacy Clearing House (Data Breaches Chronology, 2024), um aumento de 2.385,34%.

Em outra perspectiva, um relatório da IT Governance Europe (Data Breaches and Cyber Attacks, 2024) revelou que cerca de dois bilhões de registros foram violados em incidentes apenas entre novembro de 2023 e abril de 2024, na Europa. Nota-se, portanto, que a problemática dos incidentes não representa uma novidade, ao contrário, trata-se de um problema histórico e que ainda não está perto de uma solução eficaz.

A América Latina, e, portanto, o Brasil, não representam uma exceção ao contexto mundial. Dados do Relatório de Segurança ESET 2023 revelaram que 69% das empresas pesquisadas na América Latina sofreram algum tipo de incidente em 2022, das quais 66% indicaram roubo ou vazamento de dados em seus relatos. A pesquisa indicou, ainda, que 65% das organizações consideram que os investimentos em cibersegurança não são suficientes para a realidade da empresa, face às ameaças de cibercriminosos (Security [...], 2024).

O Brasil, de forma isolada, também possui índices alarmantes. Segundo o relatório da empresa NordVPN, o país liderou o ranking de nações com o maior volume de dados vazados no ano de 2023, com 54 milhões de *cookies* vazados, superando Estados Unidos, Indonésia e Índia, que historicamente lideravam as estatísticas. Entre as informações usualmente comprometidas estão o nome completo, e-mails, endereços e senhas das vítimas (Santana, 2024).

Em outra perspectiva, o levantamento do CISO Advisor (Brasil [...], 2023) indicou que foram registrados 2,29 bilhões de registros violados em 2022, correspondendo a 257 terabytes. Desse total, o Brasil responde por 112 terabytes, o que significa 43% da totalidade dos dados vazados no mundo.

É possível compreender o número elevado de dados vazados no Brasil ao comparar com o índice de busca por adequação à Lei

Geral de Proteção de Dados (LGPD) no país. Segundo o estudo IT Trends Snapshot, realizado pela empresa Logicalis, em 2023 apenas 36% das empresas declararam estar em conformidade total com a lei (Lisboa; Takano, 2023). Ainda que não seja indicado afirmar que uma empresa de fato se encontre em total conformidade com a LGPD (Prado, 2022), o número alto de incidentes é mais bem compreendido quando observamos que, em 2023, 64% das empresas não possuem um nível satisfatório em seu programa de privacidade (Aderência [...], 2023), mesmo com a LGPD na iminência de completar quatro anos desde sua entrada em vigor.

Nesse sentido, importa apresentar também as consequências de um incidente. Consoante com o relatório anual Cost of a Data Breach Report 2024, realizado pela IBM Security (Cost [...], 2024), o custo médio de um incidente no mundo atingiu o maior valor da história em 2024, com US$ 4,88 milhões (maior salto desde a pandemia). O número representa um aumento de 10% em relação ao custo em 2023, de US$ 4,45 milhões. Em uma visão de longo prazo, o custo médio aumentou 35,6% em relação aos US$ 3,86 milhões do relatório de 2020. Imperioso destacar também o custo operacional, pois a depender da modalidade do incidente, conforme será explicado ao longo deste trabalho, o controlador (responsável legal pelas operações de tratamento) poderá perder o acesso aos dados que viabilizam processos internos e externos (Jimene, 2020). Analisar o dano à reputação também importa, uma vez que clientes, atuais ou futuros, terão um temor natural ao se relacionarem com organizações que não aparentam tomar os cuidados necessários com a proteção de seus dados (Zalaf, 2024).

Apresentado o contexto geral dos incidentes ao redor do globo, confirma-se a existência da "Epidemia de Vazamento de Dados". O número de incidentes vem crescendo, mas o índice máximo possível não dá indícios de ter sido alcançado. Esse cenário evidencia os riscos para as organizações, que podem ser vítimas de uma tentativa de ataque a qualquer momento. Contudo, a situação se agrava ainda mais quando os devidos cuidados com a proteção de dados não são adotados, pois a posição de vítima em um incidente, por si só, não afastará a responsabilidade e a possibilidade de sanções da ANPD por violação legal.

Incidentes de segurança: definição e categoria

Para ser apto a neutralizar a ameaça de um incidente, o controlador deve saber o que a ameaça simboliza e quais são seus aspectos principais.

Seguindo uma interpretação harmônica da LGPD, incidente é o acontecimento indesejado ou inesperado capaz de colocar em risco a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações ilícitas ou acidentais, incluindo perdas, alterações, compartilhamento ou qualquer outra forma de tratamento não autorizado (Jimene, 2022).

Sobre este ponto, destaca-se que a LGPD não detém a exclusividade no tema da proteção de dados pessoais e de segurança de informação, de forma que o conceito de incidente não é restrito à referida lei. Do contrário, existem previsões nesse sentido na Constituição Federal, *e.g.*, art 5º, X, XII e LXXII (Brasil, 1988), bem como no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet. O que singulariza a regulação da LGPD é a sua abrangência, com a enunciação de princípios, direitos, responsabilidades e demais aplicações decorrentes do tratamento de dados pessoais (Doneda, 2021), motivo pelo qual se optou por seguir os preceitos da LGPD ao se tratar de incidentes neste trabalho. Nesse sentido, a ANPD apresentou a definição de incidente na Resolução CD/ANPD nº 15, publicada em 2024:

> Art. 3º Para efeitos deste Regulamento, são adotadas as seguintes definições: [...]
> XII - incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais; (Autoridade Nacional de Proteção de Dados, 2024)

Da análise da adjetivação apresentada pela ANPD, é possível extrair detalhes importantes. No dicionário da língua portuguesa, define-se o significado da palavra "adverso" como algo não favorável, sendo o antônimo de benefício. O incidente, portanto, traz consigo um ônus ao controlador. Da mesma forma, o significado de confir-

mado se refere a uma situação que se tornou certa e comprovada (Dicio, 2010). Logo, aos olhos da LGPD, um incidente se caracteriza por sua concretude fática, não devendo se tratar de uma hipótese.

Ademais, incidentes podem ocorrer de maneira acidental ou proposital, não se restringindo a situações apenas de confidencialidade, mas abrangendo também eventos de perda ou indisponibilidade dos dados pessoais (Autoridade Nacional de Proteção de Dados, 2022). Todo vazamento de dados pessoais é um incidente, mas nem todo incidente é um vazamento (Gomes; Govea, 2024).

Salienta-se, por fim, que a simples existência de determinada vulnerabilidade em um sistema não acarreta por si só um incidente, que depende da exploração da vulnerabilidade de forma concreta e adversa ao controlador. A forma da exploração definirá a extensão das consequências aos agentes de tratamento (controladores e operadores), definindo a categorização do incidente como sendo um incidente de confidencialidade, integridade e disponibilidade.

Incidente de confidencialidade

Para realizar a categorização dos incidentes, o presente trabalho utilizou a classificação do Grupo de Trabalho do Artigo 29, extinto órgão consultivo independente da União Europeia (UE), criado pela Diretiva 95/46/CE (União Europeia, 1995).

A primeira categorização de incidente diz respeito à confidencialidade dos dados pessoais. Essa modalidade ocorre quando há acesso e/ou divulgação não autorizada pelo controlador (União Europeia, 2018). Para tais casos, é comum que os incidentes sejam acompanhados de ataques a sistemas, ocasionando a intrusão e disseminação de acessos indevidos. Aqui existe o interesse em expor dados de cunho pessoal, possibilitando formas de exploração econômica da informação. Em outros casos, incidentes de confidencialidade ocorrem quando há tentativas ou acessos não autorizados em um sistema, utilizando, para tanto, técnicas como força bruta SSH, varreduras ou fraudes de engenheira social (Bioni, 2021).

Exemplos recorrentes dessa modalidade de incidente são os casos de *phishing*, que são mensagens digitais ou de voz que visam manipular as vítimas (geralmente com publicidade enganosa),

fazendo com que ela compartilhe informações confidenciais, faça download de software malicioso, transfira dinheiro ou bens para pessoas desconhecidas ou que realize outras ações prejudiciais (O que [...], 2024).

Um exemplo notório de incidente de confidencialidade no Brasil foi o da Apelação Cível nº 1065936-51.2020.8.26.0002[1]. No caso prático, determinado cliente do serviço de telefonia móvel da Vivo ingressou com uma ação de indenização por danos morais contra a empresa. Segundo o autor, a empresa disponibilizou seus dados pessoais para uma pessoa não autorizada, sua noiva (disfarçada de mãe do autor), que telefonou para o serviço de atendimento para confirmar a existência de uma linha telefônica. Conforme o autor, a atendente não apenas confirmou a existência da linha, como também informou à noiva a data de adesão, o número de faturas emitidas e o valor das faturas pagas. Para o autor, a conta era sigilosa e não deveria ter sido compartilhada com nenhuma outra pessoa que não o seu titular. Após ter acesso às informações pela Vivo, a noiva rompeu com o noivado.

Em sentença proferida pela 2ª Vara Cível do Foro Regional de Santo Amaro, a ação foi julgada improcedente com a condenação do autor por litigância de má-fé (10% do valor da ação), sob o argumento de que a esposa simbolizava uma "pessoa de confiança" que possuía presunção de acesso para informações confidenciais.

Entretanto, o Acórdão do Tribunal de Justiça do Estado de São Paulo, relatado pelo Desembargador Costa Wagner, reverteu a de-

1 Apelação. Ação de indenização por danos morais. Prestação de serviços de telefonia. Direito do Consumidor. Responsabilidade civil. Sentença de improcedência. Recurso do Autor. Ré que confirmou dados do Autor à pessoa estranha não titular da linha telefônica. Conduta perpetrada pela Ré que violou seu dever de sigilo de dados. Ofensa clara aos ditames da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Falha na prestação de serviço verificada. Responsabilidade objetiva do prestador de serviço. Risco da atividade que não pode ser transferido ao consumidor. Situação que levou ao fim do noivado do Autor. Indenização por danos morais no importe de R$ 10.000,00 (dez mil reais). Sentença reformada. Litigância de má-fé afastada. Sucumbência invertida. RECURSO PROVIDO. (TJSP; Apelação Cível 1065936-51.2020.8.26.0002; Relator (a): L. G. Costa Wagner; Órgão Julgador: 34ª Câmara de Direito Privado; Foro Regional II - Santo Amaro - 2ª Vara Cível; Data do Julgamento: 21/02/2022; Data de Registro: 28/02/2022).

cisão, afirmando que houve negligência por parte da empresa ao disponibilizar as informações para terceiros.

Incidente de integridade

A segunda categorização diz respeito à integridade das informações, ocorrendo quando há alteração não autorizada, mesmo que não intencional, dos dados pessoais (União Europeia, 2018). Essa categoria abarca também os incidentes de autenticidade, mencionados na resolução CD/ANPD nº 15, supracitada.

Incidentes dessa categoria são comumente marcados por ações acidentais, em que uma pessoa autorizada a tratar os dados altera um ou mais dados pessoais. Todavia, casos de invasões e alterações de dados fraudulentas também são comuns (Jimene, 2022).

O Poder Judiciário Brasileiro já registra exemplos de litígios dessa modalidade de incidente, como o Recurso Inominado 0008309-97.2021.8.16.0019[2]. Em tal caso, a autora relata que se dirigiu a uma sede da empresa Lojas Americanas para comprar um portão para pet. Na ocasião, o empregado da loja procedeu com o cadastro e simulou a compra, que não chegou a ser concluída, pois a autora não concordou com o valor do frete.

Dias depois, a autora foi surpreendida com a notificação de uma compra no valor de R$ 782,69 da mesma loja, sem nunca ter realizado tal operação. Alegou, então, que seus dados cadastrais haviam sido alterados sem seu consentimento, pois o endereço e o nome do destinatário que constavam na compra eram distintos do cadastro realizado presencialmente na loja. Aduziu, ainda, que a Lojas Americanas não tomaram os devidos cuidados para a proteção dos dados pessoais, sem a verificação da integridade e acurácia dos dados no momento da compra.

2 Recurso Inominado. Residual. Compra desconhecida e não autorizada. Uso indevido de dados pessoais da consumidora. Alteração não consentida das informações cadastrais. Falha no tratamento dos dados. Segurança e prevenção não observadas. Violação à LGPD. Indenização por dano moral majorada. Adoção do método bifásico. Precedente do STJ. Adequação aos parâmetros da turma recursal e às circunstâncias do caso. Recurso conhecido e provido. (TJPR - 2ª Turma Recursal - 0008309-97.2021.8.16.0019 - Ponta Grossa - Rel.: Juiz de Direito Substituto Maurício Pereira Doutor - J. 10.06.2022).

Em segunda instância, o Juiz de Direito da Segunda Turma Recursal dos Juizados Especiais do Paraná, afirmou que não se tratava de uma simples compra não autorizada, mas de um caso de alteração unilateral e não autorizada dos dados cedidos para a finalidade do cadastro. Concluiu, então, afirmando que o ocorrido (incidente de integridade) comprovou a falha da ré na guarda dos dados pessoais, em desrespeito flagrante ao princípio da segurança previsto na LGPD.

Incidente de disponibilidade

A terceira e última categoria ocorre quando há perda de acesso ou destruição dos dados pessoais (União Europeia, 2018). Incidentes dessa modalidade são associados à perda de acesso, interrupção de serviços, destruição de dados pessoais e falhas técnicas.

O exemplo mais recorrente para ilustrar essa categoria é o *ransomware*, um modelo de *malware* que busca bloquear dados e dispositivos da vítima e depois ameaça mantê-los bloqueados caso um resgate não seja pago (Ramsomware, [s.d.]).

A crescente eficiência dos ataques de *ransomware* ajuda a ilustrar os motivos pelos quais o mundo atravessa a Epidemia de Vazamento de Dados e o motivo pelo qual os cuidados com a segurança da informação não devem ser negligenciados. Isto porque o *ransomware* possui diversas variantes como, por exemplo, a *CryptoLocker*, o *WannaCry* e o *Ryuk*, cada uma com diferentes métodos para infectar uma rede ou um dispositivo (Ramsomware, [s.d.]). A dificuldade do controlador de implementar simultaneamente medidas de combate às técnicas de *ransomware* como *phishing*, roubo de credenciais, *downloads drive-by* ou outros *malwares* aumenta a probabilidade de brechas que podem ser exploradas pelo cibercriminoso.

Nesse cenário, o Brasil já ocupa o 2º lugar no *ranking* mundial de tentativas de *ransomware* (Brasil [...], 2023), onde 83% das organizações que sofreram ataques em 2023 somaram o valor médio de R$ 6 milhões despendidos para resgate dos dados sequestrados (Sutto, 2024).

Um exemplo emblemático de *ransomware* no Brasil ocorreu em 2021 com as Lojas Renner. Em 19 de agosto de 2021, a empresa sofreu um ataque que paralisou parte de seus sistemas, incluindo o site oficial da empresa, a plataforma de comércio eletrônico e os serviços de pagamento. O funcionamento das lojas físicas também foi paralisado, tendo sido retomado apenas três dias depois, em 22 de agosto de 2021 (Renner [...], 2021).

Segundo fontes não oficiais, a empresa teria pago o valor de R$ 20 milhões (em criptomoedas) para o resgate dos dados (Após [...], 2021).

Independentemente de qualquer valor efetivamente gasto para reobter o acesso à base de dados, o caso ajuda a ilustrar a extensão do prejuízo financeiro, operacional e reputacional que um incidente de disponibilidade pode ofertar, considerando todo o período que as operações da empresa foram prejudicadas pelo *ransomware*.

Por fim, cabe ressaltar que a divisão dos incidentes em categorias de confidencialidade, integridade/autenticidade e disponibilidade não é taxativa. Trata-se de uma divisão para auxiliar na compreensão do incidente e suas consequências. Contudo, a depender das circunstâncias, um incidente pode abranger confidencialidade, integridade/autenticidade e disponibilidade ao mesmo tempo, assim como qualquer combinação entre as categorias (União Europeia, 2018).

Obrigações de adoção de medidas de segurança pelo controlador e os princípios da LGPD

O princípio da segurança – Art. 6º, VII, LGPD

Ainda que os agentes de tratamento se configurem como vítimas na ampla maioria dos casos de incidentes, tal posição não possui o condão de eximir, por si só, a organização da responsabilização pelo ocorrido perante a LGPD. A tomada de medidas de segurança administrativas e técnicas é necessária como prevenção e não apenas para remediar incidentes e violações.

Tal afirmação se encontra expressa no art. 46 da LGPD:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Brasil, 2018)

As medidas técnicas, mencionadas no dispositivo, se referem aos meios adotados no âmbito da tecnologia da informação, com a utilização de recursos informáticos que mantenham os dados pessoais seguros, ou seja, longe de acessos indevidos (Vainzof, 2022). Controle de tráfego de dados nas redes, criptografia, segregação de servidores e ferramentas de autentificação de acesso são alguns exemplos de medidas técnicas aptas a serem adotadas pelo controlador.

Medidas administrativas, por sua vez, são as ações adotadas no âmbito administrativo-gerencial, visando um funcionamento entre os indivíduos (integrantes do quadro organizacional ou externos a ele) e a organização. Exemplos de tais medidas são políticas de privacidade, acordos de confidencialidade e treinamentos de capacitação sobre proteção de dados e segurança da informação (Vainzof, 2022).

A LGPD não impõe medidas específicas e, inclusive, indica que a ANPD poderá dispor sobre os padrões técnicos mínimos para que o agente de tratamento siga o disposto no art. 46. A avaliação do nível de segurança adequado deverá ser feita pelo controlador no caso concreto, sempre mediante a análise do risco à proteção dos dados pessoais.

Ressalta-se, todavia, que o emprego do verbo "dever" no texto do art. 46 da LGPD elimina a noção de faculdade para o controlador, que se obriga a adotar as medidas também em respeito ao princípio da segurança (Cots; Oliveira, 2018).

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> VII - segurança: utilização de medidas técnicas e administrativas aptas

> a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; (Brasil, 2018)

Tal princípio representa uma herança direta do princípio da integridade e confidencialidade do General Data Protection Regulation (GDPR), que determina que o tratamento dos dados pessoais deve ser realizado de forma que garanta a segurança dos dados contra perda ou destruição, tratamentos não autorizados ou danificação, com a adoção de medidas técnicas e administrativas (Vainzof, 2021).

O GDPR destaca ainda mais a importância da adoção de medidas de segurança baseadas em análises de risco durante o tratamento por meio de seu art. 32, que também obriga o controlador a levar em conta as técnicas de segurança mais avançadas disponíveis, os custos de aplicação, o âmbito, o contexto e as finalidades do tratamento.

Penalidades pela ausência de adoção de medidas de segurança prévias a incidentes, inclusive, não são novidade em solo europeu. Em 2021 no Chipre, por exemplo, a autoridade de proteção de dados pessoais cipriota impôs uma multa de € 40 mil sobre o time de futebol Apoel FC e outra de € 25 mil para a desenvolvedora que projetou a ferramenta para comercialização dos ingressos da equipe após um incidente de confidencialidade, ocasionado por uma falha de segurança, que permitiu que um *cracker* tivesse acesso a todos os dados pessoais cadastrados na plataforma para determinado jogo da equipe.

Na fundamentação, a *Commissioner* afirmou que o clube e sua fornecedora descumpriram com o disposto no art. 32 do GDPR, pois as medidas de segurança adotadas não eram robustas o suficiente para a realidade dos tratamentos realizados na plataforma de um clube com milhares de torcedores (Fuziny *et al*., 2023).

Em outra decisão de 26 de junho de 2024, a autoridade de proteção de dados espanhola impôs uma multa à Axa Real Estate Investment Managers Iberica S.A. (“Axa”) e à Seur Geopost, S.L. (“Seur”) de € 80 mil (para cada empresa) pela negligência na adoção de medidas de segurança face a um incidente de confidencia-

lidade (Agencia Española de Protección Datos, 2024). Segundo a fundamentação apresentada na decisão, a Axa enviou pelo correio um envelope que continha um *pen-drive* com dados pessoais de 143 indivíduos para a Seur, incluindo informações sobre meios de pagamento. O *pen-drive* estava criptografado, mas a senha estava dentro do envelope. Posteriormente, o envelope foi devolvido, mas sem o pen-drive nem a senha dentro.

Ao obter ciência do ocorrido, as empresas notificaram a AEPD e realizaram buscas internas e externas para averiguar se houve vazamento das informações condidas no *pen-drive*, mas não encontraram nada. Contudo, a ausência de protocolos para tornar o procedimento mais seguro foi o suficiente para que a autoridade espanhola impusesse as multas.

Os casos citados acima ajudam a ilustrar a postura determinante das autoridades europeias em sancionar agentes de tratamento que não adotam medidas de segurança adequadas para a realidade de seus tratamentos, face ao princípio da integridade e confidencialidade do GDPR. O exemplo europeu também é fundamental para compreender a dimensão do possível prejuízo pecuniário que um agente de tratamento pode ter no Brasil, visto que as sanções previstas na LGPD já podem ser aplicadas desde 2023 (Autoridade Nacional de Proteção de Dados, 2023).

O princípio da prevenção – Art. 6º, VII, LGPD

O intuito da LGPD enquanto uma legislação de proteção de dados nacional é alterar a cultura de tratamento de dados pessoais realizada no Brasil para uma realidade mais segura e menos intrusiva aos titulares (Vainzof, 2022). Para esse escopo, é fundamental que os riscos associados ao tratamento sejam endereçados desde o princípio da atividade, antes mesmo do tratamento iniciar.

Para tanto, a LGPD obriga a adoção de ações proativas do controlador, que deve tomar medidas preventivas desde a fase de concessão do produto ou do serviço até a fase de execução. É o chamado *Privacy by Design*, respaldado principalmente pelo princípio da prevenção e pelo § 2º do art. 46.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> Art. 46. [...]
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (Brasil, 2018)

O *Privacy by Design* é um conceito desenvolvido por Ann Cavoukian, ex-Comissária de Informação e Privacidade da Província de Ontário no Canadá. O conceito busca incorporar técnicas de privacidade no processo produtivo de produtos e serviços, visando incorporar uma mudança organizacional que lide com ameaças à privacidade dos titulares antes que elas se confirmem (Costa; Alencar, 2021).

Para cumprir com o princípio da prevenção de forma plena sugere-se a aplicação do *Privacy By Design*, onde o controlador deve contemplar os sete pilares previstos por Cavoukian, a saber: (i) *Proactive not Reactive – Preventative not Remedial:* adoção de postura e medidas preventivas, evitando ações reativas; (ii) *Privacy as the Default:* as configurações padrões dos sistemas devem visar a preservação da privacidade do usuário; (iii) *Privacy Embedded into Design:* a arquitetura dos sistemas e modelos de negócio devem incorporar a privacidade, tornando a proteção de dados um elemento essencial; (iv) *Full Functionality – Positive-Sum, not Zero-Sum:* os interesses legítimos do controlador e do titular devem ser levantados e informados de forma transparente, evitando falsas dicotomias que acarretem a mitigação de direitos; (v) *End-to-End Security – Li-*

fecycle Protection: a segurança aos dados pessoais é incorporada para todo o ciclo de vida do dado, garantindo prevenção de ponta-a-ponta; (vi) *Visibility and Transparency:* todos os envolvidos no tratamento devem ser informados transparentemente acerca do modelo de operação e dos componentes utilizados, sempre com base na premissa do tratamento; e (vii) *Respect for User Privacy:* os interesses do usuário/titular devem ser respeitados, mantendo o padrão da privacidade o mais alto possível (Information and Privacy Commissioner of Ontario, 2018).

Quando da aplicação do *Privacy by Design*, caberá ao controlador formular e balizar as regras de governança e boas práticas de sua organização para melhor atender os titulares e a demanda interna.

O caso do navegador de internet *Mozilla Firefox* pode ser utilizado como um exemplo positivo de incorporação aos pilares do *Privacy by Design*. Conforme o manifesto da empresa, o design de todos os produtos é pensado para evitar surpresas ao usuário, transferindo o máximo de controle ao titular de dados e utilizando a menor quantidade de dados possível. Assim, a experiência do usuário passa por menos tópicos sensíveis, aumentando os índices de segurança (Manifesto [...], [s.d.]).

Ademais, para além de uma política de privacidade detalhada para cada produto, diversas funcionalidades de privacidade são ativadas por padrão, acrescentando segurança ao navegador sem que a experiência do usuário seja atrapalhada por requisições tardias. Algumas das medidas adotadas pelo navegador são: (i) navegação privada que não salva o histórico de pesquisa, cookies ou dados temporários; (ii) gestão de permissões fragmentadas que permite ao usuário optar por consentir sobre o uso de câmera, localização, notificações, etc.; (iii) uso de criptografia de ponta-a-ponta; e (iv) configurações de privacidade que permitem a visualização da coleta de dados e possíveis ajustes (Princípios [...], [s.d.]).

Assim, o exemplo do Mozilla pode servir de inspiração para organizações que buscam implementar o *Privacy by Design* em seus produtos e serviços.

O princípio da responsabilização e prestação de contas – Art. 6º, X, da LGPD

Não seria lógico que a LGPD obrigasse o controlador a adotar medidas de prevenção sem prever meios de responsabilização caso tais obrigações não fossem cumpridas. De tal forma, o princípio da responsabilização e prestação de contas, previsto expressamente por meio do art. 6º, X da LGPD reafirma a necessidade do cumprimento das exigências legais, determinando, ainda, a demonstração da eficácia das medidas adotadas.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018)

Dessa forma, o controlador deverá analisar a conformidade legal e implementar as medidas de proteção de dados com base nas suas próprias ponderações de risco, levando em conta todo o ciclo de vida do dado pessoal sob sua responsabilidade.

Nesse sentido, a realização das avaliações de conformidade não possui determinações específicas pela LGPD. Contudo, práticas de mercado recomendam que o controlador avalie o tratamento com base nos princípios da LGPD, com destaque para os princípios da finalidade, da adequação e da necessidade, analisando se os direitos dos titulares não são sobrestados pelo tratamento de dados e se a hipótese legal alocada é válida (Vainzof, 2022).

Já no tocante à prestação de contas, o controlador deverá realizar o registro de suas operações de tratamento (Art. 37 da LGPD). Esse registro, denominado *Record of Processing Activities* (RoPA) ou Registro de Atividades de Tratamento de Dados Pessoais, possui dupla funcionalidade, uma vez que poderá ser exigido a qualquer momento pela ANPD, para averiguação de conformidades diversas (Art. 55-J, IV da LGPD) e em razão de hipóteses de reversão de ônus da prova a favor do titular dos dados (Art. 42, § 2º da LGPD).

Ademais, o agente de tratamento que causar dano patrimonial, moral, individual ou coletivo a outrem em razão do exercício do tratamento será obrigado a repará-lo (Art. 42, *caput*, da LGPD).

Nesse sentido, a lei prevê duas possibilidades quanto à responsabilidade solidária dos agentes de tratamento. A primeira ocorre quando o operador, ao realizar o tratamento em nome do controlador, agir em desacordo com as instruções recebidas do controlador ou em violação à LGPD, responsabilizando ambos pelos danos resultantes. O controlador é chamado à cadeia de responsáveis nesse caso pois ele tem a obrigação de selecionar e supervisionar adequadamente os operadores que tratarão dos dados em favor dele, garantindo que estes sigam as diretrizes de segurança necessárias para a proteção dos dados (Art. 39 da LGPD).

A segunda ocorre quando dois ou mais controladores estão diretamente envolvidos na atividade de tratamento e dela decorrer uma violação à LGPD que resulte em danos aos titulares. Nesses casos, todos os controladores podem ser considerados solidariamente responsáveis e aquele que primeiro reparar o dano ao titular terá direito de regresso contra os demais responsáveis, limitado a medida de participação de cada controlador no evento danoso (Art. 42, §4º, da LGPD).

Assim, ao analisar o regime de responsabilidade trazido na LGPD, conclui-se que controladores podem ser responsabilizados por ações realizadas por outros agentes de tratamento dentro da cadeia de tratamento.

Por tal motivo, a atenção deve ser redobrada para fins de segurança e prevenção, pois a ocorrência de incidentes pode indicar ausência ou falhas graves de *compliance* aos termos da LGPD, tornando o controlador responsável pelas ações de terceiros envolvidos no tratamento mesmo que o incidente não se relacione com nenhuma de suas ações diretas ou sistemas. O controlador, portanto, é responsável pelas atividades de tratamento decorrentes das relações comerciais que estabelece, inclusive quando ocorrem incidentes.

O Poder Judiciário brasileiro já registra casos decididos em que o controlador foi sancionado em decorrência da ação de outro membro da cadeia de tratamento. Em um deles, julgado pelo Tribunal de Justiça do Rio de Janeiro (Apelação nº 0418456-71.2013.8.19.0001) a

empresa Bracom Campos Veículos S.A. (“Bracom”), que tratava dados de clientes da empresa BV Financeira S.A. Crédito Financiamento e Investimento (“BV Financeira”) em virtude de relação comercial, delegou a manutenção de seu banco de dados para a empresa Smarty Solutions Treinamento Profissional LTDA. ME (“Smarty Solutions”), que armazenava os dados por meio do endereço eletrônico: http://girassolpresentes.com.br. Durante o período aproximado de três meses, todos os dados contidos em tal site, ficaram totalmente disponíveis na internet, sem a aplicação de qualquer medida de segurança, possibilitando, portanto, o acesso por qualquer interessado. As rés alegaram que o incidente de confidencialidade, ocorreu por conta da ação de um hacker.

Posteriormente, em Ação Civil Pública, o Magistrado condenou a Bracom (controladora) e a Smarty Solutions (operadora) por danos morais coletivos em R$ 500 mil e por danos materiais e morais em R$ 1 mil por consumidor atingido. Na fundamentação, foi alegado que: (i) a atuação do hacker não altera a responsabilidade das empresas perante os riscos atinentes à atividade desenvolvida (atividades financeiras), bem como as obrigações de segurança da LGPD; (ii) o controlador é responsável pela cadeia de tratamento oriunda das relações comerciais que desenvolve; e (iii) a figuração do operador no polo passivo é legítima, visto que a empresa era uma das responsáveis pelo banco de dados[3].

3 Apelação cível. Ação civil pública. Disponibilização indevida de banco de dados de consumidores na rede mundial de computadores. Sentença de procedência. Legitimidade ativa do Ministério Público para defesa dos direitos difusos e individuais homogênios. Aplicabilidade do Código de Defesa do Consumidor. Legitimidade passiva de todos os fornecedores de serviços e produtos que integram a cadeia de consumo para responder pelos danos causados pela falha na prestação dos serviços. Responsabilidade objetiva. Teoria do risco do empreendimento. Inexistência de cerceamento de defesa. [...]. Divulgação indevida de dados. Ofensa a direitos personalíssimos dos consumidores e em especial daqueles integrantes do banco de dados mantido ou utilizado pelas rés. Direito à intimidade e ao sigilo de dados violado. Dano moral coletivo. Dano moral in re ipsa. Desnecessidade da demonstração de prejuízos concretos ou de efetivo abalo moral. Precedentes da corte superior. Valor indenizatório que se mostra razoável e condizente com a relevância do tema e com o caráter repressor da indenização. Eventual comprovação do prejuízo individual que deve se realizar em fase de liquidação de sentença, conforme previsto no artigo 97 do código de defesa do consumidor. Coisa julgada in utilibus. Recurso desprovido. (0418456-71.2013.8.19.0001 - Apelação. Des(a). Fabio Dutra - Julgamento: 23/02/2021 – Décima Câmara de Dieito Privado (antiga 1a Câmara Cível).

Obrigações do controlador no processo de comunicação de incidentes de segurança

Conforme já apresentado, o aumento do número de casos de incidentes vem sendo verificado conforme a passagem dos anos. Notou-se também o aumento no custo médio relacionado ao incidente, ressaltando o abalo financeiro que violações de segurança podem causar. Um dos motivos para a ampliação dos valores, para além da valorização que os dados pessoais adquiriram na sociedade informacional, é a diversificação das consequências decorrentes do incidente, diretas ou indiretas.

São custos diretos aqueles que objetivamente decorrem do incidente, como: (i) notificação à ANPD e comunicação aos titulares; (ii) investimentos em cibersegurança; (iii) sanções e multas; (iv) assessoria de imprensa; (v) honorários advocatícios; e (vi) investigações técnicas. Os custos indiretos, por outro lado, podem não representar valores financeiros diretamente, mas se relacionam ao incidente, trazendo prejuízo de tempo e confiança ao controlador. São exemplos de custos indiretos: (i) aumento de prêmio de seguros; (ii) reestruturação de rotinas e treinamentos internos; (iii) perda de valor (confiança) junto aos clientes; (iv) descumprimento de cláusulas contratuais; (v) desvalorização da marca; e (vi) revelação de segredos comerciais (Xavier, 2021).

Face a tantas ameaças, o controlador deve se preparar não apenas para prevenir a ocorrência do incidente, mas para identificar rapidamente a possibilidade de ações adversas que possam caracterizá-lo, mitigando as consequências dentro do possível. Incidentes, entretanto, não possuem causas singulares, podendo ocorrer de diversas maneiras e ter diversos resultados. O monitoramento, portanto, é dificultado.

Pensando nesse cenário, a Information Commissioner's Office (ICO), autoridade de proteção de dados do Reino Unido, disponibilizou uma sessão para monitoramento e respostas a incidentes no seu *Accountability Framework* (Breach [...], [s.d.]).

Segundo a autoridade britânica, o controlador deve ter procedimentos para garantir a detecção, o gerenciamento e o registro adequados de incidentes. Tais procedimentos incluem: (i) treina-

mento adequado para que os membros da organização possam reconhecer um incidente; (ii) indicação de uma pessoa ou de um time designado para lidar com o tema; (iii) realização de treinamentos para que os membros da organização avisem o responsável, ou os responsáveis, acerca do incidente; (iv) adoção de sistemas que facilitem a identificação de problemas vinculados à segurança da informação; (v) consolidação de um plano de resposta; e (vi) consolidação de registro de todos os ocorridos, mesmo daqueles que acabem não sendo comunicados à ICO, incluindo as causas, o relato completo, os dados pessoais afetados, as medidas de mitigação adotadas e as consequências do incidente.

Em outro *framework*, denominado NIST Special Publication 800-61 Rev. 2 (2012) o National Institute of Standards and Technology recomenda que o agente de tratamento registre não somente o status do incidente, mas liste as informações obtidas durante a averiguação do ocorrido. Assim, a lista deverá conter: (i) um sumário; (ii) indicadores; (iii) indicativos de outros incidentes que se relacionam com o do registro; (iv) avaliação de impacto; (v) dados diversos sobre os agentes de tratamento envolvidos, como sistemas afetados e seus proprietários; (vi) evidências levantadas; (vii) comentários e impressões dos envolvidos e responsáveis pelo incidente; e (viii) próximos passos a serem tomados pelo controlador (National Institute of Standards and Technology, 2012).

A adoção de tais frameworks e procedimentos, ainda que estabelecidos por entidades estrangeiras, pode auxiliar as organizações brasileiras no estabelecimento de medidas para identificar e mitigar um incidente.

Avaliação de risco

A LGPD determina expressamente que o controlador deve comunicar à ANPD e aos titulares afetados sobre a ocorrência de um incidente que possa acarretar risco ou dano relevante aos titulares (Art. 48 da LGPD). De tal determinação, é possível verificar que a LGPD não impõe a comunicação para todo caso.

Risco decorre da ideia de correr perigo, uma combinação de probabilidade que leva um evento a ocorrer e acarretar dano. Já o

dano relevante se trata do prejuízo expressamente sofrido, podendo ser material ou moral (Diniz, 1998).

Tais noções importam para frisar que diversos incidentes verificados no dia a dia das organizações não devem ser reportados, uma vez que não possuem o condão de causar risco ou dano relevante aos titulares.

Nesse sentido, ensina Jimene (2022):

> [...] são corriqueiros os incidentes de segurança da informação dentro das organizações, inclusive da ordem de centenas de milhares por dia a depender do porte da entidade, mas não necessariamente, importam em risco ou prejuízos ao titular dos dados pessoais, pois de níveis de gravidade variados. A perda de um *pen drive*, o furto de um *notebook*, a interrupção de acesso a um sistema, podem ser considerados do ponto de vista técnico incidentes de segurança, porquanto a informação corporativa estará exposta a uma ameaça. Porém, na grande maioria dos casos, sequer envolvem dados pessoais, de modo que não configurariam uma ocorrência hábil de propiciar risco ou danos relevantes aos titulares dos dados pessoais. (Jimene, 2022)

A comprovação fática do risco ou do dano relevante ao titular é, dessa forma, a baliza que determina a necessidade de comunicação do incidente à ANPD e aos titulares.

Outro ponto relevante está na centralização do prejuízo aos titulares, de forma que a LGPD não estará preocupada com os danos decorrentes de um incidente se esses forem observados tão somente para a organização (como perda de valor econômico ou de confiança de clientes), sem respaldos em pessoas físicas.

Dessa forma, a ANPD já afirmou que um incidente poderá acarretar risco ou dano relevante quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver: (i) dados pessoais sensíveis; (ii) dados de crianças, adolescentes e idosos; (iii) dados financeiros; (iv) dados de autenticação em sistemas; (v) dados protegidos por sigilo legal, judicial ou profissional; ou (vi) dados em larga escala. Ainda, a verificação será efetivada quando a atividade de tratamento impedir o exercício de direitos ou a utilização de serviços pelo titular, além

de ocasionar dano moral ou patrimonial (Art. 5º, caput e § 1º, da Resolução CD/ANPD nº 15/2024).

A autoridade também já concedeu exemplos de incidentes aptos a causarem dano e risco relevante aos titulares:

> Invasão de uma rede de computadores de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais. A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados, impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde. A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras. (Comunicação [...], 2022).

A divulgação dos casos demonstra o interesse da ANPD em ressaltar o caráter adverso e confirmado de casos de incidentes aptos a serem notificados. Para auxiliar na análise do caso, o agente de tratamento deve considerar "dano" como a hipótese em que os dados pessoais forem corrompidos, alterados ou não estiverem mais completos. Já a "perda", deverá ser vista como a situação em que ainda é possível que os dados pessoais existam, mas o controlador não os controla, não tem acesso ou não tem em sua posse. Em último, o tratamento ilícito inclui a divulgação de dados pessoais a terceiros não autorizados, assim como qualquer outra forma de tratamento que não esteja em acordo com os termos legais (Bioni, 2021).

Por fim, destaca-se que a ANPD ainda poderá divulgar novas orientações para auxiliar os agentes de tratamento na avaliação de incidentes, conforme disposto no art. 5º, § 3º, da Resolução CD/ANPD nº 15/2024 (Autoridade Nacional de Proteção de Dados, 2024).

Notificação à ANPD

A atuação do controlador em incidentes só poderá ser efetivada após a ponderação sobre o risco e o dano relevante ao titular, uma vez que esta é a baliza trazida pela LGPD para determinar as hipóteses de comunicação.

Diante de um incidente sem risco relevante, o controlador deverá registrar o ocorrido em seu RoPA, especificando os motivos que o levaram a crer que não havia prejuízo. Já em hipóteses com risco relevante, o controlador deverá não só anotar o ocorrido, mas notificar a ANPD, comunicar os titulares e ativar o plano de resposta a incidentes. Por fim, casos com dano relevante também devem ser registrados, com a notificação e a comunicação respectivas, mas com uma atuação mais robusta em relação ao plano de resposta (Bioni, 2021).

Quando necessária a notificação à ANPD, o controlador terá o prazo de três dias úteis a partir da ciência de que o incidente afetou dados pessoais para realizá-la, ressalvada a existência de prazo para comunicação previsto em legislação específica (Art. 6º, *caput* e § 1º, da Resolução CD/ANPD nº 15/2024). O protocolo deverá ser realizado via envio de Formulário de Comunicação de Incidentes de Segurança com Dados Pessoais ("Formulário") (Art. 6º, §5º, da Resolução CD/ANPD nº 15/2024) no Sistema Eletrônico de Informações (SEI), onde a entidade deverá ser representada pelo encarregado (Art. 5º, VIII, da LGPD) ou representante constituído via procuração.

Como medida de salvaguarda, recomenda-se que o cadastro no sistema SEI seja realizado de forma preventiva, antes da ocorrência do incidente, uma vez que a efetivação do cadastro não é imediata e pode demorar até três dias úteis.

Visando facilitar o processo de notificação, o formulário possui os seguintes campos a serem preenchidos pelo controlador: (i) dados do controlador; (ii) dados do encarregado; (iii) dados do notificante/representante legal; (iv) tipo de comunicação; (v) avaliação do risco do incidente; (vi) da ciência da ocorrência do incidente; (vii) da tempestividade da comunicação do incidente; (viii) da comunicação do incidente aos titulares dos dados; (ix) descrição do incidente; (x) impactos do incidente sobre os dados pessoais; (xi) riscos e

consequências aos titulares dos dados; (xii) medidas de segurança técnicas e administrativas para a proteção dos dados pessoais; e (xiv) assinatura (Comunicação [...], 2022).

Acerca do tipo de comunicação, a ANPD segmenta as modalidades em comunicação completa, preliminar e complementar, com as seguintes descrições:

> Completa – Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.
> Preliminar – Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a comunicação aos titulares ainda não foi realizada.
> Complementar – Complementação de informações prestadas em comunicação preliminar. (Comunicação [...], 2022).

Nesse sentido, o protocolo da comunicação preliminar não cumpre o requisito de comunicação prevista no art. 48 da LGPD, sendo exigida a complementação fundamentada em até vinte dias úteis contados a partir do protocolo da comunicação preliminar (Art. 6º, § 3º, da Resolução CD/ANPD nº 15/2024).

Entretanto, necessário destacar que os prazos das notificações (preliminar e complementar) serão contados em dobro caso o controlador seja um agente de pequeno porte (Art. 6º, § 8º, da Resolução CD/ANPD nº 15/2024).

A divisão de categorias de comunicação representa uma alternativa proposta pela ANPD, em linha com o texto da LGPD, para permitir ao controlador que inicie o atendimento aos requisitos legais, mesmo que ele não possua todas as informações relacionadas ao incidente.

Antes de finalizar o protocolo, o controlador deve ainda indicar o nível de acesso que cada documento protocolado possui. Documentos sem nível de acesso limitado devem ser indicados como "público", ao passo que documentos com limitações de acesso devem ser indicados como "restrito".

O ponto tem o potencial de trazer dúvidas ao controlador, que pode desejar sigilo no processo de notificação para evitar reper-

cussões mediáticas negativas. Contudo, o SEI traz um rol taxativo de quatorze hipóteses de sigilo válidas, todas previstas no ordenamento brasileiro (Ministério da Gestão e da Inovação em Serviços Público, 2020).

Sobre a relação de sigilo em documentos, a ANPD já se pronunciou afirmando que os processos de fiscalização devem seguir o princípio da publicidade e da máxima publicação, em respeito à Lei nº 12.527/11 (Brasil, 2011). Dessa forma, atividades do setor público, como processos de fiscalização, devem ser acessíveis ao público. O sigilo se configura como exceção, com a limitação de acesso se restringindo aos trechos que de fato possuem respaldo legal de confidencialidade e segredo (Autoridade Nacional de Proteção de Dados, 2024).

Outrossim, não existe uma indicação legal específica para o tempo que a ANPD levará para analisar um incidente. Por meio do Voto nº 18/2023/DIR/MW/ANPD, entretanto, a autoridade já propôs que os seguintes critérios fossem levados em conta na priorização de análises pela Coordenação Geral de Fiscalização (CGF) (Autoridade Nacional de Proteção de Dados , 2023):

> 1. A CGF deve priorizar a análise de processos de comunicados de incidentes de segurança nos quais o controlador: a) não realizou a comunicação aos titulares de dados pessoais; e b) verifique-se a presença de, ao menos, uma das seguintes condições: (b.1.) o incidente abrange dados sensíveis, dados de crianças e adolescentes ou dados que exponham o titular à fraude; (b.2.) recorrência, isto é, o mesmo controlador comunicou a ocorrência de outros incidentes nos últimos dois anos; ou (b.3.) a principal atividade do controlador afetada pelo incidente de segurança envolve tratamento de alto risco, nos termos do art. 4º da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Por fim, é fundamental que o controlador acompanhe diariamente o processo cadastrado no SEI para verificar andamentos vinculados ao incidente e atuar tempestivamente quando necessário.

Comunicação aos titulares

Tendo em vista que todo processo de comunicação de incidentes parte da análise de risco ou do dano relevante aos titulares, não seria lógico que os próprios titulares, enquanto os mais afetados, não fossem informados acerca do ocorrido e de suas consequências.

Assim como a notificação à ANPD, a comunicação aos titulares é de responsabilidade do controlador, com o prazo de três dias úteis a partir da ciência de que o incidente afetou dados pessoais. Seu conteúdo deverá conter minimamente: (i) a descrição da natureza e da categoria de dados pessoais afetados; (ii) as medidas técnicas e de segurança utilizadas para a proteção dos dados; (iii) os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; (iv) os motivos da demora, no caso de a comunicação não ter sido feita no prazo de três dias úteis; (v) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; (vi) a data do conhecimento; e (vii) dados de contato do controlador e do encarregado, quando possível. Adicionalmente, a inclusão de medidas que o titular pode adotar para mitigar efeitos poderá ser considerada uma boa prática pela ANPD (Art. 9º, § 5º, da Resolução CD/ANPD nº 15/2024).

Ademais, a comunicação deverá fazer uso de linguagem simples e de fácil entendimento, ocorrendo de forma direta e individualizada, ou seja, feita pelos meios usualmente utilizados pelo controlador (sítio eletrônico, e-mail, telefone, etc.). Assim como a notificação à ANPD, o prazo para comunicação aos titulares será contado em dobro para agentes de pequeno porte (Art. 9º, § 6º, da Resolução CD/ANPD nº 15/2024).

O racional por trás da comunicação é potencializar a autodeterminação informativa, isto é, o controle pelo titular do trânsito de seus dados, possibilitando a tomada de medidas preventivas contra fraudes, furtos de identidade e assédios comerciais (Vainzof, 2022).

Nesse sentido, a falta de comunicação de incidentes aos titulares resultou na primeira decisão do Conselho Diretor da ANPD, que rejeitou o recurso do Instituto Nacional do Seguro Social (INSS) e

manteve sanção à instituição no sentido de publicizar a infração à LGPD (Castro, 2024).

A decisão trata de um incidente de confidencialidade ocorrido em 2022 no Sistema Corporativo de Benefícios do INSS (SISBEN), em que foram expostos nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes do titular. O INSS reportou o incidente à ANPD, destacando o risco e o dano relevante aos titulares. Contudo, o INSS se recusou a realizar a comunicação, alegando que: (i) não havia como precisar quais dados haviam sido ilegalmente tratados; (ii) diante da abundância de titulares, não havia meios de rastrear os afetados e comunicá-los individualmente; e (iii) a comunicação geraria insegurança e pânico aos segurados.

Apesar das alegações do INSS, o Conselho Diretor manteve a decisão da CGF, determinando que o INSS publicasse a seguinte mensagem na primeira página de seu site:

> O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos. Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em

> questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: encarregado@inss.gov.br. (Autoridade Nacional de Proteção de Dados, 2024).

O caso torna-se emblemático não apenas por se tratar da primeira decisão do Conselho Diretor da ANPD, mas por reforçar a posição de defesa da Autoridade aos titulares em casos de incidentes.

Registro

As obrigações do controlador frente ao incidente não se limitam às ações de comunicação, pois o registro interno do ocorrido também é necessário. Tal registro deverá ser mantido pelo prazo de cinco anos, mesmo que o controlador tenha optado por não notificar a ANPD nem comunicar aos titulares (Art. 10º da Resolução CD/ANPD nº 15/2024).

O conteúdo do registro deverá abranger no mínimo: (i) a data de conhecimento; (ii) descrição geral das circunstâncias; (iii) natureza e categoria dos dados pessoais; (iv) o número de titulares afetados; (v) avaliação de risco e dano relevante aos titulares; (vi) medidas de correção e mitigação adotadas; e (vii) os motivos da não comunicação (Art. 10º, § 1º, da Resolução CD/ANPD nº 15/2024).

As entidades públicas previstas no art. 23 da LGPD estão desobrigadas ao prazo, desde que observem as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade própria ou definidas pelo Conselho Nacional de Arquivos (Art. 10º, § 2º, da Resolução CD/ANPD nº 15/2024).

Conclusão

Diante do exposto neste trabalho, conclui-se que a redação dos incisos VII, VIII e X do art. 6º e do art. 46 da LGPD (Brasil, 2018) atribui como ato ilícito a não adoção de medidas administrativas e técnicas para a redução do risco de incidentes pelo controlador.

Incidentes não simbolizam uma ameaça isolada, do contrário, o mundo enfrenta uma Epidemia de Vazamento de Dados que re-

presenta uma ameaça de escala global de prejuízos milionários para organizações e danos irreparáveis aos indivíduos. Os números apresentados neste trabalho demonstram como o Brasil não é exceção à epidemia mencionada, apresentando diversos casos de incidentes ao longo dos anos.

Portanto, para evitar cenários de ilicitude, é fundamental que o controlador brasileiro pondere sobre a realidade dos tratamentos realizados *in house*, bem como nas cadeias de tratamento que integra, avaliando as melhores soluções de segurança da informação disponíveis para a realidade fática da organização. Adicionalmente, destaca-se que a segurança dos dados pessoais continua sendo uma obrigação do controlador mesmo após o fim do tratamento (Art. 47 da LGPD).

Dessa forma, é imperativo que os agentes de tratamento implementem medidas eficazes de segurança da informação, não apenas para cumprir as exigências legais, mas também para proteger a integridade, a disponibilidade e a confidencialidade dos dados pessoais sob sua responsabilidade. A adoção de uma abordagem proativa na gestão de riscos, incluindo a constante atualização e aprimoramento das técnicas e procedimentos de segurança, é essencial para minimizar a ocorrência de incidentes e evitar as consequências decorrentes da negligência.

Nesse sentido, a posição de vítima não exime o controlador da responsabilização pela ocorrência de incidentes. Do contrário, diversas obrigações, como as previstas no art. 48 da LGPD, se apresentam ao controlador em cenários de incidente, incluindo o reconhecimento, a notificação à ANPD, o comunicado aos titulares e o registro.

Em última análise, a responsabilidade pela segurança dos dados pessoais deve ser vista como um compromisso contínuo, refletindo uma postura de diligência e respeito à privacidade dos titulares dos dados. Apenas assim, será possível utilizar as normas de proteção de dados como uma "vacina" para a Epidemia de Vazamento de Dados enfrentada globalmente.

Referências

Agencia Española Protección Datos. **Decisión sobre el Procedimiento Sancionador PS/00117/2024**. Disponível em: https://www.aepd.es/documento/ps-00117-2024.pdf. Acesso em: 22 jul. 2024.

ADERÊNCIA à LGPD: apenas 36% das empresas brasileiras estão em conformidade total. **Datacenter Dynamics**. 31 mai. 2023. Disponível em: https://www.lgpdbrasil.com.br/aderencia-a-lgpd-apenas-36-das-empresas-brasileiras-estao-em-conformidade-total/. Acesso em: 29 jul. 2024.

ADVERSO. **Dicio**. 2010. Disponível em: https://www.dicio.com.br/adverso/. Acesso em: 29 jul. 2024.

Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf. Acesso em: 29 jul. 2024.

_____. **Nota Técnica nº 22/2024/FIS/CGF/ANPD**. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_0125695_nota_tecnica_22.pdf. Acesso em: 26 jul. 2024.

_____. **Relatório de Instrução nº 01/2024/CGF/ANPD**. 25 jan. 2024. Disponivel em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio-de-instrucao-1_2024.pdf. Acesso em: 28 jul. 2024.

_____. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 29 jul. 2024.

APÓS ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos. **Exame**. 20 ago. 2021. Disponível em: https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/. Acesso em: 30 jul. 2024.

BIONI, Bruno. Riscos do tratamento de dados e arquitetura de segurança da informação: lições extraídas de grandes vazamentos de dados. In: **II Seminário Internacional – Lei Geral de Proteção de Dados:** Arquitetura da privacidade no Brasil. 29 abr. 2021. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2021/04/apresentacao_justicafederal_brunobioni.pdf. Acesso em: 25 jul. 2024.

BRASIL já ocupa o 2º lugar no ranking mundial de ransomware. **CISO Advisor**. 20 mai. 2023. Disponível em: https://www.cisoadvisor.com.br/brasil-ja-ocupa-o-2o-lugar-no-ranking-mundial-de-ransomware/. Acesso em: 25 jul. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República,. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Constituicao.htm. Acesso em: 31 out. 2024.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011**. Lei de Acesso à Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 31 OUT. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jul. 2024.

BRASIL responde por 43% do volume de dados vazados no mundo. **Ciso Advisor**. 16 mar. 2023. Disponível em: https://www.cisoadvisor.com.br/brasil-responde-por-43-do-volume-de-dados-vazados-no-mundo/. Acesso em: 29 jul. 2024.

BREACH Response and Monitoring. **ICO**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/breach-response-and-monitoring/#incidents. Acesso em: 25 jul. 2024.

CASTRO, Grasielle. Em decisão inédita, ANPD rejeita recurso e INSS terá que publicizar infração à LGPD. **JOTA**. 26 jul. 2024. Disponível em: https://www.jota.info/executivo/em-decisao-inedita-anpd-rejeita-recurso-e-inss-tera-que-publicizar-infracao-a-lgpd-26072024. Acesso em: 28 jul. 2024.

COMUNICAÇÃO de incidente de segurança. **Autoridade Nacional de Proteção de Dados**. 23 dez. 2022. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 25 jul. 2024.

COSTA, Marcella; ALENCAR, Ana Catarina de. Privacy by design e privacy by default. In: TORANZO, Bruno (coord.), **DPO (Encarregado)**: Gestão dos programas de privacidade e proteção de dados. [S.l.]: Opice Blum, 2021.

COST of a Data Breach Report 2024. **IBM Security**. 2023. Disponível em: https://www.ibm.com/downloads/cas/LNGW4X4M. Acesso em: 08 ago. 2024.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2018.

DATA Breaches and Cyber Attacks – Europe 2024 Report. **IT Governance**. 19 jun. 2024. Disponível em: https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-2024-in-europe. Acesso em: 29 jul. 2024.

DATA Breaches Chronology. **Privacy Rights Clearing house**. 2024. Disponível em: https://privacyrights.org/data-breaches. Acesso em: 29 jul. 2024.

DINIZ, Maria Helena. **Dicionário Jurídico**. v. 4. São Paulo: Saraiva, 1998.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: RT, 2021.

FUZINY, Livia Clozel. Insuficiência de medidas técnicas e organizacionais para garantir a segurança da informação em solução tecnológica. In: TOMASEVICIUS FILHO, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura; DALESE, Pedro (coords.). **GDPR**: Regulamento Geral sobre a Proteção de Dados da União Europeia. Indaiatuba: Foco, 2023.

GOMES, Maria Cecília Oliveira; GOUVEA, Thaianny Estefanato. Incidentes de segurança envolvendo dados pessoais: uma breve análise da comunicação de incidentes para a ANPD. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (coords.). **Proteção de dados**: temas controvertidos. v. 2. Indaiatuba: Foco, 2024.

HARTZOG; Woodrow; SOLOVE, Daniel. **Breached!:** Why Data Security Law fails and how to improve it. Oxford: Oxford University, 2022.

INFORMAÇÃO sigilosa no SEI. **Ministério da Gestão e da Inovação em Serviços Públicos**. 16 abr, 2020. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/processo-eletronico-nacional/noticias/2020/informacao-sigilosa-no-sei. Acesso em: 26 jul. 2024.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO. **Privacy Breach Notification Guidelines**. jan. 2018. Disponível em: https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd-1.pdf. Acesso em: 29 jul. 2024.

JIMENE, Camila do Vale. Capítulo VII: Da Segurança e das Boas Práticas. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados Pessoais Comentada. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

_____. Da importância da segurança da informação para adequação à LGPD. In: BLUM, Renato Opice (org.). **Proteção de Dados**: desafios e soluções na adequação à Lei. Rio de Janeiro: Forense, 2020.

LISBOA, Sofia; TAKANO, Yassuki. IT Trends Snapshot 2023. **Logicalis**. 2023. Disponível em: https://imagine.la.logicalis.com/hubfs/IT%20Snapshot%202023/it-trends-snapshot-2023_logicalis.pdf. Acesso em: 29 jul. 2024.

MANIFESTO Mozilla. **Mozilla**. Disponível em: https://www.mozilla.org/pt-BR/about/manifesto/. Acesso em: 26 jul. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Computer Security Incident Handling Guide**: Special Publication 800-61 Revision 2. Disponível em: https://csrc.nist.gov/pubs/sp/800/61/r2/final. Acesso em: 29 jul. 2024.

O QUE é *phishing*? **IBM**. 17 mai. 2024. Disponível em: https://www.ibm.com/br-pt/topics/phishing. Acesso em: 29 jul. 2024.

PARANÁ. Tribunal de Justiça do Estado do Paraná. **Recurso Inominado nº 0008309-97.2021.8.16.0019**. 2a Turma Recursal. Relator: Maurício Pereira Doutor (Juiz de Direito Substituto). Julgamento em: 10 jun. 2022. Publicação em: 12 jun. 2022. Disponível em: https://portal.tjpr.jus.br/jurisprudencia/j/2100000020503051/Ac%C3%B3rd%C3%A3o-0008309-97.2021.8.16.0019#. Acesso em: 29 jul. 2024.

PRADO, Luiz Fernando. **Sua organização não deve mais fazer um projeto de adequação**. 25 mar. 2022. LinkedIn: Luis Fernando Prado. Disponível em: https://www.linkedin.com/pulse/sua-organiza%C3%A7%C3%A3o-n%C3%A3o-deve-mais-fazer-um-projeto-de-adequa%C3%A7%C3%A3o-prado/. Acesso em: 29 jul. 2024.

PRINCÍPIOS de Privacidade de dados. **Mozilla**. Disponível em: https://www.mozilla.org/pt-BR/privacy/principles/. Acesso em: 26 jul. 2024.

RANSOMWARE. **IBM**. Disponível em: https://www.ibm.com/br-pt/topics/ransomware. Acesso em: 29 jul. 2024.

RENNER restabelece app e e-commerce após ataque hacker. **Exame**. 24 ago. 2021. Disponível em: https://exame.com/tecnologia/renner-restabelece-app-e-e-commerce-apos-ataque-hacker/. Acesso em: 29 jul. 2024.

RIO DE JANEIRO, Tribunal de Justiça do Estado do Rio de Janeiro. **Apelação nº 0418456-71.2013.8.19.0001**. Décima Câmara de Direito Privado. Relator: Dea, Fábio Dutra. Julgamento: 23 fev. 2021. Publicação: 10 mar. 2021. Disponível em: https://www3.tjrj.jus.br/EJURIS/temp/5ee4945f-34d1-4611-a8d9-59d3b3bbd339.html. Acesso em: 25 jul. 2024.

SANTANA, Joana. Brasil lidera em vazamento de dados na internet. **Folha de S.Paulo**. 18 abr. 2024. Disponível em: https://www1.folha.uol.com.br/colunas/painelsa/2024/04/brasil-lidera-em-vazamento-de-dados-na-internet.shtml. Acesso em: 29 jul. 2024.

SÃO PAULO, Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 1065936-51.2020.8.26.0002**. 34a Câmara de Direito Privado. Relator: Des.

Luiz Guilherme da Costa Wagner Júnior. Julgamento em: 21 fev. 2022. Publicação: 28 fev. 2022. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15443468&cdForo=0. Acesso em: 29 jul. 2024.

SECURITY Report 2023: Protegendo os ativos digitais: uma análise do cenário de segurança cibernética em empresas na América Latina e no Brasil. **ESET**. 2024. Disponível em: https://web-assets.esetstatic.com/wls/2023/2023-09/eset-security-report-2023.pdf. Acesso em: 29 jul. 2024.

SUTTO, Giovanna. 83% das companhias que sofreram ataques hackers no Brasil pagaram resgates em 2023. 09 mai. 2024. Disponível em: https://www.infomoney.com.br/business/83-das-companhias-do-pais-pagaram-resgates-apos-ataque-hacker-em-2023-diz-estudo/. Acesso em: 29 jul. 2024.

União Europeia. Article 29 Data Protection Working Party. **Guidelines on Personal data breach notification under Regulation 2016/679**. Adopted on 3 October 2017. Revised and adopted on 6 February 2018. Brussels: European Commission, Directorate General Justice, 2018.

_____. **Diretiva 95/46/CE, de 23 de novembro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 29 jul. 2024.

_____. **General Data Protection Regulation**. Disponível em: https://gdpr-info.eu/. Acesso em: 29 jul. 2024.

VAINZOF, Rony. Capítulo I: Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados Pessoais Comentada. 4. ed. São Paulo: Thomson Reuters Brasil, 2022.

_____. Dados pessoais, tratamento e princípios. In: MALDONADO; Viviane Nóbrega *et al.*, **Comentários ao GDPR**: Regulamento Geral de Proteção de Dados da União Europeia. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

XAVIER, Fabio Correa. Custo de incidentes de segurança aumentam 10% em 2021 e alcançam o maior valor em 17 anos. **MIT Technology Review**. 27 dez. 2021. Disponível em: https://mittechreview.com.br/custo-de-incidentes-de-seguranca-aumentam-10-em-2021-e-alcancam-o-maior-valor-em-17-anos/. Acesso em: 25 jul. 2024.

ZALAF, Henrique. Os custos financeiros de um incidente de segurança da informação. **Consultor Jurídico**. 22 mai. 2024. Disponível em: https://www.conjur.com.br/2024-mai-22/os-custos-financeiros-de-um-incidente-de-seguranca-da-informacao/. Acesso em: 25 jul. 2024.

2º lugar

Diga-me o que você curte, que eu lhe direi quem você é: o direito à explicação na Lei Geral de Proteção de Dados

Eduarda Costa Almeida

Resumo

A todo momento, as pessoas são impactadas por decisões automatizadas tomadas com base em dados pessoais para acesso a produtos e serviços oferecidos por entidades públicas ou privadas. A Lei Geral de Proteção de Dados (LGPD) determina um direito de receber informações sobre os critérios e procedimentos utilizados na decisão automatizada sempre que ela afetar os interesses das pessoas, um direito à explicação. Esse direito é uma das facetas da autodeterminação informativa, enquanto fundamento de proteção de dados. A autodeterminação visa dar poder de decisão ao titular sobre como suas informações serão tratadas por terceiros. Ao mesmo tempo que esse conceito tem sido ressignificado, ele influencia sobremaneira a interpretação da lei, principalmente de seus princípios e direitos. Entre os direitos do titular, o direito à explicação surge como ferramenta para se compreender o processo de tomada de decisão automatizada e, com isso, garantir os outros direitos do titular, contestar, solicitar revisão da decisão e verificar a conformidade do tratamento com a LGPD, principalmente com seus princípios. Dessa forma, apesar de não haver orientações objetivas sobre os parâmetros para se atingir esse direito, ele é previsto pelo art. 20

da lei e visa equilibrar a distribuição de poderes na tomada de decisão, a fim de garantir que o titular participe, proporcionalmente, do processo de decisão que afete seus interesses.

Palavras-chave: *proteção de dados; autodeterminação informativa; direito do titular; decisão automatizada; direito à explicação.*

Introdução

As decisões que mais importam para a delimitação do comportamento e da personalidade das pessoas, cada vez mais, estão sendo tomadas por algoritmos. Essas ferramentas realizam recomendações de compras, sugestões de opiniões e de atividades culturais, inferências de vontades, formação de perfis e determinam o acesso a serviços públicos, a benefícios sociais ou mesmo ao exercício de direitos e liberdades. Em um contexto de *big data*, não cabe mais a apenas um ser humano ou a uma burocracia checar as condições para que uma pessoa execute atividades corriqueiras. Algoritmos decidem a partir do processamento de informações, inclusive pessoais, sobre as condições de um empréstimo bancário, de um benefício social ou até sobre os conteúdos direcionados a usuários de redes sociais, por exemplo.

O desenvolvimento da tecnologia, principalmente associado ao poder computacional e ao acesso facilitado a dispositivos conectados à internet e os riscos advindos do uso dessas ferramentas indicaram a necessidade de regulamentar o fenômeno do tratamento de dados pessoais. Entre os anos 70 e 80, diferentes normas e documentos foram elaborados no intuito de controlar a tecnologia e garantir direitos aos usuários, principalmente aqueles relacionados à dignidade da pessoa humana, autonomia, liberdade e privacidade. Dentre eles, um direito foi reconhecido, o direito à autodeterminação informativa, como cunhado pela Corte Constitucional Alemã, em 1983. Com o passar do tempo, o movimento de regulação da proteção de dados foi se espraiando por diversas regiões do mundo com o objetivo de tutelar o fluxo de dados pessoais

diante do potencial impacto na esfera de direitos de seus titulares (Alimonti, 2020, p. 181).

No Brasil, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD) foi resultado de um debate multisetorial, que levou em conta a comunidade jurídica, defensores de direitos humanos, técnicos, pesquisadores, formuladores de políticas públicas, autoridades estatais, empresas de tecnologia, comunicação e marketing, além de outras, diante de um debate nacional e internacional sobre proteção de dados. Essa discussão também passou a ser relevante para que o Brasil atendesse aos requisitos de um fluxo transfronteiriço de dados pessoais adequado, principalmente em vista das obrigações de transferência internacional de dados estabelecidas pelo Regulamento 2016/679 (Regulamento Geral de Proteção de Dados ou RGPD) e das relações comerciais existentes entre o Brasil e a União Europeia (UE).

Já existiam legislações esparsas que tratavam do tema de dados pessoais em contextos específicos no Brasil, a exemplo das previsões no Código de Defesa do Consumidor (CDC), na Lei do Cadastro Positivo (LCP), na Lei de Acesso à Informação (LAI), e no Marco Civil da Internet (MCI). No entanto, essas legislações disciplinavam o fluxo de dados pessoais apenas de modo pontual, e, por isso, haveria a necessidade de uma lei que regulamentasse o tema de forma geral aplicável à maior parte das relações jurídicas. Assim, a LGPD, em 2018, inaugurou a regulação de proteção de dados pessoais no Brasil com um modelo próximo ao desenvolvido na UE. Vale destacar que, em 2022, a proteção de dados passou a compor de forma explícita o rol de direitos fundamentais descritos no art. 5º da Constituição Federal (Brasil, 1988).

Dentre os tópicos abordados pela LGPD, tem-se o de decisões automatizadas. O uso massivo deste tipo de decisão pode indicar escolhas mais ágeis e personalizadas para o titular de dados. Porém, essas decisões envolvem riscos já identificados em casos concretos[1]. A LGPD, entre outros objetivos, também busca mitigar

1 Dentre os principais riscos à proteção de dados, destacam-se (i) a vigilância, (ii) a discriminação e (iii) a opacidade desses sistemas de decisão. Esses riscos estão associados a desafios éticos no uso de IA, porém também estão ligados aos funda-

esses potenciais malefícios. Para tanto, todo o arcabouço regulatório incide sobre esse tipo de tratamento de dados pessoais, como seus princípios, direitos dos titulares e capacidade fiscalizatória da Autoridade Nacional de Proteção de Dados (ANPD). Mais especificamente, a lei prevê que os titulares dos dados devem ser informados sobre os critérios e os procedimentos utilizados em uma decisão automatizada sempre que ele solicitar. Para alguns, esse dispositivo seria suficiente para depreender-se um direito à explicação, não obstante, esse direito pode encontrar limites técnicos, jurídicos e práticos.

Diante desse contexto, formulou-se a seguinte pergunta de pesquisa: quais os parâmetros de um direito à explicação na tomada de decisão automatizada baseada em dados pessoais previsto na LGPD? A hipótese fixada é de que existe um direito à explicação fundado no conceito de autodeterminação informativa, que determina as balizas da concretização desse direito. Esta pesquisa possui como eixo (i) a decisão automatizada com base em dados pessoais e (ii) o direito à explicação como meio de concretização da autodeterminação informativa. Como a lei busca regular um tratamento de dados pessoais que observe os direitos fundamentais, bem como a inovação e o desenvolvimento tecnológico, garantir a concretude de seus fundamentos é relevante para a construção do sistema inaugurado pela LGPD em bases sólidas. Nesse sentido, a autodeterminação informativa pode ser reconhecida como fio condutor na interpretação da lei, e, assim, o direito à explicação pode ser percebido como um vetor de garantia da autodeterminação quando o titular é exposto à decisão automatizada que afeta interesses.

mentos de regulação da proteção de dados, na medida em que são consequência do tratamento indevido de informação pessoal. Esses temas são trabalhados nos seguintes documentos: ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Estados Unidos: Perseus Books, LLC, 2021. BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. **Big data and Society**, jan.-jun., 2016. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Bias in Algorithms – Artificial Intelligence and Discrimination**. Luxembourg: Publications Office of the European Union, 2022.

As decisões automatizadas baseadas em dados pessoais

Associado ao *big data*, ferramentas de Inteligência Artificial (IA) também proporcionaram um novo cenário para um processo de tomada de decisão (Reino Unido, 2016, p. 10). Com técnicas de IA, a análise de dados em um contexto de *big data* é potencializada pela capacidade de processar dados nos mais diversos padrões de tamanho, forma, extensão e linguagem. Ferramentas de IA funcionam como uma chave para destravar o valor das informações contidas no *big data* (Reino Unido, 2017, p. 8). O processo de escolha e tomada de decisão, seja por pessoas físicas, seja por empresas, governos ou outras entidades, é expressivamente alterado a fim de aprimorar esse processo em benefício dos interesses daqueles que tomam a decisão, agora baseada em dados, inclusive pessoais. Por isso, analisar os direitos relacionados à tomada de decisões automatizadas também é analisar sistemas de IA[2].

Ainda, o desenvolvimento da técnica e dos recursos necessários para disseminação de sistemas de IA deixou rastros na regulação de proteção de dados, visto que muitas dessas ferramentas funcionam a partir do tratamento de dados pessoais e já há impactos explícitos no campo dos direitos dos titulares de dados. No Brasil, o tema é regulado pelo art. 20 da LGPD, que delimita seu âmbito de aplicação especificamente às decisões baseadas unicamente no tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito ou os aspectos de

2 Na definição de um conceito de decisão automatizada, é importante dar um passo atrás e pontuar que sistemas de IA são diferentes de simples sistemas automatizados. Técnicas de automação são utilizadas desde a primeira revolução industrial, em que era possível que máquinas se movessem sem intervenção humana. Em caso de simples automação, é possível prever facilmente o resultado de saída, de acordo com as ordens dadas e as informações de entrada, já no caso de IA há relativa incerteza sobre o resultado, os dados ganham centralidade, e há a capacidade de aprender com os resultados, esses são requisitos para que a ferramenta funcione devidamente (Hankiewicz, 2018). Assim, nem todo sistema automatizado é um sistema de IA, mas o conceito de decisão automatizada abarca tanto sistemas automatizados quanto sistemas de IA.

personalidade do titular. Sendo assim, as decisões objeto de regulação pela LGPD são: (i) decisões automatizadas, ou seja, sem interferência humana; (ii) com base em dados pessoais, e (iii) que afetem interesses dos titulares (Brasil, 2018).

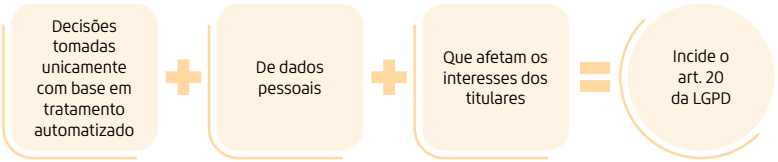

***Figura 01** - Conceito de decisão automatizada na LGPD*

Fonte: autora

Não há definição de parâmetros mais concretos sobre o que seria considerada uma decisão automatizada no escopo do art. 20[3]. A ANPD já indicou sua intenção em apresentar diretrizes sobre o tema de direito dos titulares e IA durante os anos de 2023 e 2024, em vista também dos seus influxos na proteção de dados. Apesar dessa possível lacuna no Brasil, o tema de decisão automatizada foi regulamentado por outras legislações de proteção de dados, de forma que outras autoridades já se debruçaram pelo tema, como o exemplo europeu.

O art. 22 do RGPD regula decisões baseadas exclusivamente no tratamento automatizado que afetam a esfera jurídica do titular ou afetam-no de forma significativa (União Europeia, 2018). Para o Grupo de Trabalho do Art. 29, está no escopo deste conceito as decisões que não possuem um humano envolvido de forma efetiva no processo, ou seja, quando não há uma pessoa com autoridade ou competência para mudar a decisão. Ainda, a esfera jurídica do

3 Para sanar qualquer indeterminação sobre o conceito de decisão automatizada, está em tramitação no Senado Federal o Projeto de Lei (PL) 4496, de 2019, que visa alterar a LGPD para dispor de forma específica sobre o conceito de decisões automatizadas enquanto qualquer processo que utilize técnica computacional para escolher, classificar, aprovar ou rejeitar, atribuir média, cláusula risco ou probabilidade. Para mais informações, acesse: https://www25.senado.leg.br/web/atividade/materias/-/materia/138136.

titular seria impactada quando à decisão: (i) permitir ou negar um determinado benefício social concedido por lei; (ii) limitar sua liberdade de ir e vir e se associar, como a recusa da entrada de uma pessoa na fronteira, ou sujeitá-la a medidas de segurança ou vigilância acrescida pelas autoridades competentes; ou (iii) alterar seus direitos ou estado legal em um contrato, como desconectar automaticamente o serviço de telefonia móvel por quebra de contrato, porque se esqueceu de pagar sua conta (Article 29 Data Protection Working Party, 2017, p. 10).

Como exemplo, o Grupo de Trabalho destaca os casos de aceite ou recusa automática de pedido de crédito on-line, de práticas de recrutamento eletrônico sem qualquer intervenção humana, ou de publicidade direcionada, dependendo (i) da intrusividade do processo de elaboração do perfil, (ii) das expectativas e desejos das pessoas envolvidas, (iii) da forma como o anúncio é entregue, e (iv) das vulnerabilidades particulares das pessoas visadas. Outro exemplo seria caso de definição de preços de forma automatizada que resulta em preços diferentes para agentes diferentes quando os preços forem expressivamente altos e, por isso, barrarem efetivamente alguém de acessar certos bens ou serviços (Article 29 Data Protection Working Party, 2017, p. 22). Esses parâmetros ainda não foram definidos no contexto brasileiro.

Os termos utilizados para caracterizar uma decisão automatizada como aquela que interfere significativamente na esfera de direitos do titular são circunstanciais, de forma que a análise da relevância da decisão automatizada é feita caso a caso. Em 2021, o Tribunal de Justiça de Amsterdam julgou o caso C/13/687315 / HA RK 20-207 (Rechtbank Amsterdam, 2021a) sobre a pertinência de uma decisão automatizada. No caso, a empresa Uber foi processada por uma associação de motoristas de aplicativo por, dentre outras questões, estar utilizando ferramentas de decisão automatizada sem a devida informação ao titular. O tribunal entendeu que o sistema da Uber de pareamento do passageiro com o motorista mais próximo e de precificação das corridas não seria uma decisão significativa para a esfera de direitos do titular, apesar de serem decisões que afetam o desempenho do contrato entre o Uber e o motorista.

Em outro caso, o C/13/692003/HA RK 20-302 (Rechtbank Amsterdam, 2021b), o mesmo tribunal analisou a decisão tomada automaticamente de bloquear temporariamente o acesso ao aplicativo a um motorista após um sinal de fraude, sem intervenção humana. Para a corte, este bloqueio temporário não teve nenhum efeito duradouro ou permanente, de modo que a decisão automatizada não teve consequências legais ou afetou significativamente o motorista.

Apesar das semelhanças, as normas de proteção de dados brasileira e europeia enunciam uma regulação sobre decisão automatizada para finalidades diferentes: o art. 22(1) do RGPD proíbe, em regra, que um titular de dados seja submetido a decisões automatizadas que o afetem significativamente (União Europeia, 2018). Já o art. 20 da LGPD destaca as decisões automatizadas para apresentar um direito de revisão e de informação sobre os critérios e procedimentos utilizados (Brasil, 2018). Para além das lacunas interpretativas, há certa convergência entre os conceitos de decisões automatizadas reguladas pelas normas de proteção de dados brasileira e europeia. As duas se ocupam de decisões sem intervenção humana fundamentadas em dados pessoais e com impacto relevante para o titular, apesar da flexibilidade do que significa esse impacto relevante para cada contexto.

Direito à explicação como faceta da autodeterminação informativa

Os debates iniciais sobre um direito à explicação guardam origem nos princípios de proteção de dados da boa-fé, transparência e *fairness*, já enunciados no *Fair Information Practice Principles* (Kaminski, 2019, p. 209). A capacidade do titular autodeterminar-se é determinada também pela explicação que este passa a conhecer quando é submetido a decisões automatizadas em um contexto de *big data*.

A ideia de autodeterminação informativa tradicional foi estruturada a partir de 1983 com a decisão do Tribunal Constitucional Federal Alemão sobre a Lei do Censo da época. A constitucionalidade dessa lei foi levada ao tribunal diante do risco que ela representava para os direitos gerais de personalidade por falta de precauções

processuais e de finalidade na coleta e na organização dos dados do recenseamento. O tribunal entendeu que a Lei Fundamental garantiria o poder do indivíduo de decidir por si mesmo sobre a divulgação e o uso de seus dados pessoais, que resultaria no direito à autodeterminação informativa. Assim, foi reconhecido ao cidadão um direito amplo e flexível de não ser submetido a tratamentos de dados por terceiros que violem sua capacidade de desenvolver sua personalidade livremente (Martins, 2005, p. p. 237).

No ordenamento jurídico brasileiro, a autodeterminação foi prevista expressamente apenas com a LGPD, porém seus efeitos já se relacionavam com outros instrumentos jurídicos. Antes mesmo da entrada em vigor da LGPD, o Supremo Tribunal Federal (STF) reconheceu a existência de um direito à proteção de dados vinculado ao direito de autodeterminação informativa, tendo em vista esse direito ser uma chave para interpretação do primeiro. O julgamento brasileiro se deu em um contexto fático bastante similar ao alemão, que reconheceu a autodeterminação como direito fundamental no contexto de uma lei de recenseamento da população. Aqui, a discussão era sobre a constitucionalidade de uma Medida Provisória (MP) que determinava o compartilhamento de dados dos usuários do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia do novo coronavírus. O tribunal brasileiro fixou entendimento pela impossibilidade de compartilhamento de dados e pela existência de um direito à proteção de dados, que deve ser protegido por meio da fixação de salvaguardas mínimas e suficientes para a garantia dos direitos fundamentais e da dignidade humana (Brasil, 2020).

A autodeterminação foi argumento central neste julgamento e o é na LGPD, já que é um dos fundamentos da lei e, com isso, é fio condutor que direciona a interpretação a ser dada às obrigações previstas na legislação, inclusive quanto aos princípios da LGPD e aos direitos dos titulares. No entanto, esse conceito já passou por processos de ressignificação. Em um primeiro momento, a autodeterminação era sinônimo da coleta do consentimento do titular, que, apenas assim, poderia controlar de forma autônoma seus dados pessoais. Com o consentimento, em regra, os titulares

decidem no momento da coleta dos dados sobre se consentem ou não com aquele tratamento, porém as verdadeiras consequências do uso dos dados pessoais não podem ser conhecidas quando eles tomam essas decisões. Além disso, as consequências são cumulativas e não podem ser adequadamente avaliadas em uma série de transações isoladas (Solove, 2013, p. 1893).

Por outro lado, a autodeterminação informativa, em seu sentido mais tradicional, se preocupa com a capacidade do titular controlar e participar de todo o processo de tratamento de dados. Com a evolução do conceito, o consentimento foi se distanciando da autodeterminação e, assim, dando espaço para obrigações de transparência, como é o caso do direito à explicação. Apesar de inicialmente o direito à explicação decorrer do princípio da transparência (Monteiro, 2018, p. 05), ele não se confunde com simples obrigação de ser transparente sobre o processo de tomada de decisão automatizada. Esse direito se relaciona com diversos outros princípios de proteção de dados, como é o princípio da prevenção, responsabilização e prestação de contas, que "colabora na construção de espaços de deliberação para discutir o que seria 'informação qualificada' ou como mitigar problemas em decisões futuras [...] e possibilita endereçar questionamentos a respeito dos segredos comercial e industrial" (Bioni; Luciano, 2019, p. 218).

Para Rodotà (2008), cabe ao titular exercer controle direto sobre a forma de processamento de suas informações pessoais, que é feito por agentes que adquirem poder a partir dessa atividade. Isso quer dizer que "a possibilidade de controlar não serve apenas para assegurar ao cidadão a exatidão e o uso correto das informações a ele diretamente relacionadas, mas pode se tornar um instrumento de equilíbrio na nova distribuição de poder que vai se delineando" (Rodotà, 2008, p. 37). Assim, a noção de controle relacionada à autodeterminação informativa não se esgotaria no exercício de um controle individual[4] pelo titular como um fim em si mesmo, mas

4 Rodotà destaca a importância do coletivo para a devida proteção de dados pessoais para além das fronteiras do indivíduo como centro da privacidade. Para ele, "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso desses dados por parte de tais organizações. Além disso,

como uma ferramenta de realocação de poder na sociedade.

A autodeterminação informativa, como concebida nos moldes tradicionais do titular controlar individualmente qual terceiro e de que forma esse trata seus dados, encontra fronteiras em um cenário de assimetria entre os agentes de tratamento e os titulares de dados. Por isso, faz-se necessária uma releitura do conceito para que ele fundamente o estabelecimento de uma estrutura mais complexa de controle. Essa estrutura está abarcada pela moldura de proteção de dados ao conceber que o titular de dados, junto a outros agentes, também exerce sua capacidade de controlar seus dados quando estes são tratados, em uma análise contextual, para uma finalidade previsível e de acordo com suas legítimas expectativas (Bioni, 2019, p. 265). Nesse sentido, é possível construir o seguinte diagrama com os principais conceitos relacionados à autodeterminação.

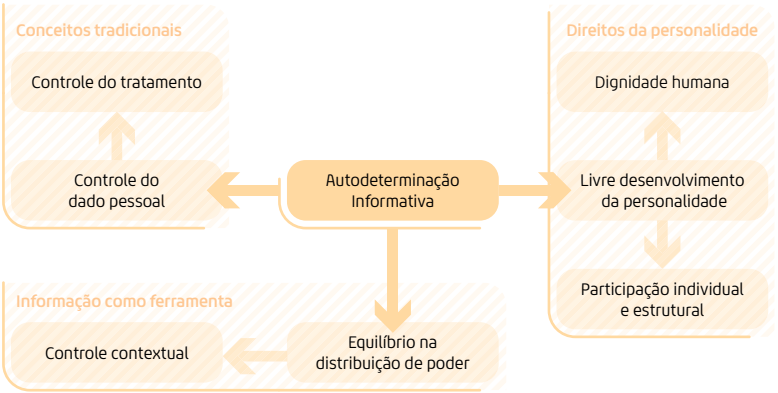

***Figura 02** - Diagrama de conceitos relacionados à autodeterminação informativa*

Fonte: autora

é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair como perdedor" (Rodotà, 2008, p. 37).

O direito à explicação é uma das decorrências do fundamento da autodeterminação, conceito que passa por um processo de ressignificação. Isso porque a perspectiva de o titular ocupar o centro do tratamento de dados o coloca em evidência para participar e controlar o uso que é feito de seus dados e, com isso, diminuir a disparidade de informação e poder entre os atores envolvidos nesse processo. Um dos mecanismos para permitir essa minimização do desequilíbrio de poder é a explicação sobre o sistema automatizado que o titular é submetido para que, a partir de informações concedidas a ele, ele possa compreender, questionar, perceber incongruências e opor-se ao tratamento de dados.

No entanto, desde as primeiras manifestações da academia sobre esse direito, houve discordâncias sobre sua existência e seu escopo. Por isso, este tópico busca explicar o que seria um direito à explicação e seus principais efeitos para os titulares. Com o início do desenvolvimento da tecnologia, pesquisadores norte-americanos e europeus debateram sobre a necessidade de maior transparência sobre os sistemas de decisão automatizados. Nesse contexto inicial, transparência significava (i) que o código fonte do algoritmo e o conjunto de dados deveriam ser submetidos a escrutínio público; ou (ii) que deveriam ser elaboradas avaliações de impacto algorítmico diante de denúncias de terceiros ou de auditorias externas (Kaminski, 2019, p. 210). Porém, já nesse momento, percebeu-se que esses mecanismos não seriam suficientes para garantir maior transparência para os titulares afetados, já que determinado nível de transparência não seria útil para eles, podendo inclusive causar danos, por minimizar a visibilidade das informações relevantes e distraí-los sobre o que realmente importa (Ananny; Crawford, 2018, p. 984).

Um debate sobre os efeitos do RGPD na regulação de decisões automatizadas reanimou as discussões sobre a existência ou não de um direito à explicação nas leis de proteção de dados, especificamente nos artigos 13(2)(f), 14(2)(g) e 15(1)(h) do RGPD (União Europeia, 2018). Esses dispositivos determinam, dentro de um escopo amplo de direito à informação, o direito de o titular acessar e receber informação relevante sobre a lógica da decisão automatizada, bem como a importância e os efeitos do tratamento para o titular dos dados.

Antes mesmo da entrada em vigor do RGPD, Goodman e Flaxman (2017, p. 56) reconheceram um direito à explicação baseado nos efeitos desses artigos. Como consequência, para os autores, os titulares poderiam intervir no processo de tomada de decisão, impondo novos parâmetros no desenvolvimento de um algoritmo ou exigindo supervisão adicional. Para eles (Goodman; Flaxman 2017, p. 55), uma explicação razoável forneceria, no mínimo, relatos de como os dados de entrada se relacionam com as previsões finais, indicando quais parâmetros são mais ou menos relevantes na tomada de decisão de forma transparente e acessível aos titulares.

No entanto, esse reconhecimento logo foi rebatido por Wachter, Mittelstadt e Floridi (2017, p. 77). Eles entendem que não há correspondência entre um direito à explicação e as obrigações de informar sobre a lógica da decisão, sendo estas apenas um desdobramento do direito de informação. Para os autores, um direito à explicação teria dois significados diferentes: (i) um referente à funcionalidade do sistema, ou seja, a lógica, significado, consequências previstas e funcionalidade geral de um sistema automatizado de tomada de decisão, e (ii) outro sobre as decisões automatizadas específicas, que seria a lógica, as razões e as circunstâncias individuais de uma decisão específica, não geral. Ainda, essa explicação poderia ser dada (i) antes da tomada de decisão, que não estaria associada a explicações sobre uma decisão específica por suas características ainda não terem sido analisadas, ou (ii) após a decisão ser fixada, podendo abordar tanto a funcionalidade do sistema quanto a decisão específica (Wachter; Mittelstadt; Floridi, 2017, p. 78).

Nesse sentido, para que um direito à explicação específico passasse a existir, esses requisitos deveriam ser definidos, tendo em vista a fundamentalidade dessas condições para aplicação concreta do direito. Na lógica da explicação, os controladores deveriam apresentar evidências de decisões automatizadas relativas às características (*features*) levadas em consideração, ponderação de peso dessas características, árvore de decisão ou estrutura de classificação e lógica geral do sistema de tomada de decisão automatizada. Para os autores, a previsão de um direito à explicação possui implicação direta na concretização de outros direitos, como o direito de contestar a decisão, que não teria razão de ser se o titu-

lar não possuísse as ferramentas para entender como as decisões foram tomadas (Wachter; Mittelstadt; Floridi, 2017, p. 97).

A associação entre o direito à explicação e os princípios de proteção de dados é relevante para a definição do que seria esse direito, isto é, da sua extensão ou escopo. Em vista dessa relação de retroalimentação entre direitos e princípios, o direito à explicação seria uma ferramenta disponível para que o titular exerça seus outros direitos quando exposto a uma decisão automatizada e para que ele possa perceber o cumprimento dos princípios no tratamento automatizado, principalmente da transparência e livre acesso, finalidade, necessidade e adequação e não discriminação. A partir dessas informações sobre a decisão automatizada, o titular teria ferramentas concretas para se autodeterminar, ou seja, participar do processo de tratamento de dados e exercer controle contextual sobre suas informações como consequência de maior equilíbrio na distribuição do poder garantido em uma sociedade da informação.

Margot Kaminski (2019, p. 213) entende que existe uma relação evidente entre os direitos individuais de proteção de dados, como a contestação, correção e apagamento, e o tipo de transparência individualizada que a matéria requer. Com isso, a autora evidencia que a substância de outros direitos subjacentes determina a extensão do princípio da transparência. Assim, se o titular tem um direito de correção, ele precisa ser capaz de ver erros possíveis em sistemas automatizados. Se o titular tem um direito de não discriminação, ele precisa ter as ferramentas para ver quais fatores são usados em uma decisão automatizada. Caso contrário, as assimetrias de informação tornam os direitos subjacentes efetivamente nulos.

Usando a classificação de Wachter, Mittelstadt e Floridi (2017, p. 78) sobre a funcionalidade do sistema e as decisões automatizadas específicas, as explicações da funcionalidade do sistema incluem, entre outros, a especificação de seus requisitos, as árvores de decisão, os modelos pré-definidos, os critérios e as estruturas de classificação. Já as explicações sobre as decisões específicas incluem informações sobre a ponderação de *features*, as regras de decisão específicas de cada caso, e dados sobre grupos de referência ou de perfil.

Porém, Selbst e Powles (2017, p. 240) entendem não existir tal separação. Para eles, as regras e a ponderação de *features* que

constituem o sistema algorítmico decidem os casos de forma semelhante e consistente. Isso quer dizer que é difícil construir uma explicação relevante da funcionalidade do sistema que não oferece informações significativas sobre decisões específicas, porque, por definição, um titular precisaria de explicação suficiente para reivindicar seus direitos. Assim, para um direito à explicação, o que realmente importaria seriam os dados de entrada, já que são necessários para determinar a decisão específica, mas uma vez que o modelo é construído e os dados de entrada são conhecidos, a lógica determinaria o resultado (Selbst; Powles, 2017, p. 239).

Uma posição explícita nos quatro artigos de referência para descrição de um direito à explicação, ou a um direito de informação sobre a lógica do sistema, é que esse direito é relevante para que o titular sujeito a decisões automatizadas possa exercer seus direitos de proteção de dados, como oposição e contestação do tratamento, além da revisão da decisão[5]. Com isso, é possível concluir que esse direito está intrinsecamente associado aos princípios de proteção de dados, bem como os demais direitos dos titulares, já que, sem um direito à explicação, o titular estaria de mãos atadas para exercer seus outros direitos e verificar se o tratamento de dados é devido. Por meio dele, o titular poderia verificar se está sujeito a uma decisão automatizada, qual a finalidade dela, quais dados leva em consideração, se são dados atualizados, se ele é discriminado abusiva ou ilegalmente, entre outros requisitos de conformidade com a matéria.

O direito à explicação está abarcado por todo o sistema de proteção de dados e se relaciona com ele. O fundamento da autodeterminação informativa é reafirmado em uma lógica de explicação, já que, sem ela, o titular passa a não ter ferramentas de controle sobre seus dados pessoais quando utilizados em decisões auto-

5 As referências estão evidenciadas em: KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019, p. 215. GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". **AI MAGAZINE**, 2017, p. 55. WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017, p. 97. SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017, p. 242.

matizadas, de forma a afetar seu livre desenvolvimento da personalidade. Nesse sentido, para se atingir esse direito à explicação, outras formas de transparência podem incidir em casos concretos. Muito se discute sobre o acesso ao algoritmo em seu formato de desenvolvimento, com expressões matemáticas e regras não acessíveis para pessoas leigas, porém, diante de um direito à informação contextual, não é útil que as pessoas tenham acesso a essas informações, mas pode ser útil para outros agentes (Kaminski, 2019, p. 215; Selbst; Powles, 2017, p. 239).

Por isso, o direito à explicação, diante de um ecossistema de proteção de dados, garante que os titulares tenham acesso a uma forma de explicação, e especialistas e reguladores a outra. Esta abordagem multifacetada da transparência não deve ser descartada, já que esse direito é mais profundo do que um sistema de respostas contrafactuais[6] ou uma visão sistêmica, mas superficial. Nesse sentido, Kaminski (2019, p. 217) entende que um direito à explicação está acoplado a outras medidas de transparência que vão no sentido de fornecer supervisão tanto de terceiros quanto de reguladores sobre a tomada de decisões algorítmicas.

Portanto, o direito à explicação deve ser interpretado de forma funcional, flexível, e deve, no mínimo, permitir que o sujeito dos dados exerça seus direitos previstos na lei de proteção de dados. Em resumo, o direito à explicação é um direito do titular ser informado com conteúdo significativo, relevante, sobre a lógica adotada no processo de tomada de decisão. Isso é alcançado diante dos seguintes requisitos, que vão de uma explicação simples para uma

6 Wachter, Mittelstadt e Russell entendem que explicações contrafactuais são relevantes para explicar uma decisão automatizada. Os autores afirmam que "ao contrário das abordagens existentes que tentam fornecer uma visão da lógica interna dos algoritmos da caixa preta, as explicações contrafactuais não tentam esclarecer como as decisões são tomadas internamente. Em vez disso, elas fornecem insights sobre quais fatos externos poderiam ser diferentes a fim de se chegar a um resultado desejado. É importante ressaltar que as explicações contrafactuais são computadas eficientemente para muitos classificadores padrão, particularmente redes neurais. Como nossa nova forma de explicação difere significativamente dos trabalhos existentes, justificamos sua natureza como uma explicação com referência a trabalhos anteriores na literatura filosófica e nos primeiros sistemas de IA" (tradução livre) (Wachter; Mittelstadt; Russell, 2018, p. 41).

explicação complexa, que pode variar, proporcionalmente, de acordo com o contexto da aplicação do sistema de decisão automatizada (quem são os titulares afetados, que tipo de serviço é ofertado ou restringido, quais os riscos envolvidos, entre outros):

Checklist do direito à explicação

- O interessado recebe informações de acordo com o risco do sistema para os direitos do titular, principalmente dos direitos de personalidade;
- O interessado recebe informações de acordo com seu interesse e expectativa, se titular, auditor externo, auditor interno, autoridade de proteção de dados;

- O titular sabe que está exposto a sistemas que tratam dados pessoais para decisões automatizadas;
- O titular sabe os parâmetros de tratamento e sua ponderação baseado no modelo do sistema;
- O titular sabe quais os dados pessoais são tratados pelo sistema e suas fontes;
- O titular sabe qual a finalidade, a duração e quem é o controlador responsável pelo tratamento realizado pelo sistema;
- O titular sabe o grau e o modo de contribuição do processamento automatizado para a decisão tomada;
- O titular sabe o impacto e os efeitos da decisão tomada pelo sistema;

- O titular sabe os parâmetros de tratamento e, quando apropriado, sua ponderação no caso concreto;
- O titular sabe quais mudanças em seus dados de entrada (inputs) teriam feito com que a decisão automatizada fosse diferente;
- O titular sabe como os inputs são transformados em outputs, informações que, por definição, podem não ser completas;

- O titular sabe as intenções na criação do modelo, os parâmetros utilizados para treinar o sistema, e as características do sistema de IA utilizado;
- O titular sabe as métricas de performance do sistema, em quais casos mais falha e a capacidade de previsão do sistema quando utilizado em dados diferentes dos de treinamento;
- O titular sabe quais são as características dos indivíduos que receberam tratamento semelhante ao dele;
- O titular sabe as propriedades não desejadas do sistema e como ele decide nessas situações.

***Figura 03** - Checklist do direito à explicação*[7] / Fonte: autora

7 Esta checklist foi elaborada com base nos seguintes artigos: EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm? Why a "right to explanation" is probably not

Todo esse arcabouço de um direito à explicação está relacionado à possibilidade do interessado na decisão de saber os motivos que levaram o sistema a decidir pelo resultado específico. Com isso, é possível que esse interessado analise os parâmetros da decisão, os elementos levados em consideração, encontre inconsistências e questionamentos tanto sobre a forma de decidir quanto sobre o resultado.

Essa inclinação guarda similaridade com o art. 93, IX, da Constituição Federal (Brasil, 1988), que, dentro de outro contexto, de um Estado Democrático de Direito, determina a necessidade de fundamentação em todas as decisões do Poder Judiciário. Isso quer dizer que os juízes, enquanto legitimados pelo Estado, "devem expor as razões que os conduziram a eleger uma solução determinada em sua tarefa de dirimir conflitos", cumprindo um dever fundamental de prestar contas quanto à coerência e equanimidade das decisões (Mendes; Gonet; Branco, 2019, p. 1077). Esta pesquisa não afirma que o peso de uma decisão judicial é o mesmo que o de decisões automatizadas impactadas por um direito à explicação, ou seja, aquelas tomadas sem intervenção humana e que impactam nos direitos e interesses dos titulares. Porém, essa previsão na Constituição indica para o interesse da sociedade brasileira, organizada em um Estado Democrático de Direito, em não estar sujeita a decisões arbitrárias, que não podem ser contestadas ou mesmo analisadas.

A necessidade de explicações sobre sistemas autônomos não está restrita ao debate de dados pessoais, o tema perpassa inclusive as discussões sobre uma possível regulação dos usos de IA em sentido mais amplo. Desde a tramitação dos primeiros projetos de lei (PL) sobre IA, especialmente o PL 21/2020, que culminou nas discussões do PL 2338/2023, especialistas brasileiros destacaram a necessidade de um direito à explicação que observe os limites de compreensão e conhecimento dos receptores dessa informação,

---

the remedy you are looking for. **Duke Law and Technology Review**, v. 16, n. 1, 2017, p. 58. EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? **IEEE Security & Privacy**, v. 16, n. 3, 2018, p. 5. REINO UNIDO. Information Commissioner's Office. **Explaining decisions made with IA**. 2022, p. 52. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf. Acesso em: 14 mar. 2023.

seja o titular, o público em geral ou os profissionais da área. A mera publicização do código-fonte do sistema poderia não atender às necessidades do titular e colocar os mecanismos de segurança do sistema em risco (Senado Federal, 2022, p. 109). Segundo os participantes, o segredo de negócio pode ser um óbice à transparência, ao mesmo tempo que a falta de acesso à informação compromete a fiscalização e a auditoria sobre os sistemas (Senado Federal, 2022, p. 111). Porém, não houve consenso sobre a viabilidade de explicações das decisões tomadas por esses sistemas, diante de sua opacidade, acompanhada da necessidade de confiança nessa tecnologia por conhecer seu funcionamento e evitar violação de direitos (Senado Federal, 2022, p. 115).

Diante dos debates com base na LGPD e nos PLs, é razoável perceber a necessidade de se utilizar sistemas de decisão explicáveis. Para tanto, esses sistemas devem ser capazes responder perguntas comumente feitas a processos de decisões humanas, assim será possível notar se e onde as demandas de explicação devem ser diferentes entre os sistemas de IA e os humanos. Essa equiparação entre perguntas feitas a humanos e máquinas é interessante para que se evite um cenário em que os sistemas autônomos tenham "passe livre" para decidir sem nenhum escrutínio que os humanos passam, ou mesmo em que se exija tanto desses sistemas a ponto de dificultar a inovação e o desenvolvimento tecnológico (Doshi-Velez, 2019, p. 21).

Após essa análise sobre um direito à explicação, depreende-se que: (i) o direito à explicação não é igual à transparência, pois este conceito é um princípio amplo aplicável às normas de proteção de dados e que abarca, além da explicação de uma decisão automatizada, outros mecanismos; (ii) no âmbito da proteção de dados, o direito à explicação é um direito de informação específico aplicável às decisões automatizadas relevantes aos interesses dos titulares e baseadas em dados pessoais; (iii) ainda não há uma definição unânime sobre quais elementos compõem taxativamente um direito à explicação, mas, por meio dele, busca-se saber sobre a racionalidade de uma decisão automatizada; (iv) não foi definido o momento que esta explicação deve ser dada, uma corrente afirma pelo direito de solicitar explicações antes do tratamento de dados

e outra corrente defende a concretização desse direito após a decisão ser feita, guardada a proporção da explicação a ser dada.

Direito à explicação na LGPD

Além dos fundamentos teóricos da autodeterminação informativa e do direito à explicação, o controlador de dados que atua sob incidência da LGPD e se utiliza de decisões automatizadas baseadas em dados pessoais com impacto aos interesses do titular, também deve se observar o disposto no art. 20 da lei. No *caput*, é previsto o direito de revisão da decisão e, no §1º, o direito à explicação é determinado, já que o controlador deve informar os critérios e procedimentos utilizados para a decisão automatizada, observados os segredos comerciais aplicáveis (Brasil, 2018). Assim como a doutrina percebeu lacunas para delimitação desse direito, a LGPD não fixa parâmetros objetivos para cumpri-lo. No caso brasileiro, esse direito incide nos casos em que o titular está sujeito a uma decisão sem interferência humana a fim de que conheça informações complementares sobre o processo de decisão para além dos dados coletados, mas também sobre a forma de utilização dos dados pessoais e os possíveis resultados a partir do tratamento.

Esse direito de conhecer informações específicas do processo de tomada de decisão automatizada, como descrito na LGPD, deve estar atento à forma da explicação, que deve ser clara e adequada ao contexto em que se aplica. Isso porque decisões automatizadas, como apresentado anteriormente, estão sendo aplicadas em diversos contextos, inclusive para definir perfil[8] e permitir acesso ou não a bens, serviços e direitos. Assim, a forma e a extensão da explica-

8 Rafael Zanatta entende que o uso de técnicas de perfilização na LGPD implica em obrigações de três naturezas: "(i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) anti-discriminatória, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um "processo dialógico" com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas". Essa última obrigação está relacionada ao fundamento da autodeterminação quando o titular é submetido à decisão automatizada (Zanatta, 2019, p. 3).

ção devem estar em acordo com o sujeito e seus efeitos concretos, de modo que o direito a receber explicação ganha relevância, caso essa decisão venha impactar funções sociais constitucionalmente protegidas, como direito à saúde, trabalho, moradia, liberdade de expressão, entre outros (Mulholland; Frajhof, 2019, p. 273).

Traçando um paralelo com o RGPD, é possível perceber que o §1º do art. 20 não especifica o sujeito do direito à explicação, como faz no *caput* do artigo e o RGPD, que, em uma interpretação literal, limita a incidência desse direito aos titulares de dados sujeitos à decisão (União Europeia, 2018). Como afirmado anteriormente, essa não especificação, somada ao fato de que sistemas de decisões automatizadas, em regra, são aplicados de forma massiva, pode indicar para um direito que pode ser exercido por outros interessados potencialmente impactados pela decisão. Por outro lado, o RGPD não limita o direito de explicar a um critério de requisição, ao contrário da LGPD, que cria a obrigação de explicar o sistema após solicitação do interessado. As discussões sobre uma explicação específica a uma decisão individual ou sistemática também não foram definidas na lei brasileira, sendo possível os dois modelos.

Para além da definição pela existência ou não de um direito à explicação, surgem diversas questões sobre a forma de alcançá-lo, ou seja, sobre a definição de parâmetros objetivos que indiquem para uma explicação suficiente ou não, como apresentado no tópico anterior. Diante dos desafios de se concretizar um direito à explicação, é possível defender-se que "o parâmetro a ser buscado é a inteligibilidade e explicação dos aspectos fundamentais da decisão automatizada: o seu propósito, os seus inputs, os seus resultados e os critérios e fundamentos para o julgamento" (Frazão; Carvalho; Milanez, 2022, p. 340). Esses aspectos também estão presentes na Figura 03 - Checklist do direito à explicação. A partir desses elementos mínimos, o direito à explicação pode ser percebido como efetivo aos interesses dos titulares, já que funciona como instrumento de "ampliação do poder de barganha dos indivíduos com garantias e qualificadores que buscam conferir maior equilíbrio às assimetrias" (Alimonti, 2020, p. 183). Essa dimensão individual de um direito à explicação também pode ser complementada com mecanismos de dimensão coletiva e estrutural.

Está expressa no §1º, do art. 20 da LGPD (Brasil, 2018) a incidência dos limites do segredo de negócio na definição do que deve ser explicado. Essa determinação, à primeira vista, restringe o conteúdo a ser informado ao interessado a título de explicação sobre o sistema automatizado sempre que a informação versar sobre segredo de negócio. No entanto, isso não significa que o controlador pode se valer dessa justificativa para negar explicação, sua utilização só "poderia ser cogitada em casos excepcionais e devidamente justificados, sob pena de esvaziar por completo diversos dos princípios da própria LGPD" (Frazão; Carvalho; Milanez, 2022, p. 343). A imposição do segredo de negócio como limitador da extensão desse direito também está em debate na tramitação do PL 21/2020, em que os especialistas, durantes as audiências públicas e contribuições por escrito, divergiram sobre ser o segredo de negócio um direito das empresas que pode se sobrepor ou restringir o direito das pessoas.

Quando o argumento do segredo comercial ou industrial for utilizado para não fornecer explicações, a LGPD determina que a ANPD poderá realizar auditorias para a verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais, em acordo com o §2º do art. 20. É importante notar que, assim como previsto no art. 58(1)(b)(e) do RGPD, a autoridade brasileira, apoiada no art. 55-J, tem competência para realizar auditorias em situações que houver descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. Nesse sentido, o §2º apenas especifica a competência da ANPD de realizar auditorias em casos de indícios de tratamentos indevidos, que abarca casos de tratamentos discriminatórios.

No sistema normativo brasileiro, outras normas e documentos de orientação do governo são relevantes para a definição de um direito à explicação. O art. 5º, IV e V, da LCP determina expressamente um direito de informação ao cadastrado sobre principais elementos e critérios considerados para a análise de risco e sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento.

Com base nesses direitos, o cadastrado passa a conhecer, ter explicado, de forma mais específica, sobre o sistema que foi submetido para avaliação de crédito. Um direito à explicação já havia sido reconhecido pelo Superior Tribunal de Justiça que culminou com a publicação da Súmula 550, em que o tribunal entende pela possibilidade do uso de *score* de crédito, desde que o consumidor possa solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo[9]. Além disso, o art. 1º, §3º, da LCP também prevê a proibição de anotar informações sensíveis para fins de concessão de crédito, como a origem étnica, orientação sexual, convicções políticas, religiosas e filosóficas, e informações de saúde e genética, de forma a preservar o cadastrado de tratamentos discriminatórios. Diante desse contexto fático e desse nível de proteção jurídica, Renato Monteiro (2018, p. 08) entende que a espinha dorsal do direito à explicação de decisões automatizadas é formada a partir da combinação de um direito à transparência e da não discriminação.

De maneira mais abrangente, o CDC, em seu art. 6º, III, determina um direito de informação aos consumidores sobre os produtos e serviços, indicando especialmente as características e riscos que apresentam, corroborando para o desenvolvimento de uma relação de consumo informada e baseada na boa-fé. Somado a isso, o art. 43 do código apresenta um direito de os consumidores acessarem informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Esses direitos à informação e ao acesso a dados pessoais podem ser percebidos como primeiras expressões de um direito à explicação, porém ainda limitado ao contexto de consumo e sem previsões sobre o processo automatizado em si, que segue uma lógica específica e relevante para os interesses das pessoas sujeitas a essas determinações.

Em suma, no Brasil, o direito à explicação é especificamente previsto na lei de proteção de dados. A definição de critérios e pro-

9 Súmula 550. A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

cedimentos, somado às construções doutrinárias e jurisprudenciais sobre o tema, são relevantes para a sedimentação teórica desse direito e consequente desenvolvimento prático. A partir desse reconhecimento e delimitação, será possível que os titulares o exerçam quando estiverem submetidos a decisões automatizadas que afetem seus direitos, bem como a autoridade fiscalize o atendimento a este direito. Ao mesmo tempo, os desafios que circundam a implementação desse direito ainda são expressivos, especialmente quando busca-se extrair a razão de ser e os limites de um direito de receber explicações sobre decisões automatizadas que afetam a esfera de direitos ou interesses dos envolvidos.

Conclusão

Estar sujeito a decisões automatizadas é uma realidade e essas decisões impactam os cidadãos em diversos contextos, seja para definição de publicidade direcionada, recomendação de entretenimento, *score* de crédito, preço de seguros, atuação em aplicativo de transporte e entrega, ou seja, para acesso a tratamentos de saúde, educação e políticas públicas específicas. Em regra, essas decisões têm como base algoritmos e sistemas treinados de diversas formas e desenvolvidos em ferramentas de complexidade distintas que levam a resultados interpretáveis e explicáveis em graus também diversos.

Ainda não está sedimentado no contexto brasileiro em quais casos essas decisões afetariam os titulares, dificuldade também enfrentada no contexto europeu. Para este cenário, o Grupo de Trabalho do Artigo 29 entende que para avaliar o impacto da decisão nos interesses do titular, deve ser considerado se a decisão (i) permite ou nega um determinado benefício social concedido por lei; (ii) limita sua liberdade de ir e vir e se associar, como a recusa da entrada de uma pessoa na fronteira, ou sujeitá-la a medidas de segurança ou vigilância acrescida pelas autoridades competentes; ou (iv) altera seus direitos ou estado legal em um contrato, como desconectar automaticamente o serviço de telefonia móvel por quebra de contrato, porque se esqueceu de pagar sua conta (Article 29 Data Protection Working Party, 2017, p. 10).

As decisões automatizadas são utilizadas para predizer comportamentos humanos, impactos sociais e formar perfis sobre os titulares. Esses sistemas foram criados para, com base nos dados pessoais, seja aqueles expressamente informados para o controlador, seja aqueles compartilhados ou coletados por meio do comportamento online do titular, dizerem quem os titulares são. Nesse sentido, a hipótese fixada nesta pesquisa, qual seja, de que existe um direito à explicação fundamentado na autodeterminação informativa, foi corroborada. Isso porque o conceito da autodeterminação está em processo de ressignificação para deixar de estar associado apenas à noção de controle individual do titular sobre seus dados e estar relacionado a uma noção de poder de decisão e participação no tratamento de dados pessoais. Dessa forma, o fundamento da autodeterminação é justamente a ferramenta que habilita que o titular conheça, controle e participe do processo de decisões a que está sujeito.

De acordo com as ideias de Rodotà (2008, p. 37), a autodeterminação informativa não se esgotaria no exercício de um controle individual pelo titular como um fim em si mesmo, mas como uma ferramenta de realocação de poder na sociedade. Um sentido similar à autodeterminação é indicado por Bruno Bioni ao apresentar o conceito de co-deliberação informacional, que se opõe ao de dominação informacional e reconhece a deliberação conjunta sobre tratamento de dados (Bioni, 2021, p. 242). É notória a mudança de sentido atribuída à autodeterminação e a noção de autodeterminação como equilíbrio na distribuição de poder está mais alinhada aos desafios atuais enfrentados pela proteção de dados pessoais, inclusive no uso de sistemas automatizados.

É nesse contexto que surge a necessidade de positivação de um direito à explicação, especialmente quando titulares de dados são sujeitos a sistemas de decisões automatizadas baseadas em seus dados pessoais e com impacto nos seus interesses. No Brasil, esse direito está expresso no §1º, do art. 20, da LGPD (Brasil, 2018). Conhecer o processo de decisão permite que os titulares intervenham no processo de tomada de decisão (Goodman; Flaxman, 2017, p. 55), se oponham de forma fundamentada ao resultado, além de

estar informados sobre o modo que seus dados serão utilizados e impactam na personalidade do titular.

Não existe uma fórmula rígida a respeito do momento em que esse direito deve ser atendido, se apenas após a decisão automatizada. Na LGPD, a obrigação de explicar os critérios e procedimentos utilizados para a decisão surge após a solicitação do interessado. Antes disso, o direito à informação especificado no art. 9º da lei deve ser observado e toda informação garantida ao titular deve ser contextual, em linguagem simples, acessível e com conteúdo relevante, para que, assim, o desequilíbrio de poder entre o agente de tratamento e o afetado seja minimizado.

Dessa forma, o direito à explicação permite que os outros direitos dos titulares se concretizem, como o direito de revisão da decisão, de correção de dados desatualizados ou mesmo da eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD. A autodeterminação informativa, enquanto um dos fundamentos da matéria de proteção de dados, é reafirmada em uma lógica de explicação, já que, sem ela, o titular passa a não ter ferramentas de controle sobre seus dados pessoais quando utilizados em decisões automatizadas, de forma a afetar seu livre desenvolvimento da personalidade. Os novos sentidos atribuídos à autodeterminação corroboram com a ideia de um maior equilíbrio de poder detido pelos agentes que manipulam as informações, inclusive pessoais. Dessa forma, a explicação se mostra como uma ferramenta atual para se alcançar esse fundamento, em vista da disseminação de sistemas de decisão automatizada e do impacto desses para os direitos e as liberdades dos afetados.

Ainda não há definição unânime da extensão de um direito à explicação. O §1º do art. 20 da LGPD (Brasil, 2018) apresenta obrigações quanto à forma da explicação, que deve ser transmitida por meio de uma informação clara e adequada, ou seja, não deve ser extensa, impertinente ou de difícil compreensão. Já a matéria da explicação deve variar de acordo com o caso concreto, com os impactos da decisão para o titular, bem como com os riscos envolvidos. A partir desses requisitos, esta pesquisa elaborou a Figura 03 - Checklist do direito à explicação para evidenciar parâmetros já estabelecidos pela doutrina no sentido de garantir uma explicação

ao titular, seja ela mais simples, destacados na caixa verde, ou mais robustos, delineados na caixa vermelha. Uma explicação adequada é garantida nos casos em que é evidente que o tratamento de dados é resultado de decisão automatizada, bem como se sabe quais os dados pessoais, os parâmetros e as ponderações feitas pelo sistema. Ainda, é relevante que se saiba quais mudanças nos dados pessoais de entrada teriam feito com que a decisão automatizada fosse diferente, o impacto da decisão nos interesses do afetado e os riscos envolvidos no sistema.

No entanto, essa explicação pode não ser suficiente para que o titular possa se autodeterminar em um contexto de disseminação de sistemas de IA e *big data*. Os limites do direito à explicação na garantia do fundamento da autodeterminação devem ser destacados, já que esse direito é apenas mais uma das ferramentas estabelecidas nas normas de proteção de dados que permite, especificamente, o entendimento e a oposição das decisões automatizadas. Outros mecanismos, como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), as auditorias feitas pela autoridade, as soluções de governança de dados, a proteção de dados por design (Casey; Farhangi; Voglp, 2019, p. 179) e o teste nos sistemas de IA (Estados Unidos da América, 2016) se mostram complementares para a concretização da autodeterminação. Além de não ser o único, o direito à explicação encontra limites expressivos na garantia da autodeterminação informativa ao, por exemplo, impor ao titular um ônus excessivo de depender dele a requisição de explicações sobre a decisão. Como consequência, na falta de uma cultura de proteção de dados, existe o risco desse direito ser concretizado apenas por jornalistas e especialistas que conhecem o ciclo de vida de seus dados, e não por titulares comuns (Edwards; Veale, 2018, p. 6).

O próprio sistema de IA impõe limitações para o direito à explicação, mas que não invalidam esse direito. As ferramentas de tomada de decisão automatizada devem ser transparentes para com os titulares de acordo com o contexto de sua aplicação, os interesses dos titulares e os riscos envolvidos na aplicação do sistema. No entanto, essa transparência pode gerar cenário de ocultamento de informação, fadiga na quantidade de documentos fornecidos e

falha na comunicação com os interessados sobre o impacto e os riscos do sistema. As pessoas geralmente não entendem as informações recebidas sobre seus dados e, com isso, não ocupam posição para tomar decisões ponderadas sobre custo-benefício de se sujeitar a determinado tratamento de dados (Solove, 2022, p. 20).

Especificamente sobre o conteúdo da transparência, a simples informação sobre os dados de *input* já se mostrou incapaz de garantir explicações analíticas sobre o funcionamento do sistema e um possível efeito discriminatório, com isso explicações por meio de testes se mostram ferramenta útil para concretizar o direito à explicação. Outra barreira é a proteção do segredo de negócio, que, à primeira vista, poderia impedir o conhecimento do sistema, porém não há definição do escopo dessa proteção, de forma a permitir uma interpretação restritiva desse conceito.

Diante das obrigações de transparência, Helen Nissenbaum (2011, p. 36) destacou a existência de um paradoxo da transparência. Segundo a autora, é improvável que se atinja uma transparência do significado textual e uma transparência da prática, quando se tem um não se tem outro. Isso porque a informação considerada de forma específica, estanque, não está de acordo com um contexto mais amplo e impede que as pessoas possam compreender os riscos de efeitos colaterais e procedimentos falhos no contexto. Em regra, a transparência não é sinônimo de confiança, já que as pessoas se sentem confortáveis mesmo quando submetidas a sistemas que não conhecem. Nesse sentido, para além da transparência, as pessoas se baseiam em expectativas e confiam no conhecimento técnico dos profissionais, na supervisão de entidades de fiscalização, e, sobretudo, no interesse do sistema, qualquer que seja a sua origem, pelo bem-estar humano.

O objetivo de determinar obrigações de transparência e um direito à explicação é garantir que o titular possa escolher de forma livre e autônoma, concretizando, assim, o fundamento da autodeterminação informativa. Porém, transparência não é sinônimo de que a pessoa irá decidir autonomamente a partir dessas informações. Na verdade, existe um paradoxo em que, mesmo quando as pessoas entendem os documentos de transparência, elas não são informadas de maneira relevante sobre as decisões a que estão

submetidas (Barocas; Nissenbaum, 2014, p. 59). Ananny e Crawford (2018, p. 984) afirmam que a transparência é uma forma limitada de conhecer os sistemas e não pode ser usada para explicar um conjunto de sistemas que utilizam dados produzidos por agentes humanos e não humanos cujo significado não reside internamente, mas relacionalmente.

Portanto, o direito à explicação está previsto no cenário brasileiro e é uma das facetas do fundamento da autodeterminação informativa, mesmo diante de seus novos sentidos. Esse direito é pressuposto para a concretização dos outros direitos de proteção de dados nos casos em que a pessoa é sujeita a decisões automatizadas, como o de oposição, atualização dos dados e revisão do resultado. Ao mesmo tempo, esse direito não é suficiente para tutelar a proteção de dados dos interessados frente aos novos desafios do *big data* e dos sistemas de IA, à dimensão coletiva da proteção de dados, o paradoxo da transparência e do impacto das decisões automatizadas, seja inferindo dados pessoais[10], realizado predições ou determinando escolhas dos afetados. Esse direito encontra fronteiras inclusive na concretização da autodeterminação enquanto um direito de personalidade, o que indica para as limitações da própria matéria de proteção de dados pessoais, em vista das iminentes barreiras culturais, éticas e técnicas. Esses elementos são agenda para uma nova pesquisa que se debruce inclusive sobre um devido processo informacional (Crawford; Schultz, 2014), tendo em vista que os debates sobre um eventual direito à explicação sobre a decisão convergem para ideia de *fairness*, igualdade, autonomia e não discriminação no resultado.

10 "Dado os novos riscos da análise de *big data* e da tomada de decisões algorítmicas, as inferências não podem justificadamente permanecer como dados pessoais de 'classe econômica'. Os interesses de privacidade dos sujeitos dos dados exigem uma proteção renovada para restaurar o equilíbrio justo entre os interesses individuais, públicos e comerciais que inspira a lei de proteção de dados. O mandato atual da lei de proteção de dados funciona bem para governar os dados inseridos, mas não fornece um controle significativo sobre como os dados pessoais são avaliados" (tradução livre) (Wachter; Mittelstadt, 2019, p. 85).

Referências

ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coords). **Lei Geral de Proteção de Dados**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New media and society**, v. 20, n. 3, 2018.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679**. 2017. Disponível em: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963. Acesso em: 14 dez. 2022.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. In: LANE, Julia et al. **Privacy, Big Data, and the Public Good**: frameworks for engagement. Cambridge: Cambridge University Press, 2014.

BIONI, Bruno. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

BIONI, Bruno Ricardo. ***Accountability* na regulação de dados pessoais: virtudes e vicissitudes**. Tese (Doutorado) - Faculdade de Direito da Universidade de São Paulo, 2021.

BRADFORD, Anu. The Brussels Effect. **Northwestern University Law Review**, v. 107, n. 1, 2012.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Constituicao.htm. Acesso em: 31 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jul. 2024.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal**. Relatora Rosa Weber. 2020. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf. Acesso em: 16 nov. 2022.

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. **Big data and Society**, jan.-jun., 2016.

CASEY, Bryan; FARHANGI, Ashkon; VOGLP, Roland. Rethinking explainable machines: the GDPR's right to explanation debate and the rise of algorithm audits in enterprise. **Berkeley Technology Law Journal**, v. 34, 2019.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. **B. C. L. Rev**., vol. 55, 2014.

DOSHI-VELEZ, Finale, et al. Accountability of AI Under the Law: The Role of Explanation. **arXiv:1711.01134**. 2019. Disponível em: https://doi.org/10.48550/arXiv.1711.01134. Acesso em: 15 mar. 2023.

EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? **IEEE Security & Privacy**, v. 16, n. 3, 2018.

ESTADOS UNIDOS DA AMÉRICA. **Preparing for the future of artificial intelligence**. 2016. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Acesso em: 22 nov. 2022.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Bias in Algorithms – Artificial Intelligence and Discrimination**. Luxembourg: Publications Office of the European Union, 2022.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". **AI MAGAZINE, 2017**.

HANKIEWICZ, Kamila. **What Is The Real Difference Between Automation And AI?** 2018. Disponível em: https://becominghuman.ai/what-is-the-real-difference-between-automation-and-ai-366513e0c 910. Acesso em: 2022.

MARTINS, Leonardo. **Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_de-jurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em: 11 nov 2022.

MENDES, Gilmar Ferreira; GONET BRANCO, Paulo Gustavo; **Curso de Direito Constitucional**. 14ª Edição. São Paulo: Saraiva Educação, 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**, Artigo Estratégico, n. 39, 2018.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de Dados Pessoais Fundamentos da LGPD**. 1ª Edição. Rio de Janeiro: Forense, 2022.

KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019.

RECHTBANK AMSTERDAM. **C/13/687315 / HA RK 20-207. 11 mar. 2021a**. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/687315_/_HA_RK_20-207. Acesso em: 26 dez. 2022.

RECHTBANK AMSTERDAM. **C/13/692003/HA RK 20-302**. 11 mar. 2021b. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/692003/HA_RK_20-302. Acesso em: 26 dez. 2022.

REINO UNIDO. Government Office for Science. **Artificial intelligence: opportunities and implications for the future of decision making**. 2016. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf. Acesso em: 19 dez. 2022.

REINO UNIDO. Information Commissioner's Office. **Big data, artificial intelligence, machine learning and data protection**. 2017. Disponível em: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Acesso em: 19 dez. 2022.

REINO UNIDO. Information Commissioner's Office. **Explaining decisions made with IA**. 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf. Acesso em: 14 mar. 2023.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Rio de Janeiro: Renovar, 2008.

SELBST, Andrew D; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017.

SENADO FEDERAL. Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito. **Relatório final** da Comissão de Juristas responsável por subsidiar a elaboração de Substitutivo sobre Inteligência Artificial instituída pelo Ato do Presidente do Senado nº 4, de 2022, aprovado em 1º de dezembro de 2022. Brasília, 2022.

SOLOVE, Daniel. Privacy Self-Management and the consent Dilemma. **Harvard Law Review**, v. 126, 2013.

SOLOVE, Daniel. The Limitations of Privacy Rights. **GW Law Faculty Publications and Other Works**, 2022.

UNIÃO EUROPEIA. **Guidelines on Personal data breach notification under Regulation 2016/679**. Brussels: European Commission, Directorate General Justice, 2018.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, 2017.

WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age on big data and AI. **Colum. Bus. L. Rev**. 2019.

ZANATTA, Rafael. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais?channel=-doi&linkId=5c7078f8a6fdcc4715941ed7&showFulltext=true. Acesso em: 23 mar. 2023.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. Estados Unidos: Perseus Books, LLC, 2021.

3º lugar

Entre a transparência e a proteção: a compatibilização da Lei de Acesso à Informação à Lei Geral de Proteção de Dados na divulgação de dados públicos

Fernanda Magni Berthier

Resumo

O acesso à informação e a proteção de dados pessoais são direitos fundamentais no sistema brasileiro, gozando de proteção constitucional e regulamentação infraconstitucional – respectivamente, pela Lei de Acesso à Informação (Lei nº 12.527/2011, LAI) e pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018, LGPD). Em que pese ambos os direitos desempenhem funções complementares no controle social e no fortalecimento do Estado Democrático de Direito, há inevitáveis conflitos permeando a sua relação, especialmente no que tange à divulgação de dados pessoais pela administração pública com a finalidade de atender a um suposto interesse público. Diante disso, o presente artigo analisa de que forma é possível compatibilizar a LAI com a LGPD com o objetivo de permitir a sua coexistência harmoniosa no ordenamento jurídico. Para tanto, é empregada a metodologia dedutiva, com a realização de uma revisão de literatura especializada. Ao final, são identificados critérios de ponderação a serem empregados de forma casuística pelas autoridades diante das solicitações de acesso à informação, são examinadas propostas de alteração legislativa e são sugeridas outras medidas a serem adotadas no âmbito administrativo.

***Palavras-chave**: acesso à informação; proteção de dados pessoais; transparência; privacidade; ponderação.*

Introdução

Servidores públicos têm seus salários publicizados em portais de transparência, listas são divulgadas contendo os nomes de pessoas beneficiadas com o Auxílio Emergencial no contexto da pandemia de COVID-19 e pensões de familiares de militares expulsos são noticiadas na mídia. Diversas são as reportagens tratando de informações que vieram ao conhecimento do público desde a promulgação da Lei de Acesso à Informação, acendendo discussões acerca da compatibilização entre a promoção da transparência e a proteção da privacidade na sociedade da informação.

O acesso à informação propicia a participação cidadã nos negócios públicos, aprimorando o controle democrático e a prestação de contas do governo à sociedade (Sarlet; Molinaro, 2014, p. 22), de modo que "a informação é o oxigênio da democracia" (Article 19, 1999, p. 1)[1]. Nessa lógica, a publicidade é essencial para o funcionamento de governos democráticos, e o sigilo assume um caráter excepcional (Bobbio, 1986, p. 85). Em vista disso, há mais de 250 anos, a Suécia assumiu o pioneirismo na regulamentação do acesso a documentos públicos[2], impulsionando o desenvolvimento

1 A organização Article 19, nomeada em homenagem ao art. 19 da Declaração Universal dos Direitos Humanos da ONU, advoga pelo direito à liberdade de opinião e expressão e pelo direito ao acesso à informação a nível mundial. Em uma de suas iniciativas, produziu um conjunto de princípios internacionais com o objetivo de traçar parâmetros de avaliação de legislações nacionais de acesso a informações oficiais de acordo com as melhores práticas. São eles: (i) divulgação máxima; (ii) obrigação de publicar; (iii) promoção de um governo aberto; (iv) abrangência limitada das exceções; (v) procedimentos facilitadores de acesso; (vi) baixos custos; (vii) reuniões abertas; (viii) divulgação com precedência; e (ix) proteção dos denunciantes (Article 19, 1999).

2 O *Freedom of the Press Act* de 1766, de natureza constitucional, foi a primeira legislação no mundo a regulamentar o acesso à informação, dispondo sobre o direito dos cidadãos de requerer ao governo a disponibilização de documentos, exceto nos casos previstos no *Secrecy Act*, em que era determinado o sigilo sobre determinadas informações por prazo determinado. Por mais de 100 anos, a Suécia se

de legislações em diversas jurisdições – atualmente, esse direito é regulamentado em aproximadamente 140 países[3].

No caso do Brasil, a Constituição Federal já assegura as dimensões individual e coletiva do direito à informação, reconhecendo-o como o direito a receber dos órgãos públicos informações de interesse mediante requerimento, observadas as hipóteses de sigilo (art. 5º, XXXIII). Ademais, é consagrado no texto constitucional o instituto do *habeas data*, voltado ao acesso e à retificação de informações pessoais contidas em bancos de dados (art. 5º, LXXII)[4]. De todo modo, somente em 2012, a partir da vigência da LAI, conjuntamente com o Decreto nº 7.724/2012, houve uma verdadeira alteração sistêmica na relação entre a administração pública e os cidadãos, buscando-se o desenvolvimento de uma cultura de transparência e divulgação proativa, independentemente de solicitação (Sarlet; Molinaro, 2014, p. 32).

De outra banda, a proteção dos dados pessoais também é um valor protegido, considerando que, muitas vezes, há o reconhecimento da identidade de pessoas de forma apenas indireta, a partir da representação de sua personalidade com base em dados pessoais (Doneda, 2011, p. 106; Bioni, 2021, p. 56). Nesse sentido, a LGPD surgiu para tutelar os dados pessoais de forma autônoma, esta-

manteve como o único país em que o acesso à informação tinha status de direito legal (Naib, 2005, p. 1-2). Atualmente, a legislação foi modernizada, estando vigente o *Freedom of the Press Act* de 1976. Diante do ingresso da Suécia na União Europeia e da entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia ("GDPR"), são suscitadas novas discussões sobre as limitações ao acesso à informação no país, especialmente tendo em vista a grande importância que a transparência desempenha no sistema jurídico sueco.

3 A partir de uma iniciativa do *Centre for Law and Democracy* e do *Access Info*, foi desenvolvido o *RTI Rating*, que consiste em uma metodologia utilizada para a análise da qualidade das legislações regulamentadoras do direito ao acesso à informação em diferentes países, atribuindo pontos conforme o preenchimento de indicadores determinados. Em 2024, o ranking é composto por 140 países com regulamentações próprias, sendo liderado pelo Afeganistão e contando com Palau na última posição. O Brasil, por sua vez, ocupa o 28º lugar no ordenamento (RTI, 2024).

4 O *habeas data* pode ser definido como uma ação constitucional voltada tanto à defesa do acesso à informação como da proteção de dados pessoais, uma vez que seu surgimento se deu com o objetivo de permitir aos cidadãos o acesso a informações pessoais detidas pelo poder público, especialmente no que diz respeito aos registros da repressão durante o regime militar (Doneda, 2011, p. 104).

belecendo uma série de normas a serem seguidas pelos agentes de tratamento, inclusive pelo poder público, com o objetivo de garantir o livre desenvolvimento da personalidade e da dignidade da pessoa humana[5]. Houve, portanto, uma nova alteração sistêmica no contexto da sociedade de vigilância, devido ao reconhecimento de que os dados pessoais não são apenas um *commodity*, servindo, também, ao desenvolvimento social[6].

Atualmente, a proteção de dados pessoais é, assim como a transparência pública, um direito fundamental. Apesar de a LGPD não ter revogado expressamente nenhuma disposição trazida pela LAI, o aparente paradoxo entre publicidade e privacidade causa dúvidas sobre a harmonização de ambos os diplomas legais, pois, muitas vezes, para conferir transparência a seus atos, a administração pública é compelida a divulgar dados pessoais. Do mesmo modo, já foram constatadas diversas ocorrências em que a proteção de dados pessoais foi utilizada como fundamento para a negativa de disponibilização de informações[7].

5 Explica Danilo Doneda que o tratamento da proteção de dados pessoais nos seus moldes atuais é o reflexo de uma tendência observada após o desenvolvimento de diferentes gerações de leis desde a década de 1970, perpassando um modelo mais restrito e individualista até alcançar um padrão mais amplo e coletivo, visando a garantir uma tutela mais eficaz a esse direito. Constatando-se a indispensabilidade do fornecimento de dados pelos cidadãos para a sua efetiva participação na vida social, as normas tutelam não só o consentimento do titular com a utilização de seus dados, como, também, todo o processo de tratamento de dados pessoais, abrangendo a sua utilização por terceiros e a garantia de autodeterminação informativa (Doneda, 2011, p. 96).

6 Há muitos anos, é reconhecido o valor econômico dos dados pessoais na economia moderna, sendo frequentemente descritos como "o novo petróleo" (The world's..., 2017). Como destaca Bruno Bioni, desenvolveu-se uma "economia de vigilância" na qual os titulares são posicionados em uma condição de passividade em relação ao fluxo de seus próprios dados, que são extraídos e comodificados de forma escalável (Bioni, 2021, p. 12). Contudo, devem ser reconhecidos os limites morais do mercado no que diz respeito aos direitos fundamentais, tendo em vista o seu potencial danoso para as relações sociais (Roessler, 2015, p. 159). Nessa lógica, mostra-se relevante a utilização dos dados pessoais não apenas como ativos econômicos, mas, também, como ferramentas para auxiliar no progresso da sociedade, por meio, *e.g.*, da implementação de políticas públicas a partir da tomada de decisões baseadas em dados.

7 De acordo com o relatório disponibilizado pela Controladoria-Geral da União, entre 2012 e 2024, foram formulados 1.408.197 pedidos de acesso à informação. Em

O presente artigo tem como objetivo, portanto, o exame do conflito entre os direitos supostamente antagônicos de acesso à informação e proteção de dados pessoais, proporcionando a sua harmonização e sistematização diante de casos concretos. A partir da utilização da metodologia dedutiva e da realização de análise bibliográfica, sugerem-se, ao final, critérios de ponderação a serem adotados pelas autoridades brasileiras para a resolução do impasse e propõe-se a realização de alterações legislativas e a adoção de outros mecanismos.

Aparente conflito entre o acesso à informação e a proteção de dados pessoais

Princípio da máxima divulgação e excepcionalidade das limitações ao acesso à informação

No contexto da Constituição Federal de 1988, promulgada após o fim de um regime ditatorial de mais de 20 anos, o direito de acesso à informação em face do poder público surge como um desdobramento da liberdade de expressão e do direito à informação, transformando-se em "uma espécie de garantia supranacional da Democracia e da efetividade dos demais direitos" (Sarlet; Molinaro, 2014, p. 16). A partir da LAI e de seu respectivo Decreto, enfim, o acesso à informação foi verdadeiramente regulamentado, a partir do estabelecimento da obrigação das autoridades públicas de permitir o acesso à informação às partes interessadas e da previsão de um procedimento a ser adotado para tanto[8].

69,78% dos casos, o acesso foi concedido; em 8,00%, negado; e, em 5,08%, parcialmente concedido. Dentre os casos de negativa, os principais motivos apresentados foram a proteção de dados pessoais (24,09% das recusas) e o fato de as informações solicitadas serem sigilosas (16,93% das recusas) (CGU, 2024).

8 Como destacam John Ackerman e Irma Sandoval-Ballesteros (2006, p. 94), mesmo em países nos quais há garantias constitucionais de direito à informação ou à liberdade de expressão, a edição de regulamentos específicos é importante devido à dificuldade de aplicação direta de normas constitucionais sem a intermediação da legislação infraconstitucional. Assim, no caso do Brasil, apesar de o acesso à informação ser uma norma definidora de direito fundamental com aplicação imediata

A LAI atua como uma ferramenta de democratização e construção da cidadania, assegurando o acesso à informação pelos interessados com transparência, clareza e linguagem de fácil compreensão (art. 5º da LAI). Nesse sentido, a transparência é operacionalizada tanto passiva como ativamente, *i.e.*, além de prestar informações específicas a pedido dos interessados (pessoas físicas ou jurídicas devidamente identificadas)[9], o Estado deve proativamente promover a divulgação de informações de interesse público em locais de fácil acesso (Valim, 2015, p. 41)[10].

Sob a égide da LAI, vigora a publicidade como preceito geral e o sigilo como exceção (art. 3º da LAI). A própria legislação expressamente excepciona o livre acesso a informações em casos de: *(i)* informações protegidas por outras hipóteses legais de sigilo – a exemplo dos arts: art. 5º, XII, XIV e XXXIII; art. 93, IX; e art. 139, III,

(art. 5º, § 1º, da Constituição Federal), permitindo-se desde já a extração de efeitos jurídicos vinculativos ao poder público, a LAI assegura o seu exercício (Sarlet; Molinaro, 2014, p. 29).

9 Uma problemática na transparência passiva diz respeito à obrigatoriedade de identificação do requerente no procedimento de solicitação de acesso à informação, conforme estabelecido no art. 10 da LAI e reforçado no art. 12 do Decreto nº 7.724/2012. Em alguns casos, constatou-se que a falta de proteção dos dados dos solicitantes ocasionou situações de discriminação, constrangimento, intimidação e perseguição (ARTICLE 19, 2018). No caso do Brasil, a ausência de proteção se dá, em grande parte, devido à vedação constitucional ao anonimato (art. 5º, IV, da Constituição Federal). Inclusive, no projeto que originou a LGPD, havia disposição no seu art. 23, II, determinando que seriam "protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado", mas a previsão foi vetada pelo Poder Executivo, e o veto foi mantido pelo Congresso Nacional. Assim, vislumbra-se como possíveis soluções paliativas para a problemática a adoção de medidas como a restrição à identidade do solicitante, a permissão à utilização de pseudônimos e, até mesmo, a utilização de tecnologias de criptografia (Rodrigues; Michener, 2018, p. 314).

10 Mais recentemente, em 2021, foi editada a Lei nº 14.129/2021 (Lei do Governo Digital), a qual estabeleceu diversos mecanismos visando ao aprimoramento da eficiência da administração pública. Em seu art. 29, § 1º, estabeleceram-se como requisitos a promoção da transparência ativa de dados pelo poder público, dentre outros: "I - observância da publicidade das bases de dados não pessoais como preceito geral e do sigilo como exceção;" e "VIII - respeito à privacidade dos dados pessoais e dos dados sensíveis, sem prejuízo dos demais requisitos elencados, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);".

todos da Constituição Federal – segredo de justiça e segredo industrial (art. 22 da LAI); *(ii)* informações imprescindíveis à segurança da sociedade ou do Estado, que podem ser classificadas como ultrassecretas, secretas ou reservadas e ter seu acesso restrito pelos prazos de 25, 15 ou 5 anos, respectivamente (arts. 23 e 24 da LAI); e *(iii)* informações pessoais, relativas à intimidade, vida privada, honra e imagem (art. 31 da LAI), cujo acesso pode ser restrito apenas ao titular e a agentes públicos legalmente autorizados pelo prazo máximo de 100 anos, contados da produção da informação (art. 31, § 1º, I, da LAI)[11].

É comum entre as normas que regulam o acesso à informação em diferentes jurisdições a previsão de exceções à transparência com fundamento na proteção de informações privadas (Naib, 2005, p. 18) – sobretudo em países como o Brasil, em que remanescem resquícios de uma cultura de sigilo e opacidade da administração pública (Valim, 2015, p. 36). Em relação às informações pessoais sensíveis, a LAI, além de reconhecer a obrigação dos órgãos e das entidades do poder público de proteger as informações pessoais (art. 6º, III, da LAI), possibilita a restrição ao seu acesso em determinadas circunstâncias, como forma de tutelar a personalidade da pessoa a que se refiram (art. 31 da LAI).

Tendo em vista esse panorama, ao sopesar os princípios da publicidade e da transparência e os direitos fundamentais à intimidade e à vida privada, o STF decidiu, no julgamento do Tema 483 em 2015[12], que "[é] legítima a publicação, inclusive em sítio eletrônico mantido pela administração pública, dos nomes dos seus servidores e do valor dos correspondentes vencimentos e vantagens pecuniárias". Dessa forma, justificar-se-ia uma relativização da privacidade dos agentes públicos no exercício de suas funções, auto-

11 De todo modo, mesmo nos casos em que há alguma restrição à publicidade aplicável, quando possível, não deve ser obstaculizado o acesso à integralidade do conteúdo do documento objeto de pedido de transparência (art. 7º, §2º, da LAI). Ainda, nos casos de exceções ao acesso à informação, a rigor, a análise acerca da justificação do sigilo varia conforme o transcurso temporal, considerando o desaparecimento ou a redução do seu potencial danoso (Naib, 2005, p. 13).

12 STF. Plenário. Tema 483 – Divulgação, em sítio eletrônico oficial, de informações alusivas a servidores públicos, inclusive seus nomes e correspondentes remunerações. ARE 652.777. Min. Rel. Teori Zavascki. Brasília, 23.06.2015.

rizando-se, por conseguinte, a publicização de informações pessoais contidas em bases de dados estatais como forma de promover o interesse público preponderante.

Proteção de dados pessoais públicos sob a égide da LGPD

Paralelamente ao desenvolvimento da legislação voltada à garantia do acesso à informação, ocorreu o aprimoramento da tutela dos direitos de personalidade. No processo de "constitucionalização" da pessoa, passa-se da proteção da privacidade, compreendendo o direito a ser deixado só, à proteção dos dados, envolvendo o controle sobre a circulação de informações sobre o indivíduo, impactando na construção de sua própria personalidade (Rodotà, 2003, p. 17). Assim, a partir da vigência da LGPD e do reconhecimento da proteção de dados como um direito fundamental[13], é inaugurada uma nova noção de dados pessoais, percebida como um direito autônomo que faz jus a um regime protetivo próprio (Bioni, 2021, p. 109).

Nessa lógica, apesar de a LAI atuar como um embrião da proteção de dados no setor público, a sua definição de "informações pessoais" compreende dados que identificam direta ou indiretamente os seus titulares, sendo protegidos somente quando a sua divulgação indevida puder potencialmente causar prejuízos à preservação da privacidade e da integridade moral de seu titular (art. 31, §1º, I, da LAI)[14]. Portanto, nesse âmbito, a tutela estaria estrita-

13 Por meio da EC 115/2022, a proteção de dados passou a gozar do *status* de direito constitucional, seguindo a tendência que já era observada em diversos outros países desde o final do século XX – a exemplo de Portugal, cuja Constituição de 1976 já contemplava referida proteção. Antes disso, o plenário do STF já havia reconhecido a proteção de dados pessoais e a autodeterminação informativa como direitos fundamentais autônomos no julgamento conjuntos das ADI 6.387, 6.388, 6.393 e 6.390 em 07.05.2020. Nesses casos, buscava-se a declaração da inconstitucionalidade da Medida Provisória nº 954/2020, que permitia o compartilhamento de dados por empresas de telecomunicações com o IBGE para fins de estatística durante a pandemia do coronavírus, mas decidiu-se que tais providências não atendiam aos princípios de razoabilidade e proporcionalidade. Como consequência da atribuição da condição de direito fundamental à proteção de dados, ela assume o mesmo nível hierárquico do acesso à informação, não havendo uma prevalência *a priori* em relação àquele.

14 A respeito da proteção das informações pessoais na LAI: "Certo é que no direito

mente relacionada à coibição de efeitos na esfera dos direitos da personalidade, exigindo um amplo esforço interpretativo na determinação das consequências de seu acesso aos seus titulares (Viola; Doneda, 2016, p. 126).

Por sua vez, na redação da LGPD, os dados pessoais são considerados como qualquer informação relacionada a uma pessoa natural identificada ou identificável, ao passo que os dados pessoais sensíveis compreendem quaisquer dados vinculados a pessoas naturais envolvendo "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II, da LGPD)[15]. Como consequência, a LGPD expande o regime protetivo a certos dados que não estariam configurados como informações pessoais à luz da LAI, como é o caso dos dados cadastrais, cuja divulgação é restrita aos casos de contratações com a administração pública[16]. Na ausência

brasileiro existe um dever constitucional do Estado em assegurar a gestão transparente da informação, para tanto o Estado está obrigado na proteção da informação, garantindo sua disponibilidade à cidadania, ademais de proteger de igual modo a informação sigilosa e a informação pessoal" (Sarlet; Molinaro, 2014, p. 38).

15 Em relação à categoria de dados pessoais sensíveis, sua criação decorre da necessidade de conferir a esses dados um tratamento distinto dos demais, em razão de seu potencial utilização de forma discriminatória ou lesiva aos seus titulares. Nessa ótica, o princípio da igualdade material apresenta-se como um valor que justifica a tutela da pessoa exorbitando os cânones tradicionalmente vinculados à privacidade. Como sintetiza Danilo Doneda: "é necessário ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações nas quais a discriminação pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos" (Doneda, 2021). No que diz respeito ao acesso à informação, justificar-se-ia, por exemplo, a vedação da revelação de dados pessoais sensíveis na divulgação de resultados de estudos de saúde pública (ANPD, 2022, p. 38).

16 Antes da vigência da LGPD, em 2014, o TCU havia emitido parecer consignando que "dados cadastrais, em processos de controle externo, de endereço de responsáveis, seja pessoa física ou jurídica, de interessados, de sócios de pessoa jurídica, e de seus respectivos procuradores, para fins de comunicação processual, não deve ser considerado informação pessoal, haja vista que não constitui qualquer ofensa à intimidade, vida privada, honra ou imagem dos jurisdicionados" (TC 034.351/2014-0). Posteriormente, com vistas à harmonização com a LGPD, o entendimento foi

de uma definição comum de informações pessoais na LAI e na LGPD, as disposições de ambos os regramentos devem ser consideradas diante de pedidos de acesso à informação (Banisar, 2011, p. 18).

No âmbito da administração pública federal, o Guia de Boas Práticas da Lei Geral de Proteção de Dados destaca as diferenças de tipologia trazidas pela LGPD em comparação com a LAI, ampliando a tutela conferida aos dados pessoais:

> Diferentemente da LAI, no entanto, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais (GOV.BR, 2020, p. 20).

Apesar do aparente paradoxo, não há incompatibilidade entre a proteção de dados e o acesso à informação[17]. Inclusive, a tutela de dados pessoais públicos está no berço do desenvolvimento dos sistemas de proteção de dados pessoais, tendo em vista a preocupação com a ameaça a direitos e liberdades fundamentais dos ci-

mitigado, definindo-se que "os dados pessoais inseridos nos preâmbulos dos contratos, convênios e afins, celebrados pela Administração Pública, devem limitar-se aos nomes das partes e seus respectivos CPF/CNPJ e endereços, por se tratarem dos elementos minimamente necessários à identificação e localização dos agentes para fins de controle social e de exigência de cumprimento das obrigações contratuais assumidas. Por outro lado, quando se tratar de representante legal de pessoa jurídica da contratada, o número de CPF deve ser divulgado de forma descaracterizada, de modo a evitar, ao mesmo tempo, os homônimos e o uso desautorizado de tal dado por terceiros" (CGU, 2021, p. 10).

17 Acerca da compatibilidade entre as legislações, destaca-se o Enunciado n. 688 da IX Jornada de Direito Civil: "A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelecem sistemas compatíveis de gestão e proteção de dados. A LGPD não afasta a publicidade e o acesso à informação nos termos da LAI, amparando-se nas bases legais do art. 7º, II ou III, e art. 11, II, a ou b, da LGPD." No mesmo sentido, o Enunciado n. 04/2022 da Controladoria-Geral da União: "A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos".

dadãos diante da administração de seus dados pelo Estado, a partir da criação de bancos de dados a serem controlados por órgãos públicos (Doneda, 2021). Nesse ponto, percebe-se a existência de "uma relação mútua entre a construção de espaços ao privado e ao público na perspectiva de estabelecimento de uma autodeterminação informativa", na medida em que o controle sobre as próprias informações nominativas de um indivíduo é essencial à promoção do livre desenvolvimento de sua personalidade (Cachapuz, 2019, p. 1560). Por conseguinte, há uma relação de convergência entre o objetivo da LAI de assegurar a transparência do Estado e o da LGPD de garantir a opacidade dos cidadãos (Bento, 2020, p. 188).

Assim, o tratamento de dados pessoais pelo poder público para atender às diretivas de acesso à informação deve ser "realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (art. 23 da LGPD). Apesar da redação confusa, essa previsão determina que o detentor da informação pública explicite "quais são: a previsão legal, a finalidade, os procedimentos e as práticas utilizadas nesse tratamento, devendo inclusive ser indicado um encarregado que passará a responder por essas atividades" (Canhadas, 2020). Portanto, há uma relação de instrumentalidade entre o dever de transparência da administração pública e a realização da proteção de dados (Gasiola et al., 2021).

A CGU orienta que as decisões relativas a pedidos de publicidade de dados de pessoas físicas sejam fundamentadas exclusivamente nas disposições da LAI, norma específica de regência processual e material desse procedimento administrativo (CGU, 2023b, p. 8). Inclusive, ao tratar da restrição de acesso a informações relativas a despesas médicas, assim justifica:

> A restrição de acesso à informação não se dá pelo fato de serem dados pessoais – que podem ser de natureza pública ou privada - mas porque a revelação desses dados ameaçaria a intimidade, vida privada, honra e imagem das pessoas em questão, suas liberdades e garantias individuais, uma vez que vulneram o pleno exercício e desenvolvi-

> mento de suas individualidades no seio da coletividade. Nesses casos, realizando-se uma ponderação de princípios, os direitos à privacidade e à proteção de dados pessoais superam o direito de acesso a informações. (CGU, 2023b, p. 25-26).

Em países em desenvolvimento, como é o caso do Brasil, cuja história é marcada por casos de corrupção e períodos de secretismo, há normalmente uma maior sensibilidade à transparência e ao acesso à informação em detrimento da tutela da privacidade e dos dados pessoais (Bento, 2020, p. 193). Contudo, considerando a inexistência de hierarquia entre a LAI e a LGPD, esta também deve ser observada nos procedimentos de acesso à informação regidos por aquela lei (ANPD, 2022, p. 38).

O problema é que, frequentemente, a privacidade de agentes públicos ou de terceiros é utilizada de forma irrestrita e indevida para cercear e obstaculizar o acesso à informação, fortalecendo um discurso na mídia de que as leis de privacidade – e, por associação, de proteção de dados – visam a ocultar as atividades do governo (Banisar, 2011, p. 16)[18]. Com efeito, em que pese a LAI e a LGPD sejam duas legislações compatíveis entre si e de suma importância para a efetivação dos direitos fundamentais de acesso à informação e proteção de dados, notam-se as mazelas em sua inadequada intepretação e instrumentalização. À vista disso, evidencia-se a necessidade de sua harmonização por meio de uma interpretação sistemática.

Proposta de harmonização entre a LGPD e a LAI

Aplicação da ponderação a partir da Lei de Colisão de Alexy

Tanto o acesso à informação como a proteção de dados são direitos fundamentais cuja eficácia não é absoluta, podendo sofrer intervenções restritivas diante de outros valores e direitos protegidos (Sarlet; Molinaro, 2014, p. 30). A LAI não atua como uma carta

18 Até 2022, em um levantamento preliminar, já haviam sido constatadas menções à LGPD no indeferimento de mais de 300 solicitações, incluindo, por exemplo, pedidos relativos à localização geográfica de determinadas doenças e ao cadastro de fornecedores da administração pública (Impactos da LGPD..., 2022, p. 16).

branca em relação ao acesso a informações públicas, de forma que devem ser observadas determinadas limitações à transparência administrativa – a chamada "transparência proibida" (Canhadas, 2020). Do mesmo modo, nos regimes democráticos atuais, superando a metáfora do "homem de vidro"[19], a esfera particular é objeto de tutela estatal, reconhecendo-se o direito de cada cidadão à sua intimidade e privacidade, e, mais recentemente, à proteção de seus dados. Dessa forma, são consideradas legítimas apenas as limitações necessárias ao controle social e à formação da opinião pública (Rodotà, 2003, p. 16)[20].

Em casos de colisão entre princípios[21], em que uma norma limita a possibilidade jurídica de cumprimento da outra, Robert Alexy defende a realização de uma análise diante do caso concreto de qual princípio possui um maior peso e deve prevalecer (Alexy, 1993, p. 89). Dessa forma, não há uma determinação em abstrato de que um princípio não é válido e deve ser eliminado do ordenamento jurídico, mas, tão somente, a indicação de condições que condu-

19 A metáfora nazista do "homem de vidro" (na tradução da expressão alemã "*gläserner mensch*") é utilizada por Stefano Rodotà para aludir à ideia totalitarista de vigilância, em que as pessoas são reduzidas de cidadãs à condição de súditos, repudiando-se a preservação de uma esfera mínima de privacidade e intimidade. Nessa lógica, cada indivíduo é desnudado frente ao Estado e às demais pessoas, contrariando a própria essência democrática (Rodotà, 2003, p. 15-16). Em desacordo com os ideais do Estado Democrático de Direito, os indivíduos são subjugados, ao passo que o Estado se oculta perante os cidadãos.

20 No que diz respeito à utilização indevida da proteção de informações pessoais para restringir o acesso à informação pública, a Controladoria-Geral da União emitiu parecer tratando de diversos temas. Em seu atendimento, não é justificável que se obste a publicização de informações como os títulos acadêmicos e os documentos entregues à administração como requisito para acesso a cargo ou função pública; os registros de vídeo dos processos de concurso público, como exames orais; os registros de entrada e saída de visitantes em prédios públicos, inclusive no Palácio do Planalto, em casos de visitas oficiais, visitas de agentes privados com interesses particulares e visitas de pessoas politicamente expostas; e as listagens de nomes de usuários bloqueados em perfis de autoridades públicas em redes sociais (CGU, 2023b).

21 Dentro da distinção de normas jurídicas entre regras e princípios trazida por Alexy, os direitos fundamentais ao acesso à informação e à proteção de dados podem ser qualificados como princípios, na medida em que gozam de um nível relativamente alto de generalidade e podem ser cumpridos em diferentes graus, a depender das possibilidades reais e jurídicas (Alexy, 1993, p. 83 e ss).

zem à precedência de um princípio sobre o outro, as quais variam casuisticamente (Alexy, 1993, p. 91-92).

Na atividade de ponderação, em síntese, a partir da máxima da proporcionalidade em sentido amplo, extraem-se as máximas parciais de adequação, necessidade e proporcionalidade em sentido estrito, as quais devem ser satisfeitas de acordo com a finalidade da norma (Alexy, 1993, p. 111-112). Especialmente no que diz respeito à proporcionalidade em sentido estrito, um fator relevante na análise sobre a possibilidade de publicização de dados pessoais é o seu potencial danoso em relação a garantias individuais do titular de dados pessoais, como é o caso da própria proteção da privacidade e da autodeterminação informativa (ANPD, 2024, p. 8).

Utilizando-se dessas premissas, Fernando Canhadas (2020) aplicou a lei de colisão de Alexy ao caso da divulgação dos vencimentos dos agentes públicos, concluindo que a medida de publicização é *(i)* adequada à finalidade pretendida de transparência de despesas públicas; *(ii)* necessária para a consecução da finalidade, não havendo uma alternativa menos restritiva de direitos fundamentais; porém, *(iii)* extremamente gravosa à intimidade, ferindo a proporcionalidade em sentido estrito. Assim, sugere, em sua substituição, a mera menção a números de matrículas ou de registros funcionais em substituição ao nome dos servidores (Canhadas, 2020).

Tratando da mesma questão, Maria Cláudia Cachapuz aponta que caminho diverso ao da interpretação segundo as regras de proporcionalidade de Alexy vem sendo adotado pelos tribunais brasileiros diante da colidência entre o interesse público e o interesse privado (Cachapuz, 2019, p. 1577). Nesse ponto, critica a decisão do STF no Tema 483, na medida em que os argumentos dos julgadores destacam, *a priori*, a prevalência do interesse público sobre fatos históricos e pessoas públicas (incluindo servidores públicos), afastando a realização da ponderação em relação à proteção dos dados sensíveis daqueles que desempenham funções públicas (Cachapuz, 2019, p. 1579).

A questão é polêmica: desde o julgamento do ARESS 3.902[22], anterior ao Tema 483, o STF já havia exarado posicionamento em

22 STF. Plenário. ARESS 3.902. Rel. Min. Ayres Britto. Brasília, 09.06.2011.

relação aos limites das informações pessoais publicizadas, determinando a sua restrição aos nomes e aos vencimentos dos agentes públicos e proibindo a revelação do endereço residencial, do CPF e da CI de cada servidor. De todo modo, questiona-se a necessidade de publicização da relação entre nomes e vencimentos diante da LGPD.

Mesmo quando o juízo interpretativo conduzir a uma decisão favorável à publicização de informações, é necessário ter em vista que o princípio da finalidade atua como limitador à utilização de dados pessoais obtidos a partir da LAI, devendo o seu tratamento ser compatível com o motivo que fundamentou a sua coleta – *e.g.*, por força do art. 8º do Decreto nº 6.135/2007, os dados de identificação das famílias do Cadastro Único somente podem ser utilizados para a "formulação e gestão de políticas públicas" e a "realização de estudos e pesquisas" (Viola; Doneda, 2016, p. 129).

Dentro do escopo da proteção de dados, a finalidade, estabelecido no art. 6º da LGPD, determina que a utilização dos dados pessoais está restrita aos objetivos que foram comunicados ao titular antes de sua coleta, prestando-se a valorar a razoabilidade de certas formas de utilização potencialmente abusivas (Doneda, 2011, p. 100). A título exemplificativo, mesmo antes da edição da LGPD, o STJ[23] já havia se manifestado a respeito do princípio da finalidade no registro de dados pessoais em caso envolvendo cadastros de crédito[24]. Portanto, ainda que seja admitida, por exemplo, a divulgação dos vencimentos dos servidores públicos, como no caso analisado acima, não seria legítima a utilização desses dados com

23 STJ. Quarta Turma. REsp 22.337-8. Rel. Min. Ruy Rosado de Aguiar. Brasília, 13.02.1995.

24 Extrai-se do voto do Relator, Ministro Ruy Rosado de Aguiar: "O Serviço de Proteção ao Crédito (SPC), instituído em diversas cidades pelas entidades de classe de comerciantes e lojistas, tem a finalidade de informar seus associados sobre a existência de débitos pendentes por comprador que pretenda obter novo financiamento. É evidente o benefício que dele decorre em favor da agilidade e da segurança das operações comerciais, assim como não se pode negar ao vendedor o direito de informar-se sobre o crédito do seu cliente na praça, e de repartir com os demais os dados que sobre ele dispõe. Essa atividade, porém, em razão da sua própria importância social e dos graves efeitos dela decorrentes – pois até para inscrição em concurso público tem sido exigida certidão negativa no SPC – deve ser exercida dentro dos limites que, permitindo a realização da sua finalidade, não se transforme em causa e ocasião de dano social maior do que o bem visado".

a finalidade de estabelecer o perfil de consumidor de um agente visando à posterior comunicação de conteúdo publicitário a ele.

A partir dessa análise, percebe-se como a aplicação da lei de colisão de Alexy traz importantes balizas para a harmonização entre o acesso à informação e a proteção de dados diante de casos concretos. Não se pode admitir a definição apriorística de uma relação de prevalência de um direito sobre o outro, devendo ser realizado um sopesamento acerca de qual princípio possui um maior peso em determinadas circunstâncias.

Análise comparada da experiência espanhola

Além da utilização da clássica regra de ponderação, vislumbra-se adequada a adoção de critérios interpretativos e de outros mecanismos para a promoção do equilíbrio entre o acesso à informação e a proteção de dados na legislação nacional. Nesse sentido, é relevante a análise das soluções empregadas em outros ordenamentos jurídicos, a partir da metodologia de estudo comparativo, como forma de contribuir com a evolução do sistema brasileiro. Para tanto, utiliza-se como referência o direito espanhol[25], em que há a previsão expressa de critérios de ponderação e a regulamentação de duas autoridades independentes, responsáveis pelo acesso à informação e pela proteção de dados, que atuam conjuntamente.

No ordenamento jurídico espanhol, a *Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno* ("LTAIB") preceitua, em seu art. 15, regras, critérios e diretrizes para a solução de conflitos entre a transparência e a proteção de dados. Em que pese o referido sistema esteja embasado nas antigas Diretiva 95/46/CE e *Ley Orgánica 15/1999*, que foram substituídas pelo GDPR e pela *Ley Orgánica 3/2018*, suas disposições permanecem aplicáveis, haven-

25 Reconhece-se que o sistema espanhol de promoção de acesso à informação não está imune a críticas, especialmente devido à inexistência de um direito constitucional de acesso à informação e à constatação de limitações ao escopo da publicização, de forma que o país ocupa a 96ª posição no ranking RTI (2024). A despeito disso, para os fins do presente estudo, focam-se apenas em aspectos da legislação concernentes às técnicas de ponderação e às medidas promocionais adotadas.

do, inclusive, referência expressa ao seu conteúdo na nova legislação nacional de proteção de dados (Guerrero, 2023, p. 71).

Nesse regime, os dados pessoais são categorizados, havendo, em um primeiro plano, os dados especialmente protegidos, que *"revelen la ideología, afiliación sindical, religión o creencias"*, cuja divulgação depende do consentimento do titular, ou que *"hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor"*, os quais podem ser publicizados consensualmente ou por autorização legal (art. 15, 1, LTAIB). Por sua vez, os dados meramente identificativos estão *"relacionados con la organización, funcionamiento o actividad pública del órgano"*, e incide sobre eles uma presunção relativa de legitimidade de divulgação, sujeito a um juízo de ponderação no caso concreto a respeito de eventual prevalência da proteção de dados ou de outros direitos em relação ao interesse público de transparência (art. 15, 2, LTAIB).

Finalmente, há uma terceira categoria, por exclusão, de dados não especialmente protegidos, cujo acesso depende de prévia ponderação, a qual observará uma série de critérios, incluindo a justificação de acesso à informação para fins históricos, científicos ou estatísticos e a maior garantia dos direitos dos titulares caso os dados se refiram a crianças ou adolescentes ou a sua divulgação possa afetar a sua privacidade ou segurança (art. 15, 3, LTAIB). Como destaca Manuel Guerrero (2023, p. 64-65), a lista de critérios elencados não é exaustiva, permitindo também o emprego de outras técnicas interpretativas, incluindo a doutrina constitucional sobre a esfera pública e a esfera privada. De todo modo, a sua inclusão na legislação definitivamente teria facilitado a complexa tarefa desempenhada pelos agentes públicos espanhóis no atendimento às solicitações de acesso à informação.

No mesmo sentido, sugere-se que a promoção de alterações na LAI com vistas à inclusão de critérios mais detalhados proporcionaria um maior suporte legal para os servidores públicos ao decidirem sobre pedidos de acesso à informação. Tais mudanças não apenas clarificariam o processo de divulgação de dados no Brasil, como também garantiriam um equilíbrio mais eficaz entre

a transparência e a proteção de dados pessoais, alinhando-se aos padrões internacionais de proteção de dados.

Outro ponto de destaque é que, na Espanha, é adotado um modelo que conta com duas autoridades federais responsáveis pelo controle do acesso à informação e da proteção de dados – respectivamente, o *Consejo de Transparencia y Buen Gobierno e a Agencia Española de Protección de Datos*. Nesses regimes duais, a principal vantagem é o desenvolvimento de maior especialização de cada órgão na proteção de um direito específico, entretanto, existe uma preocupação relativa a potenciais conflitos entre as autoridades (Banisar, 2011, p. 23–24).

A fim de solucionar essa problemática, na LTAIB, é determinada de forma expressa a cooperação entre as entidades na adoção das normas de ponderação em seus âmbitos de atuação (disposição adicional 5ª, LTAIB). Assim, o *Consejo de Transparencia y Buen Gobierno e a Agencia Española de Protección de Datos* atuam conjuntamente, tendo acordado na utilização, como critério de equilíbrio entre o acesso à informação e a proteção de dados pessoais, "a contribuição efetiva da informação solicitada para a promoção da transparência e do *accountability* de autoridades públicas (teste de interesse público) vis a vis a exposição da privacidade ocasionada pela divulgação dos dados pessoais envolvidos (teste de dano)" (Bento, 2020, p. 193). Dessa forma, rechaçam-se pedidos que aparentemente decorrem de uma mera curiosidade, e não de uma verdadeira busca por controle social.

Nesse ponto, um exemplo relevante é o Critério Interpretativo 004/2015 publicado por ambas as autoridades, envolvendo a publicidade ativa de dados do DNI, documento nacional de identificação espanhol, e das assinaturas manuscritas em arquivos públicos. Conforme apontado, tanto o DNI como as assinaturas consistem em dados pessoais e a sua publicização não seria necessária para o cumprimento da obrigação de divulgar a identidade dos adjudicatários de contratos com a administração pública, bastando a menção ao seu nome, sobrenome e cargo (Bento, 2020, p. 193). Ainda, foram destacados os riscos na disponibilização dessas informações, sobretudo na usurpação da identidade dos titulares dos dados pessoais.

No caso do Brasil, o regime adotado é, ao menos em teoria, dual, uma vez que o controle da LAI compete à CGU, em âmbito federal, e a cada autoridade de fiscalização e monitoramento, prevista no art. 40 da legislação, em outros âmbitos; e as atribuições relacionadas à LGPD incumbem à Autoridade Nacional de Proteção de Dados (ANPD). Efetivamente, a CGU exerce diversas funções relevantes para a efetivação do acesso à informação, incluindo a disponibilização do Painel da LAI, com estatísticas a respeito da implementação da norma pelo poder executivo federal (CGU, 2024). Contudo, o órgão não possui uma especialização exclusiva na matéria tal como o *Consejo de Transparencia y Buen Gobierno*, o que seria muito favorável à garantia de transparência a nível nacional.

Além disso, a exemplo da relação existente entre o *Consejo de Transparencia y Buen Gobierno e a Agencia Española de Protección de Datos*, sugere-se o estreitamento dos vínculos entre a CGU – ou outra autoridade que venha a substituí-la – e a ANPD. Desde 2022, notaram-se maiores aproximações entre as autoridades, por meio da condução de reuniões (ANPD e CGU estreitam..., 2022) as quais culminaram na assinatura de um Acordo de Cooperação Técnica com o objetivo de promover ações conjuntas sobre assuntos de interesse recíproco, incluindo as seguintes medidas:

> a) Criação de um canal de comunicação institucional para intercâmbio de informações, diagnósticos e modelos de boas práticas visando fortalecer a cultura de transparência e de privacidade e proteção de dados na Administração Pública Federal;
> b) Elaboração de normas, estudos e processos em conjunto para a construção de entendimento e de metodologia de aplicação harmônica entre a LGPD, a LAI e demais normas de transparência;
> c) Apoio institucional e intercâmbio de informações acerca de processos de fiscalização em curso quanto à aplicação da LGPD, da LAI e demais normas de transparência, nos órgãos e entidades da Administração Pública Federal; e
> d) Elaboração conjunta decursos de formação e capacitação relacionados à transparência e à proteção de dados pessoais, bem como de campanhas informativas ao público em geral (CGU, 2023a, p. 3).

Assim, a assinatura do Acordo de Cooperação Técnica entre a CGU e a ANPD se apresenta como um excelente exemplo da conjugação de esforços entre as autoridades públicas para a harmonização da interpretação e aplicação das normas da LAI e da LGPD de forma articulada, com o objetivo de garantir a efetivação dos direitos fundamentais ao acesso à informação e à proteção de dados, nos termos em que preceitua a Constituição Brasileira.

Perspectivas de alteração legislativa e outras soluções administrativas passíveis de adoção

Considerando a problemática interpretativa acerca do alcance da tutela dos dados pessoais na administração pública e das restrições à sua disponibilização, são diversas as iniciativas que buscam alterar o regramento atual.

Dentre os projetos de lei em tramitação, merece atenção o PL 4178/2019, de iniciativa do Deputado Roberto de Lucena (PODE/SP), que trata da criação do Instituto Nacional de Acesso à Informação – órgão com as atribuições de promoção e fiscalização do cumprimento das obrigações de transparência pública previstas na LAI – e da adoção do "teste de dano e interesse público" como procedimento de avaliação dos riscos relacionados à publicização de determinadas informações e dos eventuais danos à privacidade decorrentes. Esse teste, com algumas nuances, é também disposto no PL 251/2022, proposto pelos Deputados Felipe Rigoni (União/ES), Tabata Amaral (PSB/SP), dentre outros[26].

Por sua vez, o PL 3101/2021, de iniciativa de um grupo de Deputados incluindo Adriana Ventura (NOVO/SP) e Marcel Van Hattem (NOVO/RS), trata da inserção na LGPD do princípio da garantia de acesso a informações sobre agentes públicos no exercício de suas funções e agentes privados que interajam com a administração pública, vedando a utilização da legislação como fundamento para negativas de acesso à informação sobre agentes públicos no

26 O PL 251/2022 foi apensado ao PL 4178/2019, em 24 de fevereiro de 2022, por despacho do Presidente da Câmara dos Deputados, tramitando conjuntamente desde então.

exercício de suas funções e sobre agentes privados na condição de beneficiários ou administradores de recursos públicos.

No ponto, acredita-se que devem ser privilegiadas propostas legislativas que favoreçam a interpretação sistêmica da interação entre a LGPD e a LAI diante de cada caso concreto, sem estabelecer, *a priori*, a prevalência do acesso irrestrito à informação em detrimento da proteção de dados pessoais, tal como pretende o PL 3101/2021, ou vice-versa. Dessa forma, as medidas sugeridas pelo PL 4178/2019 e pelo PL 251/2022, com seus devidos ajustes[27], mostram-se mais adequadas ao impor a análise casuística dos pedidos de acesso à informação, mitigando a ocorrência de negativas carentes de adequada fundamentação que culminem na violação de direitos fundamentais.

Além disso, outras medidas podem ser adotadas pela administração pública, independentemente de alterações legislativas, para aprimorar o sistema. É o caso da mobilização da CGU e da ANPD na busca por um equilíbrio entre a LGPD e a LAI, fornecendo diretrizes para a consecução do acesso à informação sem comprometer a tutela dos dados pessoais – tal como se pretende a partir do Acordo de Cooperação Técnica já mencionado. Nesse âmbito, destacam-se o Parecer da CGU a respeito da revisão de atos que impuseram indevidamente o sigilo sobre documentos públicos (CGU, 2023) e a recente iniciativa da ANPD de publicação da Nota Técnica nº 22/2024, em junho de 2024, consolidando orientações aos servidores acerca da publicização de documentos com fulcro na LAI a partir de parâmetros de transparência informacional (ANPD, 2024).

27 No caso do PL 4178/2019, foi apresentada uma proposta de procedimento dotada de maior robustez, prevendo, em seu art. 9º, a aplicação do teste de danos por meio de Unidades de Transparência e Acesso à Informação, entidades colegiadas vinculadas ao Instituto Nacional de Acesso à Informação. Essas Unidades terão "um número ímpar de servidores públicos ou de pessoal que o órgão ou entidade determinar, incluindo o responsável pela área de controle interno do órgão ou entidade". Nesse ponto, há uma preocupação, por exemplo, quanto à composição dessas entidades, sendo necessária a vedação a cargos comissionados ou com gratificação de confiança, como forma de impedir a ingerência política sobre tais decisões (Rodrigues et al., 2023, p. 10). Assim, os debates públicos são essenciais para o seu aperfeiçoamento técnico.

Ademais, sempre que possível e compatível com a finalidade de responsabilização e prestação de contas da administração pública, os dados pessoais devem ser anonimizados, processo que consiste na "retirada do vínculo da informação com a pessoa a qual se refere" (Doneda, 2021). Não há um método ou uma combinação de métodos passível de ser definida *ex ante* como parâmetro aplicável a todos os processos de anonimização, sendo necessária a análise contextual diante das características de cada dado e do conjunto de informações em que ele está inserido (Bioni, 2021, p. 63).

É reconhecida a falibilidade do processo de anonimização especialmente em razão do efeito mosaico, segundo o qual há dados que, isoladamente, são considerados como irrelevantes, mas, em conexão com outros, podem desnudar a personalidade de um indivíduo (Conessa, 1984, p. 44-45)[28]. De todo modo, a partir do critério da razoabilidade, há uma exclusão da dicotomia mutuamente excludente entre dados pessoais e dados anonimizados, compreendendo-se que não configuram dados pessoais aqueles obtidos mediante um procedimento de reversão com o empreendimento de esforços razoáveis (Bioni, 2021, p. 66)[29].

Outra ferramenta adequada é a aplicação de tarja sobre informações pessoais contidas em documentos públicos[30] a fim de evi-

28 No original: *"Existen datos a priori irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad del ciudadano, al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significados."*

29 O art. 12, § 1º, da LGPD, traz parâmetros para a definição do conceito de "esforços razoáveis" diante do caso concreto: "A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios". De forma similar, no âmbito do GDPR europeu, é disposto em seu Considerando 26 que "para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica".

30 Recentemente, a CGU anunciou a implementação de um software de inteligência artificial em seus sistemas com a finalidade de tarjar automaticamente dados pessoais em documentos públicos objeto de solicitações de acesso à informação ou demandas de ouvidoria (CGU implementa..., 2024).

tar as negativas de acesso – em consonância com o art. 7º, § 2º, da LAI, que assegura "o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo". A partir da ocultação, é assegurada a conformidade tanto com a LAI como com a LGPD, uma vez que os documentos podem ser publicizados ao mesmo tempo em que são garantidos os direitos dos titulares à proteção de dados.

Portanto, além de reformas legais, a administração pública pode adotar medidas práticas para equilibrar o acesso à informação e a proteção de dados. A colaboração entre CGU e ANPD, como demonstrado em pareceres e orientações técnicas, é fundamental para orientar a transparência sem comprometer a privacidade, e a anonimização e a aplicação de tarjas nos dados em documentos públicos são estratégias eficazes que permitem a divulgação de informações, respeitando-se tanto a LAI quanto a LGPD.

Conclusão

A dicotomia entre a transparência e o sigilo envolve a ponderação entre dois direitos fundamentais que são imprescindíveis para o funcionamento do Estado Democrático de Direito: ao passo que o acesso à informação possibilita aos indivíduos o controle dos atores públicos; a proteção dos dados pessoais e da privacidade lhes assegura o desenvolvimento de suas potencialidades e a liberdade de autodeterminação. Nesse ponto, a LAI e a LGPD, apesar de tutelarem bens jurídicos diversos e aparentemente contraditórios, são compatíveis entre si.

Inicialmente, conclui-se ser necessária a observância do princípio da proporcionalidade no sopesamento entre o acesso à informação e a proteção de dados casuisticamente, conforme preceitua Alexy. Assim, devem ser publicizados apenas os dados pessoais indispensáveis para o atendimento da finalidade pública, desde que, na atividade interpretativa, constate-se que tal divulgação não sacrifica de sobremaneira a tutela dos dados pessoais dos titulares.

Ainda, sugere-se a realização de alterações na legislação com o objetivo de estabelecer critérios claros de interpretação das limitações ao acesso à informação fundadas na proteção de dados

pessoais, além de criar uma autoridade federal especializada na promoção da transparência, para atuar em conjunto com a ANPD no desenvolvimento de soluções de harmonização desses direitos.

Ademais, sempre que possível, é recomendada a condução de procedimentos de anonimização de dados, que poderão ser veiculados e acessados livremente, e da aplicação de tarjas nos dados pessoais em documentos públicos, a fim de permitir a sua publicização sem comprometer a privacidade e a intimidade dos titulares de dados pessoais.

Referências

ACKERMAN, John; SANDOVAL-BALLESTEROS, Irma. The global explosion of freedom of information laws. **Administrative Law Review**, vol. 58, n. 1, 2006.

ANPD – Autoridade Nacional de Proteção de Dados. **Guia orientativo**: tratamento de dados pessoais pelo poder público. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 2 jul. 2024.

ANPD – Autoridade Nacional de Proteção de Dados. **Nota Técnica nº 22/2024/FIS/CGF/ANPD**. Brasília: ANPD, 2024. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_0125695_nota_tecnica_22.pdf>. Acesso em: 20 jun. 2024.

ANPD e CGU estreitam relações para aplicação da LGPD e da LAI. Brasília: GOV.BR, 2020. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cgu-estreitam-relacoes-para-aplicacao-da-lgpd-e-da-lai>. Acesso em: 25 jul. 2024.

ARTICLE 19. **Identidade revelada**: entraves na busca por informação pública no Brasil. São Paulo: Article 19, 2018. Disponível em: <https://artigo19.org/wp-content/blogs.dir/24/files/2018/05/Identidade-Revelada-entraves-na-busca-por-informação-pública-no-Brasil.pdf>. Acesso em: 15 ago. 2024.

ARTICLE 19. **The public's right to know**: principles on freedom of information legislation. Londres: Article 19, 1999. Disponível em: <https://www.access-info.org/wp-content/uploads/Article_19_principles_on_the_public_right_to_know.pdf>. Acesso em: 25 jul. 2024.

BANISAR, David. The Right to Information and Privacy: Balancing Rights and Managing Conflicts. **World Bank Institute Governance Working Paper**,

2011. Disponível em: <https://dx.doi.org/10.2139/ssrn.1786473>. Acesso em: 10 jul. 2024.

BENTO, Leonardo Valles. Critérios de ponderação entre o direito de acesso a informações públicas e o direito à proteção de dados pessoais: lições a partir do modelo espanhol. **Revista da CGU**, v. 12, n. 22, p. 184-195, jul.-dez. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BOBBIO, Norberto. **O futuro da democracia:** uma defesa das regras do jogo. Trad. Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1986.

CACHAPUZ, Maria Cláudia. Informação e transparência: o acesso e a proteção de dados nominativos. **Revista Jurídica Luso-Brasileira**, a. 5, n. 1, p. 1557-1580, 2019.

CANHADAS, Fernando Augusto Martins. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e administração pública**. São Paulo: Revista dos Tribunais, 2020.

CGU implementa software para tarjar dados pessoais no sistema Fala.BR. Brasília: **CGU**, 2024. Disponível em: <https://www.gov.br/acessoainformacao/pt-br/noticias-1/cgu-implementa-software-para-tarjar-dados-pessoais-no-sistema-fala.br>. Acesso em: 17 ago. 2024.

CGU – Controladoria-Geral da União. **Painel Lei de Acesso à Informação**. Brasília: CGU, 2024. Disponível em: <https://centralpaineis.cgu.gov.br/visualizar/lai>. Acesso em: 13 ago. 2024.

CGU – Controladoria-Geral da União. **Acordo de Cooperação Técnica s/n, de 17 de maio de 2023**. Brasília: CGU, 2023a. Disponível em: <https://repositorio.cgu.gov.br/handle/1/77100>. Acesso em: 5 ago. 2024.

CGU – Controladoria-Geral da União. **Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1º de janeiro de 2023**. Brasília: CGU, 2023b. Disponível em: <https://www.gov.br/acessoainformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/copy_of_parecerfinalsobreacessoinformao_cgu_fev2023.pdf>. Acesso em: 3 ago. 2024.

CGU – Controladoria-Geral da União. **Parecer n. 00001/2021/CONJUR-CGU/CGU/AGU**. Brasília: CGU, 2021. Disponível em: <https://repositorio.cgu.gov.br/bitstream/1/67796/3/Parecer_001_2021_CONJUR_CGU_CGU_AGU.pdf>. Acesso em: 1 ago. 2024.

CONESA, Fulgencio Madrid. **Derecho a la intimidad, informática y Estado de Derecho**. Valencia: Universidad de Valencia, 1984

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul.-dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 2021. E-book não paginado.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A administração pública entre transparência e proteção de dados. **Revista de Direito do Consumidor**, vol. 135, p. 179-201, maio-jun. 2021.

GOV.BR. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). Brasília: GOV.BR, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf>. Acesso em: 2 ago. 2024.

GUERRERO, Manuel Medina. El conflicto entre la transparencia y la protección de datos tras la entrada en vigor del Reglamento General de Protección de Datos. **Revista Española de la Transparencia**, n. 17, p. 51-73, 2023.

IMPACTOS da LGPD nos pedidos de LAI ao governo federal. São Paulo: Fiquem Sabendo, 2024. Disponível em: <https://fiquemsabendo.com.br/transparencia/relatorio-lgpd>. Acesso em: 15 jul. 2024.

NAIB, Sudhir. **The Right to Information Act 2005:** a handbook. Oxford: Oxford, 2012.

RODOTÀ, Stefano. Democracia y protección de datos. **Cuadernos de Derecho Público**, n. 19-20, maio-dez. 2003.

RODRIGUES, Gustavo Ramos; ROMAN, Juliana; VIEIRA, Victor Barbieri Rodrigues; PEREIRA, Wilson Guilherme Dias. **Nota técnica - LGPD e LAI:** uma análise de propostas legislativas. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), 2023. Disponível em: <https://irisbh.com.br/wp-content/uploads/2023/05/Nota-tecnica-LGPD-e-LAI-Uma-analise-de-propostas-legislativas-IRIS.pdf>. Acesso em: 22 jun. 2024.

RODRIGUES, Karina Furtado; MICHENER, Robert Gregory. A necessidade de identificação como barreira ao acesso à informação: evidências e barreiras práticas no Brasil e no mundo. **Administração Pública e Gestão Social**, Viçosa, vol. 10, n. 4, p. 304-315, out.-dez. 2018.

ROESSLER, Beate. Should personal data be a tradable good? On the moral limits of markets in privacy. In: ROESSLER, Beate; MOKROSINSKA, Dorota (eds.). **Social Dimensions of Privacy:** Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2015.

RTI. **Global Right to Information Rating**, 2024. Country data by country. Disponível em: <https://www.rti-rating.org/country-data/>. Acesso em 12 jul. 2024.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. Direito à informação e direito de acesso à informação como direitos fundamentais na Constituição Brasileira. **Revista da AGU**, Brasília, a. XIII, n. 42, out.-dez. 2014.

THE world's most valuable resource is no longer oil, but data. Nova Iorque: The Economist, 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 jul. 2024.

VALIM, Rafael. O direito fundamental de acesso à informação pública. *In*: VALIM, Rafael; MALHEIROS, Antonio Carlos; BACARIÇA, Josephina (coord.). **Acesso à informação pública**. Belo Horizonte: Editora Fórum, 2015.

VIOLA, Mario; DONEDA, Danilo. Proteção de dados pessoais como limite ao acesso à informação e seu tratamento posterior. *In:* SARLET, Ingo Wolfgang; MARTOS, José Antonio Montilla; RUARO, Regina Linden (coord.). **Acesso à informação como direito fundamental e dever estatal**. Porto Alegre: Livraria do Advogado, 2016.

www.gov.br/anpd

ANPD

Autoridade
Nacional de
Proteção de Dados