



1º PRÊMIO
DANILO
DONEDA
DE MONOGRAFIAS

Monografias
vencedoras



ANPD

I Concurso de Monografias da ANPD

— *Prêmio Danilo Doneda* —



Monografias vencedoras

Supervisão Editorial
Lucas Costa Dos Anjos

ANPD
Brasília, DF
2023

Autoridade Nacional de Proteção de Dados

Diretor-Presidente

Waldemar Gonçalves Ortunho Junior

Diretores

- | Arthur Pereira Sabbat
- | Joacil Basilio Rael
- | Miriam Wimmer
- | Nairane Farias Rabelo Leitão

Comissão Julgadora

- | Diego Carvalho Machado
- | Joacil Basilio Rael
- | Katia Adriana Cardoso De Oliveira Lima
- | Lucas Costa Dos Anjos
- | Lucas Borges De Carvalho
- | Miriam Wimmer

Comissão Organizadora e Equipe de Apoio

- | Albert Franca Josua Costa
- | André Scofano Maia Porto
- | Fernanda Silva De Magalhães
- | Marcelo Santiago Guedes
- | Maria Luiza Duarte Sá

Revisão e Organização Textual

- | Diego Carvalho Machado
- | Maria Luiza Duarte Sá

Projeto Gráfico, Editoração Eletrônica e Capa

- | André Scofano Maia Porto

1ª edição

Publicação digital – PDF (2023)

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.anpd.gov.br



Sumário

| 05 |

Apresentação da obra

| 08 |

Apresentação dos três autores

Monografias classificadas

| 10 |

1º Inteligência artificial no contexto da proteção de dados: garantindo-se a transparência com o titular

| 53 |

2º O tratamento irregular de dados pessoais e a possibilidade de reconhecimento de um dano extrapatrimonial presumido

| 81 |

3º O tratamento de dados pessoais de crianças e adolescentes: análise das bases legais juridicamente válidas

Apresentação da obra

É com grande prazer que apresentamos este livro, uma coletânea das três monografias premiadas no I Concurso de Monografias da Autoridade Nacional de Proteção de Dados (ANPD), “Prêmio Danilo Doneda”. Esta obra representa o resultado de uma iniciativa que visa a impulsionar a produção científica de alta qualidade em instituições de ensino superior do Brasil, além de oferecer valiosas contribuições para a agenda regulatória da ANPD. A realização do Prêmio Danilo Doneda não apenas destaca o talento acadêmico emergente em nosso país, mas também representa a consecução dos mandatos legais da ANPD: promover a conscientização do público em geral sobre normas e políticas públicas de privacidade e proteção de dados pessoais, além de fomentar estudos sobre práticas nacionais e internacionais neste campo.

O nome do prêmio é uma homenagem póstuma ao Prof. Danilo César Maganhoto Doneda, uma das maiores referências na área de privacidade e proteção de dados pessoais na história do Brasil. Sua influência notória, acadêmica e política, contribuiu para o avanço e a consolidação da proteção de dados pessoais como objeto de estudo, políticas públicas e debates jurídicos e legislativos, especialmente em nosso país. Em todos os momentos mais relevantes da história da Lei n. 13.709/2018, a Lei Geral de Proteção de Dados, Danilo Doneda esteve, de algum modo, presente e participativo: desde a elaboração do Anteprojeto de Lei na Secretaria Nacional do Consumidor e na consulta pública de 2015, e, a partir de 2016, durante os processos legislativos que culminaram na aprovação da Lei Geral de Proteção de Dados e na instituição da ANPD, a “autoidade de garantia” – em terminologia por ele muito apreciada e difundida – do direito fundamental à proteção de dados pessoais no sistema brasileiro.

Não foi apenas essa, aliás, a situação em que esta Autoridade e o homenageado se entrecruzaram: Danilo Doneda integrou a estrutura organizacional da ANPD como membro do Conselho Nacional da Proteção de Dados e da Privacidade, indicado pela Câmara dos Deputados. Ao honrar a memória do Prof. Danilo Doneda, a ANPD

busca não apenas reconhecer suas inestimáveis contribuições à proteção de dados, mas também inspirar uma nova geração de estudiosos. Doneda era um defensor apaixonado da pesquisa rigorosa e do pensamento crítico e, com este prêmio, incentivamos os jovens pesquisadores a prosseguir com esta importante tradição.

As monografias apresentadas neste livro representam o futuro da proteção de dados pessoais no Brasil. Em sua maneira, elas refletem a diversidade e a singularidade do pensamento acadêmico emergente neste campo e apontam para novas direções para a regulamentação e a prática da proteção de dados. Ao compartilhar essas pesquisas com um público mais amplo, buscamos aumentar a conscientização e o entendimento sobre esta área crucial e em constante evolução. A ANPD está comprometida com o fortalecimento da cultura de proteção de dados no Brasil. Por meio de iniciativas como o Prêmio Danilo Doneda e a publicação deste livro, nós nos esforçamos para promover o debate, incentivar a produção de pesquisa de qualidade e ajudar a formar a próxima geração de estudiosos do campo da proteção de dados.

A monografia que alçou a primeira colocação explora os desafios gerados pela evolução dos sistemas de inteligência artificial, com ênfase particular na privacidade e proteção de dados. O trabalho aborda o complexo desafio enfrentado pelas organizações que desenvolvem e operam esses sistemas, principalmente em relação à obrigação de transparência para com os titulares de dados. Além disso, o trabalho busca esclarecer questões como o significado de “ser transparente” no contexto da proteção de dados e inteligência artificial, as informações que devem ser prestadas e os momentos adequados para sua divulgação. A monografia buscou fornecer orientações para agentes de tratamento, sugerindo práticas que podem auxiliá-los a cumprir suas obrigações de transparência desde o desenvolvimento até a utilização desses sistemas de inteligência artificial.

Já a segunda colocação consiste em uma monografia que aborda os desafios apresentados pela Lei Geral de Proteção de Dados em relação à definição dos critérios para a caracterização de danos extrapatrimoniais resultantes do tratamento irregular de dados. A pesquisa questiona especialmente os critérios causais para tal ca-

racterização, incluindo a possibilidade de presunção do dano. Com a utilização de um método exploratório, foram analisados textos legais, produções doutrinárias e decisões jurisprudenciais. Ao fim, a monografia apresenta reflexões sobre a impossibilidade de se reconhecer um dano extrapatrimonial presumido resultante de todo tratamento irregular de dados pessoais.

O trabalho classificado em terceiro lugar analisa, sob uma perspectiva doutrinária, jurisprudencial e internacional, as três hipóteses legais para o tratamento de dados pessoais de crianças e adolescentes, conforme proposto pelo Estudo Preliminar da ANPD e regulado pela Lei nº 13.709/2018. As hipóteses incluem o consentimento dos pais ou responsável legal, a aplicação exclusiva das hipóteses legais para dados sensíveis, e a aplicação das hipóteses legais, desde que observado o princípio do melhor interesse. A monografia também explora o princípio do melhor interesse, o paradigma do consentimento e o legítimo interesse.

É imprescindível ainda ressaltar que, embora a Autoridade Nacional de Proteção de Dados publique estes trabalhos como resultado do I Concurso de Monografias desta instituição, a ANPD não se responsabiliza pelo conteúdo das monografias publicadas. Os pontos de vista e opiniões expressos nestes trabalhos são exclusivamente de seus autores e não refletem ou representam, necessariamente, as posições institucionais da ANPD sobre os temas abordados.

Convidamos todos a lerem este livro, aprenderem com as perspectivas únicas de suas autoras e autores, bem como se juntarem a nós na promoção de uma cultura de proteção de dados forte e vibrante no Brasil, em honra ao legado do Prof. Danilo Doneda. Acreditamos que a proteção de dados pessoais é um direito fundamental e um pilar essencial para a construção de uma sociedade justa e equitativa, e estamos animados em compartilhar as contribuições desses jovens estudiosos para essa causa crucial.

Waldemar Gonçalves Ortunho Júnior

Diretor-Presidente da ANPD

Miriam Wimmer

Diretora da ANPD e Presidente da Comissão Julgadora

Apresentação dos três autores



1º lugar Jean Michel Duarte Santana

Graduando em Segurança da Informação pela UNIFACS e cursando o mestrado profissional em Propriedade Intelectual e Transferência de Tecnologia para Inovação (“PROFNIT”). Jean é graduado em Direito pela Universidade Federal da Bahia (UFBA), licenciado, por intermédio do programa de dupla titulação, em Direito pela Universidade de Coimbra, e pós-graduado em Advocacia no Direito Digital e Proteção de Dados pela Universidade São Judas Tadeus/EBRADI.



2º lugar Evelyn Pinto Pereira

Graduanda em Ciências Jurídicas e Sociais (Direito) pela Universidade Federal do Rio Grande do Sul. Pesquisadora de Proteção de Dados e Monitora de Parte Geral do Direito Civil, ambos sob a orientação do Prof. Dr. Bruno Miragem. Discente Líder da Equipe da IES UFRGS qualificada para a final da X Olimpíada de Conhecimento Jurídico realizada pela Academia Brasileira de Direito Civil. Foi estagiária do Des. Vicente Barroco de Vasconcellos no TJRS, recebendo Voto de Louvor pelo trabalho prestado. Atualmente, integra a equipe de Resolução de Conflitos do escritório Souto Correa Advogados.



3º lugar Júlia Teixeira de Barros Francatto

Estudante do 4º semestre de Direito na Pontifícia Universidade Católica de São Paulo (PUC-SP). Estagiária na área de Tecnologia e Proteção de Dados do escritório Pinheiro Neto Advogados. Já participou como researcher da equipe da PUC-SP na JESSUP Moot Court Competition e atualmente está envolvida, pelo grupo do escritório Pinheiro Neto Advogados, na 3ª Edição no CSD-ABPI Moot. Até o presente momento também está realizando o curso de Data Privacy and Technology, oferecido pela Harvard University.



Monografias classificadas



1º lugar

Inteligência artificial no contexto da proteção de dados: garantindo-se a transparência com o titular

Jean Michel Duarte Santana ✍

Resumo

Tão grande quanto os potenciais benefícios a sociedade decorrentes da evolução dos sistemas de inteligência artificial, são os desafios gerados por estes sistemas, sobretudo na seara da privacidade e proteção de dados. Dentre estes desafios, talvez o de maior complexidade para as organizações desenvolvem, treinam, operacionalizam e empregam esses sistemas seja o de atender às suas obrigações de transparência para com os titulares de dados, dado que, além de muitas vezes esses sistemas não serem criados para serem transparentes, dúvidas podem surgir quanto ao adequado conteúdo das obrigações de transparência no contexto desses sistemas, por exemplo, (i) o significado de “ser transparente” no contexto da proteção de dados e inteligência artificial; (ii) as informações que, em concreto, devem ser prestadas; (iii) os momentos em que as informações devem ser fornecidas. Tomando isso em consideração, o presente trabalho buscará orientar os agentes de tratamento sobre práticas que podem lhe auxiliar a melhor adimplir suas obrigações de transparência, desde o desenvolvimento à utilização desses sistemas.

Introdução

Sistemas de inteligência artificial vêm apresentando um rápido desenvolvimento nas últimas décadas, tanto em relação a sua capacidade, quanto a amplitude de sua aplicação e seus efeitos práticos no dia a dia de indivíduos. Se, por um lado, essa evolução traz grande potencial de desenvolvimento socioeconômico, por outro é fonte de uma série de desafios, sobretudo na seara de privacidade e proteção de dados, às organizações que desenvolvem, treinam, operacionalizam e empregam esses sistemas.

Dentre os maiores desafios no contexto da relação entre sistemas de inteligência artificial e privacidade e proteção de dados, destaca-se garantir a adequada transparência e explicabilidade desses sistemas. Isso porque, além destes muitas vezes não serem criados para serem transparentes, dúvidas podem surgir quanto ao adequado adimplemento das obrigações relacionadas a transparência e explicabilidade, por exemplo, (i) qual o significado de “ser transparente” no contexto da proteção de dados e inteligência artificial? (ii) quais informações devem ser prestadas? (iii) em quais momentos essas informações devem ser prestadas?

O presente trabalho buscará responder estes questionamentos, visando orientar os agentes de tratamento sobre práticas que podem lhe auxiliar a melhor adimplir suas obrigações de transparência, desde o desenvolvimento à utilização desses sistemas.

Inteligência artificial

Antes de prosseguir com o presente trabalho é necessário delinear o seu objeto, isto é, o que se busca referir quando do emprego do termo “Inteligência Artificial” (“I.A.”).

Nesse sentido, com base no guia sobre inteligência artificial e proteção de dados (“*Guidance on AI and data protection*”) da autoridade de proteção de dados do Reino Unido (“*Information Commissioner’s Office*” ou “ICO”), se pode entender “I.A.” como um termo guarda-chuva, empregado pela indústria para abranger uma gama de tecnologias, as quais são capazes de (i) aprender com base em experiência e imitar comportamentos humanos; e/ou (ii) são capazes de perfor-

mar tarefas que normalmente requeiram inteligência humana¹. De modo similar, Teixeira e Cheliga (2020) descrevem inteligência artificial como um “sistema computacional criado para simular racionalmente as tomadas de decisão dos seres humanos, tentando traduzir em algoritmos o funcionamento do cérebro humano”².

Com base nos conceitos apresentados, podemos conceituar sistemas de inteligência artificial, a princípio, como agentes artificiais capazes de, em um certo grau, simular a inteligência humana, apresentando soluções para problemas (ou tarefas) que comumente dependeriam de uma inteligência humana.

No entanto, o grau de “capacidade” a qual nos referirmos quando abordamos sistemas de inteligência artificial pode gerar uma série de discussões e impactos, jurídicos e práticos, pelo que merece ser adequadamente delineado. Nesse sentido, conforme bem pontua Costa Neto, a I.A. pode, grosso modo, ser dividida em duas classificações (i) a inteligência artificial geral (*Artificial General Intelligence*), ou “inteligência artificial forte”, categoria ainda não existente, mas que remete ao imaginário do senso comum quando se fala em I.A.: seriam os sistemas dotados de capacidade de replicar com perfeição o cérebro humano “ponderando sentimentos, percepções e experiências subjetivas com raciocínio lógico”, bem como “atingir uma quantidade ilimitada de objetivos pré-determinados” e mesmo “definir novos objetivos em situações incertas ou imprecisas”; (ii) inteligência artificial estreita (*narrow artificial intelligence*), ou inteligência artificial fraca, que são os sistemas atualmente empregados, capazes de executar tarefas específicas, pré-determinadas e “precisamente definidas”, empregando “forma ou técnica entendida como inteligente”³.

1 INFORMATION COMMISSIONER'S OFFICE. **Guidance on AI and data protection**. Wilmslow: ICO, 2023. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/>. Acesso em: 03 abr.2023

2 TEIXEIRA, Tarcísio; CHELIGA, Vinicius. **Inteligência Artificial: aspectos jurídicos**. 2. ed. Salvador: Ed. JusPODIVM, 2020. p. 16–17.

3 COSTA NETO, Geraldo Romeiro. **Criações de Inteligência Artificial**: reflexos no direito de patentes. Rio de Janeiro: Lumen Juris, 2021. p. 24–27

O objeto deste trabalho será a análise da aplicação do princípio da transparência previsto na Lei Geral de Proteção de Dados aos sistemas de inteligência artificial fraca, razão pela qual sempre que utilizado o termo I.A. ou outro com similar conotação, deverá ser entendido por “*narrow artificial intelligence*”.

O princípio da transparência no contexto da inteligência artificial

O princípio da transparência encontra previsão no art. 6º, VI, da Lei Geral de Proteção de Dados (LGPD), traduzindo-se como uma garantia aos titulares de obter, e, conseqüentemente, um dever dos agentes de tratamento em fornecer, “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”⁴. Consubstancia-se, conforme bem pontua Basan, em meio pelo qual se proporciona ao titular “identificar, de maneira cristalina, a legalidade, a legitimidade e a segurança do tratamento de dados pessoais”⁵, de modo que ele possa compreender os processos ao qual encontra-se sujeito e, entendendo adequado, exercer seus direitos.

Para uma adequada interpretação do princípio supramencionado no contexto do uso de inteligência artificial, entretanto, não se deve limitar ao texto legal da LGPD, sendo necessário, ainda, levar em consideração o princípio da “transparência e explicabilidade” constante no *framework* principiológico de regulação da inteligência artificial elaborado pela OCDE (*OECD AI Principles*), sobretudo considerando a sua aderência pelo Estado Brasileiro em 21 de maio de 2019 ao texto oficial aprovado (*Recommendation of the Council on Artificial Intelligence*)⁶.

4 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

5 BASAN, Arthur Pinheiro. Art. 6. In: MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. Indiatuba: Foco, 2022. p. 53-66.

6 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Re-**

Citado *framework* convoca os atores do ecossistema de inteligência artificial a adotarem medidas de modo a, em atenção ao contexto em que se encontram e ao estado da arte, fornece informação suficientemente adequada a (i) permitir que o público melhor entenda sistemas de inteligência artificial; (ii) conscientizar as partes interessadas que estas estão a interagir com sistemas de inteligência artificial; (iii) permitir que aqueles afetados pelo sistema entendam seus resultados – isto é, a decisão, recomendação, previsão ou outro *output* gerado pelo sistema; (iv) permitir que aqueles adversamente afetados pelo sistema possam, se entenderem adequado, impugnar seus resultados.

Mas como esses dois textos se relacionam? Conforme se vi-sualizará mais adiante, o princípio da transparência, na Lei Geral de Proteção de Dados, encontra suas principais materializações em dois dispositivos, os art. 9 e 20º, §1º. Analisemos cada um destes dispositivos e suas interações com o *framework* da OCDE.

O primeiro deste dispositivo, o art. 9º, delimita o dever do agente de tratamento de fornecer informações sobre o tratamento ao qual o titular encontrar-se-á sujeito de forma proativa, disponibilizando-as de “*forma clara, adequada e ostensiva*”, e firma o conteúdo mínimo das informações a serem prestadas ao titular, a saber: (a) finalidade específica do tratamento; (b) forma e duração do tratamento, observados os segredos comercial e industrial; (c) identificação do controlador; (d) informações de contato do controlador; (e) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (f) responsabilidades dos agentes que realizarão o tratamento; (g) se o tratamento é condição para o fornecimento de produto ou de serviço ou para o exercício de direito⁷.

Por sua vez, o princípio da “transparência e explicabilidade” impõe aos atores de inteligência artificial (que, considerando o objeto deste trabalho, serão, via de regra, agentes de tratamento) a obri-

commendation of the Council on Artificial Intelligence, Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr.2023

7 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

gação de fornecer, de forma proativa, no mínimo, informações que permitam que o titular (a) compreenda, em linhas gerais, o que é uma inteligência artificial; (b) encontre-se ciente que interagirá com um sistema de inteligência artificial⁸. Cabe, contudo, questionar: seria o fornecimento dessas informações previstas no *framework* da OCDE, uma obrigação nova, em relação ao texto legal da LGPD? Entende-se que não, tratando-se, como será ulteriormente apresentado, de mera especificação do teor, em concreto, de algumas das informações requeridas pelo retrocitado art. 9º, mais especificamente, a “forma do tratamento”.

Por sua vez, o art. 20, §1º, positiva o direito do titular de dados de exigir uma explicação de decisões automatizados, isto é, de obter, observados eventuais segredos comerciais e industriais, “informações claras e adequadas” a respeito dos processos de decisão automatizada a que se encontrem sujeitos⁹ – em outras palavras, é uma obrigação reativa do agente do tratamento, o qual, uma vez provocado, deverá fornecer informações sobre como um sistema de inteligência artificial alcançou um resultado em específico ao indivíduo afetado. Este direito aparenta ser perfeita materialização dos deveres dos atores de inteligência artificial de fornecer informações suficientes para que as partes afetadas por sistemas de inteligência artificial entendam seu resultado e, sendo o caso, possam questioná-lo¹⁰, com a LGPD, inclusive, prevendo o direito de realizar-se esse questionamento (direito de revisão), nos termos do *caput*, de seu art. 20¹¹.

8 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**, Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr.2023

9 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

10 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**, Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr.2023

11 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

Isto posto, temos que a tradução do princípio da transparência para cenários em que existe o emprego de sistemas de inteligência artificial denota duas posturas complementares por parte dos agentes de tratamento: uma postura ativa e outra reativa. Ativamente o agente de tratamento deve fornecer ostensivamente uma série de informações, dentre as quais o fato de o titular encontrar-se sujeito a uma I.A. e uma explicação a respeito do significado desta informação. Por sua vez, passivamente, isto é, mediante requisição do titular, a organização deve fornecer informações suficientes sobre um determinado resultado do sistema, que permita, ao titular, uma compreensão razoável de seu significado e como ele foi alcançado, de modo, inclusive, a ser apto a questioná-lo, se assim entender adequado.

Aplicação prática dos princípios da transparência aos sistemas de inteligência artificial

A adequada transparência para com o titular na prática revela-se um dos grandes desafios no desenvolvimento e emprego de sistemas de inteligência artificial, com dificuldades enfrentadas mesmo por organizações especialistas na temática, conforme se assevera da decisão da autoridade italiana de proteção de dados (*Garante per la Protezione dei Dati Personali* ou GPDP) em face da OpenAI L.L.C., organização responsável pelo desenvolvimento e gerenciamento do famoso sistema de inteligência artificial ChatGPT, na qual aplicou a sanção de limitação temporária do processamento de dados no território italiano pela retrocitada ferramenta, a qual foi motivada, dentre outros pontos, a (i) ausência de prestação de informações aos usuários e demais partes interessadas cujos dados são coletados e tratados pelo serviço do ChatGPT; (ii) ausência, em determinadas situações, de correspondência entre os resultados prestados pelo ChatGPT e a realidade¹².

12 GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. Provvedimento del 30 marzo 2023 [9870832]. Roma: GPDP, 2023. Disponível em: <https://www.garante->

Grande parte das dificuldades enfrentadas decorrem da ausência de clareza sobre (i) em quais situações informações devem ser prestadas ao titular afetado; (ii) quando citadas informações devem ser prestadas aos titulares; (iii) quais informações devem ser prestadas ao titular.

Em relação ao primeiro dos pontos que merecem esclarecimento, ao se estudar a aplicação dos princípios da transparência e do livre acesso nos sistemas de inteligência artificial, em geral, podem ser levadas em consideração, pelo menos, duas situações distintas, as quais demandam a prestação de informações pelo agente de tratamento ao titular (i) o uso de dados de indivíduos para o treinamento da I.A.; e (ii) o emprego do sistema de inteligência artificial no indivíduo, neste último caso merecendo ainda uma subdivisão em relação a (a) informação que deve ser prestada de forma prévia ao indivíduo, sobre o tratamento de dados, em abstrato, pelo sistema de inteligência artificial; e (b) informação que deve ser prestada em concreto, mediante solicitação do titular, para explicação de uma dada decisão. Analisemos, à luz dessas hipóteses em que a prestação de informações se faz necessária, os demais pontos levantados.

Transparência no treinamento de sistemas de inteligência artificial

Quando se faz uso dos dados para treinamento dos sistemas de inteligência artificial, um dos fatores de maior relevância para a adequada transparência para com o titular parece ser a forma com que o dado é coletado e o consequente momento de prestação da informação.

Nas situações em que o dado é coletado diretamente do indivíduo, seja em situação na qual este é coletado com a finalidade originária de realizar o treinamento do sistema (caso em que, a princípio, se demandaria o consentimento dos titulares afetados), seja quando o treinamento do sistema é um uso secundário para

privacy.it/home/docweb/-/docweb-display/docweb/9870832. Acesso em: 03 abr.2023

os dados coletados dos titulares em razão de uma relação previamente existente (em que se enxerga o emprego de outras bases legais, como, por exemplo, o legítimo interesse), deve-se informar ao titular sobre o uso de seus dados para o treinamento do modelo de forma prévia ao seu emprego para este fim e, sempre que possível, de forma prévia a coleta dos dados.

Subsistindo um relacionamento prévio com o titular, a prestação dessa informação deve ser razoavelmente simples, podendo, se operar tanto (i) no momento de coleta dos dados (quando já se conheça a possibilidade de seu uso para este fim) – caso em que a informação pode ser prestada, por exemplo, nos documentos utilizados para transparecer ao titular sobre as práticas de tratamento de dados da organização (ex. o termo de consentimento a ser fornecido pelo titular ou, mais comumente, o aviso/política de privacidade); (ii) em momento posterior, mas antecedente ao emprego dos dados no treinamento do sistema, quando a necessidade de utilização daqueles dados para o treinamento da I.A. surge de forma posterior ao início do relacionamento com o titular, caso em que a organização pode, a título de exemplo, modificar o aviso/política de privacidade, comunicando o titular desta alteração pelos meios de comunicação disponíveis (ex. notificando-o em tela quando este acessar a aplicação de *internet* ou encaminhando-lhe um e-mail).

Ocorre que muitas vezes os dados tratados para o treinamento de sistemas de inteligência artificial não são coletados diretamente dos titulares afetados, sendo coletados de terceiros fornecedores (os *Databrokers* ou, como mais comumente conhecidos em território nacional, “bureaus de dados”) ou mesmo extraídos (minerados) de ambientes publicamente acessíveis, neste último caso, usualmente com base nas hipóteses constantes no art. 7º, §§ 3º, 4º, 7º, da LGPD. Nessas hipóteses a recomendação apresentado pelo ICO, em seu supracitado guia, é que os titulares sejam comunicados em um período razoável, no mais tardar, dentro de um mês¹³.

Embora a legislação pátria não apresente uma obrigação ex-

13 INFORMATION COMMISSIONER'S OFFICE. **Guidance on AI and data protection.** Wilmslow: ICO, 2023. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/>. Acesso em: 03 abr.2023

pressa de comunicação ao titular quando da coleta de dados de terceiros, considerando que, (i) como bem pontua Faleiros Júnior, o princípio da transparência, ao demandar que o titular tenha acesso facilitado a informações, gera uma expectativa de ação proativa dos agentes de tratamento¹⁴; (ii) sem essa comunicação, em regra, dificilmente o titular terá conhecimento sobre o tratamento de seus dados; (iii) mesmo nas hipóteses de tratamento de dados publicamente disponíveis, a legislação não isenta o agente de tratamento de aderência aos princípios previstos na legislação, dentre os quais o dever de transparência (art. 7º, §7º, da LGPD)¹⁵, entende-se pela existência de um dever de notificar, pelo menos, nas hipóteses em que os meios razoavelmente disponíveis aos agentes de tratamento permitam a realização desta notificação, com a recomendação de prazo apresentada pelo ICO, minimamente, devendo ser vista como uma boa-prática à luz da LGPD.

Isto posto, idealmente, quando os dados são fornecidos por *Databrokers*, além de se executar a devida *due diligence* para verificar a licitude do fornecimento desses dados para fins de treinamento do sistema, é recomendável que o agente de tratamento avalie se as informações prestadas pela fonte dos dados ao titular são suficientes para garantir adequada transparência ao seu uso para o treinamento do modelo e, não o sendo, realizar a comunicação tão logo quanto possível, garantindo a transparência da operação de tratamento. De igual modo, quando os dados são obtidos a partir de sua coleta (“mineração”) de informações publicamente acessíveis, idealmente, o titular deve ser informado dessa operação.

Note-se que o uso do termo “idealmente” não é sem razão, uma vez que, por vezes, nas situações descritas acima, o agente de tratamento poderá não deter os meios necessários para a realização da comunicação e/ou a sua realização é compreendida, mediante

14 FALEIROS JÚNIOR, José Luiz de Moura. Art. 9. In: MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. Indiatuba: Foco, 2022. p. 110-114.

15 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

uma análise de razoabilidade, como desproporcional ou inviável – nessas hipóteses, sugere-se que os agentes de tratamento minimizem os impactos aos titulares, preferencialmente anonimizando ou pseudonimizando os dados a serem utilizados no treinamento do modelo (ex. convertendo-os em dados estatísticos ou eliminando identificadores da base tratada), de modo a evitar quaisquer impactos significativos ao titular em decorrência do processo de teste.

Transparência quanto ao emprego da inteligência artificial no indivíduo

Mais comumente o emprego de um sistema de inteligência artificial em um dado indivíduo (isto é, o uso de um sistema de inteligência artificial para a emissão de um resultado relacionado a um dado indivíduo – devendo-se entender “resultado relacionado a um indivíduo” em um sentido amplo, abarcando tanto decisões propriamente ditas, quanto análises probabilísticas, perfilização e outras situações do gênero) decorre de uma relação previamente existente entre o agente de tratamento e o indivíduo, pelo que, em regra, as informações sobre o sistema de tomada de decisão automatizado devem ser prestados nos documentos disponibilizados ao titular, de modo a garantir a transparência sobre o tratamento de seus dados. Mas quais informações devem ser prestadas? Como bem pontua Faleiros Júnior, o art. 9º, da LGPD positiva a “garantia de acesso facilitado do titular de dados a informações sobre atividades de tratamento que lhe digam respeito”¹⁶, sendo o marco legal que estabelece o conteúdo mínimo de informações a serem prestadas ao titular, seja, para os fins deste trabalho, em relação ao uso de seus dados para o treinamento de sistemas de inteligência artificial, seja no emprego propriamente dito desses sistemas para a tomada de decisões automatizadas. Analisar-se-á nas linhas abaixo cada um dos itens demandados pelo artigo, buscando-se, quando adequado, apresentar orientações sobre como

16 FALEIROS JÚNIOR, José Luiz de Moura. Art. 9. In: MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. Indiatuba: Foco, 2022. p. 110-114.

melhor fornecê-los em situações de emprego de sistemas de inteligência artificial.

a) Finalidade específica do tratamento (art. 9º, I)

O conteúdo do inciso aparenta ser autoexplicativo, devendo-se fornecer ao titular a(s) finalidade(s) para as quais o tratamento se destina, inclusive, para permitir que o titular realize o controle finalístico do uso de seus dados – isto é, (i) se os seus dados apenas estão sendo utilizados para a finalidade que lhe foi apresentada; (ii) se é razoável a utilização dos dados tratados pelo agente de tratamento na persecução da finalidade apresentada.

Cumpre, contudo, fazer algumas pequenas observações lastreadas na NBR ISO/IEC 29184/2021 (norma técnica sobre avisos de privacidade *online*) que, muito embora aplicáveis a qualquer operação de tratamento, ganha especial relevância ao se abordar a necessidade de transparecer operações de tratamento executadas por meio de sistemas de inteligência artificial: (i) a descrição utilizada deve permitir que o titular “entenda de forma clara e imediata o propósito” para o qual o seu dado será utilizado, – isto é, devem ser evitados o emprego de textos genéricos, sobretudo quando o contexto em que a informação é prestada não permite com que o titular compreenda quais categorias de dados serão tratadas para qual finalidade (ex. a organização presta uma gama de serviços e limita-se a pontuar que “utilizará os dados para prestação e aprimoramento dos serviços contratados”)¹⁷. Nesse sentido, aliás, a ANPD, em sede da Nota Técnica nº 49/2022/CGF/ANPD, entendeu que a apresentação de uma justificativa ampla para o uso de dados pela aplicação de internet Whatsapp (“operar, fornecer, melhorar, entender, personalizar, oferecer suporte e anunciar nossos Serviços”) era “dispersa e sem a especificação necessária” exigida pela legislação pátria; (ii) se a categoria de dados tratados variar em acordo com a finalidade perseguida, a organização deve fornecer essa informação

17 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.

ao titular, pontuando quais categorias de dados são utilizadas para cada finalidade¹⁸.

Isso é especialmente relevante em se tratando de transparência quanto ao tratamento de dados pessoais por sistemas de inteligência artificial, vez que permite que o titular faça uma análise prévia da razoabilidade da decisão a ser tomada, tanto em relação aos dados utilizados (ex. embora seja razoável que o *score* de crédito seja utilizado para uma decisão a respeito do meu limite de crédito pelo banco, talvez não seja razoável que uma universidade utilize este dado para avaliar se um candidato será aprovado para ingressar na mesma), quanto em relação ao *output* gerado (ex. se o titular conhece os principais fatores utilizados em uma tomada de decisão a respeito do limite de crédito concedido pelo banco, antes de apresentar qualquer questionamento a instituição financeira, ele pode realizar uma avaliação prévia, se o limite de crédito que lhe é fornecido é razoável).

Cumprir pontuar que isso não significa que o aviso de privacidade deva ser excessivamente extenso, sob pena de desincentivar a leitura do mesmo pelo titular, tornando-o inócuo. A organização pode (e é recomendável que o faça) adotar técnicas de redação que permita que o titular obtenha uma visão geral sobre com os seus dados serão utilizados, aprofundando esse entendimento conforme seu interesse – por exemplo, o agente de tratamento pode elaborar um aviso de privacidade em camadas, fornecendo informações mais gerais sobre o tratamento de dados em um dado produto/serviço/fim em um documento principal e disponibilizando um documento complementar que permita que eventuais titulares interessados obtenham informações mais específicas sobre o tratamento de seus dados em cada processo que compõe este produto/serviço/fim – inclusive, os processos de tomada de decisão automatizada porventura existentes.

18 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 49/2022/CGF/ANPD**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd-versao_publica.pdf. Acesso em: 04 abr.2023

b) Forma e duração do tratamento, observados os segredos comercial e industrial (art. 9º, II)

O inciso II, do art. 9º, apresenta, em verdade, dois requisitos informacionais a serem apresentados pelo agente de tratamento (i) a forma com que o tratamento se operará; (ii) o período em que os dados pessoais serão retidos, abordar-se-á um, depois o outro¹⁹.

Talvez um dos itens menos claros a respeito das informações que devem ser prestadas ao titular é a forma do tratamento, tendo em vista que muito embora a legislação assevere a necessidade do fornecimento desta informação, não descreve o que, exatamente, deve se entender por “forma do tratamento”.

Tendo em vista esta realidade, uma vez mais utilizar-se-á da NBR ISO/IEC 29184:2021 para buscar compreender o que deve se entender por “forma do tratamento”. A mencionada norma técnica apresenta a recomendação de inclusão de alguns itens que, a princípio, entende-se que podem compor a ideia de “forma do tratamento” (i) os elementos de dados pessoais que estão sendo coletados; (ii) o método de coleta de dados pessoais; (iii) o momento e localização da coleta de dados pessoais; (iv) o método de uso de dados pessoais; (v) a geolocalização e jurisdição legal dos dados pessoais utilizados²⁰.

Os comentários relevantes quanto ao primeiro deste item (elementos de dados pessoais que estão sendo coletados) foram descritos nos comentários sobre a apresentação da finalidade do tratamento. Passando-se para o segundo tópico (método de coleta de dados pessoais), o normativo apresenta quatro metodologias gerais de coleta de dados: (i) dados são coletados diretamente do titular (o próprio titular fornece os dados a serem utilizados); (ii) dados são coletados indiretamente (dados são coletados de fontes terceiras, como *Databrokers*, ou informações publicamente disponíveis); (iii) dados são observados pelo controlador (os dados usu-

19 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

20 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

almente são coletados a partir da observação de ações executadas pelo titular); (iv) dados são inferidos pelo controlador (a partir de um conjunto de características, ações ou outros dados a respeito do titular – é o caso, por exemplo, da perfilização, uma espécie de decisão automatizada)²¹. Essa informação guarda especial relevo quando nos referimos a tomada de decisão por sistemas de inteligência artificial, tendo em vista que quando a coleta de dados se opera por meios que não o próprio titular, poderão subsistir riscos relevantes relacionados a qualidade dos dados tratados, sobretudo sua acurácia, que impliquem em uma aplicação inadequada do modelo desenvolvido ao titular, gerando-se uma decisão inadequada e, muitas vezes, menos favorável, a qual pode ser objeto do exercício dos direitos de explicação e revisão previstos no art. 20, da LGPD – lançando mão do exemplo da concessão de crédito pela instituição financeira, se o titular sabe que dados a respeito de sua renda são coletados de um *Databroker*, ele pode entender pela possibilidade de que estes dados encontrem-se desatualizados (sobretudo se o titular sofreu um modificação recente em sua renda) e, conseqüentemente, a decisão sobre o crédito que lhe foi concedido pode ter sido menos favorável do que aquela que decorreria com sua remuneração real, por ter sido pautada em dados inexatos, o que gera o exercício dos supramencionados direitos para a correção da decisão inadequada.

Ademais, nos termos já vistos, dados gerados por práticas de inferências (ex. perfis ou predições a respeito do comportamento do titular), usualmente são obtidos por intermédio de sistemas de decisão automatizada, sobretudo inteligência artificial, pelo que informações sobre as inferências obtidas podem representar verdadeira explicação da finalidade do emprego desses sistemas.

Em relação ao momento e localização da coleta de dados pessoais, esta é uma informação cujo fornecimento é recomendável naquelas situações em que o dado não é coletado diretamente dos titulares, buscando-se, sobretudo, explicitar aos mesmos

21 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.

em que termos e condições a coleta de dados se opera, naquelas situações de não obviedade²² – imagine-se, por exemplo, que o titular ingressará em uma área privada de alta sensibilidade (ex. um prédio designado para guarnecer os servidores físicos de um grande provedor de serviços de armazenamento e processamento de dados em nuvem), na qual é empregado um sistema de videovigilância com identificação biométrica com o objetivo de identificar eventuais invasores. Nessa situação, placas alertando-o deste fato podem ser apresentadas nas entradas das instalações e o eventual aviso de privacidade pode esclarecer que a biometria facial do titular poderá ser captada pelo sistema de videovigilância pelo período em que ele estiver fisicamente presente nas instalações da controladora.

Já em relação ao quarto item (método de uso de dados pessoais), a NBR ISO/IEC 29184 destaca quatro métodos de uso do dado: (i) usados como estão (isto é, sem qualquer modificação. Por exemplo, utiliza-se o número de telefone do titular para contatá-lo); (ii) usados após a realização de algum tratamento (isto é, os dados são submetidos a um dado processo, como pseudonimização, após o qual serão utilizados para o alcance da finalidade declarada); (iii) combinados com outros dados (ou seja, acrescenta-se o dado obtido do titular com outras informações, para se atingir a finalidade pretendida); e, por fim, (iv) utilizando-se técnicas de tomada automatizada de decisão, que é o caso em análise²³.

Assim, este é o momento em que o agente de tratamento deve informar ao titular se este está sendo sujeito à decisão tomada por sistemas de inteligência artificial e, em caso positivo, em quais condições/processos (ex. se durante um processo de contratação de um crédito, o processo de análise do crédito é feito por um sistema de inteligência artificial, essa informação deverá ser fornecida ao titular) – sendo, esta informação, inclusive, um requisito para que o

22 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

23 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

titular possa exercer seus direitos relacionados à tomada de decisão automatizada, previstos no art. 20 da LGPD.

Aliás, nesse sentido, dentre os princípios propostos pela OCDE para o desenvolvimento de sistemas de inteligência artificial inovativos, confiáveis e aderentes aos direitos humanos, os quais foram aderidos pelo Brasil em maio de 2019, encontra-se o princípio de “transparência e explicabilidade”, cujo um dos requisitos mínimos, é, justamente, ser transparente sobre quando um sistema de inteligência artificial se encontra em uso²⁴.

Ainda com base na OCDE, tendo em vista que um dos objetivos que os atores de inteligência artificial devem atingir por meio do princípio da transparência é “aumentar o entendimento geral sobre sistemas de inteligência artificial”²⁵, recomenda-se que além de apresentar o fato de que o titular interagirá com uma I.A, uma breve explicação geral sobre esta espécie de tecnologia seja fornecida em conjunto com o fato dela ser empregada em um dado processo.

Ademais, a OCDE recomenda, ainda, que sejam prestadas informações que possibilitem que o público entenda como os sistemas são “desenvolvidos, treinados, operacionalizados e empregados”²⁶, de uma forma que seja suficientemente cognoscível pelo usuário médio. Para tanto, Chivot e Bhatia recomendam que sejam fornecidos aos titulares algumas informações sobre o funcionamento do sistema, por exemplo, (i) como as decisões são tomadas pelo sistema²⁷; (ii) quais são as suas capacidades e limitações; (iii) qual é o grau de acuracidade expectável para as finalidades determinadas; e (iv) em quais condições o sistema deve se encontrar para o seu adequado funcionamento. Os autores recomendam, ainda, que par-

24 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Transparency and explainability** (Principle 1.3). Paris: OCDE, 2019. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 05 abr.2023

25 Tradução livre de: “to foster a general understanding of AI systems”. Ibid.

26 Tradução livre de: “enabling people to understand how an AI system is developed, trained, operates, and deployed”. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Transparency and explainability** (Principle 1.3). Paris: OCDE, 2019. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 05 abr.2023

27 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.p. 113.

tes externas (como auditores e grupos de usuários) revisem as informações apresentadas, para que seja validada se as informações (i) fazem sentido para um usuário médio; (ii) são claras do ponto de vista legal²⁸.

Por sua vez, a informação sobre a geolocalização e jurisdição em que os dados serão tratados trata de fornecimento, ao titular de dados, da localização geográfica em que os dados pessoais serão tratados (isto é, se existe transferência internacional e, em caso positivo, para quais países), considerando-se, sobretudo que (i) diferentes Estados soberanos podem possuir diferentes níveis de proteção de dados pessoais e/ou intrusão na privacidade, pelo que o titular pode não se sentir confortável com a transferência de seus dados para determinados países, optando por não seguir com o relacionamento com o controlador; (ii) permitir que o titular avalie se a transferência internacional encontra-se fundamento adequado em uma das hipóteses do art. 33º da LGPD, as quais formam, conforme Frajhof e Kremer, um “rol exaustivo das circunstâncias possíveis”²⁹ em que a transferência internacional pode ocorrer. Ainda quanto a identificação da forma de tratamento, Chivot e Bhatia, recomendam que, em se tratando de sistemas de inteligência artificial, sejam fornecidos aos titulares algumas informações sobre o funcionamento do sistema, com o objetivo de garantir a transparência e a explicabilidade dos mesmo, por exemplo, (i) como as decisões são tomadas pelo sistema³⁰; (ii) quais são as suas capacidades e limitações; (iii) qual é o grau de acuracidade expectável para as finalidades determinadas; e (iv) em quais condições o sistema deve se encontrar para o seu adequado funcionamento. Os autores recomendam, ainda, que partes externas (como auditores e grupos de usuários) revisem as informações apresentadas, para que seja

28 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.p.122-123

29 FRAJHOF, Isabella Z; KREMER, Bianca. Art. 33. *In*: MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. Indiatuba: Foco, 2022. p. 341-347.

30 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.p. 113.

validada se as informações (i) fazem sentido para um usuário médio; (ii) são claras do ponto de vista legal³¹.

Por fim, em relação ao período de retenção dos dados, trata-se de informar ao titular o prazo (identificado ou identificável), em que os dados serão mantidos, em atenção aos requisitos legais dos arts. 15 e 16 da LGPD. Aqui, cumpre fazer algumas considerações: em primeiro lugar, o período de retenção descritos, conforme bem pontua a NBR ISO/IEC 29184:2021, podem se operar tanto na forma de uma data em específico, quanto na forma de um prazo contado de um termo inicial identificado, quanto pelos critérios por meio do qual pode-se chegar ao prazo de retenção³² – o relevante é que seja possível, ao titular, identificar com clareza por qual o tempo previsível em que os seus dados serão mantidos, conferindo-lhe a possibilidade de controlar se a organização procedeu a eliminação de suas informações dentro do prazo adequado. Assim, informações genéricas, que não permitam, sem o fornecimento de dados e informações complementares a identificação do prazo de armazenamento, devem ser evitados (ex. a organização não deve limitar-se a pontuar que “armazenará os dados pelo prazo em que perdurarem obrigações legais”, sem identificar quais os prazos dessas obrigações legais ou, pelo menos, quais são essas obrigações legais).

Em segundo lugar, deve-se ter em consideração que, a interpretação conjunta dos artigos supramencionados, leva a conclusão de que os dados devem ser retidos apenas até o esgotamento da finalidade para o qual foram coletados, após o qual devem ser eliminados, ressalvadas algumas situações excepcionais (ex. a existência de obrigação legal de sua manutenção, nos termos do art. 16, I, da LGPD³³).

31 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020. P. 122-123

32 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

33 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

Ocorre que a legislação não veda, que dados sejam tratados para mais de uma finalidade, e, no contexto do sistema de inteligência artificial, via de regra, os dados utilizados para que um sistema gere um *output*, também são utilizados para o treinamento do sistema, inclusive por meio do fornecimento de uma devolutiva ao sistema sobre o resultado prático de seu *output*. Nessas hipóteses, a organização deverá se atentar aos prazos necessários ao atingimento de todas as finalidades lícitamente perseguidas e, em atenção a NBR ISO 29184:2021, sempre que possível, fornecer os prazos de retenção individualizados por finalidade³⁴.

Em se tratando especificamente de limitação do armazenamento de dados utilizados no treinamento de sistemas de inteligência artificial, uma complexidade a mais encontra-se presente, pois, como bem pontuam Chivot e Bhatia, se, por um lado, existem obrigações regulamentares relacionadas a limitação do armazenamento e que o armazenamento de altos volumes de dados implicam em maior risco para a organização, por outro lado sistemas de inteligência artificial usualmente precisam de grandes volumes de dados para funcionar com acurácia, de modo que a eliminação de dados pode prejudicar a integridade desses sistemas³⁵.

Muito embora, como bem pontuam os autores, já existam pesquisas e soluções que busquem contornar esse problema (por exemplo, substituindo a prática de coleta e tratamento massivo de dados do *big data*, pelo emprego de profissionais de estatística ou de profissionais dados inteligentes (*smart data*), de modo a, minimizando-se dados, gerar informações capazes de treinar os sistemas de inteligência artificial na obtenção de resultados tão acurados quanto os dos sistemas tradicionais)³⁶, grande parte dos sistemas ainda depende da coleta e tratamento massivo de dados para garantir a assertividade de seus resultados.

34 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

35 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.p. 165-167

36 CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.p. 167

Isto posto, ao fornecer informações quanto aos prazos de retenção e descarte, os agentes de tratamento deverão considerar, também, os prazos de manutenção dos dados utilizados para o treinamento dos sistemas de inteligência artificial, bem como, métodos de permitir a sua eliminação sem prejudicar a acuracidade do sistema – para tanto, os agentes de tratamento podem avaliar métodos de treinamento que possibilitem o uso de dados anonimizados (por exemplo, eliminando-se identificadores dos dados tratados ou fazendo uso de dados estatísticos).

c) Identificação do controlador (art. 9º, III)

O dever de identificar o controlador é uma obrigação cuja compreensão não é fruto de maior complexidade, com a NBR ISO 29184:2021 pontuando pela possibilidade de atendimento deste requisito pelo fornecimento do nome da empresa, o qual pode ser acompanhado de outras informações relevantes (como o endereço de sua sede e seu número de empresa, isto é, o CNPJ)³⁷.

d) Informações de contato do controlador (art. 9º, IV)

Embora o inciso em comento não especifique quais meios de contato devem ser fornecidos, considerado (i) o papel do Encarregado enquanto canal de comunicação da organização com o titular e com a ANPD (art. 5º, VIII); (ii) seu dever de receber solicitações dos titulares e da ANPD e de tomar providências (art. 41, §2º, I, II); (iii) e o dever das organizações em divulgar a sua identidade e o seu contato (art. 41, §1º)³⁸, o canal de contato a ser divulgado, em regra, será o canal de contato do encarregado, ressalvada as hipóteses de dispensa de nomeação do encarregado, previstas em regulamento. Neste último caso, o agente de tratamento deverá disponibilizar um canal alternativo (art. 11, §1º, da Resolução CD/ANPD nº 02, de 27 de janeiro de 2022)³⁹.

37 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação – Avisos de privacidade on-line e consentimento**. Rio de Janeiro: ABNT, 2021

38 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

39 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº**

e) Informações acerca do uso compartilhado de dados pelo controlador e a finalidade (art. 9º, V)

Conforme o próprio texto legal sugere, e a NBR ISO 29184:2021 auxilia a compreender, trata-se de fornecimento de informação se, no curso normal dos negócios, os dados em questão serão transferidos para terceiros e, em caso positivo, com qual finalidade⁴⁰. Embora a texto legal não assevere essa necessidade de forma expressa, tendo em vista que a funcionalidade de prestação de informações aos titulares é que estes exerçam algum grau de controle sobre o fluxo de seus dados pessoais, é recomendável que se inclua, também, informações a respeito de (i) quais dados serão objeto de compartilhamento; (ii) quais partes (ou categorias de partes) receberão quais dados – aliás, a ANPD parece ter se posicionado nesse sentido, ao, em sede da Nota Técnica nº 49/2022/CGF/ANPD, realizar crítica a Política de Privacidade do Whatsapp, pontuando que “não estão dispostas de forma objetiva para facilitar a compreensão do titular de quais tipos de dados são usados de forma compartilhada com quais empresas”⁴¹.

f) Responsabilidades dos agentes que realizarão o tratamento (art. 9º, VI)

O inciso VI complementa o seu antecessor, pontuando que, para além do agente de tratamento estabelecer quais são os entes com quem realiza uso compartilhado de dados e a finalidade do compartilhamento, deverá informar o papel exercido por cada agente interventor no processo.

Mais especificamente, dentro do contexto do emprego de sistemas de inteligência artificial, o agente de tratamento deve adim-

02, de 27 de janeiro de 2022. Brasília: ANPD, 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper>. Acesso em: 04 abr.2023

40 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação** – Avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021

41 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 49/2022/CGF/ANPD.** Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nt_49_2022_cfg_anpd_versao_publica.pdf. Acesso em: 04 abr. 2023

plir este item por meio de uma apresentação a respeito das partes envolvidas em todo o ciclo de vida do sistema de inteligência artificial, desde o seu desenvolvimento até a sua implementação – para tanto, este poderá utilizar-se da metodologia de explicação de sistemas de inteligência artificial “baseada em responsabilidade”, a qual será apresentada no item 4.3 deste trabalho.

g) Direitos do titular, com menção explícita aos direitos contidos no art. 18 (art. 9º, VII)

Trata-se de previsão destinada a informar os titulares sobre os seus direitos e como exercê-los, cumprindo verdadeira função educativa, em relação a qual cabe apenas uma breve consideração: muito embora a legislação apenas obrigue que os direitos previstos no art. 18 sejam expressamente citados, considerando que, conforme preleciona a OCDE, em sua Recomendação do Conselho quanto a Inteligência Artificial (*Recommendation of the Council on Artificial Intelligence*), quando diante do emprego de um sistema de inteligência artificial, a transparência se opera para, dentre outros, possibilitar que as pessoas afetadas (i) compreendam o resultado; e possam (ii) desafiar o resultado, caso negativamente afetadas por ele⁴², é recomendável que, nessas hipóteses, apresente-se, também, ao titular os direitos contidos no art. 20 da LGPD, quais sejam: (i) direito de explicação da decisão automatizada, isto é, de requerer do controlador “*informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial*” (art. 20, §1º); (ii) direito de revisão, isto é, de solicitar que o controlador reveja uma certa decisão relevante tomada unicamente com base em tratamento automatizado (art. 20, *caput*)⁴³, bem como, os procedimentos que devem ser adotados para o seu exercício, caso difiram daque-

42 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**, Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr.2023

43 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República,2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

les adotados para o exercício dos demais direitos, em atenção ao quanto disposto no método de explicação “baseado em responsabilidade”⁴⁴, a ser descrito no item 4.3.

h) Se o tratamento é condição para o fornecimento de produto ou de serviço ou para o exercício de direito (art. 9º, §3º)

Por fim, a legislação requer que seja informado, de forma destacada, se uma operação de tratamento é requisito para a prestação de um dado produto/serviço ou para o exercício de determinado direito.

Apenas um breve destaque: considerando que (i) conforme pontua Modenesi a doutrina entende que, por meio do §2º, do seu art. 46, a LGPD positivou a obrigatoriedade de adoção do *privacy by design*; e que (ii) um dos princípios do *privacy by design* é o *privacy by default*, segundo o qual, conforme leciona Modenesi, requer que as organizações limitem a coleta de dados, enquanto padrão, às “informações essenciais ao funcionamento do produto ou à prestação do serviço”, promovendo-se a “minimização de dados (*data minimisation*), em obediência ao princípio da *necessidade*”⁴⁵, entende-se que o tratamento apenas poderá ser condicional para a prestação de um produto/serviço ou para o exercício de um direito quando, considerada uma esfera de razoabilidade, a qualidade e a segurança mínimas esperadas, não se faça possível o fornecimento do produto/serviço ou o exercício do direito, sem a operação de tratamento em questão.

44 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**. Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr. 2023

45 MODENESI, Pedro. Art. 42. In MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. Indiatuba: Ed. Foco, 2022, p. 110-114.

Transparência após a tomada de uma decisão por sistema de inteligência artificial: explicabilidade do sistema de inteligência artificial

Quando tratamos de transparência em sistemas de inteligência artificial, talvez um dos maiores desafios enfrentados seja explicar, de uma forma minimamente compreensível, como o sistema empregado alcançou uma dada decisão. Não obstante, para além de ser um requisito demandado pela legislação pátria aos controladores, nos termos do art. 20º, §1º, da LGPD, é um dos propósitos mínimos do princípio da “transparência e explicabilidade” apresentado pela OCDE na *Recommendation of the Council on Artificial Intelligence*, a qual foi aderido pelo Brasil, nos termos já vistos⁴⁶.

Mas, afinal, o que se traduz por “explicar” uma decisão tomada por inteligência artificial? O ICO, em seu guia sobre a explicação de decisões automatizadas (*Explaining decisions made with AI*), apresenta duas macrocategorias de explicações possíveis de sistemas de inteligência artificial: as baseadas em processo (*Process-based explanations of AI systems*), em que se explana os processos executados durante a concepção e uso do sistema, usualmente buscando se demonstrar a adoção de boas-práticas, e a baseada em resultados (*Outcome based explanations of AI systems*), em que se busca demonstrar a lógica por detrás de uma decisão específica “de modo simples, facilmente compreensível e utilizando de uma linguagem do dia a dia”⁴⁷.

Em que se pese a reconhecida relevância das explicações baseadas em processo, entende-se que o momento mais adequado de as fornecer é de forma prévia ao emprego dos sistemas, em sede do aviso de privacidade ou documento congênere, nos termos já

46 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**. Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr. 2023

47 Tradução livre de: “in plain, easily understandable, and everyday language”. INFORMATION COMMISSIONER’S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr.2023

vistos, devendo-se o atendimento do direito de explicação voltar-se, justamente, a compreensão de como se chegou a um resultado em concreto. Do contrário, não se faria possível atender aos requisitos firmados pelo princípio de “transparência e explicabilidade” da OCDE, o qual requer que os “atores de inteligência artificial” forneçam informações que permitam ao indivíduo afetado (i) compreender o resultado gerado por um sistema de inteligência artificial; (ii) permitir que aqueles negativamente afetados possam se insurgir contra o resultado, “com base em informação simples e fácil de entender sobre os fatores e a lógica utilizada como base para predição, recomendação, ou decisão”⁴⁸.

Deste modo, embora, para fins de completude, possa vir a se apresentar modelos de explicabilidade cuja maior aplicação prática seja voltada às “explicações baseadas em processo”, não se aprofundará em sua aplicação para este fim, buscando-se, sobretudo, identificar os melhores modelos voltados as explicações “baseadas em resultados” e em quais condições estes podem (ou devem) ser aplicados.

Ademais, deve-se destacar que não se propõe, nas linhas abaixo, se esgotar a temática, tampouco apresentar soluções absolutas (considerando-se, inclusive, que os desafios envolvendo a explicabilidade de sistemas de inteligência artificial podem variar grosseiramente de acordo com o método de decisão adotado por cada modelo – por exemplo, as razões de uma decisão tomada por um sistema que adota um modelo decisório de “árvore de decisão”, em regra, serão razoavelmente fáceis de explicar, diferente de uma inteligência artificial opaca, cujo processo de tomada de decisão pode ser, a princípio, desconhecido, inclusive, pelos seus próprios desenvolvedores), apenas se apresentará algumas soluções propostas, cujo emprego pode ser avaliado por eventuais agentes de tratamento interessados, em atenção às suas próprias necessidades e limitações.

48 Tradução livre de: “based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision”. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Transparency and explainability** (Principle 1.3). Paris: OCDE, 2019. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 05 abr. 2023

Tendo esclarecido este ponto, passemos para os modelos de explicabilidade: o ICO, em seu guia supramencionado sobre a explicação de decisões tomadas por sistemas de inteligência artificial, apresenta seis modelos de explicação: (i) racional (*Rationale explanation*); (ii) baseado em responsabilidade (*Responsibility explanation*); (iii) baseado em dados (*Data explanation*); (iv) baseado em equidade (*Fairness explanation*); (v) baseado em segurança e performance (*safety and performance explanation*); (vi) baseado em impacto (*impact explanation*)⁴⁹. Apresentar-se-á, nas linhas que seguem, uma visão geral destas metodologias e como implementá-las, bem como eventuais considerações sobre a sua adequação em garantir a explicabilidade da decisão, a começar pelo modelo racional.

a) Modelo de explicação “racional”

O modelo racional pauta-se no fornecimento, ao titular, das razões que levaram àquela decisão em específico⁵⁰ e, por tanto, parece ser o modelo mais adequado a se atender o dever de explicação, embora sua implementação muitas vezes não seja simples ou viável, do ponto de vista técnico ou comercial.

Baseado no guia do ICO, para o adequado emprego desta modalidade de explicação, o agente de tratamento poderá ter que demonstrar ao titular (i) a operação, em concreto, executada pelo sistema para alcançar um dado *output* (como ele performou e se comportou, bem como, como os diferentes componentes do sistema o fizeram transformar os *inputs* em *outputs*, inclusive quais “características, interações e parâmetros foram os mais relevantes”⁵¹; (ii) como o “contexto em concreto e a situação de vida do indiví-

49 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

50 Ibid.

51 Tradução livre de: “which features, interactions, and parameters were most significant”. INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

duo”⁵² foram considerados na utilização do sistema; e (iii) como os componentes técnicos do sistema podem fornecer evidência que suportam a lógica da decisão tomada – o que deverá transcorrer em “linguagem simples e facilmente compreensível”⁵³.

Para tanto, ainda com base no guia da autoridade britânica⁵⁴, existem algumas ações que devem ser executadas pelo agente de tratamento, nomeadamente, este deverá: (i) realizar uma prévia verificação do sistema, comparando-o as suas especificações formais, de forma que se confira que o mesmo “opera de forma confiável e se comporta em acordo com a funcionalidade desejada”⁵⁵; (ii) extrair do sistema a racionalidade técnica por detrás do *output*, por exemplo, (a) em caso de um sistema baseado em árvore de decisão, qual foi o “caminho” percorrido para se gerar o resultado final, ou (b) em caso de uma inteligência artificial de maior opacidade, quais atributos foram considerados e os pesos e pontuações que lhe foram atribuídos. Para se atender a esse requisito, caso o sistema não o permita por *design*, o agente de tratamento poderá avaliar o emprego de algumas tecnologias e metodologias disponíveis no mercado, como o *toolkit AI Explainability 360*, da IBM, que podem ser utilizados para auxiliar o agente de tratamento a compreender a racionalidade técnica por detrás da decisão; (iii) traduzir a racionalidade técnica para uma linguagem leiga, explicitando-se os papéis exercidos pelos atributos avaliados na resolução do problema real que o sistema busca resolver, incluindo, uma explicação de como esse modelo foi aplicado, em concreto, para o titular em questão, em atenção aos itens acima pontuados – por exemplo, apresentando-lhe uma explicação de como funciona o sistema, quais atributos (dados do titular), concretamente, foram considerados e a importância atribuída a eles, destacando-se aqueles que

52 Tradução livre de: “to the concrete context and life situation of the affected individual”. Ibid.

53 INFORMATION COMMISSIONER’S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

54 Ibid.

55 Tradução livre de: “operate reliably and behave in accordance with its intended functionality”. Ibid.

mais influenciaram a decisão, de modo que o titular possa ter uma compreensão razoável da racionalidade por detrás da decisão e, entendendo adequado, possa questioná-la ou alterar o seu comportamento para que, no futuro, obtenha um resultado que lhe seja mais apazível.

b) Modelo de explicação baseado em responsabilidade

Conforme apontado pelo ICO, o método baseado em responsabilidade, busca explicitar as partes envolvidas no gerenciamento, desenvolvimento e implementação de um sistema de inteligência artificial, bem como fornecer informações sobre como o titular pode obter uma explicação de decisões tomadas ao seu respeito⁵⁶.

A despeito do fato da metodologia ser relevante para a construção do aviso de privacidade (fornecendo, por exemplo, explicações sobre os papéis do agente de tratamento e/ou sobre como exercer os direitos de explicação e revisão), bem como para demonstrar as boas-práticas adotadas no desenvolvimento e emprego do modelo, nos termos já vistos, o próprio ICO admite que é uma metodologia, via de regra, inteiramente voltada para uma explicação baseada em processo⁵⁷, razão pela qual não é capaz, a princípio, de se explicar como se chegou ao resultado de uma decisão, razão pela qual sua aplicação não será abordada com maior profundidade.

c) Modelo de explicação baseado em dados

O método baseado em dados pode ser traduzido, conforme leciona o ICO, em possibilitar que o titular compreenda quais dados sobre ele foram utilizados em uma determinada decisão e as suas respectivas fontes, bem como o significado do *output* (isto é, do produto gerado pela decisão), caso este não seja suficientemente claro⁵⁸. Citada proposta em muito se aproxima daquela apresentada por Prado, a qual possui como base o julgado do Recurso Espe-

56 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

57 Ibid.

58 Ibid.

cial nº 1.457.199-RS do STJ, em que a corte, ao proferir julgamento sobre a licitude do *credit scoring*, compreendeu que, muito embora a modalidade de decisão automatizada seja lícita, alguns direitos da pessoa afetada deveriam ser respeitados, dentre os quais o de obter esclarecimentos sobre a decisão em comento, esclarecimentos estes que, se por um lado não necessitariam abranger a metodologia de cálculo utilizada (considerada resguardada pelo segredo empresarial), deveria abranger, minimamente, “informações claras, precisas e pormenorizadas acerca dos dados considerados e as respectivas fontes”⁵⁹. Isto posto, Prado apresenta como conteúdo mínimo do dever de explicabilidade o fornecimento de informações quanto a “(i) origem dos dados utilizados; (ii) Tipos de dados utilizados pelos algoritmos para a tomada de decisão; e (iii) finalidade das atividades”, recomendando, ainda, o autor, que sejam fornecidas “informações sobre os critérios e procedimentos utilizados para a decisão automatizada”, considerado o adequado balanceamento entre a transparência e o segredo comercial e/ou industrial do agente de tratamento⁶⁰. Cumpre realizar algumas considerações sobre o modelo baseado em dados, nos termos acima citado: em primeiro lugar, tendo em vista que, (a) um dos objetivos centrais do direito de explicação, conforme preleciona o ICO em seu guia sobre a explicação de decisões automatizadas (*Explaining decisions made with AI*), é fornecer ao titular informação que lhe permita compreender suficientemente a decisão em concreto, de modo que possa “obter informações adequadas, apresentar o seu ponto de vista e contestar a decisão”⁶¹ ou mesmo, caso entendam que a decisão seja razoável, ter a possibilidade de alterar o seu comportamento para que,

59 PRADO, Luis Fernando. Algoritmos e decisões automatizadas: buscando a conformidade com a LGPD. In: PALHARES, Felipe (Coord.). **Estudos sobre privacidade e proteção de dados**. São Paulo: Thomson Reuters Brasil. 2021, p.107-135.

60 PRADO, Luis Fernando. Algoritmos e decisões automatizadas: buscando a conformidade com a LGPD. In: PALHARES, Felipe (Coord.). **Estudos sobre privacidade e proteção de dados**. São Paulo: Thomson Reuters Brasil. 2021. p.107-135.

61 Tradução livre de: “obtain meaningful information, express their point of view and contest the decision”. INFORMATION COMMISSIONER’S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

no futuro, atinja o resultado pretendido; (b) sem conhecimento dos dados concretamente utilizados, não será possível que o titular questione a decisão, tendo em vista que não poderá verificar a acuracidade dos dados utilizados; (c) a supramencionada decisão do STJ comanda que sejam fornecidas “informações pormenorizadas” sobre os dados tratados⁶²; (d) o princípio do livre acesso garante ao titular o direito de aceder aos dados a seu respeito⁶³, entende-se que, caso opte pelo modelo baseado em dados, a explicação deverá abranger o fornecimento dos dados concretamente utilizados para a tomada da decisão em questão.

Ademais, para os agentes de tratamento tentados a limitar o atendimento da requisição ao conteúdo mínimo acima apresentado, direciona-se especial atenção para a recomendação de Prado quanto ao fornecimento de informações sobre os critérios e procedimentos utilizados, considerado o balanceamento entre transparência e o segredo industrial do agente de tratamento⁶⁴, de modo que limitar a explicação ao fornecimento de informações a respeito dos dados utilizados apenas é justificável quando, consideradas as circunstâncias em concreto, não se faça possível o fornecimento de informações mais abrangentes pelo agente de tratamento (ex. este utiliza um sistema de decisão automatizado fornecido por terceiro, de modo que embora conheça os *inputs* fornecidos, isto é, os dados do titular e sua respectiva origem, desconhece os pormenores da metodologia, cuja propriedade intelectual envolvida é de titularidade do fornecedor) ou, ainda que seja possível, o fornecimento destas informações possa implicar grave prejuízo para a organização em questão, na medida em que comprometam eventuais vantagens competitivas decorrentes do sigilo sobre a metodologia utilizada.

62 STJ *apud* PRADO, Luis Fernando. Algoritmos e decisões automatizadas: buscando a conformidade com a LGPD. In: PALHARES, Felipe (Coord.). **Estudos sobre privacidade e proteção de dados**. São Paulo: Thomson Reuters Brasil. 2021. p.107-135.

63 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.

64 PRADO, Luis Fernando. Algoritmos e decisões automatizadas: buscando a conformidade com a LGPD. In: PALHARES, Felipe (Coord.). **Estudos sobre privacidade e proteção de dados**. São Paulo: Thomson Reuters Brasil. 2021. p.107-135

Por fim, reforça-se que, para se utilizar adequadamente do modelo de explicação baseado em dados, a organização deve, de forma prévia, ter mapeado os fluxos de dados dos processos envolvendo o sistema de inteligência artificial em análise, bem como empregado técnicas apropriadas que permitam a verificação da linhagem dos dados (ex. o estabelecimento e manutenção de um catálogo de dados), de modo que seja possível identificar com precisão quais dados são utilizados pelo modelo e sua exata origem⁶⁵.

d) Modelo de explicação baseado em equidade

Segundo o ICO, a metodologia baseada em equidade possui dois objetivos principais (i) demonstrar as ações adotadas para garantir que a decisão em comento seja, em regra, “equitativa e livre de vieses”; e (ii) permitir com que os titulares afetados “avaliem se eles foram tratados de forma equitativa”. Para tanto, a organização poderá ter que demonstrar que ela adotou práticas de equidade quanto (i) aos dados utilizados para treinar o sistema de inteligência artificial; (ii) quanto ao design do modelo; (iii) quanto aos seus *out-puts*; (iv) quanto ao emprego do sistema⁶⁶.

Em relação a equidade nos dados utilizados para o treinamento do modelo, a autoridade britânica pontua que a organização pode, por exemplo, demonstrar que os dados (a) são representativos do público afetado; (b) são suficientes, de forma qualitativa e quantitativa, para representar a população afetada e o fenômeno objeto do modelo; (c) são coletados de “fontes adequadas, confiáveis e imparciais e obtidos através de métodos de coleta apropriados”⁶⁷; (d) pos-

65 Segundo a DAMA (2017), linhagem de dados é o “caminho através do qual os dados se movem, de seu ponto de origem para os seus pontos de utilização, por vezes chamados de cadeia de dados” (Tradução livre). DAMA INTERNATIONAL. **DAMA-DMBOK: Data Management Book of Knowledge**. 2 Ed. Basking Ridge: Technics Publications, 2017. P. 28

66 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

67 Tradução livre de: “suitable, reliable and impartial sources of measurement and has been sourced through sound collection methods”. INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022.

suem níveis adequados de qualidade, isto é, são “atualizados e refletem de forma acurada os indivíduos, a população e o fenômeno”⁶⁸ objeto do modelo; (e) são relevantes para a finalidade perseguida⁶⁹.

A equidade no design busca demonstrar, conforme apresentado pelo ICO, que os elementos que formam a arquitetura do modelo (seus processos, atributos, variáveis e sua estrutura analítica – isto é, aquilo que o modelo infere, correlaciona e interage) são razoáveis e justificáveis⁷⁰.

O ICO fornece algumas ações que podem ser tomadas para promover a equidade no design, notadamente, (i) identificar, na etapa inicial do projeto, eventuais vieses estruturais, isto é, “padrões e práticas institucionalizadas que conferem vantagens para certos grupos e desvantagens para outros”⁷¹, os quais podem influenciar nas ações dos desenvolvedores do sistema, como na seleção de atributos ou dados; (ii) mitigar eventuais vieses nos dados a serem utilizados antes do seu processamento, tendo em vista elementos contextuais como a realidade organização e o setor – recorda-se, aqui, o famoso caso do sistema de inteligência artificial da Amazon desenvolvido para realizar a análise de currículos, o qual foi descontinuado por apresentar tendências discriminatórias contra mulheres, dado o fato de ter sido treinado com base nas contratações da empresa nos dez anos antecedentes, contratações estas predominantemente masculinas, considerando que a mesma se insere no mercado de tecnologia, o qual ainda é composto majoritariamente por homens⁷², fator este que, em acordo com o guia do ICO,

Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

68 Tradução livre de: “up-to-date and accurately reflects the characteristics of individuals, populations and the phenomena”. Ibid “. Ibid.

69 Ibid.

70 Ibid.

71 Tradução livre de: institutional patterns and practices that confer advantage to some and disadvantage to others based on identity”. UNIVERSITY OF NORTH GEORGIA. **Types of Bias**. UNG. Disponível em: <https://ung.edu/diversity/bias.php#:~:text=Structural%20Bias,McIntosh%201988%3B%20Rosette%202006>. Acesso em: 06 abr. 2023

72 AUTRAN, Felipe. IA da Amazon usada em análise de currículos discriminava mulheres. **Tecmundo**, 2018. Disponível em: <https://www.tecmundo.com.br/sof>

deveria ser considerado ao se selecionar os dados utilizados para o treinamento do modelo; (iii) mitigar vieses nos atributos e parâmetros selecionados, modelando-se, testando e avaliando estágios do processo de tomada de decisão, levando-se em consideração os objetivos de redução de vieses da organização; (iv) avaliar se as práticas analíticas do modelo treinado (correlações, inferências e interações) são razoáveis e justificáveis, considerando a finalidade almejada; e (v) avaliar proxies ocultos (*hidden proxies*) em busca de potenciais recursos discriminatórios que afetem o modelo⁷³.

A equidade quanto ao resultado, que pode ser o item mais relevante para o objeto em análise, busca garantir que o *output* da I.A. não gere “impactos discriminatórios ou injustos às pessoas afetadas”⁷⁴. Para tanto, o ICO sugere que (i) a organização demonstre que definiu explicitamente o que entende por “equidade”, considerando que diferentes entendimentos sobre a temática podem levar a decisões diversas sobre como implementá-la, em concreto, no modelo; e (ii) a metodologia utilizada para operacionalizar o conceito de equidade estabelecido pela organização⁷⁵.

A equidade quanto a implementação, busca demonstrar que o emprego do sistema se opera por intermédio de “usuários suficientemente treinados para implementá-lo responsavelmente e sem vieses”⁷⁶. Para tanto, o ICO aconselha que os usuários sejam

[tware/135062-ia-amazon-usada-analise-curriculos-discriminava-mulheres.htm](https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/). Acesso em: 06 abr. 2023

73 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

74 Tradução livre de: “discriminatory or inequitable impacts on the lives of the people it affects”. INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

75 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

76 Tradução livre de: “users sufficiently trained to implement it responsibly and without bias”. INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions**

treinados para problemáticas, como (i) evitar confiança ou desconfiança excessivas nos sistemas de inteligência artificial – o que se entende que poderia ser atendido por uma análise crítica do seu resultado; (ii) que o resultado apenas seja utilizado em atenção ao contexto em que a decisão foi tomada; (iii) compreender as limitações dos sistemas, por exemplo, compreender a margem de erro de um sistema⁷⁷.

Estabelecidos os elementos que devem ser levados em consideração relativos a equidade do sistema, o ICO fornece algumas orientações sobre quais passos devem ser tomados para explicar o resultado, nomeadamente (i) detalhar como os critérios de equidade explicitados foram implementados em uma decisão em concreto; (ii) apresentação das métricas relevantes de equidade na entrega do modelo; (iii) apresentar ao titular como outros indivíduos similares foram tratados (ex. se eles obtiveram resultados parecidos)⁷⁸.

Cumprir realizar um último comentário em relação ao modelo: sem prejuízo dos seus méritos, considerando-se que (i) a sua principal finalidade é, nos termos já vistos, demonstrar a equidade do sistema e da decisão gerada por intermédio do mesmo⁷⁹; (ii) o modelo não fornece ao titular uma explicação a respeito de como se chegou a decisão em si; entende-se que o seu uso apenas deve se operar para atender o direito de explicação previsto na LGPD quando o objeto de questionamento é, justamente, a equidade da decisão (ex. o titular apresenta suspeitas de que o processo decisório é discriminatório), tendo em vista que, do contrário, dificilmente

made with AI. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

77 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI.** Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

78 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI.** Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

79 Ibid.

será entendida como uma forma suficientemente adequada de explicitar, ao titular, informações dos “critérios e dos procedimentos utilizados para a decisão automatizada”, conforme requerido pelo §1º, do art. 20º, da lei.

e) Modelo de explicação baseado em segurança e performance

O ICO apresenta a explicação baseada em “segurança e performance” como uma metodologia voltada a explicar ao titular como a organização atua para garantir que o modelo tenha a sua robustez, acuracidade, confiabilidade e segurança maximizadas em relação aos resultados apresentados pelo sistema⁸⁰. Com este fim, a autoridade britânica elenca alguns elementos que talvez podem necessitar serem demonstrados para apresentação de uma explicação adequada, nomeadamente (i) o grau de acuracidade do modelo (ex. partindo de uma amostra, quantas decisões corretas ele gerou?); (ii) o sistema é confiável para a finalidade empregada? Isto é, ele executa o que, de fato, foi programado para fazer? (iii) A capacidade do sistema de garantir a sua integridade, isto é, possui medidas de segurança capazes de manter a sua integridade e de suas partes; (iv) o sistema é resistente a situações adversas? Isto é, como seu funcionamento é afetado por situações adversas, por exemplo, a ocorrência de um ciberataque⁸¹.

Segundo o ICO, a explicação de decisões com base neste modelo, se opera por meios de uma demonstração, ao titular, que no momento de execução do sistema para tomada de decisão ao seu respeito este operava de forma confiável, segura e robusta⁸². Não obstante, considerando que este modelo não apresenta explicações sobre como o sistema chegou a uma decisão em específico, entende-

80 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

81 Ibid.

82 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023.

-se que seu uso não satisfaz o dever previsto no art. 20, §1º, da LGPD.

Isso não significa, contudo, que o modelo deva ser descartado, tendo em vista que seu uso pode se mostrar essencial para o cumprimento de outros deveres relevantes em matéria de privacidade e proteção de dados, notadamente em decorrência de sua capacidade de auxiliar na identificação e mensuração de riscos quando do emprego de sistemas de inteligência artificial, sobretudo riscos relacionados a segurança do sistema e a qualidade de seus *outputs*, de modo a permitir que a organização adote controles proporcionais a esses riscos (Art. 44, II, da LGPD), bem como atenda a sua obrigação de demonstração de “medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais” e da eficácia das medidas por si adotadas, decorrente do princípio da responsabilidade e prestação de contas (art. 6º, X, da LGPD)⁸³, inclusive por intermédio da elaboração de um relatório de impacto à proteção de dados pessoais (RIPD)⁸⁴.

f) Modelo de explicação baseado em impacto

O ICO pontua que, por intermédio do modelo baseado em impacto, a organização pode demonstrar como considerou os impactos do sistema de inteligência artificial no indivíduo, bem como seus efeitos

83 BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023

84 O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD)” (ANPD, 2023). AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#:~:text=O%20RIPD%20%C3%A9%20a%20documenta%C3%A7%C3%A3o%20que%20cont%C3%A9m%20a,e%20aos%20direitos%20fundamentais%20do%20titular%20de%20dados. Acesso em: 07 abr. 2023

na sociedade, podendo, para tanto, ter que apresentar os processos pelo qual a organização passou para avaliar citados impactos⁸⁵.

Repete-se a esse modelo os mesmos comentários praticados quanto ao modelo “baseado em segurança e performance”: em que se pese o modelo seja de relevante (ou até mesmo essencial) para os processos de avaliação e mitigação de risco, entende-se que seu uso não satisfaz a obrigação prevista no art. 21º, §1º, da LGPD, considerando-se que não fornece ao titular informações sobre como o sistema alcançou uma dada decisão específica.

Conclusão

Em matéria de privacidade e proteção de dados um dos maiores desafios no emprego de sistemas de inteligência artificial é garantir aos titulares uma transparência adequada durante todo o ciclo de vida do sistema, desde o seu treinamento à obtenção de um resultado em específico.

Para superar esses desafios, os agentes de tratamento devem se atentar a dois fatores (i) a relevância dos diferentes momentos no ciclo de vida do sistema e seus impactos a respeito dos quais informações devem ser fornecidas ao titular – devendo, o agente de tratamento, preparar-se para fornecer informações, no mínimo, a respeito (a) do tratamento de dados para fins de treinamento do sistema; (b) do tratamento de dados relativo ao emprego do sistema; (c) de como o sistema chegou a uma decisão em específico (explicação *post-hoc*); (ii) a necessidade de adequar-se a aplicação do princípio da transparência, e as obrigações positivadas dele decorrentes, ao *framework* regulatório de sistemas de inteligência artificial da OCDE, considerada a aderência do Brasil ao mesmo, de modo que (a) os textos de avisos de privacidade (ou documentos congêneres, destinados a adimplir o dever geral de transparência) permitam que o titular compreenda o que é um sis-

85 INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr. 2023

tema de inteligência artificial e que interagirá com um; e (b) que a explicação *post-hoc* permita que o titular compreenda como uma decisão foi tomada suficientemente para, caso entenda ter sido prejudicado, questioná-la.

Nesse sentido, temos que os principais desafios dos agentes de tratamento quando do uso de dados pessoais para o treinamento de sistemas de inteligência artificial é, justamente, o de fornecer informações adequadas aos titulares, sobretudo, naquelas situações em que os dados não são coletados diretamente dos titulares – por exemplo, minerando-se dados disponíveis publicamente ou coletando-se dados pessoais de terceiros (*data brokers*). Nessas situações é dever do agente de tratamento garantir que o titular seja informado do tratamento de seus dados para fins de treinamento do sistema, seja por intermédio do fornecedor desses dados (se existente), seja, quando os meios razoavelmente disponíveis o possibilitarem, notificando diretamente o titular, ressalvadas as situações em que essa notificação não se faça possível ou razoável, caso em que o agente de tratamento deverá adotar medidas que garantam a minimização dos impactos do tratamento.

Por sua vez, quando do emprego do sistema de inteligência artificial em um dado indivíduo, o principal desafio encontra-se em adequar o aviso de privacidade (ou documento congênere) a realidade do uso do sistema de inteligência artificial, o que, além de demandar um conhecimento aprofundado sobre o fluxo de dados no sistema, requererá que o agente de tratamento se atente a (i) a necessidade de, ao se descrever a forma com que o dado será tratado, (a) explicitar o uso de um sistema de inteligência artificial; (b) fornecer, ao titular, informações que lhe permitam compreender o que é um sistema de inteligência artificial; (c) fornecer informações que permitam ao titular compreender como o sistema normalmente se comporta, seus objetivos e limitações; (ii) a necessidade de deixar claro ao titular a origem dos dados ao seu respeito que servirão de *input* no sistema, sobretudo quando não coletados diretamente do titular; (iii) conscientizar, o titular, sobre os direitos que lhe são conferidos em relação a tomada de decisões automatizadas, bem como os meios para exercê-los.

Por fim, a explicação *post-hoc*, isto é, o dever de, uma vez provocado, fornecer ao titular informação que lhe permita compreender a decisão em nível suficiente a, caso entenda adequado, questioná-la, é um dos deveres mais complexos a serem adimplidos pelo agente de tratamento, já existindo, contudo, algumas tecnologias e metodologias, disponíveis no mercado para este fim.

Dentre as metodologias estudadas aquela que melhor atende, em abstrato, o dever em análise é o modelo de explicação racional, por meio do qual busca-se traduzir, a uma linguagem leiga, a racionalidade utilizada pelo sistema. Não obstante, seja por limitações técnicas, seja pela necessidade de resguardar segredos comerciais e industriais, seu emprego não se faz sempre possível (ou adequado). Para essas situações, pode-se avaliar o emprego de outros métodos, o baseado em dados, em que se busca demonstrar ao titular os dados dele utilizados no sistema e sua respectiva origem, de modo que ele possa realizar, pelo menos, um controle de acuracidade, e, naquelas situações em que o titular questiona a justiça da decisão, o modelo “baseado em equidade”, em que se busca demonstrar ao titular que a decisão foi tomada de forma equitativa.

Ademais, não se entende adequada a utilização, para os fins de atendimento do art. 20, §1º, da LGPD, das metodologias baseadas em responsabilidade, segurança e performance e baseado em impacto, dado que não fornecem explicações adequadas sobre como o sistema alcançou uma decisão em específico, muito embora possam ser de relevada importância para o cumprimento de outras obrigações legais – nomeadamente (i) para o primeiro modelo, a elaboração do aviso de privacidade, especificamente, na redação das “responsabilidades dos agentes que realizarão o tratamento” (art. 9º, VI); (ii) por sua vez, os demais podem ser utilizados para uma adequada avaliação dos riscos e implementação de controles adequados a estes riscos, requisito de licitude do tratamento nos termos do art. 44, II, da LGPD.

Referências

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29184: Tecnologia da informação – Avisos de privacidade on-line e consentimento**. Rio de Janeiro: ABNT, 2021.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 49/2022/ CGF/ANPD**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-epublicacoes/nt_49_2022_cfg_anpd-versao_publica.pdf. Acesso em: 04 abr.2023
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD): Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoaisripd#:~:text=O%20RIPD%20%C3%A9%20a%20documenta%C3%A7%C3%A3o%20que%20cont%C3%A9m%20a,e%20aos%20direitos%20fundamentais%20do%20titular%20de%20dados. Acesso em: 07 abr.2023
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 02, de 27 de janeiro de 2022**. Brasília: ANPD, 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper>. Acesso em: 04 abr.2023
- AUTRAN, Felipe. IA da Amazon usada em análise de currículos discriminava mulheres. **Tecmundo**, 2018. Disponível em: <https://www.tecmundo.com.br/software/135062-ia-amazon-usada-analise-curriculos%20discriminava-mulheres.htm>. Acesso em: 06 abr.2023
- BASAN, Arthur Pinheiro. Art. 6. In MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018**. Indiatuba: Ed. Foco,2022, P. 53-66.
- BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República,2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 abr. 2023.
- CHIVOT, Eline; BHATIA, Punit. **Ai & Privacy: How To Find Balance**. Publicação Independente, 2020.
- COSTA NETO, Geraldo Romeiro. **Criações de Inteligência Artificial: reflexos no direito de patentes**. Rio de Janeiro: Lumen Juris, 2021.

- DAMA INTERNATIONAL. DAMA-DMBOK: **Data Management Book of Knowledge**. 2 Ed. Basking Ridge: Technics Publications, 2017. P. 28
- FALEIROS JÚNIOR, José Luiz de Moura. Art. 9. *In* MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. Indiatuba: Ed. Foco,2022, P. 110-114.
- FRAJHOF, Isabella Z; KREMER, Bianca. Art. 33. *In* MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. Indiatuba: Ed. Foco,2022, P. 341-347.
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Provvedimento del 30 marzo 2023 [9870832]**. Roma: GPDP, 2023. Disponível em: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870832>. Acesso em: 03 abr.2023
- INFORMATION COMMISSIONER'S OFFICE. **Explaining decisions made with AI**. Wilmslow: ICO, 2022. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/>. Acesso em: 03 abr.2023
- INFORMATION COMMISSIONER'S OFFICE. **Guidance on AI and data protection**. Wilmslow: ICO, 2023. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/>. Acesso em: 03 abr.2023
- MODENESI, Pedro. Art. 42. *In* MARTINS, Magalhães Guilherme; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. Indiatuba: Ed. Foco,2022, P. 110-114.
- ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Recommendation of the Council on Artificial Intelligence**. Paris: OCDE, 2019. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. Acesso em: 05 abr.2023
- ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Transparency and explainability** (Principle 1.3). Paris: OCDE, 2019. Disponível em: <https://oecd.ai/en/dashboards/ai-principles/P7>. Acesso em: 05 abr.2023
- PRADO, Luis Fernando. Algoritmos e decisões automatizadas: buscando a conformidade com a LGPD. *In* PALHARES, Felipe (Coord.). **Estudos sobre privacidade e proteção de dados**. São Paulo: Thomson Reuters Brasil. 2021, P.107- 135

TEIXEIRA, Tarcísio; CHELIGA, Vinicius. **Inteligência Artificial**: aspectos jurídicos. 2. Salvador: Ed. JusPODIVM, 2020.

UNIVERSITY OF NORTH GEORGIA. **Types of Bias**. UNG. Disponível em: <https://ung.edu/diversity/bias.php#:~:text=Structural%20Bias,McIntosh%201988%3B%20Rosette%202006>). Acesso em: 06 abr.2023



2º lugar

O tratamento irregular de dados pessoais e a possibilidade de reconhecimento de um dano extrapatrimonial presumido

Evelyn Pinto Pereira ✎

Resumo

Com o advento da Lei Geral de Proteção de Dados (LGPD) – em vigor, majoritariamente, desde setembro de 2020 – surgiram desafios quanto à definição dos critérios para a caracterização do dano extrapatrimonial oriundo do tratamento irregular de dados, sobretudo, quanto à possibilidade de reconhecimento de um dano extrapatrimonial presumido (*in re ipsa*). A complexidade da questão, aliada ao fato de que a responsabilização por violação à LGPD encontra-se em construção na jurisprudência, reforça a necessidade de uma análise pormenorizada dos critérios para a imputação do dano na referida Lei. Assim, problematiza-se na presente pesquisa os critérios causais para a caracterização do dano extrapatrimonial decorrente da infringência às normas que regem a proteção de dados, mormente quanto à possibilidade de presunção do dano. Para tanto, utilizar-se-á o método exploratório, abarcando textos legais, produções doutrinárias e decisões jurisprudenciais. Ao final, serão apresentadas considerações a respeito da impossibilidade de se reconhecer um dano extrapatrimonial presumido oriundo de todo tratamento irregular de dados pessoais.

Introdução

A revolução tecnológica mudou a forma como o mundo era visto, mas, sobretudo, como as pessoas eram vistas pelo mundo. O extraordinário avanço apresentado pela tecnologia da informação, especialmente com a disseminação das redes sociais, fez acender um alerta vermelho para esses mecanismos que propiciam, dentre outras coisas, o cruzamento de dados pessoais e o monitoramento de pessoas¹.

A forma como esses dados são explorados e as violações que dela decorrem não se limitam, contudo, a uma mera violação da privacidade. Há diversos desdobramentos da personalidade que são colocados em risco pela economia movida a dados, tais como a individualidade e a autonomia².

A Lei Geral de Proteção de Dados (LGPD) emerge no âmbito da sociedade da informação e busca, principalmente, resgatar a dignidade dos titulares dos dados e seus direitos básicos relacionados à autodeterminação informativa³. Para tanto, além de instituir diversos direitos e deveres, a LGPD, com vistas a dar melhor interpretação aos ditames legais, traz em seu art. 5º a definição de cada termo utilizado.

Nesse sentido, tem-se que dado pessoal, previsto no inciso I, é a informação relacionada a pessoa natural identificada ou identificável. A moldura normativa da Lei apresenta uma perspectiva expansionista para o conceito de dados pessoais, de modo que não só os dados que inexoravelmente identificam uma pessoa estão sob a sua tutela, mas também todos aqueles que têm o potencial de identificá-la. Assim, adjetivar um dado como sendo pessoal ou não dependerá, em suma, de uma análise contextual que

1 VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** 2007. Dissertação (Mestrado) – Curso de pós-graduação *stricto sensu* em Direito, Estado e Sociedade: Políticas Públicas e Democracia, Universidade de Brasília, Brasília, 2007. p. 155.

2 FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPE-DINO, G; FRAZÃO, A.; OLIVA, M. D. (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 1 ed. São Paulo: Thomson Reuters Brasil, 2019. p. 100.

3 Id., *ibid.* p. 100.

revele quais tipos de informações podem ser extraídas de uma base de dados⁴.

O tratamento de dados, por sua vez, é “toda operação realizada para/com dados pessoais do titular”⁵. Em seu inciso X, a LGPD elenca um extenso rol exemplificativo sobre as hipóteses de aplicabilidade da Lei, cuja noção é bastante abrangente⁶, reconduzindo-a a vasta maioria dos problemas envolvendo a categoria dos dados pessoais⁷.

Assim, diante deste arcabouço informacional que pode vir a se caracterizar como um dado pessoal, a legislação de proteção de dados instituiu diversos direitos e deveres, dentre eles, a responsabilidade e o ressarcimento de danos decorrentes do tratamento irregular desses dados, conforme art. 42 da Lei 13.709/2018:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018).

Com efeito, ainda que a responsabilização por violação à LGPD conte com uma Seção⁸ para si, a Lei tratou da questão com bastante vagueza. Perceptível, pois, que a técnica legislativa empregada pela LGPD deixou de tratar dos critérios causais para imputação do dano extrapatrimonial decorrente da infringência às normas que regem a proteção de dados, mormente quanto à possibilidade de presunção do dano.

4 Id. *ibid.*, p. 61.

5 RABAIOLI, Laiza; LOPES, Luiza Cauduro. Os conceitos gerais da Lei Geral de Proteção de Dados: noções instrumentais sobre o tratamento de dados pessoais. *In: MENKE, F.; DRESH, R. F. V. (Coord.). Lei Geral de Proteção de Dados: aspectos relevantes.* São Paulo: Foco, 2021. p. 35.

6 Nesse ponto, importa ressaltar que esta noção, em que pese abrangente, não é plena; há hipóteses de exclusão da aplicabilidade da lei, tais como a utilização para fins exclusivamente jornalísticos e artísticos, dentre outros previstos no art. 4º da LGPD.

7 SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). Tratado de proteção de dados pessoais.* Rio de Janeiro, Forense, 2021. p. 333.

8 Seção III – Da Responsabilidade e do Ressarcimento de Danos, da Lei 13.709/2018.

Destarte, a primeira parte deste artigo busca pormenorizar a noção de dano e as respectivas modalidades que abarcam a temática ora debatida, evidenciando a construção de seus conceitos. A seu turno, a segunda parte aborda, de maneira mais específica, o bem jurídico tutelado pela LGPD, assim como os pressupostos para a configuração de um dano extrapatrimonial decorrente da violação à Lei, explorando, ainda, a possibilidade de reconhecimento de um dano *in re ipsa*.

A definição jurídica de dano

A necessidade de se ter clara a noção do que seria o dano no ordenamento jurídico vigente justifica-se, pois, como bem refere o jurista Clóvis V. de Couto e Silva, “*Sem que se estabeleça a noção de dano, não se pode ter uma ideia exata da responsabilidade civil num determinado país*”⁹.

Com efeito, estabelecer a mais acertada definição acerca do que seria o dano exige que este esteja consubstanciado em premissas que explorem a sua causa/origem; do contrário, estar-se-ia fadado a uma noção amplíssima que busca conceituá-lo a partir de seus efeitos e consequências¹⁰. A par disso, Bruno Miragem leciona que “a noção de dano toma o sentido de perda, uma lesão a um patrimônio compreendido em sentido amplo como conjunto de bens e direitos de que seja titular a pessoa. É lesão a interesses juridicamente protegidos”¹¹.

Outrossim, considerando que esta lesão a um interesse ou bem juridicamente tutelado é pressuposto da responsabilidade civil – porquanto é a existência do dano injusto que se configura causa de atribuição patrimonial para que determinado valor pecuniário

9 COUTO E SILVA, Clóvis Veríssimo do. O conceito de dano no direito brasileiro e no direito comparado. **Revista dos Tribunais**, v. 2, p. 333-348, jan./mar. 2015, p. 333.

10 CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 15 ed. São Paulo: Atlas, 2021. p. 116.

11 MIRAGEM, Bruno. **Direito Civil: responsabilidade civil**. Rio de Janeiro: Forense, 2021. p. 93.

se transfira do patrimônio do autor do dano para a vítima¹², é necessário que se tenha presente que não basta um dano hipotético. Tampouco a verificação da ocorrência de um ato ilícito é circunstância suficiente a caracterizar o dano juridicamente relevante; é imprescindível que dele resulte a interferência indevida no patrimônio jurídico alheio, conforme estabelece o art. 927 do CC¹³.

Esse ato ilícito, por sua vez, pode afetar a esfera jurídica de outrem ocasionando lesão a um interesse tanto de ordem patrimonial quanto extrapatrimonial, podendo, inclusive, dar causa às duas modalidades de dano.

O dano patrimonial é compreendido como um prejuízo econômico, decorrente de uma diminuição imediata do patrimônio da vítima ou o impedimento de obtenção de vantagem futura que razoavelmente poderia esperar obter¹⁴. O dano extrapatrimonial, a seu turno, está associado à lesão da dignidade humana nas diversas expressões da personalidade¹⁵ o seu conceito, contudo, será melhor explorado em seção própria deste artigo¹⁶, em virtude da complexidade que guarda a sua definição, assim como por constituir elemento central da temática sob análise.

A responsabilidade civil, como instituto jurídico, visa a reparar ou a compensar um dano injusto, a depender da natureza do interesse violado. Caso o bem lesado de ordem patrimonial, a indenizabilidade dar-se-á para fins de reparação do dano; por outro lado, se o interesse ofendido é de ordem extrapatrimonial, a responsabilidade civil dar-se-á para fins de compensação do dano¹⁷.

Com efeito, é importante esclarecer que o dano aqui tratado é aquele que deve estar presente no fato gerador de um evento da-

12 Id. *ibid.*, p. 94.

13 Art. 927 do Código Civil: "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

14 MIRAGEM, Bruno. **Direito Civil**: responsabilidade civil. Rio de Janeiro: Forense, 2021, p. 101.

15 TEPEDINO, Gustavo. Notas sobre o dano moral no direito brasileiro. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 30, p. 33-60, out./dez. 2021, p. 47.

16 2.1, *infra*.

17 MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9. p. 7073-7121, 2014, p. 7074.

noso para ensejar o surgimento da obrigação de indenizar¹⁸. Assim, a acepção corrente ou comum da palavra “dano”, que compreende qualquer forma de modificação pejorativa, não coincide com a noção jurídica de dano ressarcível¹⁹. Para além disso, como bem pontuado por Paulo Lôbo, “nem todo dano é considerado pelo direito, pois a vida em sociedade é caracterizada por perdas e danos que a pessoa sofre em seu cotidiano, e que devem ser suportados”²⁰.

Portanto, deve-se ter ciência de que o dano que está sob a tutela do direito é estritamente a lesão a um interesse juridicamente protegido e esta, por sua vez, deve desbordar dos dissabores cotidianos, a partir das regras da experiência comum²¹.

A caracterização do dano extrapatrimonial

Dentre as teses que buscam definir o conteúdo conceitual do dano extrapatrimonial²² no direito brasileiro²³, aquela que o define como sendo lesão a direitos da personalidade é a que melhor contrapõe à elevada discricionariedade presente quando da aplicação do instituto, uma vez que pugna pela incidência de parâmetros mais objetivos²⁴. Nesse sentido, essa afronta a direito da personali-

18 SANSEVERINO, Paulo de Tarso Vieira. **Princípio da Reparação Integral** – indenização no Código Civil. São Paulo: Saraiva, 2010. p. 145.

19 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil: responsabilidade civil**. 3. ed. Rio de Janeiro: Forense, 2022. p. 29.

20 LÔBO, Paulo. **Direito Civil: obrigações**. 10. ed. v. 2. São Paulo: Saraiva, 2022. p. 344.

21 Nos termos do art. 375 do Código de Processo Civil, “O juiz aplicará as regras de experiência comum subministradas pela observação do que ordinariamente acontece e, ainda, as regras de experiência técnica, ressalvado, quanto a estas, o exame pericial”.

22 Utilizar-se-á a denominação dano extrapatrimonial porquanto esta abrange não só o dano moral stricto sensu, mas também todos os demais danos que são tutelados pelo instituto jurídico.

23 Vide concepções negativas e positivas, em relação a esta última pode-se citar: o dano extrapatrimonial como dor e sofrimento, como lesão à dignidade humana e como lesão a direitos da personalidade.

24 BISNETO, Cícero Dantas. **Formas não monetárias de reparação do dano moral: uma análise do dano extrapatrimonial à luz do princípio da reparação adequada**. Florianópolis: Tirant Lo Blanch, 2019. p. 89.

dade deve ser entendida em espectro amplo, compreendendo três esferas: atinentes ao ser humano biológico, ao ser humano moral e ao ser humano social²⁵.

Relativamente ao ser humano biológico, tem-se a vida e a saúde, compreendida em suas manifestações física, psíquica e emocional; em relação ao ser humano moral, tem-se a integridade moral, a intimidade, a vida privada, a identidade e a expressão da singularidade pessoal; e, por fim, quanto ao ser humano social, tem-se a boa reputação, o respeito nas relações profissionais/pessoais, a não-discriminação por etnia, opção sexual, religião, educação etc²⁶.

Com efeito, em que pese seja consideravelmente difundida no Brasil a concepção de que o dano extrapatrimonial decorre de efeitos subjetivos (revelados em dor e sofrimento moral/físico), que dependem de comprovação para a sua caracterização, entende-se que tal acepção é equivocada, porquanto a configuração do dano acaba derivando não da lesão ao bem jurídico, mas de suas consequências²⁷.

Ademais, outra problemática atrelada a esse entendimento está no discernimento entre o efeito extrapatrimonial de uma lesão patrimonial e o dano patrimonial indireto; isso porque, embora este último atinja interesses não patrimoniais, a repercussão se dá no patrimônio do lesado. Esta situação pode ser evidenciada, por exemplo, quando um advogado perde clientes em razão de dano injusto à reputação profissional; nesse caso, a difamação ofende bem juridicamente tutelado não patrimonial, contudo, o dano reverbera no âmbito patrimonial, razão pela qual a indenização será para fins de reparar dano eminentemente material²⁸.

Diante deste cenário doutrinário, acertadamente definiu Judith Martins-Costa:

25 MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9, p. 7073-7121, 2014, p. 7084.

26 MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9, p. 7073-7121, 2014, p. 7086.

27 LÔBO, Paulo. *Direito Civil: obrigações*. 10. ed. v. 2. São Paulo: Saraiva, 2022, p. 351.

28 MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9, p. 7073-7121, 2014, p. 7083.

A esta altura, pode ser sintetizada noção de ‘dano moral’ compatível com o nosso sistema: trata-se de dano produzido em virtude de ato antijurídico na esfera jurídica extrapatrimonial de outrem, seja como agravo a direito da personalidade, seja como efeito extrapatrimonial de lesão à esfera patrimonial, em certos casos como a negativa indevida de cobertura de seguro saúde em situações graves²⁹.

A jurisprudência, por seu turno, tem consagrado também esse entendimento, conforme depreende-se do Recurso Especial 1.245.550, de relatoria do Ministro Luis Felipe Salomão:

(...) é possível concluir que o dano ‘moral’ se caracteriza pela ofensa a determinados direitos ou interesses. O evento danoso não se revela na dor, no padecimento, que são, na verdade, consequências do dano, seu resultado. (...) Isso porque a configuração do dano ‘moral’ não se verifica no aborrecimento, no constrangimento por parte do prejudicado, mas, ao revés, o dano se caracteriza pelo ataque a direito personalíssimo, no momento em que ele é atingido³⁰.

Assim, diante da evidente prescindibilidade da afetação do estado anímico do sujeito para identificação de dano extrapatrimonial, o que se submete a criterioso processo de produção de prova é a violação do direito, os fatos que dão causa à afetação da personalidade³¹.

Por fim, faz-se importante ressaltar, novamente, que a alta elasticidade que guarda o instituto jurídico sob análise não o faz tutelar todo e qualquer tipo de dissabores do cotidiano. Nesse sentido, ressaltou Cavalieri:

29 MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9, p. 7073-7121, 2014, p.7092

30 BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.245.550 MG – Minas Gerais**. Relator: Min. Luis Felipe Salomão, 17 de março de 2015. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201100391454&dt_publicacao=16/04/2015. Acesso em: 28 jun. 2023.

31 MIRAGEM, Bruno. **Direito Civil**: responsabilidade civil. Rio de Janeiro: Forense, 2021. p. 104.

(...) mero dissabor, aborrecimento, mágoa, irritação ou sensibilidade exacerbada estão fora da órbita do dano moral, porquanto, além de fazerem parte da normalidade do nosso dia a dia, no trabalho, no trânsito, entre os amigos e até no ambiente familiar, tais situações não são intensas e duradouras a ponto de romper o equilíbrio psicológico do indivíduo. Se assim não se entender, acabaremos por banalizar o dano moral, ensejando ações judiciais em busca de indenizações pelos mais triviais aborrecimentos³².

Desse modo, tem-se que o dano extrapatrimonial caracteriza-se pela violação a um direito da personalidade, cuja relevância jurídica deve sobrepor-se à necessária tolerância às adversidades da vida em sociedade.

O dano extrapatrimonial presumido

O refinamento do instituto jurídico sob análise encontrou bastantes empecilhos na doutrina brasileira. Isso porque, inicialmente, esteve substancialmente influenciado pela vertente subjetiva³³ de compreensão do dano extrapatrimonial³⁴ e, a partir desse entendimento, a pessoa teria de comprovar que sofreu uma afetação em seu estado anímico. Nesse sentido, pontuou Gustavo Tepedino:

A afirmação do atributo *in re ipsa* traduziria, assim, bem-intencionada proposta de solução a obstáculo criado por essa própria linha de entendimento, consistente na dificuldade (quicá, impossibilidade) de a vítima comprovar concretamente a intensidade de seu sentimento de dor ou sofrimento. A afirmação de que os danos morais se manifestam

32 CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 15. ed. São Paulo: Atlas, 2021. p. 133.

33 A correlação entre a noção de dano extrapatrimonial *in re ipsa* e a vertente subjetiva do dano extrapatrimonial manifesta-se nitidamente em: CAMBI, Eduardo. **O dano moral *in re ipsa* e sua dimensão probatória na jurisprudência do STJ**. São Paulo: Revista dos Tribunais, 2019. p. 311-336.

34 TEPEDINO, Gustavo. Notas sobre o dano moral no direito brasileiro. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 30, p. 33-60, out./dez. 2021, p. 51.

in re ipsa serviria, então, a viabilizar a concessão da tutela reparatória sem a necessidade de se percorrer a via crucis da prova do abalo psicológico, sobretudo em hipóteses consideradas particularmente graves pelo julgador³⁵.

Com a superação dessa vertente subjetiva, todavia, essa construção de presunção relacionada à comprovação da dor ou sofrimento tornou-se dispensável ao direito. De modo que, o reconhecimento da feição objetiva do dano extrapatrimonial determinou também uma nova formulação quanto à possibilidade de reconhecê-lo *in re ipsa*.

Destarte, quando se está a tratar do dano extrapatrimonial presumido, é imprescindível que se tenha claro ao que é atribuída esta presunção, sob pena de, novamente, incumbi-la a aspectos subjetivos³⁶. A partir da perspectiva objetiva, tem-se que esta presunção vai se estabelecer em relação ao dano, tão somente; isto é, a partir de determinado fato ofensivo a violação a um direito da personalidade será presumida, não sendo necessário, portanto, comprová-la.

Assim, o conteúdo conceitual desse instituto jurídico vai estabelecer que se trata de uma modalidade de dano em que é dispensada a necessidade de provar a lesão a interesses juridicamente tutelados atinentes à personalidade, porquanto decorre do simples fato ou da simples situação da coisa³⁷. Nas palavras de Cavalieri, o dano extrapatrimonial *in re ipsa* decorre “inexoravelmente do próprio fato ofensivo, de tal modo que, provada a ofensa, *ipso facto* estará demonstrado o dano ‘moral’ à guisa de uma presunção na-

35 TEPEDINO, Gustavo. Notas sobre o dano moral no direito brasileiro. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 30, p. 33-60, out./dez. 2021, p. 51.

36 Nesse sentido, já preconizava Anderson Schreiber: “Na teoria do dano *in re ipsa* parece, contudo, residir um grave erro de perspectiva, ligado à configuração do dano moral com base na dor, sofrimento e humilhação. Por essa ótica, parece mesmo que a prova do dano deve ser dispensada, na medida em que seria inusitado e, antes disso, ineficaz exigir que a vítima prove que sofreu, seja porque dor e sofrimento são fatos inteiramente subjetivos, seja porque, nessa condição, são facilmente simuláveis”. SCHREIBER, Anderson. **Manual de Direito Civil Contemporâneo**. 5ª ed. São Paulo: Saraiva, 2022. p. 254.

37 TARTUCE, Flávio. **Responsabilidade Civil**. Rio de Janeiro: Forense, 2022. p.309.

tural, uma presunção *hominis ou facti* que decorre das regras da experiência comum”³⁸.

O entendimento do Superior Tribunal de Justiça (STJ), relativamente à inscrição indevida em cadastro de inadimplentes, bem demonstra a caracterização dessa figura jurídica. A Ministra Nancy Andrighi, quando do julgamento do Recurso Especial n. 994.253, reforçou que “A jurisprudência do STJ é uníssona no sentido de que a inscrição indevida em cadastro restritivo gera dano moral *in re ipsa*, sendo despicienda, pois, a prova de sua ocorrência”.

Nesse caso, evidente que a mera inscrição, ainda que indevida, não enseja lesão a quaisquer atributos da personalidade. Ocorre que, a partir das regras da experiência comum, é possível presumir que tal dano ocorrerá em decorrência deste ato ilícito.

À luz dessa acepção, tem-se como dispensável a comprovação de lesão a honra objetiva³⁹, exemplificativamente, em uma hipótese em que a pessoa, ao pretender adquirir um bem, tem o crédito negado por ter-lhe sido atribuída a característica de má pagadora. Nesse caso, a prova do dano (ofensa à honra objetiva) não é necessária, porquanto é corolário lógico da inscrição indevida.

Esse entendimento torna-se mais claro quando se atenta para a Súmula 385 do STJ, a qual dispõe que “Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento”. Ora, evidente que se a pessoa já possuía registros pretéritos que a qualificava como má pagadora, não há se falar em quaisquer presunções relativamente a danos extrapatrimoniais, restando ao sujeito pretensões que desbordam da figura jurídica do dano extrapatrimonial *in re ipsa*.

38 CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 15. ed. São Paulo: Atlas, 2021. p. 136.

39 “De natureza social, ou objetiva, que expressa o direito da pessoa ao reconhecimento social dos atributos de que efetivamente seja titular, ou ao menos, de não lhe ser atribuídas qualidades que possam dissociar suas características pessoais e de caráter e aquelas que são divulgadas na comunidade (honra objetiva)”. MIRAGEM, Bruno. **Teoria Geral do Direito Civil**. Rio de Janeiro: Forense, 2021. p. 216.

O bem jurídico tutelado pela lei geral de proteção de dados

A compreensão quanto ao escopo da norma ora analisada e a disciplina por ela abrangida faz-se necessária, pois, não seria possível definir os critérios para a caracterização do dano extra-patrimonial – sobretudo aferir a possibilidade de reconhecimento de um dano presumido – sem que se estabelecesse o bem jurídico tutelado pela Lei.

O conteúdo conceitual dos dados pessoais e as hipóteses de tratamento irregular

Na correta inteligência doutrinária, tem-se que “o regime jurídico da proteção de dados depende, naturalmente, do que se considera um dado pessoal e de quais tipos de processamento de dados são contemplados pela regulação”⁴⁰.

Não obstante a definição acerca do que seriam dados pessoais já ter sido explorada na parte introdutória deste artigo⁴¹, cumpre ressaltar que, dentre eles, há uma categorização que visa distinguir dados considerados “comuns” dos compreendidos como “sensíveis”. Os dados pessoais sensíveis destacaram-se porquanto “apresentam potencial de dano qualificado no que tange à pessoa humana”⁴²; a sua definição, conforme art. 5º, inciso II, da LGPD, é expressiva:

Dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural.

40 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 55.

41 Vide “Introdução”, *supra*.

42 KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados e sua repercussão no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 446.

Destarte, em que pese sejam dados cujo conteúdo oferece especial vulnerabilidade deflagrada pela discriminação⁴³, a natureza desses dados, por si, não é critério a ensejar quaisquer distinções quanto à possibilidade de ocorrência de um dano extrapatrimonial *in re ipsa*.

Essa assertiva pode parecer confusa, ou até mesmo contraditória, afinal, se um dado de determinada natureza revela maior potencialidade de dano não faria sentido, em uma primeira leitura, não conceder a ele também maior tutela. Todavia, há pelo menos duas premissas que evidenciam a fragilidade dessa narrativa. A primeira, que não pode ser negligenciada no âmbito do Big Data⁴⁴, diz respeito ao fato de que dados considerados comuns, a depender das circunstâncias do tratamento e da base de dados a que se tem acesso, podem revelar um dado compreendido como sensível. Isso porque uma opinião política ou convicção religiosa pode ser identificada, sem maiores dificuldades, a partir das interações de uma pessoa nas redes sociais.

A segunda, por sua vez, vai estabelecer que um dado considerado sensível pela Lei pode não apresentar qualquer vulnerabilidade ao titular; enquanto, para determinada pessoa, tal vulnerabilidade pode ser revelada por um dado considerado comum. Essa hipótese relaciona-se com um aspecto mais contextual dos dados pessoais e pode ser facilmente ilustrada.

Cite-se, a título exemplificativo, que um dado relativo à filiação sindical de uma pessoa militante não se mostra, *a priori*, sensível, porquanto tornado público, pelo próprio titular, em defesa de uma pauta social. Por outro lado, se essa mesma pessoa sofre com ameaças constantes, o fornecimento da sua geolocalização, dado considerado comum para a LGPD, pode ocasionar um assassinato⁴⁵.

43 BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2021. p. 83.

44 De acordo com o glossário IT, Big Data pode ser considerado “ativos de informação de alto volume, alta velocidade e alta variedade que exigem formas inovadoras e econômicas de processamento de informações para uma melhor percepção da tomada de decisão”. Disponível em: <https://www.gartner.com/en/information-technology/glossary/big-data>. Acesso em 02 de maio de 2023.

45 MARCON, Daniele Verza. Dano moral e vazamento de dados: o STJ escreveu

A despeito de a legislação não ter tratado diretamente sobre o assunto, é possível extrair de seu texto tal compreensão, uma vez que, caso fosse admitido o entendimento de que há dois níveis de proteção estabelecidos pela LGPD, ter-se-ia que conceber as hipóteses elencadas pelo art. 5º, inciso II, como um rol taxativo, o que vai de encontro não apenas com o entendimento doutrinário sobre o tema⁴⁶, mas, principalmente, com a construção feita pela própria Lei. Isso porque, conforme art. 11, §1º, “aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica”.

À vista disso, tem-se que a categorização proposta pela Lei tem o intuito de limitar o acesso a tais dados, restringindo as hipóteses que autorizam o seu tratamento, isto é, visa qualificar de forma mais restrita o consentimento do titular dos dados sensíveis e afastar as hipóteses de legítimo interesse. Essa distinção, no entanto, não produz efeitos no campo da responsabilização civil, porquanto a gravidade de um tratamento irregular só poderá ser aferida, como visto alhures, a partir de uma análise contextual das informações que poderiam ser extraídas daquela base de dados e do que elas representam para aquele titular em específico.

Os tipos de processamento de dados contemplados pela regulação, por sua vez, são todas as operações realizadas para/com dados pessoais do titular, conforme visto na parte introdutória deste artigo⁴⁷. Destarte, esse tratamento será irregular em duas hipóteses: quando violar a legislação e quando não fornecer a segurança esperada pelo titular⁴⁸ – esta última deve ser cumulada com a adoção de medidas de segurança aptas a proteger os dados pessoais, prevista no art. 46 da LGPD.

certo por linhas tortas? **Revista Consultor Jurídico**, abr. 2023. Disponível em: <https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados>. Acesso em: 20 abr. 2023.

46 Acerca do tema, v. MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, São Paulo, ano XXXIX, n. 144, p. 47-53, nov. 2019.

47 Vide Introdução, *supra*.

48 Art. 44, incisos de I a III e par. ún. da Lei 13.709/2018.

A primeira hipótese guarda menos complexidade, afinal, a inobservância da Lei que regulamenta a proteção de dados pessoais, evidentemente, acarreta um tratamento irregular. A segunda, todavia, gera certa confusão quando não interpretada de forma acurada. Com efeito, poder-se-ia questionar tanto o que “a segurança que o titular dele pode esperar” representa, quanto se esta não coincide, justamente, com a adoção de medidas de segurança aptas a proteger os dados pessoais; a resposta, contudo, é negativa.

O critério de irregularidade de tratamento apresentado pelo art. 46 é amplíssimo e tem por finalidade estabelecer um conceito mínimo que será elaborado pelo art. 44; ora, seria realmente ilógico pensar que o agente teria de adotar medidas inaptas para proteger os dados pessoais, mas o universo das medidas aptas, por outro lado, é demasiadamente amplo⁴⁹. Assim, tem-se que o critério determinado pelo não fornecimento da segurança que o titular dele poderia esperar revela um filtro jurídico, qual seja, de uma expectativa juridicamente legítima⁵⁰.

Dessa forma, o tratamento será irregular quando violar o que está previsto na Lei e quando ofender a legítima expectativa de segurança do titular dos dados pessoais.

A categoria jurídica dos dados pessoais

A Lei Geral de Proteção de Dados, em seu art. 1º, estabelece que seu objetivo é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

De início, é possível aferir que a proteção de dados pessoais se relaciona intrinsecamente com os direitos da personalidade. Nesse contexto, a alocação dos dados pessoais em si na categoria jurídica dos direitos da personalidade não é motivo de divergência na dou-

49 BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, a. 9, n. 3. 2020, p. 13. Disponível em: <http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/>. Acesso em: 03 mar. 2023.

50 Id. *ibid.*, p. 14.

trina. Interessa, portanto, organizar o objeto jurídico na classificação pretendida, de modo a explorar o porquê dessa configuração.

Destarte, o livre desenvolvimento da personalidade da pessoa natural está previsto não apenas como objetivo, mas também como fundamento da Lei Geral de Proteção de Dados⁵¹. A sua relevância justifica-se, pois, a LGPD buscou impedir que a liberdade do indivíduo fosse tolhida em razão da manipulação de terceiros que, na posse de informações do titular sem o seu conhecimento, acabavam por induzi-lo⁵².

Com efeito, essa noção de decisão livre e racional da pessoa a quem os dados digam respeito – assim como a de poder jurídico relativo à determinação da possibilidade, finalidade e limites da utilização dos dados pessoais – não surgiu com a edição da LGPD⁵³. As primeiras discussões sobre o tema deram-se por influência do direito comparado, mais propriamente, a partir da dogmática alemã que, pioneira no desenvolvimento deste fundamento, consagrou o direito à autodeterminação informativa (*informationelles Selbstbestimmungsrecht*).

51 Lei 13.709/2018: “Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais”.

52 Em tal perspectiva, ressalta Fabiano Menke: “Uma das preocupações fundamentais da disciplina da proteção de dados é a de que o indivíduo não seja manipulado por informações que os seus interlocutores (sejam eles entes estatais ou privados) tenham sobre a sua pessoa, sem que ele saiba disso. Nestes casos de conhecimento prévio de informações sobre a outra parte, o detentor da informação invariavelmente se coloca numa posição privilegiada. Ele atalha caminhos, adquirindo a possibilidade de manipulação e de direcionamento. Pode fazer perguntas colocações e perguntas dirigidas, pois todo um caminho que teria de ser traçado para que chegasse a uma informação não precisa ser percorrido”. MENKE, Fabiano. *As origens alemãs e o significado de autodeterminação informativa*. In: MENKE, F.; DRESH, R. F. V. (Coord.). **Lei Geral de Proteção de Dados: aspectos relevantes**. São Paulo: Foco, 2021. p. 16.

53 MIRAGEM, Bruno. **Teoria Geral do Direito Civil**. Rio de Janeiro: Forense, 2021. p. 232.

O caso que deu azo a esse direito remonta ao ano de 1983 e teve como matéria de fundo diversas reclamações constitucionais que impugnavam a Lei Federal de Recenseamento alemã⁵⁴, editada em 1982. A decisão paradigmática do Tribunal Constitucional (*Volkszählungsurteil*) deu parcial procedência à demanda, para efeito de reconhecer a autodeterminação informativa como projeção do direito geral de personalidade⁵⁵.

Dentre os fundamentos utilizados, o entendimento de que a autodeterminação informacional era imprescindível para a participação dos cidadãos em questões públicas merece especial destaque, porquanto define que a sua inobservância acarreta violação também a outros direitos fundamentais. De acordo com o Tribunal:

Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e de quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros de comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação.

54 A Lei, aprovada por unanimidade tanto pelo Parlamento quanto pelo Conselho Federal, determinava a coleta de informações para fins de realização do censo populacional, ressalta-se que a recusa em as fornecer acarretava sanções. Dentre os dados que seriam coletados, citam-se os seguintes: nome completo, endereço, número de telefone, idade, estado civil, nacionalidade, religião, fonte principal de sustento, ocupação profissional, formação profissional e o tempo de sua duração, formação escolar, formação técnico-profissionalizante (se houvesse), endereço profissional ou do local de estudo, informações sobre os ramos de atuação do seu empregador, função desempenhada no emprego, meio de locomoção utilizado para ir ao trabalho ou ao local de estudos.

55 “O direito geral da personalidade protege elementos da personalidade que não estejam cobertos pelas garantias especiais de liberdade da Lei Fundamental. Na dogmática do direito geral da personalidade, é possível distinguir entre três categorias ou implementações, conforme o desenvolvimento do Tribunal Constitucional Federal: o direito à autodeterminação (*Recht der Selbstbestimmung*), o direito à autopreservação (*Recht der Selbstbewahrung*) e direito à autoapresentação (*Recht der Selbstdarstellung*)”. MENKE, Fabiano. As origens alemãs e o significado de autodeterminação informativa. In: MENKE, F.; DRESH, R. F. V. (Coord.). **Lei Geral de Proteção de Dados**: aspectos relevantes. São Paulo: Foco, 2021. p. 15.

(...)

Quem estiver contando que, por exemplo, a participação em uma assembleia ou em uma iniciativa popular pode ser registrada pelas autoridades, podendo lhe causar problemas (futuros), possivelmente desistirá de exercer seus respectivos direitos fundamentais (Art. 8, 9 GG). Isso não prejudicaria apenas as chances de desenvolvimento individual do cidadão, mas também o bem comum, porque a autodeterminação é uma condição funcional elementar para uma comunidade democrática e livre, fundada na capacidade de ação e participação de seus cidadãos⁵⁶.

Nesse diapasão, a autodeterminação informativa vai tratar do poder do indivíduo decidir acerca da divulgação e utilização de seus dados pessoais e, como visto, o seu surgimento esteve intimamente ligado à própria história da proteção da personalidade como direito fundamental, na medida em que se desenvolveu como um desdobramento do direito ao livre desenvolvimento da personalidade⁵⁷.

No contexto do processamento de dados, a tutela jurídica conferida aos dados pessoais impõe, indubitavelmente, uma nova fronteira aos direitos da personalidade⁵⁸, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, conseqüentemente, ao livre desenvolvimento de sua personalidade⁵⁹.

56 SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad-Adenauer-Stiftung, 2005. p. 237-238.

57 MENDES, Laura Schertel. Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da corte constitucional alemã. *In*: CUEVA, Ricardo Vilas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.). *Lei Geral de Proteção de Dados (Lei 13.709/2018) – A caminho da efetividade: contribuições para a implementação da LGPD*. São Paulo: Thomson Reuters, 2020. p. 177.

58 A propósito, a própria vinculação do conceito de dado pessoal à pessoa natural, identificada ou identificável, revela “o especial propósito de tutelar os dados pessoais como uma manifestação específica da ampla proteção assegurada à dimensão existencial da pessoa humana”. SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 333.

59 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do**

Com efeito, ainda que a LGPD tenha por objetivo a proteção da liberdade, da privacidade e do livre desenvolvimento da personalidade, a sua proteção jurídico constitucional não se resume, tampouco equivale-se, a esses direitos⁶⁰. A relevância de sua disciplina enquanto projeção de direitos fundamentais consagrados⁶¹ deu causa à Emenda Constitucional n. 115/2022, que reconheceu a proteção de dados pessoais como direito fundamental autônomo⁶².

Assim, ciente de que os dados pessoais assumem a feição de projeção da própria personalidade do titular, tem-se, portanto, que são destinatários da tutela conferida a outros bens da personalidade⁶³.

O dano extrapatrimonial decorrente do tratamento irregular de dados pessoais

A par de que o dano assume a feição de lesão a interesses juridicamente protegidos, cumpre esclarecer que a disciplina desse “interesse jurídico” será sempre determinada pela comunidade, porquanto trata-se de um reflexo daquilo que a sociedade considera digno de tutela jurídica⁶⁴. Nesse sentido, tem-se que a disse-

consentimento. Rio de Janeiro: Forense, 2021. p. 89.

60 Sobre a autonomia do direito fundamental à proteção de dados pessoais, v. SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 40-78.

61 “Relaciona-se com a proteção da vida privada e da intimidade (art. 5º, X, da Constituição da República), da dignidade da pessoa humana (art. 1º, III), e contra a discriminação (art. 3º, IV), como expressões da liberdade e da igualdade da pessoa. A Constituição da República, igualmente, assegura como direito fundamental a inviolabilidade do sigilo de dados (art. 5º, XII)”. MIRAGEM, Bruno. **Direito Civil: responsabilidade civil**. Rio de Janeiro: Forense, 2021. p. 493.

62 “É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”, art. 5º, inciso LXXIX, da Constituição Federal.

63 DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre a proteção de dados pessoais** – Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação [recurso eletrônico]. São Paulo: Expressa, 2022. p. 31.

64 MARTINS-COSTA, Judith. Os danos à pessoa no direito brasileiro e a natureza

minação e a democratização do acesso às novas tecnologias – que, por consequência, ocasionou o surgimento de novos riscos à proteção da personalidade dos indivíduos⁶⁵ –, culminou no reconhecimento da proteção de dados pessoais como parte integrante do patrimônio jurídico do seu titular.

Assim, ciente de que a infringência à norma que rege a proteção de dados pessoais pode lesionar direitos da personalidade, em virtude do bem jurídico tutelado por ela, tem-se que o tratamento indevido que venha a expor esses dados potencialmente preenche os pressupostos para a caracterização do dano extrapatrimonial.

Contudo, não necessariamente a violação à LGPD ou à expectativa legítima de segurança do titular dos dados vai dar causa ao dever de indenizar. Isso porque, para que o dado pessoal tratado irregularmente provoque uma afetação à dimensão existencial da pessoa humana, é necessário que haja o cerceamento daquilo que a Lei Geral de Proteção de Dados visou proteger: a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Destarte, o que irá determinar a ocorrência ou não desse cerceamento será a forma que o dado, inadvertidamente exposto, será utilizado e os riscos que ele apresenta para o titular. À vista disso, não é possível pré-definir uniformemente o potencial lesivo de um tratamento irregular, porquanto, ainda que exponha dados de mesma natureza, caso digam respeito a titulares diversos, a sua repercussão será diferente na esfera jurídica de cada um dos atingidos.

A Apelação Cível n. 10116844-03.2020.8.26.0068, julgada pelo Tribunal de Justiça do Estado de São Paulo⁶⁶, bem ilustra esse entendimento: a questão de fundo versa, em síntese, sobre a disponibilização de dados médicos mediante simples inserção de CPF e data de nascimento no site da prefeitura. Ocorre que o titular dos dados

de sua reparação. **Revista dos Tribunais**, São Paulo, v. 90, n. 789, p. 21-47, jul. 2001, p. 21.

65 RABAIOLI, Laiza. Da autodeterminação informativa ao consentimento: elementos balizadores da manifestação de vontade no tratamento de dados pessoais. Artigo não publicado, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2020, no original, p. 3.

66 BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível SP – São Paulo. Relatora: Heloísa Mimessi. 07 de julho de 2021. Disponível em: [link](#). Acesso em: 05 jan. 2023.

tratados irregularmente era portador do vírus HIV⁶⁷ e, em razão disso, realizava constantes consultas e exames médicos. Em dado momento, a sua supervisora passou a investigá-lo e, ao acessar o site da prefeitura, teve acesso à relação completa de todos os seus dados médicos. O autor afirma que teria pedido sigilo à supervisora, contudo, chegou a ser questionado posteriormente por outra funcionária sobre ser portador do vírus, sendo bem provável que os demais colegas de trabalho também tenham tido conhecimento. Pouco tempo depois, foi desligado da empresa e uma das motivações, segundo a própria supervisora, teria sido o tratamento médico.

Em seu voto, a Desembargadora Heloísa Mimessi acertadamente consignou que a forma como os dados eram tratados pela prefeitura tornava as informações, na prática, públicas e o vazamento do prontuário, *in casu*, “gerou situação embaraçosa e degradante no ambiente de trabalho, dada a desinformação e o indesejável estigma que, lamentavelmente, ainda grassam no meio social, com relação à citada condição de saúde”.

Indubitavelmente, os dados pessoais disponibilizados pela prefeitura deram causa à discriminação pela empregadora, razão pela qual é evidente o dano injusto ocasionado à esfera jurídica do titular dos dados decorrente da violação a sua legítima expectativa de segurança. No entanto, caso essas informações nunca tivessem sido acessadas, poder-se-ia falar em um dano extrapatrimonial decorrente da mera disponibilização? Ou, mudando o contexto do titular a quem a informação se relaciona, caso fosse uma pessoa perfeitamente saudável, qual seria possibilidade desse indivíduo sofrer qualquer lesão a um atributo da personalidade? Ou, ainda nessa hipótese, o acesso desses dados por terceiros apresentaria algum risco ao titular? Por fim, seria possível afirmar que todos os

67 De acordo com o Ministério da Saúde, “HIV é a sigla em inglês para vírus da imunodeficiência humana, causador da aids (da sigla em inglês para Síndrome da Imunodeficiência Adquirida), ataca o sistema imunológico, responsável por defender o organismo de doenças. Aids é a Síndrome da Imunodeficiência Humana, transmitida pelo vírus HIV, caracterizada pelo enfraquecimento do sistema de defesa do corpo e pelo aparecimento de doenças oportunistas”. Disponível em: <https://bvsm.sau.gov.br/hiv-e-aids/>. Acesso em: 29 jun. 2023.

cidadãos daquele município, que tivessem registro no mesmo portal, teriam pretensão indenizatória contra a prefeitura?

Esses questionamentos trazem maior concretude ao entendimento de que a capacidade de um tratamento indevido de dados pessoais ofender atributos da personalidade só pode ser aferida a partir de uma análise individual e contextualizada, visto que as informações que podem ser extraídas de uma base de dados e, principalmente, o risco que elas representam para cada titular em específico não podem ser pré-determinados uniformemente. Diante disso, é insustentável a afirmação de que todo tratamento irregular ocasionará um dano extrapatrimonial ao titular dos dados, considerando-o *in re ipsa*, porquanto eleva a discussão a uma generalidade incompatível com a disciplina da proteção de dados pessoais.

Recentemente, a 2ª Turma do Superior Tribunal de Justiça enfrentou o tema e, ainda que sob premissas questionáveis⁶⁸, concluiu que a inconveniente exposição de dados pessoais comuns, desacompanhados de comprovação do dano, não dava causa à obrigação de indenizar. De acordo com o Relator:

O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações⁶⁹.

Por fim, não se pode olvidar que há incidentes em que, ainda que tenha ocorrido um vazamento de dados pessoais, a leitura fica impossibilitada por estarem criptografados. Evidentemente,

68 Para uma análise pormenorizada das premissas adotadas no Acórdão e suas respectivas contradições, v. MARCON, Daniele Verza. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas? **Revista Consultor Jurídico**, abr. 2023. Disponível em: <https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados>. Acesso em: 20 abr. 2023.

69 BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619 SP – São Paulo**. Relator: Min. Francisco Falcão, 07 de março de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 18 mar. 2023.

essa hipótese de tratamento irregular não terá grande relevância, sendo dispensado até mesmo o dever de notificação, uma vez que o incidente relevante para a comunicação é aquele que atinge os titulares por meio da divulgação não autorizada de dados pessoais⁷⁰. Importa, contudo, mencioná-la, pois, a existência de tais casos demonstra, ao fim e ao cabo, ser essencialmente imprecisa a afirmação de que todo tratamento irregular seria capaz de ocasionar dano extrapatrimonial ao titular dos dados.

À vista disso, tem-se que o tratamento irregular de dados pessoais não irá, inexoravelmente, ocasionar uma afetação à personalidade do titular, sendo necessário que resulte do incidente de segurança a divulgação não autorizada de dados pessoais. Assim, a partir da análise contextual e individualizada dos dados expostos, será possível verificar se houve lesão a um atributo da personalidade ou não.

Considerações finais

Os danos extrapatrimoniais decorrentes do tratamento irregular de dados, assim como a gravidade dos incidentes – traduzida pela afetação que ocasiona na esfera jurídica do titular dos dados pessoais – permanecem, ainda, em construção no ordenamento jurídico brasileiro. Contudo, diante dos contornos que os dados pessoais assumiram e do modo que a proteção destes dados restou disciplinada pela LGPD, o reconhecimento de um dano extrapatrimonial presumido, à luz dos conceitos aqui explorados, mostra-se inadequado.

Com efeito, era imprescindível que houvesse uma interferência indevida no patrimônio jurídico dos titulares dos dados pessoais decorrente de todo e qualquer tratamento irregular, a fim de considerar o dano extrapatrimonial oriundo dele *in re ipsa*. Isso porque,

70 MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coord). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 362.

como visto, não é possível responsabilizar civilmente alguém por mera conduta, ainda que ilícita, que não ocasione lesão a um bem juridicamente tutelado.

Nesse sentido, o instituto da responsabilidade civil visa reparar/compensar o bem lesado, o que, no caso do dano extrapatrimonial, não se trata de mensurar o dano sofrido, mas de compensar com utilidade econômica o que se lesou no âmbito extrapatrimonial⁷¹; assim, não havendo lesão, também não há se falar em compensação.

Ante o exposto, conclui-se que a vagueza conceitual verificada no art. 42 da LGPD foi trazida propositalmente pelo legislador, a fim de que se estabelecesse uma cláusula geral de responsabilização civil. Assim, o caráter casuístico assumido pela previsão legal permite a aplicação concreta do instituto jurídico, uma vez que, com o rápido avanço da tecnologia da informação, seria impossível prever as hipóteses de caracterização do dano extrapatrimonial uma a uma na Lei.

Referências

- BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, a. 9, n. 3. 2020. Disponível em: <http://civilistica.com/responsabilidade-civil-na-proteção-de-dados-pessoais/>. Acesso em: 03 mar. 2023.
- BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2021.
- BISNETO, Cícero Dantas. **Formas não monetárias de reparação do dano moral: uma análise do dano extrapatrimonial à luz do princípio da reparação adequada**. Florianópolis: Tirant Lo Blanch, 2019.
- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 dez. 2022.
- BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em:

71 LÔBO, Paulo. **Direito Civil: obrigações**. 10 ed. São Paulo: Saraiva, 2022. v. 2. p. 353.

- https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 07 jan. 2023.
- BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 15 jan. 2023.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 27 dez. 2022.
- BRASIL. Senado Federal. **Proposta de Emenda Constitucional nº 17/2019**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0t1zu0ajget2o1jk7mm-52sogg288149.node0?codteor=1773684&filename=PEC+17/2%20019. Acesso em: 27 dez. 2022.
- BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 994.253 RS – Rio Grande do Sul**. Relatora: Min. Nancy Andrighi, 24 de novembro de 2008. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200702348176&dt_publicacao=24/11/2008. Acesso em: 08 jan. 2023.
- BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Relator: Min. Francisco Falcão, 07 de março de 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 18 mar. 2023.
- CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 15 ed. São Paulo: Atlas, 2021.
- COUTO E SILVA, Clóvis Veríssimo do. **O conceito de dano no direito brasileiro e no direito comparado**. Revista dos Tribunais, vol. 2, p. 333-348, jan./mar. 2015.
- DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre a proteção de dados pessoais – Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação [recurso eletrônico]**. São Paulo: Expressa, 2022.
- DONEDA, Danilo. **Da Privacidade à Proteção De Dados Pessoais**. 2 ed. São Paulo: Revista dos Tribunais, 2020.
- DRESCH, Rafael de Freitas Valle; FALEIROS JR., José Luiz de Moura. **Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados**. *In:*

- ROSENVALD, N.; DRESCH, R. F. V.; WESENDONCK, T. **Responsabilidade civil: novos riscos**. Indaiatuba: Editora Foco, 2019.
- FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1ed. São Paulo: Thomson Reuters Brasil, 2019a.
- FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. (coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1 ed. São Paulo: Thomson Reuters Brasil, 2019b.
- JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. In: MENKE, F.; DRESH, R. F. V. (coords.). **Lei Geral de Proteção de Dados: aspectos relevantes**. São Paulo: Foco, 2021.
- KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados e sua repercussão no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.
- LÔBO, Paulo. **Direito Civil**: obrigações. 10. ed. São Paulo: Saraiva, 2022. v. 2.
- MARCON, Daniele Verza. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas?. **Revista Consultor Jurídico**, abr. 2023. Disponível em: <https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados>. Acesso em: 20 abr. 2023.
- MARTINS-COSTA, Judith. Os danos à pessoa no direito brasileiro e a natureza de sua reparação. **Revista dos Tribunais**, São Paulo, vol. 90, n. 789, p. 21-47, jul. 2001.
- MARTINS-COSTA, Judith. Dano moral à brasileira. **Revista do Instituto do Direito Brasileiro**, ano 3, n. 9. p. 7073-7121. 2014.
- MENKE, Fabiano. As origens alemãs e o significado de autodeterminação informativa. In: MENKE, F.; DRESH, R. F. V. (coords.). **Lei Geral de Proteção de Dados: aspectos relevantes**. São Paulo: Foco, 2021.
- MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, Forense, 2021.

- MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.
- MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, vol. 1009, nov. 2019.
- MIRAGEM, Bruno. **Direito Civil**: responsabilidade civil. Rio de Janeiro: Forense, 2021.
- MIRAGEM, Bruno. **Teoria Geral do Direito Civil**. Rio de Janeiro: Forense, 2021.
- MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, set./dez. 2018.
- MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. São Paulo, **Revista do Advogado**, ano XXXIX, n. 144, nov. 2019.
- MULHOLLAND, Caitlin Sampaio. **Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)**. [Rio de Janeiro]: PUC-Rio, 2021. Disponível em: [IBERC_Responsabilidade-civil-e-dadossensíveis-CaitlinMulholland.pdf](#). Acesso em: 05 jan. 2023.
- RABAIOLI, Laiza. **Da autodeterminação informativa ao consentimento: elementos balizadores da manifestação de vontade no tratamento de dados pessoais**. Artigo não publicado, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2020, no original.
- RABAIOLI, Laiza; LOPES, Luiza Cauduro. Os conceitos gerais da Lei Geral de Proteção de Dados: noções instrumentais sobre o tratamento de dados pessoais. *In*: MENKE, F.; DRESH, R. F. V. (coords.). **Lei Geral de Proteção de Dados: aspectos relevantes**. São Paulo: Foco, 2021.
- SANSEVERINO, Paulo de Tarso Vieira. **Princípio da Reparação Integral** – indenização no Código Civil. São Paulo: Saraiva, 2010.
- SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, Forense, 2021.
- SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES, O. L. (coords.). **Tratado de proteção de dados pessoais**. Rio de Janeiro, Forense, 2021.

- SCHREIBER, Anderson. **Manual de Direito Civil Contemporâneo**. 5 ed. São Paulo: Saraiva, 2022.
- SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad-Adenauer-Stiftung, 2005.
- TARTUCE, Flávio. **Responsabilidade Civil**. Rio de Janeiro: Forense, 2022.
- TEPEDINO, Gustavo. Notas sobre o dano moral no direito brasileiro. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 30, p. 33-60, out./dez. 2021.
- VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. 2007. Dissertação (Mestrado) – Curso de pós-graduação stricto sensu em Direito, Estado e Sociedade: Políticas Públicas e Democracia, Universidade de Brasília, Brasília, 2007.



3º lugar

O tratamento de dados pessoais de crianças e adolescentes: análise das bases legais juridicamente válidas

Júlia Teixeira de Barros Francatto ✦

Resumo

A referida monografia foi realizada como o intuito de analisar, por uma perspectiva doutrinária, jurisprudencial e internacional, as três hipóteses legais, previstas pelo Estudo Preliminar da Autoridade Nacional de Proteção de Dados, aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, conforme regulado pela Lei nº 13.709/2018, sejam elas: (i) a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças; (ii) a aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, mediante a sua equiparação aos dados sensíveis; e (iii) a aplicação das hipóteses legais previstas nos artigos. 7º e 11 da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse. Ainda, busca compreender o princípio do melhor interesse, bem como o paradigma do consentimento e o legítimo interesse.

Introdução

Com o progresso tecnológico, a sociedade se viu imersa a um ambiente virtual, no qual tornou-se possível encontrar novas formas de veiculação e obtenção de informações sobre as pessoas. Tal desenvolvimento foi o principal vetor para o advento de um regime de direitos, com o fim de respeitar os princípios da finalidade, livre acesso, transparência, segurança e qualidade/correção dentro da esfera virtual, princípios norteadores do tratamento da informação¹.

No Brasil, a proteção de dados é associada ao direito à privacidade². A proteção desse direito é respaldada por previsão constitucional e tem sua menção no artigo 21 do Código Civil de 2002. No entanto, a proteção à privacidade não foi capaz de suprir as necessidades que surgiram com o advento da Internet e seus desdobramentos.

Nas últimas décadas, a Internet passou por intensos aprimoramentos, os quais foram capazes de alterar tanto a relação entre os usuários, quanto a maneira como estes são vistos por empresas e novas tecnologias³. Com o aparecimento das novas necessidades, observou-se a carência de uma lei capaz de regulamentar as atividades no ambiente virtual. Em vista disso, surgiu o Marco Civil da Internet (Lei 12.965/2014)⁴, o qual foi pioneiro no Brasil em disciplinar, por meio de direitos e deveres, as relações jurídicas-virtuais

1 HOOFNAGLE, Chris Jay. **The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)** (July 15, 2014). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418. Acesso em: 11 mai. 2023

2 BIONI, Bruno. **Tratado de Proteção de Dados Pessoais: A função e os limites do consentimento**. São Paulo: Editora Forense, 2020. p. 63-77.

3 LOREZON, Laila Neves. Análise Comparada entre Regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus Respectivos Instrumentos de *Enforcement*. **Revista do Centro de Excelência Jean Monnet da FGV Direito Rio**, Rio de Janeiro, v. 1, p. 39-52, mar. 2021, p. ?. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423>. Acesso em: 11 mai. 2023

4 BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: [?].

entre os usuários e os fornecedores de serviços na Internet. No entanto, a lei deixou uma lacuna: a forma com que os dados fornecidos pelos usuários poderiam ser utilizados, notadamente fora do ambiente virtual. Assim, em 2018, surgiu a Lei Geral de Proteção de Dados – Lei 13.709/2018 (LGPD)⁵, com inspiração no Regulamento Geral de Proteção de Dados europeu (GDPR).

Tanto a LGPD, quanto o GDPR são leis de proteção de dados que buscam determinar como as empresas e pessoas naturais devem tratar dados pessoais. De maneira semelhante, a legislação brasileira e a europeia, trazem alguns princípios que regem a utilização de dados, quais sejam, responsabilização e prestação de contas, finalidade legítima, adequação, necessidade, prevenção, não discriminação e livre acesso⁶.

Tendo em vista isso, a LGPD e a GDPR surgem a fim de permitir um melhor controle dos dados que são tratados, impor deveres e responsabilidades aos responsáveis pelo tratamento e fornecer segurança na circulação dessas informações. Sendo que o modelo estabelecido no Brasil, privilegia a prevenção de danos à pessoa humana e a segurança no tratamento de dados pessoais, instituindo deveres e responsabilidades específicas aos agentes^{7/8}, além do amplo rol de princípios e direitos aos titulares dos dados.

A discussão se torna específica quando se refere ao tratamento desses dados de crianças e adolescentes. Isso porque, a legis-

5 BRASIL. **Lei 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: [?]

6 BRANCHER, Paulo Marcos Rodrigues; KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer Costa; BRANCHER, Paulo Marcos Rodrigues. Princípios gerais de proteção de dados pessoais: uma análise dos princípios elencados no Art. 6º da Lei nº 13.709/2018 (LGPD). *In*: BEPPU, Ana Claudia; BRANCHER, Paulo Marcos Rodrigues (coord.). **Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018**. Belo Horizonte: Fórum, 2019. Disponível em: [link] Acesso em: 11 de mai. 2023

7 O caráter preventivo da LGPD é lembrado, por exemplo, nos seguintes dispositivos: arts. 6º, II, VI, VII, VIII e X, 44, 46, 47, 48, 49; e 50.

8 TEPEDINO, Gustavo; TEFFÉ, Chiara Spaccacini. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 25, n. 3, p. 83-116, jul./set. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521>. Acesso em: 11 mai. 2023.

lação brasileira confere proteção integral, especial e prioritária às pessoas que estão em condições de desenvolvimento e que não podem ser consideradas absolutamente responsáveis e capazes de discernimento, classificadas como absoluta ou relativamente incapazes pelo Código Civil brasileiro, conforme os artigos 3º e 4º. Essa dimensão protetiva prioritária se reflete na regulamentação do tratamento de seus dados pessoais.

No âmbito internacional, tanto a GDPR, quanto a Lei de Proteção da Privacidade Online das Crianças (em inglês, *Children's Online Privacy Protection Act*) dos Estados Unidos, reconhece que o contexto atual de maior facilidade de acesso a serviços e aplicações de internet, aumenta a exposição dos direitos e liberdades de crianças e adolescentes, de forma que se vê necessário uma proteção especial.

No Brasil, o debate acerca da adequação do tratamento de dados pessoais de crianças e adolescentes é protegido conforme o disposto no artigo 14 da LGPD. A legislação brasileira se adequa ao posicionamento internacional e estabelece que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse. Tal princípio é reconhecido inclusive, na Constituição Federal em seu artigo 227^{9/10}, à medida que determina que deverá ser observado seu melhor interesse, tornando as crianças e adolescentes sujeitos de direitos e titulares de direitos fundamentais.

O princípio do melhor interesse da criança foi incorporado na Declaração dos Direitos da Criança em 1959 e posteriormente na Convenção Internacional dos Direitos da Criança, a qual foi ratificada pelo Brasil em 1990 por meio do Decreto nº 99.710. Tal princípio deve ser analisado em cada contexto específico, levando em consideração sua dinamicidade.

9 BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 11 mai. 2023.

10 Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

A Convenção Internacional dos Direitos da Criança, consignou que *“todas as ações relativas à criança, sejam elas levadas a efeito por instituições públicas ou privadas de assistência social, tribunais, autoridades administrativas ou órgãos legislativos, devem considerar primordialmente o melhor interesse da criança.”*¹¹ Assim, o Comitê dos Direitos da Criança da ONU tratou de caracterizar o princípio do melhor interesse como um conceito de natureza tripla e, portanto, passível de ser considerado um direito subjetivo, um princípio jurídico fundamentalmente interpretativo ou uma regra processual.

Como direito subjetivo, o melhor interesse das crianças deve ser considerado primordial quando estejam em situações em que haja divergência de interesses, de modo a garantir que esse direito sempre seja aplicado quando se tratar de situações que afetem a criança.

Como princípio jurídico fundamentalmente interpretativo, o princípio do melhor interesse, em disposições que possam ser interpretadas por mais de uma via, deve ser sempre escolhido, a fim de garantir o interesse superior da criança.

Por fim, o princípio do melhor interesse como uma regra processual é considerado em processos nos quais devam incluir uma análise do possível impacto a ser gerado na criança. Assim, os Estados-partes deverão explicar como é que o direito foi respeitado na decisão e o que foi considerado como sendo do interesse superior da criança¹².

A legislação brasileira, ao propor a regulamentação do tratamento dos dados pessoais de crianças e adolescentes, consignou expressamente o consentimento como meio adequado para se atingir o melhor interesse da criança e do adolescente nos casos em que o tratamento de seus dados pessoais possa os atingir e influenciar diretamente.

11 UNICEF. **Convenção sobre os Direitos da Criança**. Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>. Acesso em: 11 mai.2023

12 UNITED NATIONS. **General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration**. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em: 11 mai. 2023

Deve-se, porém, refletir sobre as insuficiências do consentimento, uma vez que os pressupostos que definem o paradigma do consentimento mostram-se inadequados para proporcionar um regime de proteção efetivo e concreto, principalmente no que se refere ao controle verdadeiro do fluxo de dados pessoais por parte de seus titulares. Especialmente no caso de crianças e adolescentes, diante da vulnerabilidade dos titulares dos dados pessoais a serem tratados, devem ser debatidas a interpretação ou as possíveis reformas no artigo 14 da Lei Geral de Proteção de Dados Pessoais, com o fim de otimizar o tratamento de dados pessoais desse grupo social, buscando sempre atingir o seu melhor interesse – princípio norteador da LGPD.

Diante da divergência acerca das hipóteses legais válidas para o tratamento de dados pessoais e crianças e adolescentes, identificam-se ao menos três interpretações relevantes, as quais foram objeto de estudo da ANPD (Autoridade Nacional de Proteção de Dados, 2022)¹³. Confira-se:

- (i) a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças;
- (ii) a aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, mediante a sua equiparação aos dados sensíveis; e
- (iii) a aplicação das hipóteses legais previstas nos arts. 7º e 11 da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse.

A presente monografia propõe-se, assim, a analisar as hipóteses legais aplicáveis ao tratamento de dados de crianças e ado-

13 ANPD – Autoridade Nacional de Proteção de Dados Pessoais. **Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.** Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf>. Acesso em: 11.5.2023

lescentes através de métodos e tipos interpretativos, além de uma perspectiva jurisprudencial, doutrinária e internacional.

Métodos e tipos interpretativos a serem utilizados na regulamentação do tratamento de dados de crianças e adolescentes

De modo a interpretar a Lei Geral de Proteção de Dados, no que tange à proteção de dados de crianças e adolescentes, é preciso, antes de tudo, compreender qual o tipo e o método interpretativo mais adequado para ser utilizado. Dentre os tipos de interpretação consagrados pela doutrina jurídica, mostram-se relevantes para o propósito deste trabalho a interpretação *especificadora*, a interpretação *restritiva* e a interpretação *extensiva*.

A interpretação *especificadora* “parte do pressuposto que o sentido da norma cabe na letra do enunciado”, isto é, o conteúdo disposto em lei está de acordo com *a mens legis*, fazendo com que caiba ao legislador apenas compreendê-la, sem que haja necessidade de desdobramentos de seus significados.

A interpretação *restritiva* se limita àquilo escrito em norma, mesmo que haja possibilidade para ampliar seu significado. Assim, o tipo restritivo de interpretação trata a *mens legis* como algo que independe da vontade do legislador.

Por fim, há a interpretação *extensiva*, na qual amplia-se “o sentido da norma para além daquilo contido em sua letra”¹⁴. Dessa maneira, o intérprete passa a codificar a mensagem no sentido estrito, buscando ampliá-la. Assim, por meio da interpretação extensiva, o intérprete passa a ter o trabalho de tornar normas limitadas em vagas e amplas.

14 FERRAZ JR., Tércio Sampaio. **Introdução ao estudo do direito**: técnica, decisão e dominação. 3. ed. São Paulo: Atlas, 2001. p. 251-293.

No entanto, diferentemente da interpretação por analogia, a interpretação extensiva apenas busca ampliar o sentido da norma, para abranger um significado que já estava tipificado em lei, mas que apenas não havia sido explicitado pelo legislador, não cabendo, portanto, a esse tipo de interpretação ampliar o sentido da norma para encaixar um significado sem precedentes, caso que ocorre na interpretação por analogia.

Conforme explicitado adiante, dentre as hipóteses de interpretação do artigo 14º da Lei Geral de Proteção de Dados, a única que se presta a ampliar o sentido da norma, com o fim de englobar outros significados já amparados por lei, é a *extensiva*, uma vez que permite aplicar as hipóteses legais previstas nos artigos 7º e 11 da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse. Tal princípio deve ser garantido e, para isso, não é possível que o artigo 14º da LGPD seja aplicado estritamente.

Não obstante, é necessário também identificar o melhor método interpretativo a ser utilizado. Por se tratar de uma questão puramente pragmática, a interpretação do tratamento de dados pessoais de crianças e adolescentes deverá procurar suprir a falha nos símbolos comunicacionais na relação de comunicação entre emissores e receptores das mensagens normativas. Tal premissa é abordada no método interpretativo *teleológico-axiológico*. Isso porque, nesse método interpretativo, leva-se em conta as consequências geradas pela norma, retornando ao interior do sistema e, assim, pode ser equiparada à tentativa de prever as consequências da norma que vão, futuramente, fundamentar as decisões dos conflitos.

Portanto, diante do fato de que as divergentes hipóteses de interpretação do artigo 14º da LGPD já estão gerando controvérsias e, conseqüentemente, dando margem a futuros problemas na uniformização de decisões judiciais, é preciso adotar o método de interpretação *teleológico e axiológico*, a fim de resolver tais problemas pragmáticos, visando os fins sociais.

Logo, torna-se necessária a utilização de uma interpretação *extensiva, teleológica-axiológica* para se compreender integralmente

a proteção de dados de crianças e adolescentes, justificada pela ineficiência dos demais tipos e métodos interpretativos que serão, a seguir, demonstrados.

Interpretação restritiva como hipótese para o tratamento de dados pessoais de crianças e adolescentes

A aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças e adolescentes, decorre de uma interpretação restritiva do art. 14º, visto que aborda como única hipótese legal o disposto no texto da lei.

A Lei Geral de Proteção de dados destina o capítulo II ao tratamento de dados pessoais de crianças e adolescentes, o qual dispõe:

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. [...]

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

Assim, o art. 14 §1º da LGPD destaca que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico dos pais ou do responsável legal, exceto quando a coleta for necessária para contatar os pais ou o responsável legal, conforme disposto no §3º.

Se tal norma for interpretada restritivamente, o tratamento desses dados seria realizado unicamente pelo consentimento dos responsáveis. No entanto, a partir da análise da eficácia social desse tipo interpretativo, é possível encontrar lacunas sociojurídicas.

A empresa Purple, que fornece serviço de internet grátis e hotspots para lojas e áreas públicas, procurou fazer um experimento social, que tinha como fim comprovar que as pessoas não leem os termos de contrato e consentem com qualquer coisa escrita. Dentre as 22 mil pessoas que participaram do experimento, apenas uma foi capaz de identificar uma cláusula que previa que, para acessar os hotspots da marca, o usuário deveria aceitar cumprir mil horas de serviço comunitário¹⁵.

Além disso, em uma pesquisa realizada pela Deloitte em 2017, foi constatado que 91% dos usuários dizem concordar com os termos de uso das plataformas que utilizam, sem nunca sequer terem lido, e quando se trata de pessoas jovens (entre 18 e 34 anos de idade) esse percentual chega a 97%¹⁶.

Diante de tais fatos, demonstra-se a insuficiência do consentimento para garantir um regime protetivo efetivo e material, em especial, para assegurar um verdadeiro controle sobre o fluxo de dados pessoais pelo seu titular. Especialmente nos casos em que são tratados dados de crianças e adolescentes, diante do fato de se tratar de incapazes absolutos e relativos, a proteção deveria ser reforçada, objetivo que não é atingido apenas com o consentimento dos responsáveis legais.

Na contemporaneidade, o consentimento é utilizado como instrumento de regulação e legitimação do regime protetivo de dados pessoais, interpretado como expressão da autonomia individual e do controle do titular dos dados em torno de seus direitos

15 SEM ler os termos de uso, mais de 20 mil pessoas se inscrevem em serviços comunitários. **Estadão**, 13 jul. 2017. Disponível em: <https://www.estadao.com.br/emails/comportamento/sem-ler-os-terminos-de-uso-mais-de-20-mil-pessoas-se-inscrevem-em-servicos-comunitarios/>. Acesso em: 11 mai. 2023.

16 É fundamental ler contratos, termos de uso e políticas de privacidade. **ABEINFO**, 30 out. 2020. Disponível em: <https://abeinfo brasil.com.br/e-fundamental-ler-contratos-terminos-de-uso-e-politicas-de-privacidade/>. Acesso em: 11 mai. 2023.

de personalidade¹⁷. Não obstante, diante do desenvolvimento da publicidade comportamental e do aumento do monitoramento de usuários pela Internet, a hipótese do consentimento como medida protetiva passou a ser questionada, de modo a necessitar a revisão de seu protagonismo na legislação que rege a proteção de dados pessoais no país.

Paradigma do Consentimento

Diante do desenvolvimento tecnológico e da ascensão dos ambientes virtuais, o direito à privacidade foi transformado, segundo Bruno Bioni, ao longo das últimas cinco décadas, em um *“direito fundamental autônomo cujo âmbito de proteção está vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação”*^{18/19}.

Assim, a legislação passou a adotar o consentimento como instrumento para legitimar, justificar e alicerçar a proteção de dados pessoais. Ante o chamado “paradigma do consentimento”, o titular dos dados passa a ocupar o centro do processo para decidir o que será feito com seus dados pessoais²⁰. No entanto, os pressupostos que cerceiam o paradigma do consentimento demonstram ser insuficientes para garantir a eficácia do regime protetivo de dados.

Podem, portanto, ser destacados três pontos que ilustram as insuficiências do consentimento como instrumento de proteção: (i) as limitações cognitivas do titular dos dados pessoais para ava-

17 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 177.

18 BIONI, Bruno Ricardo. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2019. p. [?].

19 MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 20, n. 79, [intervalo de páginas], [mês] [ano], p. 48-51.

20 *“This liberal autonomy principle seeks to place the individual at the center of decision-making about personal information use. Privacy-control seeks to achieve information self-determination through individual stewardship of personal data, and by keeping information isolated from access. [...] The weight of the consensus about the centrality of privacy-control is staggering”*. SCHWARTZ, Paul M. Internet Privacy and the State. **Connecticut Law Review**, v. 32, p. [intervalo de páginas], 2000, p. [820?].

liar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular; e (iii) as modernas técnicas de tratamento e análise de dados a partir de Big Data que fazem com que a totalidade das possibilidades de utilização desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido^{21/22}.

A primeira insuficiência pode ser identificada de acordo com a dificuldade a ser enfrentada pelos usuários em interpretar e avaliar os custos e benefícios do tratamento de seus dados. Na grande maioria das vezes, as informações acerca do tratamento dos dados contidos nos termos regulatórios de aplicações de serviços da Internet são de difícil compreensão, diante de termos técnicos distantes da realidade social e, até mesmo elementos de edição, como letras miúdas, posicionadas estrategicamente a induzir o usuário a não ler cláusulas que possam comprometer na decisão do indivíduo de consentir ou com tal regulamento.

A segunda insuficiência pode ser encontrada em situações em que não há uma verdadeira opção de escolha, como nas chamadas situações “take it or leave it”²³, nas quais, em caso de não consentimento, o usuário não tem acesso ao serviço ofertado. Logo, evidencia-se que não há uma real liberdade de escolha, sendo essa noção puramente ilusória, colocando em questionamento a autonomia decisória dos indivíduos.

Por fim, a última insuficiência a ser destacada se origina do fato dos usuários não saberem a totalidade do uso de seus dados. Isto é,

21 “Equally challenging is the fact that in the age of ‘Big Data’, much of the value of personal information is not apparent at the time of collection, when notice and consent are normally given”. CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. **International Data Privacy Law**, v. 3, n. 2, p. [intervalo de páginas], 2013, p. 67.

22 BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2019. p. [?].

23 “That binary choice is not what the privacy architects envisioned four decades ago when they imagined empowered individuals making informed decisions about the processing of their personal data”. CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. **International Data Privacy Law**, v. 3, n. 2, p. [intervalo de páginas], 2013, p. 67.

o cidadão sabe que seus dados serão coletados, porém, deve-se ter em mente que há uma cadeia muito mais ampla da utilidade dos dados pessoais, que vai muito além do processo de coleta inicial como, por exemplo, as informações que são geradas a partir de seu processamento; as decisões tomadas a partir da coleta dessas informações; e, principalmente, as consequências dessas decisões, que são capazes de afetar a vida e a liberdade dos indivíduos envolvidos^{24/25}.

Além disso, conforme destaca a ANPD em seu estudo preliminar sobre as hipóteses aplicáveis no tratamento de dados pessoais de crianças e adolescentes:

(...) é necessário refletir acerca do consentimento parental como única hipótese legal para o tratamento de dados pessoais de crianças e se, de fato, o consentimento se configura como mecanismo adequado para assegurar, em todos os casos, a proteção ao seu melhor interesse. A esse respeito, deve-se considerar que, em certas situações, a concentração de toda a proteção à criança na obtenção do consentimento pode provocar uma ilusória ideia de controle, dada a assimetria de informação entre controladores e titulares, como se percebe, por exemplo, em relação às políticas de privacidade, que muitas vezes não são de fácil compreensão pela população e às vezes sequer são lidas (...)²⁶

Em suma, não se trata de inutilizar o consentimento como medida protetiva, mas é necessário avaliá-lo e reajustá-lo para garantir a maior eficácia possível e, diante de casos em que não seja suficiente, como nos casos da tecnologia Big Data, deve-se ir muito

24 “[...] os efeitos adversos oriundos dessas decisões, porque capazes de afetar a vida e a liberdade dos indivíduos envolvidos”. BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2019. p. 100.

25 ALBERS, Marion. Realizing the complexity of data protection. In: GUTWIRTH, Serge et al. (Orgs.). **Reloading data protection**. Dordrecht: Springer, 2014. p. 222-224.

26 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS. **Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf>. Acesso em: 11 mai. 2023.

além do consentimento do titular dos dados, para que seja garantida a efetiva proteção dos dados, adotando a integridade contextual (*contextual integrity*) do fluxo desses dados, observando a proteção desses dados como vetor para garantir o fluxo apropriado e esperado dentro dos moldes das “normas informacionais” (*context-relative informational norms*)²⁷.

Logo, interpretar restritivamente a lei que regulariza o tratamento de dados de crianças, isto é, entender que a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º da LGPD, seria a única hipótese legal para o tratamento de dados pessoais de crianças e adolescentes, é insuficiente para garantir a segurança jurídica dos dados pessoais dos incapazes. Isto porque, conforme já disposto acima, o consentimento já foi comprovado ser um instrumento protetivo ineficaz, limitado e muitas vezes ilusório.

Além disso, resta claro que a interpretação restritiva implicaria em concluir que os dados de crianças e adolescentes não poderiam ser tratados nem mesmo em situações para o cumprimento de obrigação legal ou para tutela de sua própria vida, conforme elencadas no artigo 7º, incisos II e VII da LGPD²⁸ – contrariando o princípio do melhor interesse.

A aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, haja vista a sua equiparação aos dados sensíveis

O art. 5, inciso II e o art. 11 da Lei Geral de Proteção de Dados versam, respectivamente, sobre quais seriam os dados pessoais sensíveis e seu adequado tratamento:

27 NISSENBAUM, Helen. A contextual approach to privacy online. **Daedalus, the Journal of the American Academy of Arts & Sciences**, v. 140, n. 4, p. [intervalo de páginas], 2011, p. 33.

28 Art 7º (...) II – para o cumprimento de obrigação legal ou regulatória pelo controlador; VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; (...). [Referência da lei citada].

Art. 5º Para os fins desta Lei, considera-se:

(...)

II – dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural;”

(...)

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- a) cumprimento de obrigação legal ou regulatória pelo controlador;
- b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- e) proteção da vida ou da incolumidade física do titular ou de terceiro;
- f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I – a portabilidade de dados quando solicitada pelo titular; ou

II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Conforme disposto em lei, os dados pessoais sensíveis são dados pessoais que abrangem 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, quando vinculado a uma pessoa natural. Esses dados sensíveis apresentam proteção especial da LGPD visto que, a depender do tratamento, podem levar a algum tipo de discriminação. Dessa maneira, a legislação não engloba indivíduos incapazes e relativamente incapazes como pressupostos caracterizantes de dados sensíveis e, portanto, explicita a maneira correta de tratar os dados desse grupo social.

Desde o princípio, portanto, verifica-se que os dados pessoais de crianças e adolescentes não poderiam ser equiparados aos dados pessoais sensíveis, unicamente por tal hipótese interpretativa não ser compatível com o texto da lei. No entanto, cumpre analisar se tal interpretação, ainda que contrária ao disposto em lei, atinge

o princípio do melhor interesse – princípio norteador do tratamento de dados de crianças.

Tal princípio deve, simultaneamente, atingir a totalidade de suas finalidades como direito subjetivo, princípio interpretativo e regra processual, devendo, portanto, ser objetivado em tudo que buscar preservar, proteger e assegurar os direitos das crianças e dos adolescentes. Assim, ao equiparar os dados de crianças e adolescentes a dados pessoais sensíveis, é preciso identificar se o princípio do melhor interesse, mesmo com as particularidades de cada caso concreto, será atingido.

Levando em consideração que as crianças e adolescentes são titulares de dados pessoais que são mais vulneráveis, e a fim de garantir o seu melhor interesse, é sugerido que o tratamento de dados desses titulares, ao serem equiparados a dados sensíveis, seja restrito às hipóteses previstas no artigo 11 da LGPD.

Em uma leitura completa do artigo 11 da LGPD, além do consentimento, a lei permite que os dados sensíveis sejam tratados para: a) o cumprimento de obrigação legal ou regulatória; b) o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) a realização de estudos por órgão de pesquisa; d) o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo ou arbitral; e) a proteção da vida ou da incolumidade física do titular ou de terceiro; f) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Entretanto, ainda que essa equiparação a dados sensíveis tente conferir maior grau de proteção aos titulares ao restringir o tratamento a hipóteses legais mais restritivas, isso pode significar um impedimento, ainda que abstrato, para o alcance do legítimo interesse.

O Legítimo interesse

O artigo 7º da Lei Geral de Proteção de Dados garante o legítimo interesse, conforme trecho da lei transcrito abaixo:

Art. 7. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo controlador;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado).

§ 2º (Revogado).

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

O legítimo interesse é uma hipótese legal que tem como objetivo permitir o processamento de dados importantes que estejam ligados ao escopo de atividades realizadas pelo responsável pelo controle dos dados, e que tenham uma razão legítima para serem processados. Entretanto, tem-se que o legítimo interesse é um conceito muito amplo de forma que possui muitas interpretações.

Assim, tendo em vista que o legítimo interesse é uma base legal flexível, é necessário analisar se o tratamento desse dado possui realmente uma finalidade, se é realmente necessário e se garante que será tratado somente dentro dos limites da proporcionalidade.

Essa análise foi uma preocupação desde o início da criação da LGPD, conforme constatado por Bioni²⁹:

29 BIONI, Bruno. **Legítimo interesse: aspectos gerais a partir de uma visão obrigacional**. Grupo GEN, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 11 mai. 2023.

Ao longo de tudo o que foi exposto, nota-se que a base legal do legítimo interesse é, em sua essência, recheada de incertezas. Para dela se valer, há a necessidade de se desvencilhar de um ônus argumentativo complexo, o qual ainda deve ser documentado.

O legítimo interesse, ainda que possua ampla finalidade, deve ser aplicado de forma adequada a cada contexto específico. É necessário a utilização de fatores de verificação como a avaliação dos interesses legítimos, o impacto sobre o titular do dado, o equilíbrio entre os interesses legítimos do controlados e o seu impacto sobre o titular. O artigo 10º da LGPD discorre, de modo mais concreto, sobre a operacionalização do legítimo interesse, confira-se:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador; e

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Cabe ressaltar que quando a base legal for o consentimento, este não será considerado legítimo interesse se não atender ao “melhor interesse” da criança e do adolescente – conforme tratado posteriormente.

Caso a equiparação de dados pessoais de crianças e adolescentes a dados sensíveis preceda, teremos uma dificuldade a tratá-los com base no legítimo interesse, seja na execução de políticas públicas, na realização de estudos por órgãos de pesquisa e entre outras operações em que o tratamento de dados poderia legitimamente amparar.

A problemática da equiparação do tratamento dos dados de crianças e adolescentes às hipóteses do artigo 11 – Rol taxativo do artigo 5

Conforme elencado pelo artigo 5º da Lei Geral de Proteção de Dados, considera-se dados pessoais sensíveis aqueles que versarem sobre 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, quando vinculado a uma pessoa natural. Logo, é evidente que os dados sensíveis não abrangem nada além das disposições listadas.

Quando a norma limita uma disposição por meio de lei ou regulamento e, assim, não abrange nada além do que foi definido, pode-se classificá-la como rol taxativo. Assim, surge o grande problema da equiparação dos dados de crianças e adolescentes aos dados pessoais sensíveis.

Em acórdão relatado pelo ministro Francisco Falcão, o Superior Tribunal de Justiça reconheceu que o artigo 5º, inciso II, da Lei Geral de Proteção de Dados Pessoais (LGPD) traz um rol taxativo dos dados pessoais considerados sensíveis, os quais, segundo o artigo 11, exigem tratamento diferenciado. Confira-se:

Já em relação a alegada ofensa ao art. 5º, II, da LGPD, constata-se assistir razão à concessionária recorrente a esse respeito, isso porque o referido dispositivo **traz um rol taxativo daquilo que seriam dados pessoais sensíveis** e, por ostentarem essa condição, exigem tratamento diferenciado, conforme previsão no art. 11 da mesma LGPD. (...) (Agravo Em Recurso Especial Nº 2.130.619. Relator: Min. FRANCISCO FALCÃO, Segunda Turma de Direito Civil, Tribunal de Justiça de São Paulo, julgado em: 7.3.2023).

Portanto, ao equiparar ambos os dispositivos, a hipótese nada mais faz do que contrariar aquilo disposto em lei, uma vez que passa a incluir o grupo de crianças e adolescentes como classificados de dados pessoais sensíveis.

Aplicação das hipóteses legais previstas nos artigos 7º e 11º da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse

Por fim, cumpre analisar a possibilidade da aplicação das disposições legais previstas nos arts. 7º e 11º da LGPD ao tratamento de dados de crianças e adolescentes, desde que observado o princípio do melhor interesse.

Primeiramente, ao estender o tratamento dos dados de crianças e adolescentes para além das hipóteses previstas no artigo 14, passando, também, a considerar as hipóteses dos artigos 7 e 11, adota-se uma interpretação extensiva, de método teleológico-axiológico.

Isso porque, esta hipótese interpretativa amplia o sentido do texto do artigo 14, ao demonstrar que deve ser estendida para cumprir tudo aquilo que foi pretendido pela *mens legis* e, assim, propõe aplicar os dispositivos dos artigos 7 e 11, de modo a escancarar a totalidade daquilo que a norma quis apresentar. Além disso, deve ser considerada uma interpretação teleológica-axiológica, pois, está diante de uma questão pragmática – o tratamento de dados de crianças e adolescentes – que se refere à relação comunicacional entre emissores e receptores das mensagens normativas, onde haja falha nos símbolos comunicacionais – consentimento que não deve ser visto como único instrumento de garantia ao melhor interesse.

A necessidade deste método interpretativo deriva da imposição do julgador reconhecer que aquilo disposto em lei diz menos do que o legislador realmente pretendia dizer. É o que considera a Ministra presidente do Supremo Tribunal Federal, Rosa Weber:

Em particulares hipóteses, a fim de compatibilizar normas jurídicas infraconstitucionais de natureza penal aos comandos da Lei Maior, bem como ao próprio sistema em que se inserem, **exsurge verdadeira imposição ao julgador no sentido de reconhecer que a lei disse menos do que pretendia (*lex minus scripsit, plus voluit*), a exigir seja emprestada interpretação ampliativa ao texto legal, respeitada a teleologia do preceito interpretado.** Precedente desta Suprema Corte. (HC 137888, Relator(a): Min. ROSA WEBER, Primeira Turma, julgado em 31/10/2017, PROCESSO ELETRÔNICO DJe-031 DIVULG 20-02-2018 PUBLIC 21-02-2018).

Logo, diante da fragilidade dos dados que são tratados pelas disposições do artigo 14 e, com o paradigma do consentimento e sua ineficácia para surtir os esperados efeitos protetivos, torna-se essencial que o tratamento dos dados pessoais de crianças e adolescentes seja ampliado para além das hipóteses do consentimento – os artigos 7 e 11 –, de modo a garantir a maior segurança jurídica possível e, conseqüentemente atingir o melhor interesse.

O melhor interesse da criança e do adolescente

O melhor interesse, citado anteriormente, vem a ser, de acordo com o Comitê Geral nº 25 de 2021 do Comitê dos Direitos da Criança, *“um conceito dinâmico que exige uma avaliação adequada em cada contexto específico”*. Assim, é dever dos Estados *“garantir que, em todas as ações relativas à disponibilização, regulação, design, gestão e utilização do ambiente digital, o melhor interesse da criança constitui uma consideração primordial”*. Para isso, *“devem envolver em tais ações os organismos nacionais e locais que supervisionam a realização dos direitos da criança”*.

Dessa maneira, diante do fato do ambiente digital ter grande importância no cotidiano das crianças e dos adolescentes, é imprescindível que o tratamento dos dados pessoais deste grupo social englobe todas as hipóteses que possam atingir o melhor interesse da criança, como a realização de estudos por órgão de pesquisa, a proteção à saúde e à vida, o legítimo interesse, a execução de contrato, entre as demais hipóteses previstas nos artigos 7 e 11 da LGPD.

Não obstante, também é preciso considerar a vulnerabilidade desse grupo social, especialmente no ambiente digital. Sabe-se que, diante do grande fluxo informacional, bem como a constante necessidade da autorização para uso dos dados dos usuários, utilização de *cookies* e contratos de uso das aplicações da internet, as crianças e os adolescentes se encontram frente à uma série de noções técnicas e jurídicas que são de difícil compreensão aos menores, colocando-os em situações vulneráveis, como a assinatura de um contrato abusivo e o tratamento de seus dados pessoais.

Logo, o princípio do melhor interesse deve ser tomado como prioritário no tratamento de dados pessoais de crianças e adolescentes, por objetivar, acima de tudo, a melhor opção possível para o bem-estar da criança.

Ampliação das hipóteses do tratamento de dados pessoais de crianças e adolescentes

Com a ampliação do rol das disposições que regulam o tratamento de dados pessoais de crianças e adolescentes, permitida a partir da interpretação de que também seria possível aplicar as hipóteses previstas nos artigos 7 e 11 da Lei Geral da Proteção de Dados, seria possível garantir uma maior certeza no cumprimento do melhor interesse da menor.

Ao se considerar apenas o consentimento como medida regulatória para o tratamento de dados pessoais de crianças e adolescentes, chega-se em um conjunto de restrições jurídicas e limitações práticas que, conseqüentemente, atentam contra os direitos fundamentais das crianças, inclusive por potencialmente gerar óbices ao tratamento de seus dados pessoais para proteção da vida e incolumidade física.

Assim, ao aplicar as hipóteses dos artigos 7 e 11 da LGPD no tratamento de dados de crianças e adolescentes, há uma maior flexibilidade e possibilidade de adequação aos casos concretos, priorizando a conformidade da proteção dos menores com o melhor interesse. Além disso, garante que não haja limitações jurídicas abstratas que possam inviabilizar ou prejudicar o devido tratamento baseado no melhor interesse.

No entanto, a ampliação dessas hipóteses não impede a restrição do tratamento de dados pessoais de crianças e adolescentes segundo as circunstâncias fáticas, uma vez que, observado o caso concreto, algumas hipóteses de tratamento poderão ser afastadas, para que se atinja o melhor interesse do indivíduo.

Portanto, evidencia-se que o princípio do melhor interesse – norteador da regulamentação do tratamento de dados pessoais de crianças e adolescentes – será mais facilmente respeitado se as possibilidades de tratamento forem ampliadas para além das disposições do artigo 14, adotando-se aquelas previstas nos artigos 7º e 11º. Com isso, além de se possibilitar a análise concreta do caso e, assim, encontrar a mais adequada aplicabilidade, torna-se possível romper a ideia ilusória de suficiência do consentimento como única hipótese a ser utilizada como medida protetiva.

Conclusão

Em conclusão, tem-se que as duas primeiras hipóteses apresentadas (a aplicação do consentimento dos pais ou responsável legal, conforme art. 14, §1º da LGPD, como única hipótese legal para o tratamento de dados pessoais de crianças e; a aplicação exclusiva das hipóteses legais previstas no art. 11 ao tratamento de dados pessoais de crianças e adolescentes, mediante a sua equiparação aos dados sensíveis) não são apropriadas para a definição das bases legais válidas para o tratamento de dados pessoais de crianças e adolescentes.

Na primeira hipótese, aplica-se a interpretação restritiva e, assim, considera-se apenas o consentimento do responsável legal como medida protetiva que, conforme evidenciado pelo paradigma do consentimento, é uma medida evidentemente ineficaz para a efetiva proteção dos dados pessoais de crianças e adolescentes.

Outrossim, a segunda hipótese não poderia ser considerada, por supor a equiparação dos dados pessoais de crianças e adolescentes aos dados sensíveis, que são taxativamente elencados pelo rol do artigo 11º da LGPD. Portanto, não estando incluídos no rol, não podem os dados pessoais de crianças e adolescentes serem

equiparados aos dados sensíveis. Ademais, sequer poderiam ser considerados dados sensíveis unicamente por serem de titularidade de menores de idade, uma vez que a faixa etária não configura automaticamente a sensibilidade de seus dados.

Por outro lado, a terceira e última hipótese que prevê a ampliação das disposições aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, englobando as hipóteses legais previstas nos artigos 7º e 11º da LGPD, desde que observado o princípio do melhor interesse, é juridicamente viável, ao se adotar uma interpretação extensiva do artigo 14º, de modo que se revela a hipótese mais eficaz a assegurar o devido tratamento dos dados dos menores.

Além disso, esta última hipótese retira de foco a priorização do consentimento como medida protetiva, uma vez que, devido à mais que comprovada noção ilusória de segurança que o ato do consentimento gera – nomeado “paradigma do consentimento” –, a hipótese prevista no artigo 14º da LGPD, isto é, a aplicação do consentimento do responsável legal como única hipótese legal para o tratamento, não se mostra suficiente para garantir o tratamento efetivo e seguro dos dados pessoais de crianças e adolescentes.

Por fim, conclui-se que a hipótese legal que deve ser utilizada como interpretação à legislação que rege o tratamento e a proteção de dados pessoais de crianças e adolescentes é a que amplia o tratamento desses dados às hipóteses legais previstas nos artigos 7º e 11º da LGPD, desde que observado o princípio do melhor interesse. Essa alternativa confere maior flexibilidade de opções a serem aplicadas de acordo com as particularidades de cada situação concreta, com o fim de garantir o melhor interesse de crianças e adolescentes.

Referências

- ALBERS, Marion. **Realizing the complexity of data protection**. In: GUTWIRTH, Serge et al. (Orgs.). *Reloading data protection*. Dordrecht: Springer, 2014. p. 222-224.
- ANPD – Autoridade Nacional de Proteção de Dados Pessoais. **Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de**

- crianças e adolescentes.** Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf>. Acesso em: 11.5.2023
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 177.
- BIONI, Bruno. **Legítimo interesse: aspectos gerais a partir de uma visão obrigacional.** Grupo GEN, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 11 mai. 2023.
- BIONI, Bruno. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2019. p. 100.
- BRANCHER, Paulo Marcos Rodrigues; KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer Costa; BRANCHER, Paulo Marcos Rodrigues. **Princípios gerais de proteção de dados pessoais: uma análise dos princípios elencados no Art. 6º da Lei nº 13.709/2018 (LGPD).** In: BEPPU, Ana Claudia; BRANCHER, Paulo Marcos Rodrigues (coord.). *Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018.* Belo Horizonte: Fórum, 2019. Disponível em: [link] Acesso em: 11 de mai. 2023
- BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 11 mai. 2023.
- BRASIL. **Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: [?].
- BRASIL. **Lei 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: [?]
- CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. **Notice and consent in a world of Big Data.** *International Data Privacy Law*, v. 3, n. 2, p. [intervalo de páginas], 2013, p. 67.
- É fundamental ler contratos, termos de uso e políticas de privacidade.** ABEINFO, 30 out. 2020. Disponível em: <https://abeinfo brasil.com.br/e-fundamental-ler-contratos-termos-de-uso-e-politicas-de-privacidade/>. Acesso em: 11 mai. 2023
- FERRAZ JR., Tércio Sampaio. **Introdução ao estudo do direito: técnica, decisão e dominação.** 3. ed. São Paulo: Atlas, 2001. p. 251-293.

- HOOFNAGLE, Chris Jay. **The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)** (July 15, 2014). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418. Acesso em: 11 mai. 2023
- LOREZON, Laila Neves. **Análise Comparada entre Regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus Respectivos Instrumentos de Enforcement**. Revista do Centro de Excelência Jean Monnet da FGV Direito Rio, Rio de Janeiro, v. 1, p. 39-52, mar. 2021. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/rpdue/article/view/83423>. Acesso em: 11 mai. 2023
- MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais**. Revista de Direito do Consumidor, São Paulo, v. 20, n. 79, [intervalo de páginas], [mês] [ano], p. 48-51.
- NISSENBAUM, Helen. **A contextual approach to privacy online**. Daedalus, the Journal of the American Academy of Arts & Sciences, v. 140, n. 4, p. [intervalo de páginas], 2011, p. 33.
- SCHWARTZ, Paul M. **Internet Privacy and the State**. Connecticut Law Review, v. 32, p. [interval de páginas], 2000, p. [820?].
- SEM ler os termos de uso, mais de 20 mil pessoas se inscrevem em serviços comunitários**. Estadão, 13 jul. 2017. Disponível em: <https://www.estadao.com.br/emails/comportamento/sem-ler-os-termos-de-uso-mais-de-20-mil-pessoas-se-inscrevem-em-servicos-comunitarios/>. Acesso em: 11 mai. 2023
- TEPEDINO, Gustavo; TEFFÉ, Chiara Spacaccini. **O consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil, Belo Horizonte, v. 25, n. 3, p. 83-116, jul./set. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521>. Acesso em: 11 mai. 2023.
- UNICEF. **Convenção sobre os Direitos da Criança**. Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>. Acesso em: 11 mai.2023
- UNITED NATIONS. **General Comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration**. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_14_eng.pdf. Acesso em: 11 mai. 2023

www.anpd.gov.br



ANPD

Autoridade Nacional de Proteção de Dados