DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Regulação Digital: Perspectivas Jurídicas sobre Tecnologia e Sociedade

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
janeiro/2024

ITS · UERJ Universidade do Estado do Rio de Janeiro · Direito UERJ · CEPED

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Regulação Digital: Perspectivas Jurídicas sobre Tecnologia e Sociedade

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
janeiro/2024

COORDENAÇÃO:
Sérgio Branco e Chiara de Teffé

PROJETO GRÁFICO, CAPA E DIAGRAMAÇÃO:
Mariana Bertoluci e Stephanie Lima

PRODUÇÃO EDITORIAL:
Instituto de Tecnologia
e Sociedade - ITS

REVISÃO:
Chiara de Teffé

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Regulação digital [livro eletrônico] :
perspectivas jurídicas sobre tecnologia e
sociedade / coordenação Sérgio Branco , Chiara
de Teffé. -- Rio de Janeiro : ITS - Instituto de
Tecnologia e Sociedade, 2024.
-- (Coleção diálogos da pós-graduação em direito
digital)
PDF

Vários autores.
Bibliografia.
ISBN 978-85-5596-006-2

1. Direito digital 2. Inteligência artificial
3. Proteção de dados - Leis e legislação 4. Regulação
- Brasil I. Branco, Sérgio. II. Teffé, Chiara de.
III. Série.

24-189066 CDU-34:004

Índices para catálogo sistemático:

1. Direito digital 34:004

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

COMO CITAR:
BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). *Regulação digital: Perspectivas Jurídicas sobre Tecnologia e Sociedade*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024. 363p.

INSTITUTO DE TECNOLOGIA E SOCIEDADE:
itsrio.org | @itsriodejaneiro | midias@itsrio.org

LISTA DE AUTORES

Amanda Carvalho dos Santos

André Luís Machado de Castro

Andrea Paula Pontes dos Santos

Bianca Coupe Foradine da Motta

Beatriz Corrêa Peixoto

Breno Dias Ferreira Maia

Bruno Blum Fonseca

Carolina Schabbach Oliveira Ribeiro

Emília de Freitas Cabreira

Izabella de Rezende Zuccari

Julia Ferrari Oliveira Lima

Juliana Adão Alves

Juliana Almeida Conte

Laura Alves Gonzaga

Maria Augusta Peres Catelli

Matheus Mantuani Nunes

Rafael Afonso Cristino Sousa Barros

APRESENTAÇÃO

Em um mundo cada vez mais conectado, o Direito Digital surge como um campo de estudo e de atuação profissional necessário, abrangendo temas como proteção de dados pessoais, inteligência artificial, regulação da rede, blockchain e crimes cibernéticos. Sendo uma das mais promissoras e demandadas áreas jurídicas, o Direito Digital dialoga com diferentes ramos do conhecimento e ambientes regulatórios. Além disso, promove o desenvolvimento de novas teorias e institutos nas mais diversas áreas do Direito, levando a tecnologia e as novas relações para os Direitos Civil, Empresarial, Penal, Tributário, Trabalhista e Constitucional, por exemplo.

Profissionais com especialização em Direito Digital são cada vez mais procurados por empresas, que buscam se adequar às novas regulamentações e mercados, pela Administração Pública, que vive um processo de digitalização e otimização de atividades, e por consumidores que demandam seus direitos no ambiente digital. Litígios e pareceres sobre o tema são constantemente solicitados por clientes e em ações judiciais, inclusive em tribunais superiores. Além de atuações em questões consultivas e contenciosas, com pessoas físicas e jurídicas, há também amplo espaço para o Direito Digital em aspectos criminais, tributários, contratuais e relacionados ao compliance.

A tendência de crescimento da área do Direito Digital continua e se fortalece em 2024. A digitalização dos negócios, a análise de dados e as aplicações cada vez mais complexas que utilizam inteligência artificial vêm acompanhadas de desafios relacionados à privacidade, proteção do consumidor, fraudes e crimes cibernéticos.

Diante desse cenário, a pós-graduação em Direito Digital oferecida pelo ITS, em parceria com a UERJ e o CEPED, representa uma resposta a essa necessidade do mercado, preparando advogado/as e profissionais que trabalham com a temática para atuar com competência frente aos novos desafios jurídicos e tecnológicos.

Nosso curso abrange sólida teoria e estudos de casos concretos, incluindo temas emergentes em blockchain, inteligência artificial e proteção de dados, além de disciplinas já consolidadas como responsabilidade civil dos provedores de internet, propriedade intelectual, contratos eletrônicos e liberdade de expressão na rede. Busca-se compreender de forma crítica e diversa o futuro do Direito na sociedade digital.

Para tanto, a pós-graduação em Direito Digital apresenta estrutura inovadora e atualizada, em aulas ao vivo e online, permitindo flexibilidade e interação em tempo real com professores altamente especializados e colegas. A possibilidade de conectar-se com pessoas de diferentes regiões do Brasil e do mundo enriquece ainda mais a experiência de aprendizado, fomentando uma compreensão mais ampla das questões apresentadas em diferentes contextos. Até o momento, nossa rede Alumni já conta com mais de 600 estudantes conectados.

APRESENTAÇÃO

A cada semestre, selecionamos para publicação artigos de nossos alunos da pós-graduação, visando a contribuir com o desenvolvimento da temática e ampliar a diversidade e a pluralidade de pensamentos.

No presente livro, foram selecionados 17 artigos de integrantes do programa de pós-graduação lato sensu em Direito Digital para compor a obra coletiva. Temas como proteção de dados pessoais; incidentes de segurança envolvendo informações pessoais; tratamento de dados de crianças no ambiente digital; a figura do encarregado; instrumentos de governança de proteção de dados; compatibilização entre a LAI e a LGPD; privacy by design; requisição de dados para investigação de ilícitos; transferência internacional de dados nos tratados de livre comércio; cookies de publicidade; herança digital; blockchain e o Sistema Tributário Brasileiro; modelos grandes de linguagem; intersecções entre a Lei Geral de Proteção de Dados, a regulação da inteligência artificial e o projeto de lei 2.338/2023; e desafios à moderação de conteúdo em plataformas são abordados na presente obra.

O ITS Rio acredita na importância da difusão e do acesso ao conhecimento. Por essa razão, esta e as demais publicações da pós-graduação encontram-se disponíveis de forma gratuita, aberta e com a licença Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Para os próximos anos, esperamos ampliar parcerias e desenvolver mais ações voltadas à educação digital que impactem positivamente a sociedade e promovam o acesso à cultura, inovação e informação. Nossas demais publicações podem ser conferidas aqui.

Observamos que o conteúdo aqui exposto não reflete necessariamente a opinião institucional do ITS Rio, ou de seus membros, representando reflexão acadêmica de responsabilidade exclusiva de seu autor.

Agradecemos a todos que contribuíram e se interessaram por esse projeto. Convidamos você a conferir as demais publicações do ITS Rio.

Ficamos à disposição e sempre abertos ao diálogo.

Rio de Janeiro, 10 de janeiro de 2024.

OS COORDENADORES

OS COORDENADORES

Chiara de Teffé

Doutora e mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ), tendo sido aprovada com distinção, louvor e recomendação para publicação. Graduada em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Atualmente, é coordenadora de pesquisa e publicações da pós-graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), em parceria com a UERJ, e professora de Direito Civil e Direito Digital na faculdade de Direito do IBMEC. Leciona em cursos específicos de pós-graduação e extensão do CEPED-UERJ, da PUC-Rio, da EMERJ e do ITS Rio. Membro da Comissão de Proteção de Dados e Privacidade da OAB/RJ. Membro da Comissão de Direito Civil do Conselho Seccional do Rio de Janeiro da OAB (2022/2024). Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia da EMERJ. Membro do Fórum permanente de inovações tecnológicas no Direito da EMERJ. Foi professora substituta de Direito Civil na UFRJ. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Membro Titular do Conselho Municipal de Proteção de Dados Pessoais e Privacidade do Rio de Janeiro. Atua como advogada em áreas do Direito Civil e do Direito Digital e como consultora em proteção de dados pessoais. Autora do livro “Dados pessoais sensíveis: qualificação, tratamento e boas práticas”.

Sérgio Branco

Cofundador e diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (Uerj). Pesquisador convidado do Centre de Recherche en Droit Publique da Universidade de Montreal. Visiting Research Fellow em Sciences Po entre 2023 e 2024. Especialista em propriedade intelectual pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Pós-graduado em cinema documentário pela FGV. Graduado em Direito pela Universidade do Estado do Rio de Janeiro (Uerj). Sócio do escritório de advocacia Rennó Penteado Sampaio.

SUMÁRIO

EIXO I — Temas em proteção de dados pessoais

SUMÁRIO

EIXO I

Temas em proteção de dados pessoais

SUMÁRIO

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO I

Temas em proteção de dados pessoais

AUTORES

André Luís Machado de Castro

Juliana Almeida Conte

Bianca Coupe Foradine da Motta

Laura Alves Gonzaga

Carolina Schabbach Oliveira Ribeiro

Andrea Paula Pontes dos Santos

Izabella de Rezende Zuccari

Maria Augusta Peres Catelli

Juliana Adão Alves

Beatriz Corrêa Peixoto

Emília de Freitas Cabreira

Amanda Carvalho dos Santos

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

Considerações sobre a aferição do dano moral em casos de vazamento de dados pessoais

ANDRÉ LUIS MACHADO DE CASTRO

ANDRÉ LUÍS MACHADO DE CASTRO[1]

Sumário: Introdução. 1. Proteção de dados pessoais como direito fundamental autônomo. 2. Precedentes do Superior Tribunal de Justiça. 3. Precedente do Tribunal de Justiça da União Europeia: Os casos "Agência Nacional de Receitas Fiscais da Bulgária" e "Empresa de Correios Austríaca". 4. Contornos da Responsabilidade Civil na LGPD: Responsabilidade objetiva ou subjetiva? 5. Dados pessoais comuns e sensíveis. 6. O dano injusto. Considerações finais. Referências.

Introdução

Em março de 2023, a Segunda Turma do Superior Tribunal de Justiça, no julgamento do Agravo em Recurso Especial nº 2.130.619 – SP, decidiu que o vazamento de dados pessoais não tem a capacidade, por si só, de gerar dano moral indenizável, sendo necessário que o titular dos dados comprove o efetivo prejuízo gerado pela exposição dessas informações.

Tratava-se de ação indenizatória ajuizada por uma consumidora contra empresa concessionária de energia elétrica, pleiteando compensação por danos morais decorrentes do vazamento e acesso por terceiros de seus dados pessoais, como nome completo, número de identidade, gênero, data de nascimento, idade, endereço, telefones fixo e celular, além de informações relativas ao contrato de fornecimento de energia elétrica, como carga instalada, consumo estimado, tipo de instalação e leitura.

O Tribunal de Justiça do Estado de São Paulo havia reformado a sentença para condenar a concessionária ao pagamento da indenização, identificando a falha na prestação do serviço pela empresa e apontando a disponibilização indevida de dados pessoais de pessoa idosa, que "deveriam ter a privacidade garantida"[2]:

> Ação indenizatória por danos morais. Prestação de serviços. Energia elétrica. "Vazamento" de dados pessoais da autora. R. sentença de improcedência, com apelo só da consumidora/acionante. Plena aplicação do CDC. Inversão do ônus probatório. Vazamento de dados reservados da consumidora, que configura falha na prestação de serviços. Dados que deveriam ter a privacidade garantida. Indicados os danos morais. Dá-se provimento ao recurso da requerente.

1. Defensor Público no Estado do Rio de Janeiro, titular e coordenador do Núcleo de Defesa dos Direitos Humanos da Defensoria Pública. Graduado e Mestre em Direito Civil pela Universidade do Rio de Janeiro (UERJ). Pós-graduando no curso de Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio de Janeiro) em parceria com o CEPED/UERJ.

2. BRASIL. Superior Tribunal de Justiça. *REsp. 2.130.619-SP*, Rel. Min. Francisco Falcão. DJe: 09/03/2023. p. 5.

Em sede de recurso especial (e do subsequente agravo), a empresa recorrente sustentou a negativa de vigência aos arts. 42, 43, II e III, 46 e 48 da LGPD, alegando comprovada conduta da empresa quanto à adoção de medidas de segurança para proteção dos dados sob sua responsabilidade, de modo que o vazamento teria decorrido de ação exclusiva de terceiro, o que justificaria a excludente de responsabilidade (culpa ou fato de terceiro).

Ainda, a empresa sustentou que os dados pessoais vazados não poderiam ser considerados dados sensíveis, nos termos do art. 5º, II, da LGPD, mas sim dados comuns. Desta forma, suscitou ofensa ao art. 42, *caput*, da LGPD[3], por não ser possível a indenização de evento incerto e futuro, acrescentando que o vazamento de dados não sensíveis não seria capaz, por si só, de causar lesão à esfera íntima da pessoa humana.

Ao decidir a questão, a 2ª Turma do STJ entendeu que não poderia examinar a alegação de culpa (ou fato) exclusivo de terceiro, por falta de adequado prequestionamento, observando que a matéria não havia sido apreciada pelo Tribunal de Justiça.

Com relação à natureza dos dados pessoais vazados, o acórdão reconheceu que, no caso concreto, se tratariam de dados pessoais comuns (ou não sensíveis) pois, de acordo com a decisão, o art. 5º, II, da LGPD "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".

Com base nessa diferenciação entre a proteção jurídica aos dados pessoais sensíveis e os comuns, o acórdão asseverou "não ser possível indenizar por dano moral o vazamento de dados informados corriqueiramente em diversas situações do dia a dia"[4], concluindo que:

> 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 informações[5].

3. 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.

4. BRASIL. Superior Tribunal de Justiça. *REsp. 2.130.619-SP*, Rel. Min. Francisco Falcão. DJe: 09/03/2023. p. 10.

5. Ibidem. p. 10.

O acórdão acolheu o entendimento de que o dano moral não havia sido comprovado e, desta forma, afastou a hipótese de aplicação da técnica do dano moral *in re ipsa*, que havia dado fundamento à decisão recorrida.

A decisão em questão traz elementos novos para a ainda incipiente jurisprudência sobre a proteção de dados pessoais no Brasil e o tema da responsabilidade civil por incidentes de segurança e tratamentos indevidos de dados.

O presente artigo se propõe a fazer um breve exame da decisão proferida no Agravo em Recurso Especial nº 2.130.619 – SP, à luz da perspectiva do direito fundamental à proteção de dados pessoais e da autodeterminação informativa, examinando os regimes de responsabilidade civil e suas repercussões nos casos de incidente de segurança de vazamento de dados pessoais comuns e dados sensíveis, bem como os meios de comprovação e liquidação do dano extrapatrimonial. Também será cotejado com a jurisprudência do Superior Tribunal de Justiça e do Tribunal de Justiça da União Europeia (TJUE), especialmente os casos contra a Agência Nacional de Receitas Fiscais da Bulgária (C-340/21 - VB contra *Natsionalna agentsia za prihodite*)[6] e e contra a Empresa de Correios Austríaca (C-300/21 - UI contra *Österreichische Post AG*)[7], versando sobre responsabilidade civil por violação ao Regulamento Geral sobre a Proteção de Dados da União Europeia (art. 82 do RGPD).

1. Proteção de dados pessoais como direito fundamental autônomo

Em meio à pandemia do novo coronavírus, no ano de 2020, o Governo Federal editou Medida Provisória determinando que as empresas de telefonia fornecessem ao IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores para o fim de produzir estatística oficial por meio de entrevistas domiciliares não presenciais. A norma foi impugnada pela ação direta de inconstitucionalidade n. 6.387.

Por entender que a norma protegeria os direitos fundamentais de acesso à informação e à saúde no contexto do combate à pandemia, a Procuradoria da República manifestou-se contrariamente ao deferimento da medida cautelar,

6. Tribunal de Justiça da União Europeia. Processo C-340/21: VB contra *Natsionalna agentsia za prihodite* (Agência Nacional de Receitas Fiscais da Bulgária). Conclusões do Advogado-Geral Giovanni Pitruzzella apresentadas em 27.04.2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=DDCCF5FAFBC93C875584F8B7C3DB165F?text=&docid=272977&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=702058. Acesso em: 20 jul.2023.

7. Tribunal de Justiça da União Europeia. Processo C-300/21: UI contra *Österreichische Post AG* (Empresa de Correios Austríaca). Acórdão proferido em 04.05.2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=2738956. Acesso em: 26 nov. 2023.

sustentando que a norma não violaria os direitos de sigilo de comunicações telefônicas e de dados, nem afrontaria as garantias de inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas[8].

Não obstante, o Supremo Tribunal Federal deferiu a medida cautelar para suspender a eficácia da Medida Provisória e reconheceu a proteção de dados pessoais e a autodeterminação informativa como "direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana"[9], realçando a importância da tutela para prevenção de riscos dos processamentos realizados por terceiros[10].

No mesmo sentido, em 2022, o Congresso Nacional promulgou a Emenda Constitucional nº 115, incluindo no rol dos direitos e garantias fundamentais "o direito à proteção dos dados pessoais, inclusive nos meios digitais" (art. 5º, inciso LXXIX).

Contudo, para o atingimento de uma efetiva proteção ainda há um longo caminho a ser percorrido. São frequentes os casos de incidentes de segurança, a exemplo dos vazamentos de informações, quando a confidencialidade dos dados pessoais é violada e estes são acessados por terceiros não autorizados. Conforme pontuado por Ronaldo Lemos, "qualquer um no Brasil hoje tem de assumir que seus dados estão expostos, incluindo CPF, nome, endereço, nome dos pais, fotos de rosto, escore de crédito, participações societárias, Imposto de Renda, imóveis, números de celular, benefícios do INSS e muito mais"[11].

O mega vazamento em questão atingiu dados pessoais de autoridades como o então Presidente da República e os Ministros do Supremo Tribunal Federal, o que deu ensejo à abertura de investigação pelo Ministro do STF Alexandre de Moraes, no âmbito do Inquérito nº. 4.781 (chamado Inquérito das *Fake News*), sob o fundamento de que a "comercialização de informações e dados privados e sigilosos de membros desta CORTE atinge diretamente a intimidade, privacidade e segurança pessoal de seus integrantes"[12].

8. BRASIL. Supremo Tribunal Federal. *ADI 6.393 MC-Ref/DF.* Rel. Min. Rosa Weber. Plenário. DJe: 07.05.2020. p. 7.

9. Ibidem. Antecipação de voto do Min. Luiz Fux. p. 55.

10. Ibidem. p. 8.

11. LEMOS, Ronaldo. *O vazamento de dados do fim do mundo: A partir de agora o Brasil se tornou também um faroeste digital*. Folha de São Paulo on-line. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml. Publicado em 31.01/2021. Acesso em: 18.07/2023.

12. BRASIL. Supremo Tribunal Federal. *Inquérito 4.781* - DF. Despacho. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/INQ4781PET.pdf. Acesso em: 25 jul. 2023.

Com especial atenção a esse tema, a Lei Geral de Proteção de Dados (LGPD) consagra como princípios para o tratamento de dados a segurança, prevenção, responsabilização e prestação de contas (art. 5º, incisos VII, VIII e X), que se encontram no centro do arcabouço protetivo, norteando a atuação dos órgãos de controle, dos agentes de tratamento e do próprio Poder Judiciário.

Em caso de incidentes, como vazamento de dados, em que pesem as medidas de mitigação de danos previstas na legislação, essas nem sempre serão capazes de impedir a exposição dos dados e a situação concreta de vulnerabilidade de seus titulares. Não se pode perder de vista a existência de um mercado (por vezes ilícito) ávido pela coleta e tratamento massivo de dados pessoais, inclusive se valendo das poderosas ferramentas de *Big Data* e *Big Analytics* que, por meio do cruzamento de informações, permitem "utilizações a aplicações que não seriam sequer imagináveis há poucos anos atrás e que, na ausência de uma regulação adequada, passaram a ser realizadas sem limites e com resultados que podem se projetar para sempre"[13].

De toda sorte, a proteção aos titulares dos dados pessoais - consagrada como direito fundamental - deve estar no centro da tutela jurídica e os danos decorrentes de incidentes de segurança poderão dar ensejo à devida reparação, na forma dos arts. 42 a 45 da LGPD, sem prejuízo da aplicação da legislação civil em geral e, nas hipóteses de relação de consumo, do Código de Defesa do Consumidor.

2. Precedentes do Superior Tribunal de Justiça

No julgamento do já comentado AREsp nº 2.130.619, a 2ª Turma do STJ fixou o entendimento de que vazamento de dados pessoais não sensíveis não gera dano moral presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

Deixaram de ser examinadas pelo acórdão as questões relativas a causas de exclusão do nexo causal por fato exclusivo de terceiro ou sobre a adequação das medidas adotadas pela empresa, por razões processuais (falta de prequestionamento). No entanto, diante da decisão concluindo pela inexistência de dano, não se haveria de perquirir o nexo de causalidade.

13. FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. (Coord.). *A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. 2. ed. São Paulo: Thomson Reuter Brasil, 2022. p. 25.

O exame dos precedentes da Corte revela que o julgado divergiu, em parte, de decisão anterior proferida pela 3ª Turma do STJ, no REsp. 1.758.799 – MG, para reconhecer a existência de dano moral presumido em caso de disponibilização não autorizada de dados não sensíveis do titular. No caso, uma empresa de banco de dados comercializava dados (não sensíveis) do autor sem o seu prévio conhecimento ou autorização causando, segundo o demandante, abalo à sua tranquilidade, por sujeitá-lo a golpes ou ao uso indevido de seus dados para a prática de atos ilegais.

O acórdão manteve a condenação da empresa gestora de banco de dados, reconhecendo o dano moral *in re ipsa*. O julgado destacou que "[o] fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados"[14], ou seja, acolheu entendimento diverso daquele adotado no acórdão da 2ª Turma, acima comentado.

Note-se que o dano em questão consistiu no "sentimento de insegurança experimentado pelo apelante ao perceber que seus dados pessoais como número de telefone, CPF, endereço e filiação se encontravam disponibilizados em banco de dados de fácil acesso por terceiros"[15].

Em outros dois julgados recentes, examinando casos de "golpe do motoboy"[16] e "golpe do boleto"[17], ambos também sob a relatoria da Ministra Nancy Andrighi, a 3ª Turma do STJ consolidou o entendimento de que a responsabilidade das instituições financeiras pelo vazamento de dados pessoais exige a demonstração de que a origem do vazamento foi o sistema bancário, observando se as devidas medidas de proteção de dados pessoais foram adotadas, nos termos da LGPD.

Nos dois casos, os golpes aplicados contra os consumidores foram praticados por terceiros, valendo-se de dados sigilosos sob a guarda dos bancos demandados.

Assim, uma vez "comprovada a hipótese de vazamento de dados por culpa da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos"[18]. Caso contrário, "inexistindo elementos

14. BRASIL. Superior Tribunal de Justiça. *REsp. 1.758.799 – MG*, Rel. Min. Nancy Andrighi. DJe: 19/11/2019..
15. Ibidem. Transcrição parcial do acórdão recorrido, do TJMG.
16. BRASIL. Superior Tribunal de Justiça. *REsp 2.015.732 – SP*. Rel. Min. Nancy Andrighi. DJe: 26/06/2023.
17. BRASIL. Superior Tribunal de Justiça. *REsp 2.077.278 – SP*. Rel. Min. Nancy Andrighi. DJe: 09/10/2023.
18. BRASIL. Superior Tribunal de Justiça. *REsp 2.015.732 – SP*. Rel. Min. Nancy Andrighi. DJe: 26/06/2023.

objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social"[19]. Nos dois casos, uma vez demonstrada a responsabilidade objetiva das empresas pelos vazamentos de dados, reconheceu-se a existência de danos morais *in re ipsa* em favor dos consumidores.

Cabe salientar que nesses dois últimos casos, as vítimas efetivamente sofreram golpes, com comprovado dano material. Já no caso do REsp. 1.758.799 –MG, não houve dano material conjugado e o dano moral (presumido) decorreu do sentimento de insegurança experimentado.

3. Precedente do Tribunal de Justiça da União Europeia: Os casos "Agência Nacional de Receitas Fiscais da Bulgária" e "Empresa de Correios Austríaca"

Em julho de 2019, a imprensa búlgara noticiou um acesso não autorizado ao sistema de informação da Agência Nacional de Receitas Fiscais (*Natsionalna agentsia za prihodite* - NAP) e que diversas informações fiscais e de seguridade social de milhões de pessoas, tanto nacionais como estrangeiras, tinham sido publicadas na internet. Várias pessoas, entre as quais V.B., ajuizaram ações contra a NAP para obter indenização por danos morais.

À semelhança do caso brasileiro citado acima, a justiça de primeira instância búlgara julgou o pedido improcedente, considerando que a difusão dos dados não era imputável à Agência, pois o ônus da prova da inadequação das medidas de segurança adotadas cabia à autora da ação. Ainda, julgou inexistir prova de dano moral indenizável.

Diante dos resultados distintos nas diversas ações indenizatórias ajuizadas no país, o Supremo Tribunal Administrativo búlgaro suspendeu a tramitação dos processos e submeteu ao Tribunal de Justiça da União Europeia[20] questões prejudiciais[21] relativas à interpretação do caso à luz do Regulamento

19. Ibidem.

20. O Tribunal de Justiça da União Europeia (TJUE) interpreta o direito europeu para garantir que este é **aplicado da mesma forma** em todos os países da UE e delibera sobre **diferendos jurídicos** entre governos nacionais e instituições europeias. Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_pt. Acesso em 26.07.2023.

21. Foram levantadas as seguintes questões prejudiciais: "1) Devem os artigos 24.° e 32.° do Regulamento (UE) 2016/679 ser interpretados no sentido de que basta que se tenha verificado a divulgação ou o acesso não autorizados a dados pessoais, na acepção do artigo 4.°, ponto 12,do Regulamento (UE) 2016/679, por pessoas que não são funcionários da administração do responsável pelo tratamento e não estão sujeitas ao seu controlo para se considerar que as medidas técnicas e organizativas tomadas não são adequadas?

Geral sobre a Proteção de Dados – RGPD, notadamente de seu art. 82, que trata do "direito à indenização e responsabilidade".

Em 27.04.2023 foi apresentada a opinião do Advogado-Geral da Corte e o caso ainda está pendente de julgamento[22]. O parecer do Advogado-Geral trouxe importantes balizas para a interpretação da RGPD, preceituando que:

> a) Com relação aos deveres da empresa responsável pelo tratamento de dados, a mera existência de uma "violação de dados pessoais"[23] não basta, por si só, para concluir que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento não estejam "adequadas" para assegurar a proteção dos dados em causa, cabendo ao órgão jurisdicional realizar uma análise concreta do conteúdo dessas medidas, do modo como foram aplicadas e de seus efeitos práticos, enfatizando que "o responsável pelo tratamento dos dados pessoais tem o ônus de provar que as medidas técnicas e organizativas são adequadas"[24], nos termos do artigo 32 do RGPD;
>
> b) O fato do incidente de segurança ter sido causado por um terceiro não constitui, em si mesmo, um motivo para isentar de responsabilidade o responsável pelo tratamento, que mantém o dever de provar que não é, de modo algum, responsável pela violação;

---

2) Em caso de resposta negativa à primeira questão, qual deve ser o objeto e o alcance da fiscalização jurisdicional da legalidade ao examinar se as medidas técnicas e organizativas tomadas pelo responsável pelo tratamento são adequadas na acepção do artigo 32.° do Regulamento (UE) 2016/679?
3) Em caso de resposta negativa à primeira questão, deve o princípio da responsabilidade na acepção do artigo 5.°, n.° 2, e do artigo 24.°, em conjugação com o considerando 74 do Regulamento (UE) 2016/679, ser interpretado no sentido de que, num processo judicial nos termos do artigo 82.°, n.° 1, do Regulamento (UE) 2016/679, cabe ao responsável pelo tratamento provar que as medidas técnicas e organizativas tomadas são adequadas na acepção do artigo 32.° do Regulamento? Pode um parecer pericial ser considerado um meio de prova necessário e suficiente para comprovar que as medidas técnicas e organizativas tomadas pelo responsável pelo tratamento foram adequadas num processo como o presente, em que o acesso não autorizado e a divulgação de dados pessoais são o resultado de um "ataque de *hacker*"?
4) Deve o artigo 82.°, n.° 3, do Regulamento (UE) 2016/679 ser interpretado no sentido de que a divulgação ou o acesso não autorizados a dados pessoais na acepção do artigo 4.°, ponto 12, do Regulamento (UE) 2016/679,como no presente processo, através de um "ataque de *hacker*" por pessoas que não são funcionários da administração do responsável pelo tratamento e não estão sujeitas ao seu controlo, constitui uma circunstância pela qual o responsável pelo tratamento não é de modo nenhum responsável e que lhe dá o direito de ser isentado de responsabilidade?
5) Deve o artigo 82.°, n. os 1 e 2, em conjugação com os considerandos 85 e 146 do Regulamento (UE)2016/679, ser interpretado no sentido de que, num processo como o presente, em que [se] verificou uma violação da proteção de dados pessoais, sob a forma de acesso não autorizado e de divulgação de dados pessoais através de um "ataque de hacker", as preocupações, os receios e as ansiedades do titular dos dados quanto a uma eventual futura utilização abusiva dos dados pessoais, por si só, enquadram-se no conceito de dano imaterial, que deve ser interpretado em sentido amplo, e conferem-lhe o direito a uma indemnização quando essa utilização abusiva não tenha sido comprovada e/ou quando o titular dos dados não tenha sofrido outros danos?". Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=DDCCF5FAFBC93C875584F8B7C3DB165F?text=&docid=272977&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=702058. Acesso em: 20 jul.2023.

22. Conforme consulta processual disponível em: https://curia.europa.eu/juris/documents.jsf?num=C-340/21. Acesso em 26 nov. 2023.

23. Definida pela LGDP como "Violação de dados pessoais: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (artigo 4.°, ponto 12).

24. UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-340/21: VB contra Natsionalna agentsia za prihodite (Agência Nacional de Receitas Fiscais da Bulgária). *Conclusões do Advogado-Geral Giovanni Pitruzzella* apresentadas em 27 de abril de 2023. op. cit.

> c) Ainda que a utilização abusiva dos dados pessoais seja apenas potencial, e não efetiva, isso poderá ser suficiente para considerar que o titular dos dados tenha sofrido um dano moral causado pela violação do RGPD. O prejuízo consistente no receio de uma eventual futura utilização abusiva dos seus dados pessoais, cuja existência tenha sido demonstrada pelo titular dos dados, poderá constituir um dano moral indenizável, desde que o titular dos dados demonstre ter sofrido individualmente um dano emocional, real e certo.

Registre-se que a ideia de que o dano extrapatrimonial possa estar configurado pelo receio de "uma eventual futura utilização abusiva" dos dados vazados se coaduna com o entendimento adotado pela 3ª Turma do STJ no REsp. 1.758.799 – MG, ao concluir que o "sentimento de insegurança experimentado" autoriza a presunção do dano moral.

Mais recentemente, o TJUE julgou seu primeiro caso sobre critérios de interpretação sobre indenização por danos morais nos termos do artigo 82 do Regulamento Geral sobre a Proteção de Dados (RGPD).

Em 04 de maio de 2023, a Corte examinou o mérito do processo C-300/21, segundo o qual o cidadão UI alegou que a empresa de correios austríaca - Österreichische Post AG - recolheu informações sobre as afinidades políticas da população austríaca, utilizando um algoritmo que leva em conta diversos critérios sociais e demográficos para definir os "endereços de grupos-alvo". O autor ajuizou ação no tribunal austríaco pedindo 1.000 euros de indenização por danos morais decorrentes do tratamento não autorizado de seus dados pessoais para fins de publicidade política, afirmando ter sofrido ofensa em razão da afinidade política que lhe foi especificamente atribuída pelos Correios Austríacos.

O Supremo Tribunal austríaco remeteu uma série de questões ao TJUE para esclarecer se o pagamento de uma indenização, nos termos do artigo 82, exige, além de uma violação do RGPD, que o requerente comprove ter sofrido danos. O Tribunal também buscava esclarecer se a reparação do dano moral exige a existência de mais do que simples transtornos causados pela infração.

Em parecer, o Advogado-Geral apontou que as violações do RGPD não justificam, por si só, uma compensação e que os danos morais devem respeitar um "limiar de gravidade" mínimo, sendo que o parâmetro que enseja a compensação é uma questão da legislação do Estado-Membro.

A decisão do TJUE seguiu a opinião do Procurador-Geral em muitos aspectos, mas não em todos. A divergência mais notável diz respeito ao afastamen-

to de um parâmetro ou limiar mínimo de gravidade para que exista um pedido de dano moral, com base no princípio da restituição integral.

Neste sentido, a Corte entendeu que (1) a mera violação do RGPD não confere direito a indenização pois, conforme a redação do artigo 82, a existência de "dano sofrido" constitui uma das três condições cumulativas do direito à indenização: uma violação do RGPD; danos materiais ou morais resultantes dessa infração e; nexo de causalidade entre a infração e o dano.

Ainda segundo o acórdão, (2) não deve ser atribuído nenhum limite de gravidade em relação aos danos morais. Nesse aspecto, o Tribunal optou por não seguir o parecer do Advogado Geral, observando que o dano moral não está definido no artigo 82 do RGPD e que a norma comunitária não faz qualquer referência a limite de gravidade. Por sua vez, tendo em vista que o Considerando 146 do RGPD afirma que "[o] conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento", o Tribunal concluiu que seria contrário à concepção ampla de dano, defendida pelo legislador da União, a reparação apenas daqueles que atingissem um certo grau de gravidade.

O Tribunal também levou em conta o estabelecido no Considerando 10, quanto à garantia de uma aplicação consistente e homogênea das regras de proteção dos direitos e liberdades fundamentais das pessoas, no que diz respeito ao tratamento de dados pessoais. Desse modo, a imposição de um limiar mínimo poderia afetar a coerência do regime do RGPD em toda a UE, uma vez que a possibilidade de obter indenizações poderia variar de acordo com a avaliação desse limiar pelo tribunal nacional competente.

Noutro giro, foi sublinhado que o titular dos dados, afetado negativamente pela violação do RGPD, não fica dispensado de demonstrar que essas consequências negativas constituem um dano imaterial.

Em outro ponto relevante, a Corte estabeleceu que (3) o RGPD não prescreve regras para a avaliação de danos. Assim, cabe ao sistema jurídico de cada Estado-Membro fixar as regras que regem as ações nos termos do artigo 82 e, em particular, os critérios para determinar a extensão dos danos, sob reserva do respeito dos princípios da equivalência e da efetividade. O Tribunal também observou que os considerandos do RGPD afirmam que a indenização se destina à "compensação integral e efetiva" dos danos sofridos e que quaisquer regras nacionais de compensação deverão satisfazer este requisito.

Importante destacar uma diferença relevante entre o caso búlgaro e o austríaco, pois neste último não houve vazamento de dados, mas sim tratamento inadequado. Talvez em razão disso, a decisão do TJUE não tenha fornecido o nível de orientação constante do parecer do Advogado-Geral no caso búlgaro, deixando ainda questões relevantes para serem tratadas pelos tribunais nacionais, especialmente com relação à configuração do dano.

Não obstante, a Corte fixou importantes precedentes no sentido da identificação da responsabilidade civil por dano moral decorrente da violação das regras de tratamento de dados previstas no RGPD, não cabendo a consideração sobre um parâmetro mínimo de gravidade para existência do dano moral, cuja demonstração cabe ao titular dos dados.

As premissas lançadas na decisão do Tribunal de Justiça da União Europeia (TJUE) no caso dos Correios austríacos e, sobretudo, na opinião do Advogado-Geral no caso da Agência de Receitas Fiscais búlgara trazem parâmetros judiciais mais consistentes do que aqueles contidos na citada decisão da 2ª Turma do Superior Tribunal de Justiça brasileiro (REsp. nº 2.130.619 – SP). Elas podem ser resumidas da seguinte forma, com relação aos pressupostos da responsabilidade civil com base no art. 82 do RGPD:

Quanto ao descumprimento da RGPD, a violação de dados pessoais é o primeiro pressuposto para a responsabilidade civil, ao lado da existência de um dano indenizável e do nexo causal entre a violação e o dano. A violação dos dados pessoais, contudo, pode ocorrer mesmo quando o responsável pelo tratamento tenha observado o dever de cuidado para assegurar a sua proteção;

No que tange ao nexo de causalidade e fato exclusivo de terceiro, o fato de o incidente de segurança ter sido causado por um terceiro não constitui, em si mesmo, um motivo para isentar de responsabilidade o responsável pelo tratamento, a quem caberá o ônus de provar a adoção das “medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco”, nos termos do artigo 32 do RGPD;

Já o dano moral estará configurado independentemente do atingimento de certo grau de gravidade, devendo a compensação ser integral e efetiva, e cabendo ao titular dos dados a sua demonstração. Ainda que a utilização abusiva dos dados pessoais seja apenas potencial, e não efetiva, poderá se configurar o dano moral por violação ao RGPD. O prejuízo consistente no receio de uma eventual futura utilização abusiva dos seus dados pessoais, pode constituir um dano moral indenizável, desde que o titular dos dados demonstre ter sofrido individualmente um dano emocional, real e certo.

Esses critérios interpretativos fixados pelo Tribunal de Justiça da União Europeia para a aplicação uniforme do RGPD, contudo, serão aplicados aos casos concretos conforme outras normas legais no âmbito dos estados-nacionais, como estabelecido na decisão do TJUE.

Com relação ao Brasil, também se pode afirmar que a interpretação isolada da LGPD não é suficiente para resolver os temas concernentes à responsabilidade civil, cabendo o exame de outros diplomas para, à luz das circunstâncias fáticas, fixar o regime de responsabilidade civil e suas consequências práticas para a configuração do dano indenizável.

4. Contornos da Responsabilidade Civil na LGPD: Responsabilidade objetiva ou subjetiva?

A LGPD tratou especificamente da responsabilidade civil na sua Seção III, do Capítulo VI, sob o título "Da Responsabilidade e do Ressarcimento de Danos". Pelo princípio da especialidade, essas normas poderão ceder espaço a normas mais específicas, como o Código de Defesa do Consumidor, conforme previsão expressa contida no art. 45 da LGPD.

Como conceito geral, a responsabilidade civil do agente de tratamento de dados surge quando, "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", sendo obrigado a reparar o dano (*caput* do art. 42). Registre-se que a norma guarda sintonia com o já mencionado art. 82 do RGPD[25].

Em outras palavras, a responsabilidade civil pode ser entendida como o dever de reparar o dano decorrente do descumprimento do "dever jurídico de não lesar"[26] que, no caso, vem a ser a violação à legislação de proteção de dados pessoais ocorrida no exercício da atividade de tratamento.

A noção de violação também abrange as omissões dos agentes de tratamento. Conforme a expressa menção do parágrafo único do art. 44 da LGPD: "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano".

25. Art. 82, 1 do RGPD: "Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos".

26. GONÇALVES, Carlos Roberto. *Responsabilidade Civil*. 5 ed . São Paulo: Saraiva, 2010. p. 46.

Diferentemente do Código de Defesa do Consumidor, que adota como regra a responsabilidade civil objetiva dos fornecedores de produtos e serviços[27], não há semelhante clareza na LGPD com relação ao regime de responsabilidade civil aplicável aos agentes de tratamento de dados pessoais.

O art. 45 da LGPD, por sua vez, preconiza que as "hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente", ou seja, a responsabilidade será objetiva como regra, com exceção da responsabilidade pessoal dos profissionais liberais. Porém, quando a hipótese não versar sobre uma relação de consumo, a doutrina se divide sobre o tema, inexistindo uma orientação jurisprudencial sedimentada.

Para os defensores da tese da responsabilidade civil objetiva, parte-se do pressuposto de que a atividade de tratamento de dados contém risco inerente (ou risco criado, conforme a cláusula geral do parágrafo único do art. 927 do Código Civil), com considerável potencial de dano para os titulares de dados, além impactos transindividuais:

> (...) a atividade desenvolvida pelo agente de tratamento é evidentemente uma atividade que impõe riscos aos direitos dos titulares de dados. Estes riscos, por sua vez, são intrínsecos, inerentes à própria atividade. Significa dizer que os danos resultantes da atividade habitualmente empenhada pelo agente de tratamento de dados, uma vez concretizados, são quantitativamente elevados - pois atingem um número indeterminado de pessoas - e qualitativamente graves - pois violam direitos que possuem natureza personalíssima, reconhecidos pela doutrina como direitos que merecem a estatura jurídica de direitos fundamentais[28].

Essa compreensão do risco criado pela atividade de tratamento de dados está presente nos princípios da segurança, precaução, responsabilização e prestação contas, expressamente previstos no art. 6º da LGPD (incisos VII, VIII e X), bem como em diversos outros dispositivos que buscam prevenir ou até minimizar os riscos intrínsecos dessa atividade (art. 5º, XVII e art. 10, §3º). São exemplos de casos de risco inerente os "vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados"[29], que mere-

27. A exceção está expressamente prevista no §4º do art. 14 do CDC: "A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa".

28. Op. cit. MULHOLLAND, Caitlin. p. 15.

29. MULHOLLAND, Caitlin. A *LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais:*

cem ampla atenção da LGPD, assim como da Autoridade Nacional de Proteção de Dados (ANPD), no exercício de sua função regulatória.

Mesmo à luz de uma abordagem consequencialista que busque mitigar a responsabilidade civil dos agentes de tratamento em favor do desenvolvimento econômico dessa atividade, Maria Celina Bodin de Moraes preleciona que "a história já demonstrou que a adoção dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não limitaram o desenvolvimento de novas tecnologias". A autora prossegue:

> Ao contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade fundado na atenção e no cuidado para com o lesado"[30] [31].

De outro lado, para aqueles que sustentam a prevalência de responsabilidade civil com a necessidade de demonstração da culpa do agente, argumenta-se que a LGPD deixou diversas indicações em seu texto apontando para a adoção da responsabilidade subjetiva.

Em apertada síntese, entende-se que a estrutura da LGPD está alicerçada na criação de deveres, indicando o padrão de conduta socialmente esperado por parte dos agentes de tratamento de dados.

Além disso, o inciso II do art. 43[32] prevê expressamente a possibilidade de isenção de responsabilidade quando for demonstrado que não houve violação à legislação de proteção de dados:

> Aqui o legislador afirma que, ainda que exista nexo causal entre a conduta do agente e o dano, se ele conseguir provar que cum-

culpa ou risco? Migalhas, 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tr%E2%80%A6. Acesso em: 21 jul.. 2023.

30. BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito "proativo". Editorial. *Revista Civilistica.com*. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/ . Acesso em: 20.07.2023.

31. Na mesma obra, Maria Celina Bodin de Moraes comenta que o regime de responsabilidade na LGPD ultrapassa os contornos das regras da teoria clássica, qualificando-se como uma forma de responsabilidade ativa, no qual não seria suficiente apenas o cumprimento da letra da lei, mas sim a demonstração, por parte do agente de tratamento, conformidade com a norma e a eficácia concreta das medidas de segurança adotadas.

32. Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

> priu todos os deveres impostos pela LGPD, tomando as medidas de segurança recomendadas, não será responsabilizado. Com isso, o agente terá demonstrado que observou o standard esperado e que, se o incidente ocorreu, não foi em razão de sua conduta culposa. Esse inciso reflete, portanto, o regime subjetivo de responsabilidade adotado pela LGPD, porque está intrinsecamente vinculado ao elemento culpa e, exatamente por isso, sua redação não se assemelha à do CDC[33].

Um aspecto relevante sobre esse tema diz respeito ao ônus probatório sobre a adoção, por parte do agente de tratamento de dados, das medidas recomendadas e proporcionais para atender aos padrões de conduta delineados pela legislação e normativas aplicáveis.

Caso se entenda que cabe ao agente de tratamento de dados o encargo de comprovar que os padrões de segurança e cuidado legitimamente esperados foram devidamente observados e, apesar disso, houve o incidente, se estará adotando a teoria da culpa presumida, transferindo ao agente de tratamento o ônus probatório do cumprimento de seu dever legal de cuidado. É esse o entendimento adotado por Gisela Sampaio da Cruz Guedes:

> O artigo 43 da LGPD seguiu exatamente esse caminho, preferindo estabelecer um sistema de presunção de culpa, do que adotar o modelo objetivo de responsabilidade e, nesse aspecto, afasta-se completamente do Código de Defesa do Consumidor. A presunção é relativa e, no caso da LGPD, o standard de "conduta socialmente esperada" foi definido pelo próprio legislador.

Uma análise aprofundada do tema é encontrada no artigo "Responsabilidade civil pelo tratamento de dados pessoais na lei geral de proteção de dados"[34], que conclui apontando para uma solução "não binária", de modo que o regime de responsabilidade civil aplicável deva se moldar às peculiaridades do caso concreto:

> Em que pese a controvérsia doutrinária, pondera-se que a solução não deverá estar, necessariamente, em um dos dois extremos: res-

33. SAMPAIO, Gisela. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (coord.). *Caderno especial: Lei Geral de Proteção de Dados (LGPD)*. São Paulo: Thomson Reuters Brasil, 2019, p. 169.

34. FERRÃO DOS SANTOS, C.; GOMES DA SILVA, J.; & PADRÃO, V. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. *Revista Eletrônica da PGE-RJ, 4(3)*. 2021. Disponível em: https://doi.org/10.46818/pge.v4i3.256.

> ponsabilidade objetiva ou subjetiva para todo e qualquer caso. A doutrina vem se esforçando na tentativa de achar soluções intermediárias, como o caso da já mencionada teoria da responsabilidade civil "proativa" e, por outro lado, até mesmo suscitando indagações sobre se o regime deveria variar de acordo com as peculiaridades do caso concreto. É o que sugerem, por exemplo, Gisela Guedes e Rose Meireles quando vislumbram a possibilidade de o regime ser objetivo nos casos específicos de tratamento de dados sensíveis[35].

Como se pode observar, o tema está longe de uma uniformização. Mas além das divergências, há também aspectos convergentes. A atividade de tratamento de dados é reconhecida como potencialmente lesiva e tem destacado relevo social, demandando dos agentes de tratamento a observância de deveres de cuidado e padrões de conduta, bem como submetendo-se à fiscalização e controle por parte da Autoridade nacional de proteção de dados, dotada de poder de polícia, notadamente consubstanciado no seu poder sancionador.

Acrescente-se que, especialmente com relação aos dados pessoais tratados em meio digital, em razão da complexidade das ferramentas tecnológicas empregadas, a aferição do adequado cumprimento dos deveres e padrões de segurança impostos pela legislação de proteção de dados consiste em uma tarefa - ou ônus probatório - impossível ao titular dos dados vítima de incidente, relevando-se sua inequívoca hipossuficiência técnica ou informacional[36].

Desta forma, os regimes da responsabilidade civil objetiva ou mesmo da culpa presumida têm o mérito de eximir o titular do ônus de produzir essa verdadeira "prova diabólica", cabendo ao agente de tratamento demostrar a inexistência de sua culpa (para os que defendem a responsabilidade subjetiva) ou a existência algumas das hipóteses de exclusão de responsabilidade objetiva (como o fato exclusivo de terceiro ou da própria vítima).

Caso a matéria seja regida pela regra da responsabilidade civil subjetiva, ainda se poderá recorrer à técnica processual da inversão (inciso VIII do art. 6º do CDC) ou da distribuição dinâmica dos ônus da prova, prevista no §1º, do art. 373 do Código de Processo Civil.

35. Ibidem, p. 29.
36. BRASIL. Superior Tribunal de Justiça. *REsp 1.155.770-PB*, Rel. Min. Nancy Andrighi. DJe: 09/03/2012.

5. Dados pessoais comuns e sensíveis

Os dados pessoais são as informações relacionadas à pessoa natural identificada ou identificável (artigo 5º, I), ao passo que os dados pessoais sensíveis são aqueles relacionados à "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. 5º, II).

De acordo com os ensinamentos de Caitlin Mulholland, independentemente do fato de os dados pessoas serem sensíveis ou não, o regime de responsabilidade civil disciplinado na Lei Geral de Proteção de Dados Pessoais deve ser único e o dano injusto resultante de sua violação deverá ser integralmente reparado, seguindo a regra geral da responsabilidade civil, notadamente o art. 944 do Código Civil, segundo o qual a indenização se mede pela extensão do dano. A professora enfatiza que:

> (...) a categoria de dados sensíveis não deve ser considerada como estruturalmente diversa da categoria de dados não sensíveis, na medida em que tanto uma quanto outra estão sujeitas à potencialidade de tratamentos discriminatórios e geradores de danos a seus titulares. Sendo assim, não deve haver uma diferenciação de regimes de responsabilidade civil, baseada numa classificação dos dados como sensíveis ou não[37].

Com efeito, a distinção com relação aos dados pessoais comuns ou sensíveis deve se deslocar para o campo de verificação e mensuração dos danos injustos provocados.

Via de regra, incidentes de segurança envolvendo dados sensíveis podem trazer consequências mais graves para os seus titulares. Tal assertiva é ainda mais válida quando o titular dos dados sensíveis for criança e adolescente, diante do reconhecimento da condição de "hipervulnerabilidade ou vulnerabilidade agravada [que] podem ser inferidos do artigo 227 da Constituição Federal, o qual dispõe acerca do princípio da prioridade absoluta aos direitos da criança e do adolescente"[38]. Nessas hipóteses, o tratamento deverá levar

37. MULHOLLAND, Caitlin. *Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)*. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensíveis.pdf. Acesso em: 20 jul. 2023.

38. TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book. p. 347.

em consideração melhor interesse do titular, a ser avaliado no caso concreto, conforme o Enunciado nº1 da ANPD[39].

Contudo, a depender das peculiaridades do caso concreto, um incidente envolvendo dados pessoais comuns pode se revelar de enorme gravidade para o seu titular. A guisa de exemplo, a disponibilização indevida de dados relativos ao endereço de uma pessoa ameaçada pode expô-la a risco de vida. Com mais frequência, podem acarretar a redução de suas chances de obtenção de emprego[40], serem usados para criação de perfis falsos em redes sociais, contratação fraudulenta de crédito ou facilitar para a aplicação de golpes bancários, temas que vêm sendo enfrentado pelo STJ nas recentes decisões já comentadas.

Também nesse sentido, foi aprovado o enunciado nº 690, na IX Jornada de Direito Civil do Conselho da Justiça Federal, dispondo que: "A proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD"[41]. Segundo o escólio da professora Chiara de Teffé, "qualquer tratamento de dados pessoais que *revele* dados sensíveis e possa causar danos ao titular" será merecedor da proteção ampliada[42].

Ainda, é sabido que a partir do processamento de dados isoladamente triviais pode-se chegar a informações sensíveis e relevantes por meio de técnicas de inferência, a exemplo do conhecido "Caso Target"[43], envolvendo a empresa varejista estadunidense e do já citado caso da Agência Postal Austríaca, julgado pelo Tribunal de Justiça da União Europeia.

39. BRASIL. Autoridade Nacional de Proteção de Dados. *Enunciado CD/ANPD nº 1*, de 22 de maio de 2023. DOU 24/05/2023. O enunciado dispõe que: "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

40. Por conta do CEP, moradores de favela relatam dificuldades para conseguir emprego. *Voz das Comunidades. (on-line)* Disponível em: https://www.vozdascomunidades.com.br/destaques/por-conta-do-cep-moradores-de-favela-relatam-dificuldades-para-conseguir-emprego/. Acesso em 26 ago. /2023.

41. BRASIL. Conselho da Justiça Federal. *IX Jornada Direito Civil: comemoração dos 20 anos da Lei n. 10.406/2022 e da instituição da Jornada de Direito Civil: enunciados aprovados (online)*. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022. p. 49. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 03 dez. 2023.

42. TEFFÈ, Chiara Spadaccini de. *Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas*. São Paulo: Editora Foco, 2022.

43. A empresa Target, uma das maiores varejistas dos Estados Unidos adotou ferramentas tecnológicas de coleta e processamento massivo de dados de seus clientes, sendo capaz de identificar um certo padrão de consumo das clientes grávidas, como a compra de loções e sabonetes sem essência, além de suplementos alimentares como cálcio, magnésio e zinco. "Com essa informação em mãos, a empresa enviava às clientes cupons de descontos e ofertas personalizadas para o período da gravidez em que se encontravam, tendo em vista o modelo preditivo construído. Todavia, houve o envio de cupons para a residência de uma adolescente que, até então, não havia revelado ao seu pai que estava grávida. Foi por meio do recebimento desses cupons que o pai veio a saber sobre a gravidez de sua filha, desencadeando um profundo debate sobre o uso ético das ferramentas de inteligência artificial e análise preditiva de dados comportamentais". Sato, Priscila Kei; Rupel, Manuela. In: Lei Geral de Proteção de Dados e Direitos Fundamentais. https://www.migalhas.com.br/coluna/questao-de-direito/341858/lei-geral-de-protecao-de-dados-e-direitos-fundamentais . Acesso em 26.07.2023.

Portanto, ainda que a legislação imponha um padrão de segurança mais elevado para os dados pessoais sensíveis – assim como um especial dever de cuidado com os dados de crianças e adolescentes –, a responsabilização pelos danos provocados em caso de incidente de segurança não podem excluir ou, sob qualquer aspecto, desproteger os dados comuns, devendo ser aferido, no caso concreto, a existência e a extensão de um dano injusto.

6. O dano injusto

O dano é o elemento nodal da responsabilidade civil. Sob influência da legislação italiana, "a discussão em torno da reparação civil centra-se não mais no descumprimento estrutural da lei (direito subjetivo), mas, sim, na violação dos valores e interesses tutelados pelo ordenamento"[44], dando ensejo ao dever de indenizar.

Além do dano patrimonial (ou material), o dano injusto pode atingir interesses extrapatrimoniais (dano moral ou imaterial) que, em sentido amplo, representam a violação de direito ou atributo da personalidade, abrangendo todas as ofensas à pessoa, "considerada esta em suas dimensões individual e social, ainda que sua dignidade não seja arranhada"[45].

Nessa perspectiva, a 3ª Turma do STJ julgou os dois casos recentes envolvendo golpes bancários (golpe do motoboy e golpe do boleto). No julgamento do REsp. nº 2.077.278 - SP, a Corte enfatizou que a responsabilidade das instituições financeiras, no que tange ao vazamento de dados pessoais que culminam na facilitação de estelionato, exige que a origem do tratamento indevido seja o sistema bancário pois, na falta de elementos objetivos que demonstrem esse nexo causal, "não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social"[46].

No caso concreto, os dados vazados correspondiam a informações próprias do contrato bancário, não tendo a instituição financeira se desincumbido de seus ônus de comprovar a causa excludente de sua responsabilidade, nos termos do §3º do art. 14, do CDC e art. 43 da LGPD. Ademais, diante dos riscos inerentes à atividade bancária, seu dever de segurança e proteção dos dados

44. TEPEDINO, Gustavo; TERRA, Aline Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos de Direito Civil: responsabilidade civil*. 2 ed. Rio de Janeiro: Forense, 2021. p. 31.

45. CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 15. Ed. Barueri. São Paulo: Atlas, 2022. p. 103.

46. BRASIL. Superior Tribunal de Justiça. *REsp 2.077.278-SP*, Rel. Min. Nancy Andrighi, DJe: 09/10/2023.

sigilosos dos consumidores é qualificado, exigindo a aplicação das melhores técnicas de tecnologia da informação.

De acordo com jurisprudência predominante do Superior Tribunal de Justiça, esposando uma acepção subjetiva do dano, uma vez demonstrada a ocorrência de ofensa injusta à dignidade da pessoa humana, pode ser dispensada a comprovação de dor e sofrimento para configuração de dano moral. A indenização, nesses casos, independerá da demonstração da repercussão psíquica do dano, traduzindo-se, pois, em consequência *in re ipsa*, ou seja, intrínseca à própria conduta causadora do dano injusto[47], tal como foi a solução adotada nos recentes casos envolvendo o golpe do boleto e o golpe do motoboy.

Observe-se que a Terceira Turma do STJ já havia reconhecido a hipótese de dano moral *in re ipsa* em caso de vazamento de dados de cliente bancário:

> 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais.
> 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos.
> 11. Hipótese em que se configura o dano moral *in re ipsa*.[48]

Noutro giro, em favor de uma abordagem mais objetiva do dano moral, parte da doutrina defende que:

> (...) a noção subjetiva de dano moral tem sido relativizada, devendo-se buscar o seu afastamento, de modo que o abalo psicológico não mais seja tido como elemento fundamental ao dano moral – ainda que possa, de certa forma, ser considerado para fins de quantificação. Deve-se, portanto, buscar privilegiar a caracterização objetiva da lesão, independentemente de repercussão psíquica do dano, garantindo-se, com isso, a tutela e reparação mais amplas

47. BRASIL. Superior Tribunal de Justiça. *REsp 1.292.141-SP*, Rel. Min. Nancy Andrighi, DJe: 12/12/2012.
48. BRASIL. Superior Tribunal de Justiça. *REsp. 1.758.799 – MG*, Rel. Min. Nancy Andrighi, DJe: 19/11/2019..

> das violações a bens existenciais.[49]

Assim, o dano moral deixa de ser concebido como o sofrimento, a angústia ou a dor sofridas pelo ofendido, mas sim "como uma lesão a um interesse existencial concretamente merecedor de tutela"[50], mais objetivamente considerado.

> Inexistiria, portanto, dualidade entre o fato lesivo e o dano moral, este apreciado objetivamente. O dano moral se configuraria a partir da própria qualificação e apreciação do fato lesivo, vale dizer, uma vez reconhecido determinado evento como injusto e violador de interesses extrapatrimoniais, restará identificado o dano, sem a necessidade de uma segunda operação hermenêutica para liquidar a reparação. A determinação da existência e extensão do dano, desta forma, se faz de acordo com as peculiaridades concretas da lesão e da vítima, objetivamente considerada. Como sustenta por Milena Donato Oliva, "[p]or isso que a doutrina alerta para a desnecessidade do recurso ao *in re ipsa* quando se adota o conceito objetivo de dano moral"[51].

A opinião do Advogado-Geral do Tribunal de Justiça da União Europeia no caso acima citado (VB contra Agência Nacional de Receitas Fiscais) parece se filiar a esse entendimento, afastando-se da noção subjetiva de abalo psicológico:

> A fronteira entre os simples descontentamentos (não indenizáveis) e os verdadeiros danos morais (indenizáveis) é tênue, mas os órgãos jurisdicionais nacionais, aos quais cabe a função de delimitar caso a caso essa fronteira, devem proceder a uma avaliação atenta de todos os elementos fornecidos pelo titular dos dados que pede a indenização, a quem caberá o ônus de alegar com precisão, e não de modo genérico, elementos concretos suscetíveis de conduzir à existência de um "dano moral efetivamente sofrido" devido à violação de dados pessoais, sem que, no entanto, esse dano atinja um limiar específico de gravidade predeterminado: o que importa é que não se trate da simples percepção subjetiva, variável e dependente igualmente de elementos de caráter e pessoais, mas de uma

49. TEPEDINO, Gustavo; TERRA, Aline Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos de Direito Civil: responsabilidade civil*. 2 ed. Rio de Janeiro: Forense, 2021. p. 43.

50. FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. *Curso de direito civil: Responsabilidade civil*. v. 7. Ed. Salvador: Ed. Juspodivm, 2022, p. 329.

51. OLIVA, Milena Donato. Dano Moral e Inadimplemento Contratual nas Relações de Consumo. In: *Revista de Direito do Consumidor*, vol. 93, São Paulo: Editora dos Tribunais, mai./jun. 2014, p. 13 – 28.

> inquietação objetiva, mesmo que ligeira mas demonstrável, na sua esfera física ou psíquica ou na sua vida pessoal, da natureza dos dados pessoais em causa e da importância que revestem para a vida do titular dos dados e talvez também da percepção que a sociedade tem, nesse momento, dessa inquietação específica decorrente da violação dos dados".

Já o acórdão da 2ª Turma do STJ no caso de vazamento de dados envolvendo a Eletropaulo (REsp. 2.130.619 – SP), em que pese o reconhecimento do fato lesivo cometido pela empresa (a violação dos dados pessoas), limita-se a afastar a técnica da presunção do dano moral (dano *in re ipsa*), atribuindo à titular dos dados (autora) o encargo de provar o dano.

Porém, partindo-se da premissa acima colocada de que o dano moral se consubstancia na apreciação objetiva do fato lesivo, a ausência no acórdão de outros parâmetros interpretativos poderá levar a uma substancial dificuldade na busca pela compensação dos danos morais em casos de vazamento de informações de dados comuns.

Considerações finais

O ordenamento jurídico brasileiro consagra a proteção de dados como um direito fundamental autônomo, manifestando-se como uma projeção dos direitos da personalidade e da própria dignidade humana.

A Lei Geral de Proteção de Dados impõe aos agentes de tratamento um conjunto de medidas de segurança, complementadas ainda por outras normativas, em especial as emanadas pela Autoridade Nacional de Proteção de Dados, que tem papel de fiscalização do dever de cuidado dos agentes para com os dados pessoais por eles tratados.

A despeito disso, os vazamentos de dados e outras modalidades de incidentes de segurança são uma realidade concreta e razoavelmente frequente. Sejam dados sensíveis ou não, é certo que o avanço das tecnologias da informação e comunicação, aliado às ferramentas como *Big Data* e *Big Analytics*, permitem a colheita e o processamento massivo desses dados, colocando-os em mãos de terceiros não autorizados um expressivo volume de dados pessoais, o que extrapola em muito as garantias fundamentais à inviolabilidade da intimidade e da vida privada de seus titulares.

Neste contexto, a função solidarista da responsabilidade civil tem um relevante papel a desempenhar na proteção às vítimas de incidentes de consumo e, como repercussão social do dever de indenizar, no incentivo ao incremento

em investimentos e adesão às regras de proteção do sigilo e da segurança dos dados pessoais, por parte dos agentes de tratamento.

Como elemento central da responsabilidade civil, o dano indenizável - patrimonial ou extrapatrimonial - deve estar sempre configurado para que surja o dever de indenizar. Quanto ao dano moral, observa-se que a jurisprudência pátria ainda aborda o tema sob uma perspectiva predominantemente subjetivista e, no que diz respeito à sua comprovação, casuística. As hipóteses de dano presumido, com a adoção da técnica do dano *in re ipsa*, facilitam a liquidação do dano em favor da vítima. Não obstante, parte da doutrina recomenda a adoção de uma aferição objetiva da conduta lesiva, de acordo com as peculiaridades concretas da lesão e da vítima.

De outro ângulo, a responsabilização por danos decorrentes de incidente de segurança devem abranger todos dos dados pessoais, sensíveis ou não, desde que se verifique no caso concreto uma conduta violadora de um dever legal, a ocorrência de dano injusto - material ou moral - e o pertinente nexo causal.

A fixação de parâmetros jurisprudenciais para a identificação e liquidação dos danos morais em casos de vazamento de dados e outros incidentes de segurança se mostra necessária, seja para se evitar uma banalização das indenizações ou, de outro lado, mitigar por demasiado esse importante instituto da responsabilidade civil, deixando os ônus dos incidentes desproporcionalmente sobre os ombros dos titulares dos dados, como parece ser o caso do acórdão proferido pela 2ª Turma do STJ, acima comentado.

As divergências existentes nos precedentes do Superior Tribunal de Justiça ainda pendem de ser dirimidas. Em sua função de uniformização da interpretação da legislação federal e da jurisprudência dos tribunais, cabe ao STJ apontar diretrizes para caracterização do dano moral em casos de vazamento ou comercialização não autorizada de dados pessoais, sensíveis ou não, e indicar bases interpretativas para as hipóteses de cabimento da presunção de dano extrapatrimonial, com base na valoração da conduta violadora da norma e seus reflexos concretos para o ofendido.

Passos nesse sentido também vêm sendo trilhados no âmbito da União Europeia e seus órgãos jurisdicionais, com base na interpretação e aplicação do RGPD. O estudo dos casos examinados acima, apontam para a afirmação do princípio da reparação integral, afastando a possibilidade de limitação de indenizações apenas para danos de maior gravidade, bem como admitindo a compensação por danos morais em casos de potencial e não efetiva utilização

abusiva dos dados pessoais. Prestigia-se, assim, uma abordagem mais objetiva do dano, com foco na lesão dos interesses existenciais atingidos pela violação concreta das normas de proteção do sigilo e da segurança dos dados pessoais.

Atento às características nacionais, desafios importantes ainda estão por ser enfrentados pela doutrina e jurisprudência pátrias na efetivação das proteções previstas na LGPD.

Referências

BODIN DE MORAES, Maria Celina. Editorial, LGPD: Um novo regime de responsabilização civil dito "proativo". *Civilistica.com*. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso em: 20 jul.2023.

BRASIL. Autoridade Nacional de Proteção de Dados. *Enunciado CD/ANPD nº 1*, de 22 de maio de 2023. DOU: 24/05/2023.

BRASIL. Conselho da Justiça Federal. *IX Jornada Direito Civil: comemoração dos 20 anos da Lei n. 10.406/2022 e da instituição da Jornada de Direito Civil: enunciados aprovados* (online). Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022. p. 49. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 03 dez. 2023.

BRASIL. Superior Tribunal de Justiça. *REsp 1.292.141-SP*, Rel. Min. Nancy Andrighi, DJe: 12/12/2012.

BRASIL. Superior Tribunal de Justiça. *REsp 1.155.770-PB*, Rel. Min. Nancy Andrighi. DJe: 09/03/2012.

BRASIL. Superior Tribunal de Justiça. *REsp. 1.758.799 – MG*, Rel. Min. Nancy Andrighi, DJe: 19/11/2019.

BRASIL. Superior Tribunal de Justiça. *REsp 2.015.732 – SP*. Rel. Min. Nancy Andrighi. DJe: 26/06/2023.

BRASIL. Superior Tribunal de Justiça. *REsp 2.077.278-SP*, Rel. Min. Nancy Andrighi, DJe 09/10/2023.

BRASIL. Superior Tribunal de Justiça. *REsp. 2.130.619-SP*, Rel. Min. Francisco Falcão, DJe: 09/03/2023.

BRASIL. Supremo Tribunal Federal. *ADI 6.393 MC-Ref-DF*. Rel. Min. Rosa Weber. Plenário. DJe: 07.05.2020.

BRASIL. Supremo Tribunal Federal. *Inquérito 4.781-DF*. Despacho https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/INQ-4781PET.pdf. Acesso em: 25 jul. 2023.

CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 15. ed. Barueri, SP: Atlas, 2022.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. *Curso de direito civil: Responsabilidade civil*. v. 7. Ed. Salvador: Ed. Juspodivm, 2022.

FERRÃO DOS SANTOS, C.; GOMES DA SILVA, J.; PADRÃO, V. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. *Revista Eletrônica da PGE-RJ, 2021*, v. 4 n. 3 . Disponível em: https://doi.org/10.46818/pge.v4i3.256. Acesso em 24 jul.2023.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 25-29.

GONÇALVES, Carlos Roberto. Responsabilidade civil. 5 ed . São Paulo: Saraiva, 2010.

LEMOS, Ronaldo. *O vazamento de dados do fim do mundo: A partir de agora o Brasil se tornou também um faroeste digital*. Folha de S.Paulo on-line, 2021. Disponível em: https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/01/o-vazamento-de-dados-do-fim-do-mundo.shtml. Acesso em: 18 jul. 2023.

MULHOLLAND, Caitlin. *A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?* Migalhas, 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tr%E2%80%A6. Acesso em: 21 jul. 2023.

MULHOLLAND, Caitlin. *Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018)*. Puc-Rio. 2021. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensíveis.pdf. Acesso em: 20 jul. 2023.

OLIVA, Milena Donato. Dano Moral e Inadimplemento Contratual nas Relações de Consumo. In: *Revista de Direito do Consumidor*, vol. 93, São Paulo: Editora dos Tribunais, mai./jun. 2014, p. 13 – 28.

SAMPAIO, Gisela. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. In: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (coord.). *Caderno especial: Lei Geral de Proteção de Dados (LGPD)*. São Paulo: Thomson Reuters Brasil, 2019, p. 169.

TEFFÈ, Chiara Spadaccini de. D*ados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas*. São Paulo: Editora Foco, 2022.

TEFFÈ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

TEPEDINO, Gustavo; TERRA, Aline Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos de Direito Civil: responsabilidade civil*. 2 ed. Rio de Janeiro: Forense, 2021. p. 31.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C- 340/21: VB contra Natsionalna agentsia za prihodite (Agência Nacional de Receitas Fiscais da Bulgária). *Conclusões do Advogado-Geral Giovanni Pitruzzella* de 27.04.2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=DDCCF5FAFBC93C875584F8B7C3DB165F?text=&docid=272977&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=702058. Acesso em: 20 jul. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-300/21: UI contra Österreichische Post AG (Empresa Postal Austríaca). *Acórdão* de 04.05.2023. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=2738956. Acesso em: 26 nov. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

2

Tratamento de dados de crianças no ambiente digital: desafios enfrentados pela indústria de jogos online e alternativas para minimização de riscos

JULIANA ALMEIDA CONTE

JULIANA ALMEIDA CONTE[1]

Sumário: Introdução. 1. Desafios enfrentados pela indústria de jogos online no tratamento de dados pessoais de crianças. 2. As bases legais aplicáveis ao tratamento de dados pessoais de crianças. 2.1. Como o Enunciado CD/ANPD nº 1 impacta o tratamento de dados de crianças no ambiente de jogos online. 2.2. O princípio do melhor interesse como norteador do tratamento de dados de crianças. 3. Alternativas e medidas de mitigação de riscos. Considerações finais. Referências.

Introdução

A disseminação do uso de tecnologias digitais está transformando consideravelmente as condições da infância em âmbito global. Estima-se que um em cada três usuários de internet em todo o mundo tenha menos de 18 anos. Essa tendência, embora sujeita a variações relacionadas a faixa etária, contextos sociais e diferenças entre países, torna evidente um aumento no acesso à internet por crianças, tanto em termos de frequência quanto de diversificação de dispositivos e serviços utilizados, o que tem ocorrido em idades cada vez mais jovens e abrange uma maior variedade de atividades online[2].

O Brasil tem se destacado como um dos principais mercados de jogos online[3], tanto em termos de consumo quanto de produção. O aumento do acesso à internet e a popularização dos dispositivos móveis contribuíram para que as crianças e jovens brasileiros se tornassem uma presença significativa nos jogos online. Segundo dados do Comitê Gestor da Internet no Brasil (CGI.br), a partir da pesquisa "TIC Kids Online Brasil 2022"[4], cerca de 92% das crianças e adolescentes entre 9 e 17 anos acessam a internet no país, sendo que grande parte desse grupo jogam jogos online. Em 2022, a porcentagem de usuários de Internet jogando online com outros jogadores foi de 59% para a faixa etária de 9 a 10 anos, 56% para 11 a 12 anos, 61% para 13 a 14 anos e 55% para 15 a 17

1. Advogada da área de Proteção de Dados, Tecnologia e Propriedade Intelectual. Graduada em Direito pela Universidade Presbiteriana Mackenzie, pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade em parceria com a Universidade do Estado do Rio de Janeiro. Certificada pela IAPP – International Association of Privacy Professionals como Certified Information Privacy Manager – CIPM/IAPP e como Encarregado de Proteção de Dados Certificado no Brasil – CDPO/BR.

2. LIVINGSTONE, S., TAMBINI, D. and BELAKOVA, N. (2018) *Research for CULT Committee – Recommendations for EU policy developments on protection of minors in the digital age*. Brussels: European Parliament, Policy Department for Structural and Cohesion Policies. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/617454/IPOL_IDA(2018)617454_EN.pdf. Acesso em 10 jun. 2023.

3. Neste artigo, "jogo online" é definido como qualquer tipo de jogo digital individual ou multijogador, por meio de qualquer dispositivo conectado à Internet, incluindo consoles dedicados, computadores de mesa, laptops, tablets e celulares.

4. Comitê Gestor da Internet no Brasil. (2020). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil [livro eletrônico]: *TIC Kids Online Brasil 2022*. Disponível em: https://cetic.br/media/docs/publicacoes/1/20230825142135/tic_kids_online_2022_livro_eletronico.pdf Acesso em 11 nov. 2023.

anos. Esses números refletem a importância dos jogos online como uma forma de entretenimento e interação social.

De acordo com o relatório *Key Insights into Brazilian Gamers - Newzoo Gamer Insights Report*[5], o Brasil ocupa a 10ª posição no ranking global de consumo de jogos, com uma receita de US$ 2,6 bilhões em 2022. Além disso, o país conta com uma indústria de desenvolvimento de jogos em expansão, com estúdios independentes ganhando reconhecimento internacional. A Pesquisa Nacional da Indústria de Games, realizada pela Associação Brasileira das Desenvolvedoras de Jogos Eletrônicos (Abragames) em parceria com a Agência Brasileira de Promoção de Exportação e Investimentos (ApexBrasil), identificou um aumento significativo no número de estúdios de desenvolvimento de jogos atuantes no Brasil. Entre 2019 e 2022, foi registrado um crescimento de cerca de 160%[6].

Essa crescente popularidade dos jogos no Brasil tem impactado diretamente o número de crianças - definidas aqui como aquelas com até 12 anos - engajadas em jogos online; cenário que vem acompanhado de uma também crescente preocupação sobre a privacidade e proteção de dados desses indivíduos. Diante do avanço tecnológico acelerado e da redução da idade em que as crianças têm o primeiro contato com atividades de lazer digital, é crucial direcionar maior atenção à considerável quantidade de dados pessoais coletados e tratados por meio de jogos online, assim como aos riscos que esse complexo mecanismo representa para a privacidade[7].

A coleta de dados pessoais tem se tornado um recurso cada vez mais utilizado e indispensável para transformar os jogos em serviços contínuos. Ao compreender o perfil dos jogadores, as empresas distribuidoras e/ou desenvolvedoras conseguem atender aos seus interesses e expectativas, podendo, inclusive, influenciar diretamente ou indiretamente o comportamento do pú-

5. Newzoo. *Key Insights into Brazilian Gamers - Newzoo Gamer Insights Report*. Disponível em: https://resources.newzoo.com/hubfs/Reports/Consumer%20Insights/2022_Key_Insights_Into_Brazilian_Gamers_Newzoo_Consumer_Insights_Report.pdf?utm_campaign=CI%20Countries&utm_medium=email&_hsmi=225857891&_hsenc=p2ANqtz-9Q5hKq1lJr-AycSQZ73v-FjUIIvyPn2i5JgUeWlHDXB02EB8HzCwqzJhJAn3S3Iil0WE94bbUedtS14UCH7KNz3uZFeH31dP2xvdP_jQrLZpzz5-_c&utm_content=225857891&utm_source=hs_automation. Acesso em 13 de novembro de 2023.

6. PACETE, Luiz Gustavo. *Estúdios brasileiros devem movimentar R$ 250 milhões em 2023*. Forbes. Maio de 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/05/estudios-brasileiros-devem-movimentar-r-250-milhoes-em-2023/. Acesso em 24 jun. 2023.

7. ENESCU, Maria-Alexandra. *Protecting children's personal data from abusive personal data processing performed by video game companies*. Thesis for: Master's Degree - LL.M in International and European Law with a Data Law specialization. Orientador: Cristopher Kuner. Vrije Universiteit Brussel. Institute for European Studies. 2019. p. 4. Disponível em: https://www.researchgate.net/profile/Maria-Alexandra-Enescu/publication/344413116_Protecting_children%27s_personal_data_from_abusive_personal_data_processing_performed_by_video_game_companies/links/5f957ebd92851c14bce580fd/Protecting-childrens-personal-data-from-abusive-personal-data-processing-performed-by-video-game-companies.pdf Acesso em 25 jun. 2023.

blico-alvo. Essa questão, contudo, se torna mais complexa quando consideramos que grande parte desse público é composta por crianças[8].

Assim, a exposição de crianças no ambiente digital levanta diversos questionamentos e desafios sob o tratamento de seus dados pessoais, diante de sua hipervulnerabilidade, das limitações cognitivas e da falta de experiência em razão do estágio de desenvolvimento intelectual desse público.

O presente artigo tem como objetivo avaliar o tratamento de dados de crianças por empresas desenvolvedoras de jogos online à luz da legislação brasileira. Para tanto, serão avaliados os dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - "LGPD") aplicáveis a tal tratamento, o recente Enunciado CD/ANPD nº 1, o princípio do melhor interesse e os potenciais riscos envolvidos, bem como as alternativas viáveis para a indústria de jogos.

A delimitação teórica do escopo, focando exclusivamente em crianças com até 13 anos incompletos, foi estabelecida devido à maior vulnerabilidade desses indivíduos. Além disso, tal escolha está em conformidade com o recorte estipulado pela Convenção sobre os Direitos da Criança, adotada pela Organização das Nações Unidas (ONU), que reconhece a necessidade de uma proteção especial para crianças devido à sua condição peculiar de desenvolvimento e maturidade.

O primeiro tópico aborda os desafios enfrentados pela indústria de jogos online no tratamento de dados pessoais de crianças, exemplificando o cenário nebuloso com alguns incidentes recentes envolvendo dados de crianças nesta indústria. O segundo tópico aborda as bases legais aplicáveis ao tratamento de dados pessoais de crianças e como o Enunciado CD/ANPD nº 1 expandiu as possibilidades para o tratamento de dados de crianças no ambiente de jogos online. No segundo tópico também é feita uma análise do princípio do melhor interesse como norteador do tratamento de dados de crianças. Por fim, o último tópico busca apresentar alternativas factíveis para a indústria de jogos online, medidas de adequação necessárias e possíveis medidas mitigadoras de riscos.

8. PINHEIRO, Ana Clara Moreira; LUZ, Gustavo; ALMEIDA, Juliana; MONTEIRO, Mariana Pires; KASPUTIS, Matheus Botsman; RIBEIRO, Natália Góis; BRAOIOS, Rafaella Resck. *Guia LGPD e games*. A year in privacy. 2022. Disponível em: https://baptistaluz.com.br/guia-lgpd-e-games-a-year-in-privacy-9/. Acesso em 25 jun. 2023.

1. Desafios enfrentados pela indústria de jogos eletrônicos no tratamento de dados pessoais de crianças

No contexto atual da Internet de alta velocidade, observa-se a crescente tendência da indústria de jogos online em se tornar *data-driven*, isto é, orientada por dados. A obtenção e utilização de dados desempenham um papel fundamental no sucesso das empresas de tecnologia contemporâneas e isso também se aplica à indústria de jogos online em constante crescimento.

As empresas de tecnologia, especialmente as desenvolvedoras de jogos online, desempenham um papel fundamental na coleta de dados pessoais e possuem a capacidade de utilizá-los para fins econômicos ou para a tomada de decisões que podem ter um impacto significativo na vida das crianças. Os dados coletados permitem que as empresas compreendam melhor seus usuários, identifiquem padrões de comportamento, personalizem as experiências de jogo e forneçam conteúdo relevante[9]. Essas informações são valiosas para melhorar a qualidade dos jogos e oferecer recursos inovadores, sendo essenciais para impulsionar o crescimento e a competitividade da indústria de jogos online.

As informações coletadas, como preferências de jogo, comportamentos de navegação e dados demográficos, podem ser empregadas para objetivos específicos com base nos interesses e características dos usuários mais jovens. A coleta e o uso dessas informações permitem às empresas desenvolverem experiências personalizadas, adaptando o conteúdo e os recursos do jogo de acordo com as preferências e necessidades individuais das crianças, com o objetivo de aumentar o engajamento e a retenção dos jogadores.

No entanto, recentes incidentes ocorridos nas indústrias de jogos online evidenciam a importância de se proteger os dados e os sistemas que os abrigam[10].

Um exemplo recente foi a grave violação de segurança no site Neopets, em julho de 2022, que resultou na exposição de informações pessoais de cerca de 69 milhões de pessoas, trazendo à luz os riscos enfrentados pelas plataformas online e os desafios relacionados à proteção de dados. A vulnerabilidade

9. LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p.16. E-book. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/12/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-its.pdf Acesso em 01 jul. 2023

10. Games Industri.biz. *Data Protection in the Games Industry: Part 1- What games business need to know about data protection*. 14 de junho de 2011. Disponível em: https://www.gamesindustry.biz/data-protection-in-the-games-industry-part-1-article Acesso em 01 jul. 2023.

do sistema permitiu que hackers obtivessem acesso indevido ao código-fonte e aos sistemas internos do jogo, o que permitiu acesso ao banco de dados que continha detalhes como nomes, endereços de e-mail, gênero, datas de nascimento, senhas criptografadas, dados de localização e informações do perfil de cada jogador, conforme trecho disponibilizado na *dark web*[11]. É importante ressaltar que o público-alvo principal desse jogo é composto principalmente por crianças, o que amplifica ainda mais as potenciais consequências negativas decorrentes desse incidente. Apesar de não informar claramente a classificação indicativa do jogo, os Termos de Uso disponíveis no site da Neopets, estabelecem que se o usuário tiver menos de 18 anos nos EUA ou for considerado uma criança na sua respectiva jurisdição, deve avaliar sua participação no jogo com seus pais[12]. Em complemento, a Política de Privacidade informa que o jogo Neopets não se dispõe a coletar dados de menores de 13 anos[13].

Mais especificamente sobre dados pessoais de crianças, a Microsoft foi multada em US$ 20 milhões pelo *Federal Trade Comission* (FTC), órgão regulador do comércio dos EUA, por violar o *Children's Online Privacy Protection Act* (COPPA) ao coletar dados de crianças que se inscreveram em seu sistema de jogos Xbox entre 2015 e 2020 sem notificar ou obter consentimento dos pais[14]. O documento do FTC também aponta que a Microsoft reteve os dados de crianças por anos, mesmo que o processo de criação das contas não tenha sido concluído. O COPPA proíbe a retenção de dados pessoais sobre crianças por mais tempo do que o razoavelmente necessário para cumprir a finalidade para a qual foram coletados.

Tais incidentes ressaltam a importância de medidas robustas de segurança cibernética e da implementação de práticas adequadas de proteção de dados para garantir a privacidade e a confiança dos usuários, sobretudo crianças, em plataformas online.

Segundo o Relatório sobre o Direito das Crianças à Privacidade, elaborado pelo Instituto Alana em colaboração com o InternetLab, crianças são particularmente vulneráveis ao uso indevido de seus dados e a riscos digitais, incluin-

11. DEMARTINI, Felipe. *Vazamento do game Neopets expõe 69 milhões de pessoas*. CanalTech, 22 de julho de 2022. Disponível em: https://canaltech.com.br/seguranca/vazamento-do-game-neopets-expoe-69-milhoes-de-pessoas-221389/ . Acesso em 04 jul. 2023.

12. Neopets. *Terms of Use*. Disponível em: https://www.neopets.com/settings/about/terms/. Acesso em 13 nov 2023.

13. Neopets. *Privacy Policy*. Disponível em: https://www.neopets.com/privacy.phtml. Acesso em 13 nov 2023.

14. HENDERSON, Juliana Gruenwald. *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent*. Federal Trade Commission, 05 de junho de 2023. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information. Acesso em: 04 jul. 2023.

do manipulação comportamental. Portanto, é de extrema importância assegurar que sejam adotados mecanismos de segurança durante o desenvolvimento e a disponibilização dos jogos[15]. Essas medidas visam a proteger a privacidade e a segurança das crianças, garantindo que suas informações pessoais não sejam exploradas de maneira inadequada e que elas não sejam expostas a práticas manipulativas no ambiente digital.

Esse contexto, somado aos crescentes esforços das autoridades reguladoras de privacidade para proteger a segurança e a autonomia das crianças online, torna evidente que as empresas de jogos online enfrentam desafios legais e comerciais significativos no que diz respeito ao tratamento de dados de crianças.

A proteção efetiva dos dados pessoais de crianças é um desafio constante. A definição da base legal mais adequada ao tratamento desses dados requer cuidadosa consideração das leis e regulamentos aplicáveis, bem como dos princípios éticos e do melhor interesse da criança. Além disso, é importante estabelecer medidas de transparência e em alguns casos mecanismos de consentimento e controle parental, que sejam robustos o suficiente para garantir a participação ativa dos responsáveis na tomada de decisões relacionadas ao tratamento de dados das crianças.

Outro grande desafio consiste na busca pelo equilíbrio entre a personalização da experiência do usuário e a proteção da privacidade das crianças, garantindo que os dados coletados sejam utilizados de forma responsável e segura, e respeitando os direitos e interesses das crianças envolvidas.

Nesse sentido, o parágrafo quarto do artigo 14 da LGPD se apresenta como um ponto crucial para a interpretação do equilíbrio adequado entre a coleta de dados e a personalização da experiência online. Tal parágrafo dispõe que "[o]s controladores não deverão condicionar a participação dos titulares de que trata o §1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade".

Essa disposição está intimamente relacionada ao princípio da necessidade, previsto no art. 6º, III da LGPD[16], que estabelece que o tratamento de dados

15. INSTITUTO ALANA; INTERNETLAB. *O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil*. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em 04 jul. 2023.

16. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://

pessoais deve ser limitado ao mínimo necessário para alcançar as finalidades específicas para as quais os dados estão sendo coletados. Este princípio implica que os controladores de dados não devem coletar informações pessoais além das estritamente necessárias para a participação nas atividades, como jogos ou aplicações de internet.

Isso significa que as empresas da indústria de jogos online devem avaliar cuidadosamente quais dados pessoais são realmente essenciais para a execução daquela atividade específica e não solicitar informações adicionais que não sejam necessárias para o propósito pretendido[17]. Ao aplicar o princípio da necessidade no contexto do parágrafo quarto, as empresas são incentivadas a adotar uma abordagem ainda mais restrita no tratamento de dados pessoais de crianças e adolescentes, evitando a coleta excessiva ou desnecessária de informações.

Além dos desafios relacionados à conformidade legal e à implementação de medidas de segurança, há também a necessidade de se considerar a usabilidade e a experiência do usuário. É preciso encontrar soluções técnicas que permitam uma abordagem adaptada às necessidades e ao desenvolvimento das crianças, considerados hipervulneráveis, e que também ofereçam uma adequada proteção de dados a elas.

Assim, no cenário atual, a indústria de jogos online enfrenta demandas cada vez mais rigorosas em relação à segurança de dados, visando a prevenir violações, como ataques cibernéticos e vazamentos de dados pessoais. Nesse contexto, a responsabilidade de criar um ambiente seguro para os jogadores, especialmente para crianças e adolescentes, recai sobre a indústria de jogos online, sendo essencial que tais empresas invistam em infraestrutura de segurança sólida, estabelecendo medidas eficazes para proteger os dados de jovens jogadores.

Em suma, a indústria de jogos online enfrenta desafios significativos em relação à segurança de dados, exigindo investimentos em medidas de proteção robustas, políticas claras de privacidade e recursos de moderação e monitoramento contínuo.

---

www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em 04 jul. 2023.

17. FERNANDES, Elora; MEDON, Felipe. *Proteção de crianças e adolescentes na LGPD*: desafios interpretativos. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, v.4 n.2, maio/ago. 2021. Disponível em https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/232/187. Acesso em 04 jul. 2023.

2. As bases legais aplicáveis ao tratamento de dados pessoais de crianças

A Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/2018, representou um marco importante na garantia da proteção aos dados pessoais, especialmente no que se refere às crianças. Com a entrada em vigor da LGPD, em setembro de 2020, foram estabelecidas diretrizes mais claras para o tratamento de dados pessoais, até antes dispostas em leis esparsas, incluindo aquelas relacionadas às crianças. Essa legislação trouxe avanços significativos ao estabelecer que o tratamento de dados de crianças deve ser realizado de forma especial, levando em consideração sua vulnerabilidade e os riscos envolvidos.

A proteção de dados de crianças de forma diferenciada é crucial devido à sua condição de vulnerabilidade e ao fato de ainda estarem em um estágio de desenvolvimento e formação de sua identidade, personalidade e habilidades cognitivas, o que as torna mais suscetíveis a influências e manipulações[18]. Além disso, elas podem ter dificuldades para compreender plenamente as implicações do compartilhamento de dados pessoais e os possíveis riscos associados a isso.

A inclusão das crianças como um grupo de proteção especial na LGPD e em outras legislações ao redor do mundo se dá em razão da necessidade de ser oferecida uma camada adicional de salvaguardas para o desenvolvimento saudável e seguro desse público no ambiente digital. Essas leis estabelecem que o tratamento de dados de crianças deve ser realizado de maneira especialmente cuidadosa, visando a minimizar riscos associados a práticas abusivas, manipulação comportamental e exposição a conteúdo inadequado, bem como garantir que os interesses e direitos das crianças sejam preservados, promovendo um ambiente seguro e respeitando sua privacidade. Dessa forma, é assegurado que o tratamento de dados de crianças seja realizado de maneira ética, responsável e em conformidade com os princípios de proteção de dados e direitos fundamentais.

No artigo 14 da LGPD são elencadas as bases legais para o tratamento de dados pessoais de crianças, as quais são fundamentais para determinar a licitude e a legitimidade do tratamento desses dados. O texto frio da LGPD estabelece que o tratamento de dados de crianças deve ser realizado, a princípio,

18. LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p.17-18. E-book. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/12/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-its.pdf Acesso em Acesso em 01 jul. 2023.

apenas com o consentimento específico e destacado dos pais ou responsáveis legais, salvo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção.

Além disso, a lei estabelece que o tratamento de dados de crianças deve ser realizado para a promoção do seu melhor interesse, levando em consideração sua proteção integral e seus direitos fundamentais. Essas diretrizes proporcionam uma estrutura clara para o tratamento de dados pessoais de crianças, garantindo uma maior proteção e segurança nesse contexto.

Tal preocupação com uma maior proteção dos direitos das crianças não foi uma inovação da LGPD. Este cuidado especial já estava concretizado em diversos dispositivos do ordenamento jurídico brasileiro. O artigo 227 da Constituição Federal, por exemplo, prevê a prioridade absoluta da família, do Estado e da sociedade em geral a proteção aos direitos da criança. Essa premissa foi reafirmada no art.4º do Estatuto da Criança e do Adolescente, Lei nº 8.069/1990, estatuto que aprofundou o arcabouço de proteção aos direitos da criança.

No entanto, mesmo com as robustas medidas legais de proteção dos direitos das crianças, a implementação prática do tratamento de seus dados pessoais continua sendo um desafio, especialmente para a indústria de jogos online.

A obtenção do consentimento dos pais ou responsáveis muitas vezes se mostra um obstáculo significativo. Um dos principais desafios é garantir que o consentimento seja obtido de forma efetiva, clara e compreensível para os pais ou responsáveis legais das crianças. É necessário fornecer informações designadas sobre como os dados serão coletados, armazenados e utilizados, bem como os riscos envolvidos. Além disso, é fundamental que os pais ou responsáveis estejam plenamente conscientes dos direitos da criança enquanto titular de dados e tenham a capacidade de exercê-los.

Diante desse cenário complexo e, por vezes, incerto, a Autoridade Nacional de Proteção de Dados acertadamente deu uma interpretação ao artigo 14 e à aplicação das bases legais que pode representar uma flexibilização no tratamento de dados de crianças, conforme será abordado no item a seguir.

2.1. Como o Enunciado CD/ANPD nº 1 impacta o tratamento de dados de crianças no ambiente de jogos online

O Enunciado CD/ANPD nº 1[19], emitido em 22 de maio de 2023 pela Autoridade Nacional de Proteção de Dados (ANPD), representou um marco importante no que tange às hipóteses legais para o tratamento de dados de crianças no Brasil. O Enunciado postula que as bases legais constantes dos arts. 7º e 11 da LGPD poderão embasar o tratamento de dados pessoais de crianças e adolescentes, sempre que observado o melhor interesse, conforme identificado no caso concreto, possibilitando que o tratamento ocorra, não mais apenas mediante o consentimento dos pais ou responsáveis legais. Essa flexibilização é importante para garantir que as crianças possam desfrutar de serviços e produtos digitais, ao mesmo tempo em que são asseguradas medidas de proteção e segurança.

O Enunciado é fruto de um longo debate levantado pela ANPD no Estudo Preliminar[20], lançado em setembro de 2022, o qual teve o objetivo de fomentar o debate público e subsidiar a tomada de decisão sobre o tema pela Autoridade. À época foi inclusive aberta Tomada de Subsídios para a coleta de sugestões da sociedade sobre o tema.

O Enunciado se alinha à terceira hipótese apresentada pela Autoridade no Estudo Preliminar, que discutiu as hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, listadas abaixo:

> **1. Consentimento Parental:** nesse caso, a única hipótese cabível para o tratamento de dados de crianças e adolescentes seria o consentimento dos pais ou responsáveis legais, conforme disposto no artigo 14 da LGPD.
>
> **2. Equiparação aos Dados Sensíveis:** nesse caso, caberia apenas a aplicação das hipóteses previstas no artigo 11, equiparando os dados de crianças e adolescentes aos dados sensíveis.
>
> **3. Flexibilidade Maior – Artigos 7º e 11:** nesse caso, haveria uma flexibilidade maior ao tratamento de dados de crianças e adolescentes, permitindo a aplicação das bases legais dos artigos 7º e 11 da LGPD, desde que observado o princípio do melhor interesse.

19. BRASIL. *Enunciado CD/ANPD No 1*, de 22 de maio de 2023. Edição 98, Seção 1, p. 129. Diário Oficial da União, Brasília, DF, 24 de maio de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em 06 jul. 2023.

20. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Estudo Preliminar - Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*. Gov.br, setembro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 07 jul. 2023.

O Enunciado 684, aprovado na IX Jornada de Direito Civil Comissão de Direito Digital[21] do Conselho da Justiça Federal, em maio de 2022, já apontava para essa terceira linha de pensamento, que acabou sendo confirmada com o Enunciado emitido pela ANPD. Os enunciados aprovados pelas comissões nas Jornadas de Direito Civil constituem um indicativo para a interpretação da legislação, estando todos diretamente relacionados a um artigo de lei, e significam o entendimento majoritário das respectivas comissões, neste caso, a Comissão de Direito Digital. Já Enunciado CD/ANPD nº 1 é uma espécie de instrumento deliberativo com a finalidade de interpretar a legislação de proteção de dados pessoais, sendo um ato próprio da ANPD e que possui efeitos vinculativos à Autoridade.

Diante desse cenário, é possível sustentar que a expansão das bases legais para o tratamento de dados de crianças também traz implicações para o ambiente digital e para a indústria de jogos online, uma vez que muitos serviços e produtos destinados ao público infantil dependem do tratamento de dados pessoais. Ao permitir que o consentimento dos pais ou responsáveis não seja mais o único requisito, o Enunciado busca conciliar a proteção da privacidade com a necessidade de oferecer experiências digitais adequadas e seguras para as crianças, fomentando a inovação e o desenvolvimento de serviços direcionados a esse público.

Assim, o tratamento de dados de crianças pode ser realizado por empresas desenvolvedoras de jogos quando necessário para executar um contrato, cumprir uma obrigação legal ou regulatória ou atender aos seus legítimos interesses como controladoras de dados. Especificamente em relação ao legítimo interesse, a ANPD publicou um Estudo Preliminar, submetido à consulta pública em 16/08/2023, que tem como objetivo analisar a incidência da base legal do legítimo interesse como hipótese autorizativa para o tratamento de dados pessoais, que traz algumas orientações específicas para o tratamento de dados pessoais de crianças e adolescentes com fundamento nessa base legal, em respeito ao princípio do melhor interesse[22].

O Estudo dispõe que o controlador deve elaborar e manter registro da justificativa para o tratamento, que deve ser adequada ao caso e capaz de de-

21. CONSELHO DA JUSTIÇA FEDERAL. *IX Jornada de Direito Civil - Enunciado no 684*. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados--2022-vf.pdf. Acesso em: 07 jul. 2023.

22. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Consulta à Sociedade de Estudo Preliminar sobre Legítimo Interesse*. Gov.br, 16 de agosto de 2023. Disponível em: https://www.gov.br/participamaisbrasil/consulta-a-sociedade-de-estudo--preliminar-sobre-legitimo-interesse-1. Acesso em: 01 dez. 2023.

monstrar: (i) o que foi considerado como sendo o melhor interesse da criança ou do adolescente; (ii) com base em quais critérios os seus direitos foram ponderados em face do interesse legítimo do controlador ou de terceiro; e (iii) que o tratamento não gera riscos ou impactos desproporcionais e excessivos, considerando a condição da criança e do adolescente. Além disso, a ANPD sugere que o tratamento de dados de crianças e adolescentes com base no legítimo interesse tende a ser mais apropriado nos casos em que exista uma relação prévia e direta do controlador com os titulares; e quando o tratamento visa a assegurar a proteção de seus direitos e interesses ou viabilizar a prestação de serviços que o beneficiem.

É válido ressaltar, todavia, que a utilização dessas bases legais, além de estar em conformidade com os princípios gerais estabelecidos na LGPD, deve considerar ainda a capacidade civil da criança e os requisitos de outras legislações aplicáveis, como o Estatuto da Criança e do Adolescente.

De qualquer maneira, independentemente da base legal utilizada para o tratamento de dados de crianças, é fundamental que o princípio do melhor interesse da criança seja sempre observado e prevaleça. Isso significa que, ao tomar decisões sobre o tratamento de dados pessoais de crianças, é necessário avaliar cuidadosamente cada caso individualmente, levando em consideração o bem-estar e os direitos da criança.

2.2. Princípio do melhor interesse como norteador do tratamento de dados de crianças

O princípio do melhor interesse da criança é um conceito fundamental quando se trata do tratamento de dados pessoais de crianças. Esse princípio estabelece que todas as ações e decisões relacionadas a crianças devem ser tomadas com base no que é mais benéfico para o seu desenvolvimento e bem-estar.

O melhor interesse da criança apareceu originalmente no texto da Convenção sobre os Direitos da Criança[23], adotada pela Organização das Nações Unidas (ONU) em 1989, quando apresentou as obrigações dos Estados para com a infância, determinando o mínimo que cada nação deveria garantir às suas crianças e adolescentes. Nesse sentido, a Convenção da ONU sobre os

23. UNITED NATIONS, HUMAN RIGHTS. *Convention on the Rights of the Child, 20 November 1989, By General Assembly resolution 44/25*. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. Acesso em 10/07/2023

Direitos da Criança, principal instrumento internacional que aborda os direitos das crianças, estabelece no art. 3. 1[24] que deve ser sempre garantido o interesse maior da criança e adolescente e definiu este conceito como sendo um princípio que visa assegurar a fruição plena e efetiva de todos os direitos reconhecidos na Convenção, o bem-estar e o desenvolvimento integral da criança. A Convenção foi ratificada no Brasil em 1990 por meio do Decreto nº 99.710/1990[25].

Em 2013, o Comitê da ONU sobre os Direitos da Criança emitiu o Comentário Geral nº 14[26], intitulado "O direito da criança de ter seu melhor interesse considerado como uma consideração primordial". Esse comentário geral interpreta e esclarece o artigo 3º da Convenção sobre os Direitos da Criança, que se refere ao princípio do melhor interesse da criança. O comentário geral destaca a importância desse princípio como um guia para todas as decisões e ações que afetam as crianças.

De acordo com o Comitê, o princípio do melhor interesse deve ser aplicado em todos os setores e ressalta a necessidade de uma abordagem individualizada, levando em consideração as necessidades específicas e circunstâncias de cada criança, como o contexto social, cultural e familiar em que a criança está inserida. Além disso, o comentário geral destaca a importância da participação ativa da criança nas decisões que a afetam, de acordo com sua idade e maturidade.

A Convenção sobre os Direitos da Criança estabelece que o melhor interesse da criança é um conceito composto por três dimensões. Primeiramente, é um direito substantivo das crianças, garantindo que seus direitos sejam considerados prioritariamente quando houver múltiplos interesses envolvidos em uma decisão. Em segundo lugar, é um princípio fundamental de interpretação, orientando que a escolha da interpretação mais favorável ao interesse da criança seja adotada quando um dispositivo legal admitir diferentes interpretações. Por fim, é uma regra processual, orientado que deve sempre haver uma avaliação do impacto da decisão nas crianças e também deve garantir uma fundamentação adequada da escolha feita, explicitando os critérios da

24. Ibid., Art. 3, item 1.

25. BRASIL. *Decreto nº 99.710*, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Brasília, DF, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm. Acesso em: 07 jul. 2023.

26. UNITED NATIONS, HUMAN RIGHTS. *Convention on the Rights of the Child*. General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para.1). 29 May 2013. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em: 07 jul. 2023.

decisão e como os direitos da criança foram ponderados contra outras considerações, sejam de políticas públicas ou questões individuais[27].

O melhor interesse da criança é reforçado expressamente no art. 14, *caput* da LGPD, o qual dispõe que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse". Assim, no contexto do tratamento de dados no ambiente digital, o princípio do melhor interesse também deve ser o critério orientador ao determinar como os dados serão coletados, armazenados, utilizados e compartilhados, exigindo que os responsáveis pelo tratamento de dados de crianças adotem medidas de proteção adequadas, garantindo a privacidade e segurança das informações pessoais, além de considerar o impacto potencial sobre a criança.

Nesse sentido, o Enunciado 691, aprovado na IX Jornada de Direito Civil Comissão de Direito Digital, em maio de 2022, corroborou a importância do melhor interesse na divulgação de dados de crianças na internet[28].

Tem-se, portanto, que o entendimento claro sobre o melhor interesse tem um impacto significativo na interpretação e na aplicação prática do artigo 14 da LGPD, assim como do recente Enunciado CD/ANPD nº 1.

Mais especificamente sobre os direitos da criança em relação ao ambiente digital, o Comitê da ONU sobre os Direitos da Criança emitiu um novo comentário, em 2021, com o objetivo de atualizar a convenção, tendo em mente o ambiente digital e seus impactos na sociedade. O Comentário Geral nº 25 destaca que o ambiente digital não foi originalmente projetado para crianças, mas desempenha um papel cada vez mais importante em suas vidas. Portanto, é fundamental que sejam adotadas medidas para garantir que o melhor interesse de cada criança seja considerado primordial em todas as ações relacionadas ao fornecimento, regulação, design, gestão e uso do ambiente digital, devendo este princípio prevalecer sobre os interesses comerciais relacionados ao tratamento de dados.

Isso é particularmente importante para a indústria de jogos eletrônicos porque, como um dos principais atores do ambiente digital, ela desempenha um papel cada vez mais relevante na vida das crianças, oferecendo oportunidades de entretenimento, aprendizado e interação social.

27. INSTITUTO ALANA; INTERNETLAB. *O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil*. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU. São Paulo, 2020. Disponível em: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf. Acesso em 04 jul. 2023.

28. CONSELHO DA JUSTIÇA FEDERAL. *IX Jornada de Direito Civil - Enunciado no 691*. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados--2022-vf.pdf. Acesso em: 07 jul. 2023.

Portanto, se o melhor interesse da criança não for identificado e considerado em determinado contexto, o consentimento ou qualquer outra base legal não será suficiente para justificar e fundamentar o tratamento de dados pessoais[29]. Isso significa que, mesmo que haja consentimento dos pais ou qualquer outra base legal disponível - sobretudo considerando a ampliação das bases legais em decorrência do Enunciado CD/ANPD nº 1 -, não será possível tratar os dados pessoais de crianças se não for observado seu melhor interesse.

Assim, é essencial que os desenvolvedores e fornecedores de jogos eletrônicos considerem o melhor interesse das crianças em todas as etapas, desde o design e desenvolvimento do jogo até a implementação de medidas de segurança e proteção de dados. Isso implica adotar práticas responsáveis de coleta e tratamento de dados pessoais de crianças, garantir a privacidade e segurança das informações, oferecer controles parentais adequados e evitar práticas abusivas ou prejudiciais.

3. Alternativas e medidas de mitigação de riscos

Diante de todos os desafios apresentados, fica evidente que as empresas desenvolvedoras de jogos eletrônicos direcionados ao público infantil devem investir em alternativas factíveis para viabilizar o tratamento adequado de dados de crianças, com o objetivo de minimizar os riscos envolvidos. Isso requer um esforço proativo na implementação de medidas de proteção de dados sólidas e eficazes.

Impedir completamente o acesso de crianças ao ambiente de jogos online aparenta ser uma ideia utópica e contraproducente. A crescente presença da tecnologia no cotidiano e a importância dos jogos como forma de entretenimento e interação social fazem com que seja inevitável o envolvimento das crianças nesse ambiente digital. Portanto, é necessário adotar uma abordagem mais realista e construtiva, focada em desenvolver meios para que as crianças possam acessar esses ambientes de forma segura e adequada à sua capacidade cognitiva.

A verificação de idade e o consentimento parental não devem ser vistos como bala de prata ou como uma proteção suficiente por si só. O objetivo não deve ser manter as crianças afastadas dos jogos online; em vez disso, é preci-

29. ZANATTA, Rafael A. F.; BIONI, Bruno; MENDONÇA, Julia. Contribution to General Comment on Children's Rights in Relation to The Digital Environment. Data Privacy BR Research, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/11/contribution_onu.pdf. Acesso em 08 jul. 2023.

so garantir que eles permaneçam seguros nesse ambiente. Para tanto, ao considerar a participação de crianças em jogos online, é crucial atentar-se para a idade mínima recomendada e a classificação indicativa atribuída a cada jogo. Estabelecer limites etários apropriados é uma medida essencial para garantir que o conteúdo dos jogos seja adequado ao estágio de desenvolvimento cognitivo e emocional das crianças. Implementar sistemas eficazes de verificação de idade e aplicar rigorosamente as classificações indicativas contribui para criar um ambiente virtual mais seguro e adaptado às diferentes faixas etárias

Tais medidas apenas funcionarão efetivamente como parte de uma abordagem mais ampla de privacidade por design[30]. Isso envolve o desenvolvimento de recursos específicos para proteção infantil, como filtros de conteúdo, controles parentais e ambientes virtuais seguros. Além disso, é fundamental fornecer orientações claras para pais, responsáveis e educadores sobre como supervisionar e orientar o uso dos jogos online pelas crianças, promovendo uma relação saudável e segura com a tecnologia.

Nesse sentido, autoridades de diversos países têm desenvolvido materiais educativos contendo orientações de extrema importância sobre o design de ambientes digitais voltados para crianças. Um exemplo notável é o *Age Appropriate Design Code* (*Children's Code*) do *Information Commissioner's Office* (ICO) no Reino Unido[31], que estabelece diretrizes para proteger a privacidade e a segurança das crianças online. Outro documento relevante é o relatório *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing da Data Protection Commission* (DPC) na Irlanda, que aborda os princípios fundamentais para o tratamento de dados voltado para crianças.

Essas iniciativas refletem um reconhecimento global da importância de se adotar uma abordagem centrada na criança no desenvolvimento e regulamentação de ambientes digitais. Elas destacam a necessidade de se considerar as necessidades, capacidades e direitos das crianças quando forem projetadas plataformas, aplicativos e serviços online direcionados a elas. Além disso, esses materiais educativos fornecem orientações práticas para as empresas e desenvolvedores, incentivando a adoção de medidas de segurança, privacidade e usabilidade que estejam alinhadas com o melhor interesse das crianças.

30. DENHAM CBE, Elizabeth; WOOD, Steve. *Data protection trends in children's online gaming*. IAPP, 12 September 2022. Disponível em: https://iapp.org/news/a/data-protection-trends-in-childrens-online-gaming. Acesso em 08 jul. 2023.

31. DENHAM CBE, Elizabeth. INFORMATION COMMISSIONER'S OFFICE. Age-appropriate design: a code of practice for online services. ICO, 2020. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 08 jul. 2023.

Dado que a maioria das empresas de videojogos tem dificuldades em cumprir os princípios básicos de minimização de dados e limitação de finalidades, é recomendável que, desde o início da interação com o jovem jogador, sejam coletados apenas os dados estritamente necessários para a disponibilização do jogo, sendo evitada a coleta de dados pessoais que não traga "um benefício óbvio para a experiência do jogador"[32].

De forma mais prática, é essencial que as empresas da indústria de jogos online considerem esses princípios desde a concepção de seus produtos e serviços, implementando medidas que assegurem o tratamento adequado dos dados pessoais das crianças. Isso inclui a aplicação de conceitos como *Privacy by Design*, em que as configurações das plataformas são pensadas com alta privacidade desde o início, desativando opções de geolocalização por padrão e evitando o compartilhamento de dados das crianças quando não for do seu melhor interesse. Além disso, é importante adotar uma abordagem adequada para verificar de forma confiável a idade dos usuários, a fim de desencorajar falsas declarações de idade.

No mesmo sentido, é importante garantir que os jogos não prejudiquem a saúde e o bem-estar das crianças, por meio de instruções apropriadas à idade que incentivem pausas em jogos prolongados e ajudem os jogadores a se desconectarem de sessões extensas. É importante desencorajar o uso de técnicas de *nudge*[33] que influenciam crianças a tomarem decisões de privacidade inadequadas, revisando práticas de marketing e parcerias em mídias sociais direcionadas a criança.

As empresas de jogos online também têm a possibilidade de aprimorar suas políticas de privacidade, tornando-as transparentes e amigáveis para crianças. Uma estratégia eficaz é simplificar as políticas existentes, utilizando uma linguagem simples e clara, evitando termos técnicos ou jurídicos que possam dificultar a compreensão dos usuários infantis. Além disso, é possível inserir pequenas animações ou personagens de jogos que expliquem os direi-

32. ENESCU, Maria-Alexandra. *Protecting children's personal data from abusive personal data processing performed by video game companies. Thesis for: Master's Degree - LL.M in International and European Law with a Data Law specialization.* Orientador: Cristopher Kuner. Vrije Universiteit Brussel. Institute for European Studies. 2019. Disponível em: https://www.researchgate.net/profile/Maria-Alexandra-Enescu/publication/344413116_Protecting_children%27s_personal_data_from_abusive_personal_data_processing_performed_by_video_game_companies/links/5f957ebd92851c14bce580fd/Protecting-childrens-personal-data-from-abusive-personal-data-processing-performed-by-video-game-companies.pdf Acesso em 25 jun. 2023

33. "*Nudge*" é um termo em inglês que significa empurrão. Essa técnica representa uma abordagem que utiliza estímulos sutis e indiretos para influenciar o comportamento das pessoas sem coagi-las ou impor uma decisão. Esses estímulos são projetados para empurrar as pessoas em direção a uma escolha específica, sem que elas percebam que estão sendo guiadas.

tos das crianças e quais salvaguardas estão disponíveis, tanto na política de privacidade quanto durante a experiência do jogo. Essa abordagem interativa pode aproximar as disposições relacionadas à privacidade de crianças de uma forma mais acessível e envolvente. Algumas empresas do setor já estão adotando essas práticas, demonstrando que é um caminho viável para promover a compreensão e a conscientização sobre a privacidade entre os usuários infantis, como é o caso da *Children's Privacy Policy*, disponível no site da Wildlife Studios[34].

Por fim, a conscientização dos pais sobre a participação de suas crianças no ambiente de jogos online é fundamental para garantir a segurança e o bem-estar desse público. Os pais devem ser orientados sobre os potenciais riscos associados aos jogos online, como exposição a conteúdos inadequados, interações negativas ou violação de privacidade. É importante que os pais se informem sobre as medidas de proteção disponíveis bem como incentivem o diálogo aberto com as crianças, promovendo a educação digital e ensinando sobre os comportamentos seguros e responsáveis online[35].

Ao promover o uso responsável e seguro do ambiente digital por crianças, essas iniciativas contribuem para criar um ambiente online mais adequado às suas necessidades e características específicas. Elas reforçam a importância de serem consideradas as implicações éticas e legais do tratamento de dados pessoais de crianças, estimulando práticas que preservem sua privacidade, protejam sua segurança e promovam seu bem-estar geral no ambiente digital.

Considerações finais

A indústria de jogos online está em constante crescimento e, à medida que isso acontece, também aumenta a sua oferta de serviços para crianças. No entanto, esse cenário coloca um desafio adicional para as empresas do setor, que precisam lidar com a intensa coleta e tratamento de dados pessoais das crianças para aprimorar a experiência de jogo.

O objetivo deste artigo foi analisar as hipóteses legais em que o tratamento de dados pessoais de crianças no ambiente de jogos online é viável à luz da legislação brasileira, levando em consideração a ampliação das bases legais

34. *CHILDREN'S PRIVACY POLICY*. Wildlife Studios, 30 March 2022. Disponível em: https://wildlifestudios.com/policy-center/privacy-policy/childrens-privacy-policy. Acesso em 25 jun. 2023.

35. ZHAO, Jun; LYNGS, Ulrik; SHADBOLT, Nigel. *What privacy concerns do parents have about children's mobile apps, and how can they stay SHARP? - KOALA Project Report 1*. Department of Computer Science University of Oxford, 28 February 2018. Disponível em: https://arxiv.org/pdf/1809.10841v1.pdf. Acesso em 25 jun. 2023.

estabelecidas pelo Enunciado CD/ANPD nº 1, os requisitos do artigo 14, §4º da LGPD, e correlacionando diferentes aspectos no tratamento de dados no ambiente digital com as recomendações relevantes da Convenção das Nações Unidas sobre os Direitos da Criança, especialmente o princípio do melhor interesse.

Após examinar os principais desafios enfrentados pela indústria de jogos online, incluindo casos de vazamento de dados de crianças neste ambiente, foi possível identificar alternativas factíveis que podem ser adotadas pela indústria de jogos online para proteger as crianças. Dentre elas, destacam-se a verificação adequada da idade dos usuários, a aplicação de conceitos de privacidade por design, a implementação de medidas de segurança adequadas e a adoção de políticas de privacidade mais claras e amigáveis. Além disso, ressalta-se a importância da conscientização dos pais sobre a participação de crianças no ambiente digital.

Assim, tem-se que a proteção efetiva dos dados pessoais de crianças pode ser alcançada por meio de uma abordagem multilateral, que envolva a indústria de jogos online, os pais e as autoridades. Essa colaboração busca garantir um nível adequado de proteção no ambiente digital, ao mesmo tempo em que permite que as crianças desfrutem da experiência de jogo e exerçam seus direitos. O desafio, nesse contexto, é encontrar o equilíbrio entre a garantia de privacidade e a liberdade de expressão e lazer das crianças, sem excluir totalmente seu acesso aos serviços de jogos.

Para atender a esse desafio, os provedores de jogos devem se esforçar para garantir altos padrões de privacidade para as crianças, em conformidade com a legislação de proteção de dados e tendo o melhor interesse como princípio central, protegendo os dados deste público contra uso indevido ou incidentes, mas permitindo que desfrutem da experiência de jogo. Assim, com uma abordagem conjunta e medidas adequadas, é possível proteger as crianças no ambiente de jogos online, garantindo uma experiência segura e adequada para esse público sensível.

Referências

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes*. Gov.br, 24 de maio 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes. Acesso em: 07 jul. 2023.

_____. *Estudo Preliminar - Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*. Gov.br, setembro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 07 jul. 2023.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidente da República, [2010]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em 06 jul. 2023.

BRASIL. *Decreto nº 99.710*, de 21 de novembro de 1990. Promulga a Convenção sobre os Direitos da Criança. Brasília, DF, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm. Acesso em: 07 jul. 2023.

_____. *Enunciado CD/ANPD No 1*, de 22 de maio de 2023. Edição 98, Seção 1, p. 129. Diário Oficial da União, Brasília, DF, 24 de maio de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em 06 jul. 2023.

_____. *Lei nº 8.069*, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 16 de julho 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art266. Acesso em 06 jul. 2023.

_____. *Lei nº 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em 04 jul. 2023.

CHILDREN'S PRIVACY POLICY. *WildLife Studios*, 30 March 2022. Disponível em: https://wildlifestudios.com/policy-center/privacy-policy/childrens-privacy-policy. Acesso em 25 jun. 2023.

CNIL publishes 8 recommendations to enhance the protection of children online. *CNIL*, 09 August 2021. Disponível em: https://www.cnil.fr/en/cnil-publishes-8-recommendations-enhance-protection-children-online. Acesso em 25 jun. 2023.

COMITE GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil [livro eletrônico]: *TIC Kids Online Brasil 2021*. Disponível em: https://cetic.br/media/docs/publicacoes/2/20221121120124/tic_kids_online_2021_livro_eletronico.pdf Acesso em 24 jun. 2023.

CONSELHO DA JUSTIÇA FEDERAL. *IX Jornada de Direito Civil-Enunciado no 684*. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 07 jul. 2023.

_____. *IX Jornada de Direito Civil - Enunciado no 691*. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 07 jul. 2023.

DEMARTINI, Felipe. *Vazamento do game Neopets expõe 69 milhões de pessoas*. CanalTech, 22 de julho de 2022. Disponível em: https://canaltech.com.br/seguranca/vazamento-do-game-neopets-expoe-69-milhoes-de-pessoas-221389. Acesso em 04 jul. 2023.

DENHAM CBE, Elizabeth. *INFORMATION COMMISSIONER'S OFFICE. Age-appropriate design: a*

code of practice for online services. ICO, 2020. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 08 jul. 2023.

DENHAM CBE, Elizabeth; WOOD, Steve. *Data protection trends in children's online gaming. IAPP, 12 September 2022*. Disponível em:https://iapp.org/news/a/data-protection-trends-in-childrens-online-gaming. Acesso em 08 jul. 2023.

ENESCU, Maria-Alexandra. *Protecting children's personal data from abusive personal data processing performed by video game companies. Thesis for: Master's Degree - LL.M in International and European Law with a Data Law specialization*. Orientador: Cristopher Kuner. Vrije Universiteit Brussel. Institute for European Studies. 2019. Disponível em: https://www.researchgate.net/profile/Maria-Alexandra-Enescu/publication/344413116_Protecting_children%27s_personal_data_from_abusive_personal_data_processing_performed_by_video_game_companies/links/5f957ebd92851c14bce580fd/Protecting-childrens-personal-data-from-abusive-personal-data-processing-performed-by-video-game-companies.pdf Acesso em 25 jun. 2023.

FERNANDES, Elora; MEDON, Felipe. *Proteção de crianças e adolescentes na LGPD:* desafios interpretativos. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, v.4 n.2, maio/ago. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/232/187. Acesso em 04 jul. 2023.

GAMES INDUSRTY.BIZ. *Data Protection in the Games Industry: Part 1- What games business need to know about data protection*. 14 de junho de 2011. Disponível em: https://www.gamesindustry.biz/data-protection-in-the-games-industry-part-1-article Acesso em 01 jul. 2023.

HENDERSON, Juliana Gruenwald. *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent. Federal Trade Commission*, 05 de junho de 2023. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information. Acesso em: 04 jul. 2023.

INSTITUTO ALANA; INTERNETLAB. *O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil*. Comentário Geral, n.25. São Paulo, 2022. Disponível em: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf. Acesso em 04 jul. 2023.

INSTITUTO ALANA; INTERNETLAB. *O direito das crianças à privacidade: obstáculos e agendas de proteção à privacidade e ao desenvolvimento da autodeterminação informacional das crianças no Brasil. Contribuição conjunta para o relator especial sobre o direito à privacidade da ONU*. São Paulo, 2020. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/03/ilab-alana_criancas-privacidade_PT_20210214-4.pdf. Acesso em 04 jul. 2023.

LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021, p.17-18. E-book. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2021/12/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes-its.pdf Acesso em Acesso em 01 jul. 2023.

LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. *Children's data and privacy online Growing up in a digital age - An evidence review. LSE Media and Communications, December 2018*. Disponível em: https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf. Acesso em 10 jun. 2023.

LIVINGSTONE, S.; TAMBINI, D.; BELAKOVA, N. (2018) *Research for CULT Committee – Recommendations for EU policy developments on protection of minors in the digital age. Brussels: European Parliament, Policy Department for Structural and Cohesion Policies*. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/617454/IPOL_IDA(2018)617454_EN.pdf. Acesso em 10 jun. 2023.

NEWZOO. *Global Games Market Report*. 2021. Disponível em: https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2021-free-version. Acesso em 24 de junho de 2023.

PACETE, Luiz Gustavo. *Estúdios brasileiros devem movimentar R$ 250 milhões em 2023*. Forbes. Maio de 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/05/estudios-brasileiros-devem-movimentar-r-250-milhoes-em-2023/. Acesso em 24 jun. 2023.

PINHEIRO, Ana Clara Moreira; LUZ, Gustavo; ALMEIDA, Juliana; MONTEIRO, Mariana Pires; KASPUTIS, Matheus Botsman; RIBEIRO, Natália Góis; BRAOIOS, Rafaella Resck. *Guia LGPD e games. A year in privacy*. 2022. Disponível em: https://baptistaluz.com.br/guia-lgpd-e-games-a-year-in-privacy-9/. Acesso em 25 jun. 2023.

REINO UNIDO. INFORMATION COMMISSIONER'S OFFICE. *Introduction to the Children's Code*. ICO. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 08 jul. 2023.

UNITED NATIONS, HUMAN RIGHTS. *Convention on the Rights of the Child*, 20 November 1989, By General Assembly resolution 44/25. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. Acesso em 10/07/2023.

_____. *Convention on the Rights of the Child. General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para.1)*. 29 May 2013. Disponível em: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf. Acesso em: 07 jul. 2023.

ZANATTA, Rafael A. F.; BIONI, Bruno; MENDONÇA, Julia. *Contribution to General Comment on Children's Rights in Relation to The Digital Environment*. Data Privacy BR Research, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/11/contribution_onu.pdf. Acesso em 08 jul. 2023.

ZHAO, Jun; LYNGS, Ulrik; SHADBOLT, Nigel. *What privacy concerns do parents have about children's mobile apps, and how can they stay SHARP? - KOALA Project Report 1*. Department of Computer Science University of Oxford, 28 February 2018. Disponível em: https://arxiv.org/pdf/1809.10841v1.pdf. Acesso em 25 jun. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

O acúmulo de cargos pelo encarregado do tratamento de dados pessoais no Brasil e na União Europeia: uma análise comparativa do conflito de interesse

BIANCA COUPE FORADINE DA MOTTA

BIANCA COUPE FORADINE DA MOTTA[1]

Introdução

Em julho de 2023, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) aplicou a primeira sanção em decorrência de descumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em face de uma microempresa, no valor de R$ 14.400,00[2]. Levando em conta a iniciação do exercício da atribuição sancionatória da autoridade, cabe aos agentes de tratamentos de dados uma atenção redobrada com relação ao cumprimento das regras estabelecidas pela entidade e pela legislação vigente.

Enquanto isso, em setembro de 2022, foi divulgada decisão em que a autoridade alemã de proteção de dados pessoais multou uma companhia varejista em € 525.000,00[3] por violação ao *General Data Protection Regulation* (GDPR), regulação referente à proteção de dados pessoais na União Europeia. Isso porque o *Data Protection Officer* (DPO) se encontrava em situação de conflito de interesse devido ao acúmulo dessa função com um cargo de gerência, o que é expressamente vedado pelo ordenamento jurídico do bloco europeu.

Esses casos concretos e a existência de diversas decisões condenatórias e sancionatórias por parte de autoridades de proteção de dados pessoais do bloco econômico evidenciam a diferença de maturidade entre o estado da arte da proteção de dados pessoais no Brasil e na União Europeia. Nesse sentido, cabe mencionar a questão do conflito de interesse do encarregado pelo tratamento de dados pessoais, tema central do presente trabalho. Isso porque na legislação brasileira há flagrante ausência de disposição vigente acerca dessa temática. Enquanto isso, no bloco europeu há expressa vedação ao acúmulo de funções e atividades pelo DPO que possam gerar conflitos de interesse.

1. Bacharela em Direito pela Fundação Getulio Vargas, pós-graduanda em Direito Digital pelo ITS-Rio e em Direito Público e Privado pela EMERJ.

2. Ministério da Justiça e Segurança Pública. (Brasil) *ANPD aplica a primeira multa por descumprimento à LGPD*. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd#:~:text=A%20Coordenação%2DGeral%20de%20Fiscalização,Geral%20de%20Proteção%20de%20Dados. Acesso em: 25 jul. 2023.

3. BlnBDI (Berlin) - Berlin DPO Conflict of Interest. Disponível em: https://gdprhub.eu/index.php?title=BlnBDI_(Berlin)_-_Berlin_DPO_Conflict_of_Interest#:~:text=The%20Berlin%20Commissioner%20for%20Data,an%20executive%20of%20the%20company. Acesso em: 25 jul. 2023.

Acredita-se que a permanência dessa lacuna na regulação seria extremamente problemática para a evolução da proteção de dados pessoais no Brasil. Especialmente, levando em consideração que ocorrendo violações que envolvam um conflito de interesse por parte do encarregado do tratamento de dados pessoais, existem poucas disposições normativas que possam nortear a atuação da ANPD ou até mesmo a dos próprios agentes de tratamento (controlador e operador).

Nesse sentido, cabe apontar que a agência reguladora de proteção de dados pessoais abriu em novembro de 2023 uma consulta pública na qual apresentou uma proposta de regulamentação complementar para o encarregado. No regulamento proposto surge pela primeira vez no Direito Brasileiro expressa vedação ao acúmulo de cargos pelo encarregado nos casos em que isso gerar conflito de interesses. Além disso, a proposta traz proibição com relação ao acúmulo do cargo de encarregado com cargos cuja responsabilidade seja tomar decisões referentes ao tratamento de dados pessoais.

Essa proposta pode significar relevante avanço quanto a regulação da proteção de dados no Brasil, já que com a sua aprovação, haveria o preenchimento de uma lacuna existente há muito tempo. Contudo, apesar disso a proposta mencionada é extremamente genérica quanto a definição de conflitos de interesses: “situação gerada pelo confronto de interesses do agente de tratamento com os do encarregado no exercício de sua função, que possa influenciar, de maneira imprópria, o desempenho das atribuições do encarregado”.

A consulta pública será encerrada em dezembro de 2023 e mesmo que aprovada a minuta de regulação apresentada, o ambiente ainda será de insegurança jurídica, tendo em vista que, por conta da omissão legislativa diversas companhias optaram por atribuir as funções do encarregado a uma pessoa que já fizesse parte do quadro de funcionários visando evitar custos. Ainda, há diversas empresas que optaram por encarregados prestadores de serviço, que atuam nessa posição em diversos empreendimentos. Tais medidas geram real possibilidade da existência de conflitos de interesses que aumentam a probabilidade de violações à LGPD.

Desse modo, espera-se da autoridade de proteção de dados a elaboração de guias, ainda que não vinculantes, para trazer maior especificidade quanto aos casos em que haveria a configuração de conflito de interesses, como os agentes e encarregados devem agir para evitar que surja esse conflito e o que devem fazer caso isso ocorra. Isso porque, a proposta trazida deixa os agentes e encarregados com mais perguntas do que respostas com relação ao conflito de interesses.

Assim, o presente artigo tem como objetivo, através de uma análise comparativa entre o Brasil e União Europeia, entender como o bloco europeu vem lidando com a questão da independência do DPO e buscar possíveis soluções para o problema do conflito de interesses.

Para isso, primeiro será abordada uma breve evolução regulatória da proteção de dados nesses ordenamentos jurídicos. Em seguida, através de doutrina e regulação brasileira e europeia se buscará compreender a figura do encarregado pelo tratamento de dados pessoais. Ademais, a questão da independência do DPO será tratada a partir de uma comparação entre os regimes jurídicos. Por fim, conclui-se que o conflito de interesses implica em um verdadeiro problema na atuação do encarregado e, por isso, propõe-se possíveis medidas a serem tomadas para sanar essa lacuna.

1. Breve histórico da proteção de dados pessoais no Brasil e na União Europeia

Levando em consideração a metodologia escolhida no presente trabalho, a análise comparativa entre o ambiente regulatório do Brasil e o da União Europeia acerca da questão do conflito de interesses do encarregado pelo tratamento de dados pessoais, se mostra relevante abordar a evolução regulatória de ambos os ordenamentos jurídicos para melhor compreender, a partir das semelhanças e diferenças, como esses regimes vêm reagindo aos avanços tecnológicos para garantir uma maior proteção aos dados pessoais.

No Brasil, os primeiros passos rumo à garantia de alguns direitos importantes e precursores da proteção de dados pessoais ocorreu com a promulgação da Constituição Federal de 1988. Assim, ganharam status de direito fundamental e de cláusula pétrea a inviolabilidade da vida privada, das residências e da correspondência, entre outras garantias associadas à privacidade dos indivíduos. Com o tempo e de maneira tímida, o assunto da proteção de dados pessoais foi ganhando espaço no cenário nacional.

Contudo, em decorrência de uma movimentação que visava regular a internet de forma restritiva e com viés penal, o que seria prejudicial para o fomento à inovação, foi elaborado o Marco Civil da Internet, para regular de forma civil e principiológica esse meio tão disruptivo[4]. Essa legislação trouxe de

4. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2021, pp. 127-128.

forma explícita princípios basilares para o uso da internet no Brasil, como a proteção de dados pessoais e a proteção da privacidade.

Apesar dos avanços dessa temática no Brasil, ainda não havia uma lei específica para tratar desse assunto. Como o início da aplicação da GDPR em 2018, ficou ainda mais evidente a importância de o país possuir sua própria lei de proteção de dados pessoais, o que influenciou os legisladores para a edição da Lei Geral de Proteção de Dados Pessoais . Vale mencionar que um dos impulsos para a edição dessa regulação foi o artigo 46 da GDPR, que criou certas exigências para a transferência de dados para países terceiros, o que poderia acabar prejudicando essa transmissão de dados entre o Brasil e o bloco europeu[5].

Dessa forma, a LGPD foi criada com o objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[6]. Para isso, essa lei traz princípios que regem o tratamento de dados pessoais, conceitos, direitos dos titulares de dados, como funciona a responsabilização no caso de infrações e como ocorre a transferência internacional de dados.

Entretanto, foi apenas em 2022, com o advento da Emenda Constitucional nº 115, que a proteção de dados pessoais ganhou status de direito fundamental. Para isso, foi incluído no artigo 5º da Constituição Federal o inciso LXXIX. Ademais, como mencionado, somente em julho de 2023 a Autoridade Nacional de Proteção de Dados aplicou a primeira sanção por descumprimento às disposições da LGPD. Apesar disso, a ANPD, criada pela legislação de proteção de dados, já elaborava há alguns anos guias orientativos sobre diversas temáticas, como a utilização de cookies e as definições de agentes e de encarregado de tratamento de dados pessoais.

Dada a importância da temática, em novembro de 2023 a ANPD abriu uma consulta pública com relação a uma proposta de regulamentação complementar para o encarregado de dados. Contudo, nessa proposta é abordada uma definição genérica de conflito de interesse, uma vedação ampla quanto ao acúmulo de cargos pelo encarregado nos casos em que houver esse conflito

5. LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, [S. l.], v. 12, n. 02, pp. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 20 jul. 2023, pp. 12-13.

6. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei no 13.853, de 2019. Brasília, Diário Oficial da União, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 25 jul 2023.

e uma expressa vedação quanto ao acúmulo nos casos de cargos cuja responsabilidade seja tomar decisões referentes ao tratamento de dados pessoais.

Apesar da falta de maiores especificações quanto aos casos em que haveria configuração de conflito de interesse e de que medidas podem ser tomadas para evitar esse conflito, a aprovação dessa regulamentação geraria mais um avanço para um estado da arte mais estável com relação à proteção de dados pessoais no Brasil. No entanto, até a elaboração desse artigo, ainda não há previsão para entrada em vigor desta normativa e persiste a lacuna quanto à regulação do conflito de interesse do encarregado de dados na regulação brasileira.

Já com relação ao regime europeu, em 1981, o Conselho da Europa[7] elaborou um tratado, a Convenção 108. Essa foi pioneira ao abordar, no âmbito internacional, a proteção de dados pessoais, em especial nos casos de tratamentos automatizados. Assim, esse tratado possui grande relevância até os dias atuais e trouxe importantes definições e princípios, como a importância da qualidade dos dados, que devem ser precisos, atualizados e armazenados apenas para propósitos legítimos e específicos.

Anos depois, em 1995, foi editada a Diretiva 95/46/CE, feita pelo Parlamento e Conselho Europeus que tinha como objetivo "a proteção das liberdades e dos direitos, fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais"[8]. Contudo, essa regulação possuía um diferencial, já que não apenas tratava da proteção de dados pessoais, mas também da livre circulação desses dados, dada sua importância para o livre comércio estabelecido entre os países do bloco europeu.

Em 2018, ganhou aplicabilidade ao General Data Protection Regulation (GDPR) que foi editada também pelo Parlamento e Conselho Europeus em 2016, no âmbito da União Europeia. Essa nova regulação também tem como objetivo a proteção de dados pessoais e a sua livre circulação no bloco de maneira segura. Contudo, esse instrumento busca atualizar as regras, já que houve diversos avanços tecnológicos desde a edição da Diretiva 95, agora revogada, entre eles o armazenamento na nuvem, big data, plataformas digitais,

7. O Conselho da Europa e o Conselho Europeu proporcionaram significativos avanços para o direito à proteção de dados pessoais, mas fazem parte de sistemas jurídicos distintos. Dessa forma, o Conselho Europeu está inserido no contexto da União Europeia, enquanto o Conselho da Europa, responsável pela Convenção 108, não tem relação com o bloco europeu.

8. CONSELHO E PARLAMENTO EUROPEUS. *Diretiva 95/46/CE/1995*. Luxemburgo. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 27 jul. 2023.

redes sociais e muitos outros que alteraram significativamente o contexto em que estava inserida a antiga Diretiva.

Além disso, outra diferença entre essas regulações é que a GDPR é aplicável a todos os países membros da União Europeia e visa uniformizar a regulação do bloco quanto a proteção de dados pessoais, enquanto a Diretiva trazia regras gerais, para que cada país as implementasse da forma que desejasse, criando suas próprias leis[9].

Ademais, de maneira semelhante as entidades regulatórias brasileiras, como a ANPD, que elabora guias orientativos e manuais, na União Europeia vale chamar atenção para os trabalhos realizados pelo *Article 29 Working Party* e pelo *European Data Protection Supervisor*. As obras realizadas por esses entes do bloco europeu trazem explicações detalhadas a partir da interpretação da GDPR em conjunto com o entendimento das Cortes Europeias acerca da legislação vigente e da importância da adoção de boas práticas para garantir uma maior proteção aos dados pessoais e evitar sanções por parte das autoridades europeias.

Havendo uma melhor compreensão do estado da arte da proteção de dados pessoais no Brasil e na União Europeia, se mostra necessário um aprofundamento acerca da figura do encarregado. Dessa forma, será possível em seguida abordar o tema central do presente trabalho, o conflito de interesse gerado pelo acúmulo de funções por parte do encarregado e a ausência de disposição regulatória no cenário brasileiro sobre essa temática.

2. A figura do encarregado pelo tratamento de dados pessoais no Brasil e na União Europeia

Primeiro, é essencial explicar que o encarregado e o *Data Protection Officer* não são sinônimos. Isso porque esses sujeitos, envolvidos no tratamento de dados, apesar de possuírem algumas semelhanças, possuem atribuições funcionais diferentes. Desse modo, ainda que o presente trabalho tenha como objetivo analisar o conflito de interesses do encarregado a partir de uma perspectiva de Direito comparado, é importante ressaltar que não é possível compreender essas duas figuras como sinônimas.

9. SILVA, Ricardo Barretto Ferreira da; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor Koketu da. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. *Migalhas*, [s. l.], 4 jun. 2018. Disponível em: https://www.migalhas.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia. Acesso em: 18 jul. 2023.

Nesse sentido, Denis Lima de Oliveira explica que a LGPD não conferiu ao encarregado a mesma relevância conferida pela GDPR ao DPO:

> Tendo em vista a cultura de proteção de dados e a maturidade que a regra europeia possui (que retoma, no mínimo, ao ano de 1995), é oportuno entender a figura do DPO europeu para uma melhor compreensão do que pode ser a melhor prática em torno do Encarregado. E o termo melhor prática é utilizado propositalmente, a fim de evidenciar que a LGPD não concede ao Encarregado a mesma relevância em suas funções e atribuições como o faz a GDPR em relação ao DPO. Encarregado não é sinônimo de DPO[10].

Assim, já esclarecida a impossibilidade de tratar o encarregado e o DPO como sinônimos, cabe abordar as atribuições desses sujeitos envolvidos no tratamento de dados pessoais. A Lei Geral de Proteção de Dados Pessoais traz no artigo 41 as atividades realizadas pelo encarregado:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

10. DE OLIVEIRA, Denis Lima. Agentes de tratamento de dados pessoais e encarregado: Guia prático sobre suas atribuições, responsabilidades e boas práticas. Tese (Mestrado em Direito dos Negócios). Escola de Direito. Fundação Getulio Vargas. São Paulo, 2021. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31490/TrabalhoDenisLima-deOliveira_2022_final_v1.pdf?sequence=6&isAllowed=y Acesso em: 23 jul. 2023, pp. 54.

Enquanto isso, o *General Data Protection Regulation* especifica no artigo 39 as funções do *Data Protection Officer*:

> 1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:
> a. Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
> b. Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
> c. Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º;
> d. Coopera com a autoridade de controlo;
> e. Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.
>
> 2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Através da comparação entre as atividades realizadas pelo encarregado no âmbito da LGPD e pelo DPO na esfera da GDPR, fica evidente que a legislação brasileira atribuiu ao encarregado atividades mínimas e genéricas, deixando a cargo da Autoridade Nacional de Proteção de Dados expandir e detalhar essas atribuições, o que está em andamento dado que em novembro de 2023 a autoridade abriu consulta pública a respeito de uma proposta de regulação para o encarregado. Enquanto isso, o regulamento europeu optou por ser mais específico tanto com as funções exercidas pelo DPO, como em que casos é necessária a contratação desse agente[11].

11. LIMA, Cíntia Rosa Pereira de. Agentes de tratamento de dados pessoais (controlador, operador e encarregado pelo

Entretanto, no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado realizado pela ANPD não foram detalhadas ou especificadas outras atividades atribuídas à figura do encarregado. No entanto, a autoridade buscou suprir algumas omissões da legislação brasileira de dados pessoais com relação a esse sujeito, como, por exemplo, a possibilidade de o encarregado ser uma pessoa que já faz parte do quadro de funcionários da organização ou um agente externo.

Ademais, dada a ausência de qualquer menção legislativa a respeito da independência do encarregado ou da relevância em se evitar conflitos de interesse, foi evidenciada, no guia, importante medida de boa prática: a garantia de que o encarregado tenha liberdade para exercer suas funções[12].

Apesar das diferenças entre o encarregado e o DPO abordadas, esses sujeitos possuem semelhanças que devem ser ressaltadas, como, por exemplo, ambos têm como principal função garantir a conformidade do tratamento de dados pessoais realizado pela organização com a regulação de proteção de dados pessoais[13]. Desse modo, atuam como elo entre o controlador, operador, o titular dos dados e a autoridade de proteção de dados.

Levando em conta a compressão das atribuições e da figura do encarregado e do *Data Protection Officer*, cabe abordar a seguir a temática central do presente trabalho: a possibilidade de conflitos de interesse a partir do acúmulo de funções por esses agentes e a ausência de previsão legal no Brasil sobre essa questão.

3. A independência do encarregado pelo tratamento de dados pessoais no Brasil e na União Europeia

Primeiro, cabe mencionar o entendimento da Norma de Certificação de Sistemas de Gestão de Compliance Antissuborno acerca do conflito de interesses:

---

tratamento de dados pessoais) In: LIMA, Cíntia Rosa Pereira (coord.). *Comentários à Lei geral de proteção de dados*: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 279-296. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788584935796. Acesso em: 25 jul. 2023, pp. 287.

12. ANPD. (Brasil) *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 23 jul. 2023, pp. 23.

13. STUART, Mariana Battochio; VALENTE, Victor Augusto Estevam; MARTINS, José Eduardo Figueiredo de Andrade. A RESPONSABILIDADE PENAL DO ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS. *Argumenta Journal Law*. 2022. Disponível em: https://seer.uenp.edu.br/index.php/argumenta/article/viewFile/2417/pdf Acesso em: 24 jul. 2023, p. 186-187.

> Convém que a organização identifique e avalie o risco de conflito de interesses interno e externo. Convém que a organização informe a todo seu pessoal, de maneira clara, o dever de relatar qualquer conflito de interesse, real ou potencial, como conexão familiar, financeira ou outra direta ou indireta, que esteja relacionada à sua linha de trabalho.[14].

A partir dessa perspectiva sobre o conflito de interesses, é possível perceber a importância de a organização e o próprio funcionário se manterem atentos ao surgimento de possíveis conflitos, já que esses podem facilitar a ocorrência de omissões e violações à regulação vigente.

É essencial para a abordagem do problema do conflito de interesses com relação às atribuições do encarregado pelo tratamento de dados pessoais, ressaltar a conexão entre a atuação independente desse agente e a ausência de conflitos. Como mencionado, a Autoridade Nacional de Proteção de Dados Pessoais, explicou no guia orientativo que é de extrema relevância assegurar a liberdade do encarregado para realizar suas funções, sendo essa uma boa prática[15].

Contudo, não há dispositivos específicos na regulação sobre esse conflito de interesses ou sobre a importância da atuação independente do encarregado. Sobre essa omissão, Caovilla, Dufloth e Timm explicam que:

> Ainda, foi suprimida a exigência de autonomia técnica e profissional do cargo. Em que pese essa ser uma decisão que possa continuar sendo tomada pelas organizações, a ausência de previsão legal nesse sentido pode ser vista como temerária, tendo em vista a necessidade de ser garantida certa independência do DPO para que possa desempenhar suas funções de forma adequada. A bem da verdade, como se verifica da experiência europeia (da qual trataremos adiante), o DPO não se traduz em figura que atua meramente para resguardar os interesses do agente de tratamento, mas, sim, como responsável por garantir o cumprimento da legislação de proteção de dados.[16]

14. ABNT. Norma de Certificação de Sistemas de Gestão de Compliance Antissuborno. 2017. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/55a-legislatura/comissao-de-juristas-administracao-publica/documentos/outros-documentos/NBRISO370012017.pdf Acesso em: 24 jul. 2023, pp. 33.

15. ANPD. (Brasil) *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf . Acesso em: 23 jul. 2023, pp. 23.

16. CAOVILLA, Renato V.; DUFLOTH, Rodrigo; TIMM, Luciano B. A Relação do Data Protection Officer (DPO) com os Reguladores. In: BLUM, Renato O.; MORAES, Henrique F.; VAINZOF, Rony (org.), *Data Protection Officer* (Encarregado). São Paulo: Thomson Reuters, 2020. p. 457-471.

Evidente que essa omissão legislativa pode ser extremamente danosa para os titulares dos dados pessoais, já que, como explicado, uma das atribuições do encarregado é garantir a conformidade do tratamento com a regulação vigente. Assim, para que esse agente possa exercer suas funções ele precisa de independência e liberdade, ou seja, ausência de conflito de interesses. Entretanto, como até o momento da elaboração desse artigo não há previsão legal vigente a respeito dessa temática no Brasil, encarregados pelo tratamento de dados pessoais estão acumulando funções e atuando eivados de conflito de interesses.

Ainda, dada a lacuna existente, os agentes de tratamento de dados (operador e controlador), os encarregados e a própria ANPD não possuem qualquer regra para nortear sua atuação frente a um caso de violação da Lei Geral de Proteção de Dados Pessoais com um possível conflito de interesses.

Enquanto isso, na União Europeia, o *General Data Protection Regulation* no artigo 38, número 6, explicita que: "O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses."Assim, evidente que a regulação do bloco europeu trata sobre a temática do conflito de interesses e inclusive atribui a responsabilidade de garantir a inexistência de conflitos de interesses aos agentes de tratamento, o controlador ou o operador, sendo permitido ao encarregado acumular diversas funções desde que respeitada essa limitação.

Nesse sentido, é de grande relevância o entendimento trazido nas *Guidelines on Data Protection Officers* realizadas pelo *Article 29 Data Protection Working Party,* em que eles explicam como a regra trazida pela GDPR será aplicada em casos concretos, de maneira a evitar conflitos de interesses:

> A ausência de conflito de interesses está intimamente ligada à exigência de agir de forma independente. Embora os DPOs possam ter outras funções, eles só podem ser incumbidos de outras tarefas e deveres, desde que não deem origem a conflitos de interesses. Isso implica, em particular, que o DPO não pode ocupar um cargo dentro da organização que o leve a determinar as finalidades e os meios de processamento de dados pessoais. Devido à estrutura organizacional específica de cada organização, isso deve ser considerado caso a caso.[17] (tradução da autora)

17. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Officers ('DPOs')*. Adotada em 13.12.2016, revisada em 05.04.2017 e ratificada pelo European Data Protection Board em 25.05.2018 conforme Endorsement

De maneira semelhante, o trabalho realizado pelo *European Data Protection Supervisor* sobre o *Data Protection Officer* explica que o controlador ou o operador devem garantir que as funções acumuladas pelo DPO não gerem conflitos de interesses. Assim, o entendimento dessa entidade é de que, apesar da necessidade de análise caso a caso, o DPO não poderia atuar em funções nas quais determinasse as finalidades e formas de tratamento de dados pessoais, já que nesses casos o conflito seria flagrante[18].

Levando em consideração as disposições regulatórias acerca do conflito de interesses na União Europeia, se mostra necessária a análise envolvendo uma condenação recente realizada pela Corte de Justiça da União Europeia em decorrência de violações à vedação ao conflito de interesses na eventualidade de acúmulo de atividades por parte dos DPOs.

Cabe mencionar o caso X-FAB Dresden GmbH & Co. KG vs. FC julgado pela Corte de Justiça da União Europeia. Trata-se de caso originário da Alemanha que envolve não somente o acúmulo de funções por parte do *Data Protection Officer*, como também das limitações impostas pela GDPR para a demissão desse agente. Com relação a temática central deste trabalho, a corte entendeu que:

> O artigo 38º, nº 6, do Regulamento (UE) 2016/679 deve ser interpretado no sentido de que pode existir um «conflito de interesses», na aceção desta disposição, quando são confiadas a um encarregado da proteção de dados outras funções ou atribuições, que levem este último a determinar as finalidades e os meios de tratamento de dados pessoais junto do responsável pelo tratamento ou do seu subcontratante, o que cabe ao juiz nacional determinar casuisticamente, com base numa apreciação de todas as circunstâncias pertinentes, nomeadamente da estrutura organizacional do responsável pelo tratamento ou do seu subcontratante e à luz de toda a regulamentação aplicável, incluindo as eventuais políticas destes últimos.[19]

1/2018. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>. Acesso em 21.jul.2023, pp. 16.

18. European Data Protection Supervisor. (União Europeia) *Position paper on the role of Data Protection Officers of the EU institutions and bodies*. 2018. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf Acesso em: 25 jul. 2023, pp. 11.

19. CJEU - C-453/21 - X-Fab Dresden GmbH & Co. KG vs. FC. Disponível em: https://gdprhub.eu/index.php?title=CJEU_-_C-453/21_-_X-Fab_Dresden_GmbH_%26_Co._KG . Acesso em 24 jul. 2023, pp. 10.

Levando em conta a análise realizada ao longo deste artigo, comparando o ambiente regulatório brasileiro com o da União Europeia, cabe a seguir tratar das conclusões extraídas do presente trabalho e propor possíveis soluções para a lacuna encontrada na regulação brasileira.

Considerações finais

Primeiro, cabe apontar que ficou evidente ao longo do presente trabalho a diferença de maturidade entre a regulação sobre a proteção de dados pessoais no Brasil e no bloco europeu. Ademais, a partir da análise comparativa proposta, foram indicadas lacunas e omissões do legislador e das entidades reguladoras que podem e vão gerar problemas e litígios no futuro envolvendo o conflito de interesses, já que a atual situação é de extrema insegurança jurídica.

Ainda, vale chamar atenção para a importância de uma participação mais ativa das entidades regulatórias como a Autoridade Nacional de Proteção de Dados Pessoais. Vale ressaltar, uma postura ativa não apenas com relação a sua atribuição sancionatória, mas também na elaboração de manuais de boas práticas e guias orientativos para que seja possível sanar essas omissões mencionadas ao longo desse artigo, de forma a garantir maior proteção de dados pessoais e maior previsibilidade.

Outrossim, necessário afirmar que, levando em consideração a análise realizada e a existência de diversos casos no âmbito da União Europeia envolvendo o conflito de interesses do *Data Protection Officer*, é perceptível que esses litígios e problemas irão surgir no Brasil também. Contudo, até o momento não há um arcabouço regulatório acerca dessa temática para que seja possível resolver esses casos.

Dessa forma, é claro que em um mundo globalizado e tendo em mente que a Lei Geral de Proteção de Dados Pessoais possui fortes inspirações na *General Data Protection Regulation*, é essencial que o Brasil e sua entidades reguladores estejam atentos aos litígios, violações e obstáculos enfrentados pela União Europeia para que seja possível uma preparação e evolução do cenário regulatório brasileiro para lidar com os avanços tecnológicos e os novos problemas que surgem a todo momento.

Dada a atual lacuna legislativa observada ao longo deste trabalho, se mostra importante a proposição de uma possível solução para essa temática. O problema do conflito de interesses não é novidade na regulação brasileira, mas é muito presente no âmbito do Direito Societário. Nessa seara, existem

diversas previsões da Lei 6.404, acerca das sociedades anônimas e da Comissão de Valores Mobiliários, que preveem medidas a serem tomadas no caso do surgimento de conflitos de interesses.

Ainda, nesse campo, existem diversos deveres atribuídos aos administradores que previnem que conflitos de interesses gerem problemas, como o dever de informar. Logo, uma possível solução para essa problemática no âmbito da proteção de dados pessoais seria uma analogia entre o encarregado do tratamento de dados e um diretor de uma companhia, que, por exemplo, não pode votar em deliberações nas quais possa ter algum conflito de interesse.

Assim, o presente artigo cumpre seu objetivo ao concluir que o acúmulo de funções pelo encarregado não é um problema. Contudo, dada a presente lacuna e omissão regulatória sobre essa questão, cria-se um problema para a evolução da proteção de dados pessoais no Brasil. Isso porque a União Europeia vem enfrentando casos a respeito do conflito de interesses do DPO, que vem sendo solucionados com base na GDPR e nos guias e trabalhos realizados por entidades reguladoras.

Ademais, a atual omissão com relação ao conflito de interesses na regulação brasileira acerca da proteção de dados pessoais criará um obstáculo à responsabilização dos agentes de tratamento (controlador e operador) nos casos de violações a LGPD que envolverem esse conflito de interesses. Logo, a temática da proteção de dados no Brasil sofrerá com esse problema à medida que será de grande dificuldade uma condenação dos agentes de tratamento com base nesse ponto.

Assim, fica evidente a importância de questionamentos, como os trazidos ao longo deste trabalho. Ainda, é de grande importância, como mencionado, uma postura mais ativa por parte do legislador e das entidades reguladoras para que essa e outras omissões não prejudiquem o caminho que vem sendo trilhado pela proteção de dados pessoais no Brasil.

Referências

Ministério da Justiça e Segurança Pública. (Brasil) *ANPD aplica a primeira multa por descumprimento à LGPD.* 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd#:~:text=A%20Coordenação%2DGeral%20de%20Fiscalização,Geral%20de%20Proteção%20de%20Dados. Acesso em: 25 jul. 2023.

BlnBDI (Berlin) - Berlin DPO Conflict of Interest. Disponível em: https://gdprhub.eu/index.php?title=BlnBDI_(Berlin)_-_Berlin_DPO_Conflict_of_Interest#:~:text=The%20Berlin%20Commissioner%20for%20Data,an%20executive%20of%20the%20company. Acesso em: 25 jul. 2023.

BIONI, Bruno Ricardo. P*roteção de Dados Pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2021.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito,* [S. l.], v. 12, n. 02, pp. 01–33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 20 jul. 2023.

Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei no 13.853, de 2019. Brasília, Diário Oficial da União, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 25 jul 2023.

CONSELHO E PARLAMENTO EUROPEUS. *Diretiva 95/46/CE/1995*. Luxemburgo. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX-:31995L0046&from=PT. Acesso em: 27 jul. 2023.

SILVA, Ricardo Barretto Ferreira da; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor Koketu da. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. *Migalhas*, [s. l.], 4 jun. 2018. Disponível em: https://www.migalhas.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia. Acesso em: 18 jul. 2023.

DE OLIVEIRA, Denis Lima. Agentes de tratamento de dados pessoais e encarregado: Guia prático sobre suas atribuições, responsabilidades e boas práticas. Tese (Mestrado em Direito dos Negócios). Escola de Direito. Fundação Getulio Vargas. São Paulo, 2021. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31490/TrabalhoDenisLimadeOliveira_2022_final_v1.pdf?sequence=6&isAllowed=y Acesso em: 23 jul. 2023.

LIMA, Cíntia Rosa Pereira de. Agentes de tratamento de dados pessoais (controlador, operador e encarregado pelo tratamento de dados pessoais) In: LIMA, Cíntia Rosa Pereira (coord.). *Comentários à Lei geral de proteção de dados*: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 279-296. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788584935796. Acesso em: 25 jul. 2023.

ANPD. (Brasil) *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 23 jul. 2023

STUART, Mariana Battochio; VALENTE, Victor Augusto Estevam; MARTINS, José Eduardo Figueiredo de Andrade. A RESPONSABILIDADE PENAL DO ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS. *Argumenta Journal Law*. 2022. Disponível em: https://seer.uenp.edu.br/index.php/argumenta/article/viewFile/2417/pdf Acesso em: 24 jul. 2023.

ABNT. Norma de Certificação de Sistemas de Gestão de Compliance Antissuborno. 2017. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/55a-legislatura/comissao-de-juristas-administracao-publica/documentos/outros-documentos/NBRISO370012017.pdf Acesso em: 24 jul. 2023, pp. 33.

CAOVILLA, Renato V.; DUFLOTH, Rodrigo; TIMM, Luciano B. A Relação do Data Protection Officer (DPO) com os Reguladores. In: BLUM, Renato O.; MORAES, Henrique F.; VAINZOF, Rony (org.), *Data Protection Officer* (Encarregado). São Paulo: Thomson Reuters, 2020. p. 457-471. p. 459.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Officers ('DPOs'). Adotada em 13.12.2016, revisada em 05.04.2017 e ratificada pelo European Data Protection Board em 25.05.2018 conforme Endorsement 1/2018. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>. Acesso em 21.jul.2023.

European Data Protection Supervisor. (União Europeia) *Position paper on the role of Data Protection Officers of the EU institutions and bodies*. 2018. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf Acesso em: 25 jul. 2023.

CJEU - C-453/21 - X-Fab Dresden GmbH & Co. KG vs. FC. Disponível em: https://gdprhub.eu/index.php?title=CJEU_-_C-453/21_-_X-Fab_Dresden_GmbH_%26_Co._KG . Acesso em 24 jul. 2023.

SAAVEDRA, Giovani Agostini. Compliance de dados In: BIONI, Bruno Ricardo (coord. executiva). Danilo Doneda (coord.) *et al*. *Tratado de Proteção de Dados Pessoais*. 1ª ed. Rio de Janeiro: Forense, 2021. E-book. ISBN 9788530992200. p. 729-743. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 22 jul. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

4

LGPD e Organizações Sociais: base legal para o tratamento de dados e interseções com o Poder Público

LAURA ALVES GONZAGA

LAURA ALVES GONZAGA[1]

Sumário: Introdução. 1. A natureza jurídica das Organizações Sociais. 1.2. O tratamento de dados pessoais sensíveis pelas Organizações Sociais. 2. A base legal para o tratamento de dados pelo poder público. 2.1. Tratamento e compartilhamento de dados pelo Poder Público e Organizações Sociais. 2.2. Outros pontos de atenção: governança e encarregado de dados no tratamento de dados pelas Organizações Sociais. Considerações finais. Referências bibliográficas.

Introdução

Desde que entrou em vigor no Brasil em 2018, a Lei Geral de Proteção de Dados (LGPD) gerou questionamentos em torno do tratamento de dados pelo Poder Público – tanto acerca da forma correta de aplicação e regulação da Lei diante das características muito específicas dos diversos entes estatais quanto acerca das atividades e serviços públicos que envolvem o tratamento de dados da população. No entanto, receberam menor atenção as consequências da aplicação da LGPD para os entes privados que cooperam com o Poder Público. É certo que o tratamento de dados nessas circunstâncias precisa ser regulado com atenção especial, visando o interesse dos titulares de dados pessoais e de seus direitos, já que as atividades de tratamento em questão diferem muito daquelas realizadas pelos demais entes privados.

No cenário atual, permanecem ainda muitas dúvidas acerca das implementações práticas da LGPD no que se refere às especificidades das Organizações Sociais (OSs), dada a sua natureza jurídica peculiar enquanto pessoas jurídicas de direito privado que, por prestarem serviços que atendem ao interesse público, recebem apoio e recursos do Estado. Entre os diversos pontos que merecem escrutínio, já que são fundamentais para a definição do regime de tratamento de dados aplicável, está a definição da base legal adequada para o tratamento de dados por esse tipo de instituição. Para entender as implicações desse ponto, será necessário, primeiro, definir o regime jurídico que rege as Organizações Sociais no Brasil, a natureza de suas atividades e o tipo de tratamento de dados envolvido. Em seguida, serão exploradas possíveis bases legais que fundamentam o tratamento de dados pelo próprio Poder Público de acordo com a LGPD, de forma a melhor avaliar os pontos de interseção

1. Advogada formada pela Universidade de São Paulo (USP), com atuação nas áreas de terceiro setor e *compliance*. Pós-graduanda em Direito Digital pelo Instituto Tecnologia e Sociedade do Rio (ITS-Rio) em parceria com a Universidade do Estado do Rio de Janeiro (UERJ).

com as bases legais adequadas para as OSs. Adicionalmente, neste tópico, será possível analisar a possibilidade de que as OSs acessem bases de dados compartilhadas pelo Poder Público e tratem esses dados para suas finalidades específicas, que diferem da maioria das demais entidades privadas. A intenção será fornecer um panorama da aplicabilidade da LGPD ao regime das Organizações Sociais a um nível principiológico, determinando e contextualizando suas obrigações e sua relação com o Poder Público sob o prisma da proteção de dados.

1. A natureza jurídica das Organizações Sociais

As Organizações Sociais (ou "OSs") são entidades privadas que contam com o apoio do Poder Público para exercer atividades de interesse social. São entidades sem fins lucrativos, integrantes do terceiro setor, que se estabelecem por iniciativa privada e, posteriormente, são habilitadas e qualificadas pelo Poder Público, com quem firmam Contrato de Gestão. Por meio desse instrumento, as Organizações Sociais concordam em se submeter parcialmente a algumas das regras de direito público, tais como aos deveres de transparência, de prestação de contas, de impessoalidade e eficiência, entre outros[2].

Suas áreas de atuação são delimitadas legalmente, já que fornecem serviços e atividades de interesse da população como um todo, cumprindo metas e prazos de execução com que se comprometem no contrato de gestão para garantir o acesso dos cidadãos em geral a direitos e serviços públicos, em áreas que não são de exclusividade do Estado. Alguns exemplos são: saúde, cultura, pesquisa científica e ensino[3].

Embora sua natureza jurídica não se altere, sendo claro que se tratam de pessoas jurídicas de direito privado (constituindo fundações privadas ou associações sem fins lucrativos) e que mantêm autonomia administrativa e financeira, é também certo que suas obrigações diante do Poder Público excedem aquelas a que estão atreladas empresas privadas, como contrapartida e condicionante pelos recursos públicos que recebem e administram. Dessa forma,

2. ROCHA, Sílvio Luís Ferreira da. *Terceiro Setor*. São Paulo: Malheiros Editores, 2003. p. 85-86.

3. No âmbito federal, as Organizações Sociais são disciplinadas pela Lei nº 9.637, de 15 de maio de 1998, e abarcam as atividades ensino, pesquisa científica, desenvolvimento tecnológico, proteção e preservação do meio ambiente, cultura e saúde (conforme disposto em seu artigo 1º).

estão inseridas no Direito Administrativo, no contexto de uma das formas de atividade administrativa (o fomento), mas também no Direito Civil, enquanto entidades privadas[4].

Inicialmente, o Poder Público concede habilitação às Organizações Sociais, de acordo com os critérios determinados pela legislação[5]. Uma vez concedida a habilitação, o ente estatal deve fiscalizar sua atividade, o cumprimento de metas e de princípios da administração pública, os indicadores de desempenho e a qualidade dos serviços, tudo como condicionantes para a disponibilização de recursos financeiros e de outros bens necessários para o cumprimento do contrato.

Como breve contextualização, nota-se que o modelo das Organizações Sociais surge no Brasil no âmbito da Reforma do Estado, no governo de Fernando Collor, e é finalmente implementado no Governo de Fernando Henrique Cardoso, sendo a lei federal que o regula publicada em 1998. Em sua essência, é um tipo de parceria público-privada, influenciada por experiências inglesas dos anos 80, em um contexto de avanço do modelo neoliberal, buscando como princípios a desestatização, a privatização e a desregulamentação[6].

É interessante considerar esse contexto observando que, décadas depois, a Lei Geral de Proteção de Dados surge para suprir uma lacuna gerada no Brasil pela ausência de uma regulação de dados nesse mesmo período histórico de estabelecimento do modelo neoliberal, quando muitos países pelo mundo priorizavam a desregulamentação em diversos setores de sua economia[7]. A primazia pela autorregulação do setor privado acabou por gerar distorções e abusos de poder pelos agentes privados que realizam o tratamento de dados, que as legislações de proteção de dados, recentemente estabelecidas, buscam corrigir - como no próprio caso europeu, que estabeleceu o paradigma para a legislação brasileira[8]. Embora os processos descritos não estejam di-

4. RESENDE, Tomáz de Aquino. *Roteiro do Terceiro Setor, Associações e fundações*: o que são, como instituir, administrar e prestar contas. Belo Horizonte: Prax, 2006. p. 128.

5. Os critérios determinados na Lei Federal nº 9.637/98, em seu artigo 2º, incluem a finalidade não-lucrativa, a natureza social de seus objetivos relativos à área de atuação, a previsão de participação de representantes do Poder Público e da comunidade no órgão de deliberação superior, e a obrigação de publicação anual dos relatórios financeiros e do relatório de execução do contrato de gestão. A aprovação da qualificação da entidade como Organização Social é um ato administrativo, em última instância discricionário, ainda que deva atender a critérios de conveniência, oportunidade, etc.

6. VIOLIN, Tarso Cabral. *Terceiro Setor e as Parcerias com a Administração Pública*. Editora Fórum, 2006. p. 201-202.

7. FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena (org.). *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters, 2019. p. 48.

8. VIOLA, Mario e TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. *In:* MENDES, Laura Schertel *et. al* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Editora Forense, 2023. p. 115.

retamente relacionados, a observação desse contexto de desregulamentação permite a melhor compreensão dos desafios enfrentados para a adequação das Organizações Sociais à LGPD e a necessidade de uma atenção especial ao tratamento e compartilhamento de dados pelo Poder Público com essas organizações privadas, o que será objeto de análise a seguir.

1.1. O tratamento de dados pessoais sensíveis pelas Organizações Sociais

Na seção anterior, foi empreendida breve análise das atividades desempenhadas pelas Organizações Sociais, necessariamente em áreas de interesse público - delimitadas, no âmbito federal, pela Lei nº 9.637/98, aos campos de ensino, pesquisa científica, desenvolvimento tecnológico, proteção e preservação do meio ambiente, cultura e saúde. Nas ordens jurídicas parciais, tais como estados e municípios, a legislação frequentemente positiva o modelo das OSs com ainda maior limitação das áreas de atuação[9]. Observa-se que as áreas definidas pela legislação federal englobam atividades de responsabilidade estatal, ligadas aos direitos fundamentais dos cidadãos positivados na Constituição Federal – saúde, educação, cultura[10]. Por essa característica, são atividades que, frequentemente, podem implicar o tratamento de dados pessoais sensíveis.

De acordo com Sergio Negri e Maria Regina Korkmaz, "dados pessoais sensíveis são aqueles ligados às opções e características basilares da *persona* e, portanto, aptos a gerar situações de discriminação e desigualdade"[11]. Essa possibilidade de seu uso para formas ilícitas de discriminação, tanto pelo Estado quanto por agentes privados, justifica a proteção especial que a LGPD confere a esses dados, uma vez que, por sua natureza, o seu tratamento inadequado pode gerar situações de violação de direitos fundamentais[12].

9. A título de exemplo, no caso do Estado de São Paulo, a Lei Complementar nº 846/1998 é mais restritiva do que a lei federal, vez que confere poderes ao Executivo Estadual para qualificar como OSs as entidades que atuam apenas nos ramos da saúde e/ou da cultura, atendidos os pressupostos legais

10. BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 30 jun. 2023.

11. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 64, jan/jun 2019.

12. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 67, jan/jun 2019.

Em seu artigo 5º, inciso II, a LGPD define dado pessoal sensível da seguinte forma:

> 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[13].

A doutrina considera que o rol que o dispositivo apresenta não é taxativo, devendo ser interpretado de maneira expansiva que permita a garantia dos direitos fundamentais envolvidos[14]. Por exemplo, se um dado não é diretamente relacionado à saúde, mas permite que sejam inferidas informações sobre a saúde do indivíduo identificado ou identificável (por exemplo, geolocalização), esse dado deve ser tratado como sensível[15].

Nesse sentido, a LGPD estabelece, em seu artigo 11, hipóteses mais restritas que autorizam o tratamento de dados sensíveis. O consentimento para o tratamento desses dados deve ser ainda mais qualificado por parte do titular[16], sendo excluídas as hipóteses de legítimo interesse do controlador ou de terceiro e de proteção ao crédito. Considera-se que a única finalidade admissível para o tratamento dos dados sensíveis é o interesse do próprio titular, que deve ser informado previamente dos usos desses dados[17], entre outras restrições.

Como observado nas seções anteriores, as Organizações Sociais, por sua própria natureza e delimitação legal, são especialmente propensas a coletar e tratar dados pessoais sensíveis, principalmente quando atuam nas áreas de saúde e educação. É notável a atenção aos dados relacionados à saúde do indivíduo pelo legislador – trata-se de exemplo evidente de dado sensível, já que

13. BRASIL. Lei nº 13.709, de 14 de agosto de 2019. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 jun. 2023.

14. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 74, jan/jun 2019..

15. TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. *In*: Schreiber, Anderson *et. al*. (org). *Problemas de direito civil: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos*. Rio de Janeiro: Editora Forense, 2021. p. 115.

16. TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. *In*: Schreiber, Anderson *et. al*. (org). *Problemas de direito civil:* homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Editora Forense, 2021. p. 108.

17. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 75, jan/jun 2019.

há grande potencial lesivo de discriminação[18] com base no status de saúde de cada pessoa, na manifestação ou não de determinadas condições de saúde, etc, que podem implicar em limitações de liberdades civis e do direito à dignidade humana[19].

Já no caso da atuação das OSs na área da educação, nota-se a maior probabilidade de que haja tratamento de dados de crianças e adolescentes - que exige um grau muito maior de atenção, dada a condição de hipervulnerabilidade de seus titulares[20]. A seção III da LGPD define condições especiais para o tratamento de dados de crianças e adolescentes, determinando que o seu tratamento deve ser sempre realizado no melhor interesse da criança ou do adolescente e considerando a prioridade absoluta da garantia de seus direitos, nos termos do artigo 227 da Constituição Federal. Os critérios para o consentimento também são mais elevados, sendo que esse consentimento deve ser específico e concedido por pelo menos um dos responsáveis legais, de acordo com o artigo 14, parágrafo 1º da LGPD. Considerando esse contexto especial referente aos dados de crianças e adolescentes, a possibilidade de tratamento de seus dados sensíveis deve ser considerada com máxima atenção aos direitos fundamentais de seus titulares[21].

Uma vez que a base legal para o tratamento dos dados pessoais sensíveis é distinta e apresenta restrições importantes, esse fator deve ser considerado na análise das bases legais de tratamento de dados pessoais pelas Organizações Sociais de forma geral, inclusive no tocante ao compartilhamento de dados tratados pelo Poder Público, como será analisado a seguir.

2. A base legal para o tratamento de dados pelo poder público

A LGPD determina, como regra geral, já em seu artigo 1º, que todo e qualquer tratamento de dados deve contar com uma base legal adequada como

18. TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. *In*: Schreiber, Anderson *et. al.* (org). *Problemas de direito civil*: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Editora Forense, 2021. p. 104.

19. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 69, jan/jun 2019.

20. NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, p. 73, jan/jun 2019

21. TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. *In*: Schreiber, Anderson *et. al.* (org). *Problemas de direito civil*: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Editora Forense, 2021. p. 123.

fundamentação para que seja considerado legítimo e lícito. Dessa forma, todas as entidades que realizam o tratamento de dados, sejam elas pessoas jurídicas de direito público ou privado, ou mesmo pessoas naturais, quando aplicável, devem identificar a base legal aplicável a suas atividades, em consonância com os princípios determinados na legislação[22]. Esse é um importante mecanismo de garantia dos direitos dos titulares de dados estabelecidos pela LGPD.

Como brevemente discutido na seção anterior, os artigos 7º e 11 da LGPD listam as diversas bases legais que autorizam o tratamento de dados - o artigo 7º determina requisitos para o tratamento de dados pessoais em geral, enquanto que o artigo 11 traz especificações para os dados pessoais sensíveis. O rol determinado por ambos os artigos para as hipóteses de tratamento é taxativo[23].

A determinação da base legal para o tratamento de dados pessoais pelo Poder Público encontra alguns desafios. Alves e Valadão afirmam que o texto da LGPD, na forma atual, não leva em consideração a multiplicidade de fatores em jogo quando o Poder Público realiza o tratamento de dados – desde a finalidade do tratamento até a relação de assimetria de poder com os titulares dos dados, todas as etapas são radicalmente diferentes das demais situações regidas pela lei, em que não há discriminação adequada para cada cenário. Os autores atribuem essa lacuna ao processo complexo de aprovação do texto final da LGPD, em meio a um cenário político instável, que impediu a devida maturação dos pontos tocantes ao setor público[24].

Uma das especificidades mais evidentes, que não encontra reflexo direto na lei, é o fato de que, de forma geral, o tratamento de dados pessoais realizado pelo setor público não tem seu ponto de partida em uma decisão voluntária do titular dos dados, mas sim deriva da própria obrigação do Estado em desempenhar as finalidades públicas a que se destina e a garantir os direitos da população que representa[25].

22. VIOLA, Mario e TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. *In*: MENDES, Laura Schertel *et. al* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Editora Forense, 2023. p. 116.

23. VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. *In*: MENDES, Laura Schertel *et. al* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Editora Forense, 2023. p. 118.

24. ALVES, Fabrício e VALADÃO, Rodrigo. Regime jurídico do tratamento secundário de dados pessoais pelo poder público. *In*: LIMA, Ana Paula e ALVES, Fabrício (coord). *Comentários aos regulamentos e orientações da ANPD*. São Paulo: Thomson Reuters, 2022. p. 136.

25. ALVES, Fabrício e VALADÃO, Rodrigo. Regime jurídico do tratamento secundário de dados pessoais pelo poder público. *In*: LIMA, Ana Paula e ALVES, Fabrício (coord). *Comentários aos regulamentos e orientações da ANPD*. São Paulo: Thomson

Aqui, é interessante explorar a diversidade de entendimentos sobre a determinação da base legal para o tratamento de dados pelo Poder Público. É possível afirmar que o tratamento de dados para o cumprimento das finalidades públicas já está devidamente contemplado nos artigos mencionados acima: o artigo 7º, inciso II, e o artigo 11, inciso II, alínea "a" da LGPD determinam as hipóteses de cumprimento de obrigação legal, de onde, em última análise, deriva toda obrigação do Poder Público que implica tratamento de dados. Esse entendimento é expressado por Viola e Teffé. Os autores consideram que o artigo 23 da LGPD traz somente "requisitos adicionais e específicos para o tratamento de dados pessoais realizado por parte da Administração Pública, complementando a base legal selecionada no art. 7º ou 11 da lei" [26].

No entanto, coexiste também o entendimento doutrinário de que o referido artigo 23 constitui a base legal mais adequada e verdadeira para o tratamento de dados no setor público. Essa visão é compartilhada por diversos autores, tais como Danilo Doneda e Laura Mendes[27], e é ancorada no entendimento de que a base legal determinada pelos artigos 7º e 11 seria insuficiente, apresentando limitações para uma interpretação tão ampla - considerando que nem toda atividade desempenhada pelo poder público pode ser considerada uma política pública[28].

De fato, o artigo 23 estabelece explicitamente a finalidade pública do tratamento de dados pelo setor público - prescrição que decorre inclusive do próprio regime jurídico de Direito Público -, determinando que o tratamento de dados de um indivíduo pela Administração Pública não pode ocorrer em proveito de terceiros ou da própria Administração, mas sim, invariavelmente, "em proveito de uma finalidade pública"[29].

Nesse ponto, é de máxima importância notar que a Autoridade Nacional de Proteção de Dados (ANPD) consolidou recentemente os entendimentos sobre o assunto ao publicar o Guia Orientativo para o Tratamento de Dados Pessoais

---

Reuters, 2022. p. 139.

26. VIOLA, Mario e TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. *In*: MENDES, Laura Schertel *et. al* (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Editora Forense, 2023. p. 118.

27. MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 555, nov/dez 2018.

28. ALVES, Fabrício e VALADÃO, Rodrigo. Regime jurídico do tratamento secundário de dados pessoais pelo poder público. *In*: LIMA, Ana Paula e ALVES, Fabrício (coord). *Comentários aos regulamentos e orientações da ANPD*. São Paulo: Thomson Reuters, 2022. p. 137.

29. ALVES, Fabrício e VALADÃO, Rodrigo. Regime jurídico do tratamento secundário de dados pessoais pelo poder público. *In*: LIMA, Ana Paula e ALVES, Fabrício (coord). *Comentários aos regulamentos e orientações da ANPD*. São Paulo: Thomson Reuters, 2022. p. 140.

pelo Poder Público, em sua segunda versão, em junho de 2023[30]. O documento foi elaborado para preencher lacunas na interpretação da LGPD no que se refere a seu âmbito de incidência nas atividades do Poder Público, buscando estabelecer parâmetros mais objetivos para a aplicabilidade de seus conceitos básicos. Com isso, a ANPD busca proporcionar maior segurança jurídica para órgãos e entidades públicos, com quem deve atuar de forma articulada e colaborativa, por força de suas atribuições legais.

Quanto à questão da base legal para o tratamento de dados, o Guia parece indicar que, para o Poder Público, ela decorre do cumprimento de obrigação legal, fundamentada pelo mesmo art. 7º, inciso II: a base legal é localizada nas normas de organização, que estruturam órgãos e entidades e estabelecem suas competências e atribuições. Ainda que o Guia não tenha natureza normativa, uma vez que não constitui uma resolução da ANPD, e opere num nível de orientação geral, trata-se de um documento extremamente importante para consolidar a evolução do entendimento da doutrina sobre o assunto. O documento reforça ainda, como princípios que constituem parte indissociável do tratamento de dados pessoais pelo Poder Público: finalidade, adequação, necessidade, transparência, e livre acesso[31]. De acordo com o Guia,

> [O] tratamento de dados pessoais pelo Poder Público deve estar sempre associado a uma finalidade pública, que seja: (i) legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais; (iii) explícita, isto é, expressa de uma maneira clara e precisa; e (iv) informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados[32].

Nesse ponto, a ANPD reforça a especificidade do tratamento de dados no âmbito do setor público, que deve necessariamente atender a uma finalidade

30. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo – tratamento de dados pessoais pelo Poder Público*. Brasília, DF: 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 jun. 2023. p. 10.

31. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo – tratamento de dados pessoais pelo Poder Público*. Brasília, DF: 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 jun. 2023. p. 22.

32. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo – tratamento de dados pessoais pelo Poder Público*. Brasília, DF: 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 jun. 2023. p. 23.

pública, em consonância com o disposto no artigo 23 da LGPD - sendo que esse dispositivo da lei é considerado como determinante de "critérios adicionais", que "complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público"[33].

2.1 Tratamento e compartilhamento de dados pelo Poder Público e Organizações Sociais

Na seção anterior, constatou-se que está positivada na LGPD a preocupação com o papel do Poder Público enquanto agente de tratamento de dados pessoais, sendo expressa a necessidade de garantir a finalidade pública desse tratamento. Como analisado no ponto da natureza jurídica das Organizações Sociais, esse regime não é aplicável diretamente a essas instituições, que configuram entes privados. No entanto, muito da determinação e dos espaços de dúvida sobre o tratamento de dados pelo Poder Público tem também implicações para o tratamento de dados pelas OSs, por dois motivos principais: (i) as OSs são também responsáveis pela execução de diversas políticas públicas; e (ii) há a necessidade de regulamentar o compartilhamento de dados com as OSs pela Administração Pública[34].

A LGPD, em seu artigo 26, trata do compartilhamento de dados, determinando que este deve "atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas". O parágrafo 1º do mesmo artigo determina ainda que ao Poder Público é vedado "transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso"[35].

A partir deste dispositivo, seria possível extrair que as OSs estariam completamente proibidas de acessar bases de dados organizadas ou mantidas pelo Poder Público, bem como de tratar esses dados de qualquer outra maneira. No entanto, o mesmo dispositivo determina os casos em que se aplicam exceções a essa regra e que incluem diversas hipóteses aplicáveis às atividades desempenhadas por Organizações Sociais de diversos tipos. Entre as exceções listadas, estão:

33. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo – tratamento de dados pessoais pelo Poder Público*. Brasília, DF: 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 jun. 2023. p. 10.

34. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral de Proteção de Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 06, p. 1699, 2021.

35. BRASIL. Lei nº 13.709, de 14 de agosto de 2019. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 jun. 2023.

a. Inciso I: hipóteses de execução descentralizada de atividade pública, quando o compartilhamento dos dados é exigido para a realização dessa atividade, exclusivamente para esse fim específico e determinado; e
b. Inciso IV: hipóteses em que haja previsão legal ou quando a transferência for respaldada em contratos, convênios ou instrumentos congêneres[36].

É interessante notar que o inciso II do artigo 23, que proibia expressamente o compartilhamento de dados com pessoas jurídicas de direito privado, acabou por sofrer veto presidencial e não constar no texto final da lei[37].

Observa-se, dessa forma, que as hipóteses descritas nos incisos I e IV do artigo 26, delimitadas acima, oferecem uma base legal que justifica o compartilhamento de bases de dados públicas para pessoas jurídicas privadas quando estas são responsáveis pela realização e execução de políticas públicas, ou seja, de atividades de interesse geral, que tenham finalidade pública, em harmonia com a base legal para o tratamento de dados pela própria autoridade pública. Da mesma forma, a transferência da obrigação de execução da política pública, respaldada em "contratos, convênios ou instrumentos congêneres", configura previsão legal e, portanto, base legal de tratamento[38].

Após as considerações sobre as exigências estabelecidas pela LGPD para o compartilhamento de dados pelo Poder Público em diversos contextos, é possível retomar a análise do caso específico das Organizações Sociais.

Como discutimos no item 1 deste trabalho, as Organizações Sociais são, necessariamente, pessoas jurídicas de direito privado sem fins lucrativos, que celebram contrato de gestão com a Administração Pública. O contrato de gestão determina a atuação da OS, que deve atender ao interesse público, executando políticas públicas e garantindo a expressão de direitos da população em suas áreas de atuação.

Nesses termos, os contratos de gestão constituem "instrumentos congêneres", nos termos do artigo 26, parágrafo 1º, inciso IV da LGPD, e o compartilhamento de dados, no limite do necessário para a efetiva realização da política pública que a Organização Social desempenha, é justificado e conta com base legal adequada.

36. BRASIL. Lei nº 13.709, de 14 de agosto de 2019. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 jun. 2023.

37. MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo Poder Público. *In*: MULHOLLAND, Caitlin (Coord.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago Editorial, 2020. p. 220.

38. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1698, 2021.

No entanto, a análise não pode ser interrompida nesse ponto. É de máxima importância avaliar a adequação de cada Organização Social e cada contrato de gestão com os fundamentos e princípios determinados pela LGPD, e buscar revisões e reformulações onde a compatibilidade com esses princípios se mostrar insuficiente. O próprio contrato de gestão deve manifestar o entendimento de que o tratamento de dados eventualmente obtidos e compartilhados pelo Poder Público deve ocorrer de forma distinta dos dados que a entidade obtém em sua condição de pessoa jurídica de direito privado, por ter sua base legal distinta[39].

2.2 Outros pontos de atenção: governança e encarregado de dados no tratamento de dados pelas Organizações Sociais

Com a evolução dos dispositivos legais sobre o tema e a consolidação progressiva da ANPD como entidade reguladora, ganha força a discussão em torno da governança e do *compliance* de dados, e como implementá-los de forma eficiente em diversos setores. É importante considerar o *compliance* como ferramenta interdisciplinar, capaz de definir de forma sistêmica "o estímulo constante à prevenção de riscos, à mitigação de danos e à propagação de uma cultura de boas práticas"[40].

Nesse sentido, o Decreto nº 10.046, de 7 de outubro de 2019, é exemplificativo ao prever normas e diretrizes para o compartilhamento de dados pela Administração Pública Federal. O dispositivo define a governança nessa área como o "exercício de autoridade e controle" no tratamento e compartilhamento de dados (em seu artigo 2º, inciso XV), prevendo a regulamentação e fiscalização dessa política de governança por um Comitê (em seu artigo 21)[41]. Em conjunto com a atuação da própria ANPD, é importante que a estruturação de bancos de dados para programas e políticas públicas já conte desde o primeiro momento com a previsão de sistemas de governança, de forma a reforçar a proteção de uma quantidade verdadeiramente massiva de dados dos cidadãos

39. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1703, 2021.

40. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1704, 2021.

41. BRASIL. *Decreto nº 10.046*, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 30 jun. 2023.

brasileiros, que não podem ser compartilhados livremente entre os órgãos do Estado sem considerar as bases legais devidas e as proteções determinadas pela LGPD[42].

É interessante notar que, no que se refere aos agentes privados de tratamento, a LGPD foi menos restrita, definindo a adoção de programas de governança como facultativa em seu artigo 50[43]. Delimita-se, então, uma notável diferença entre o compliance de dados público e o privado. Nesse caso, cabe a análise das obrigações das Organizações Sociais. De acordo com Ehrhardt Jr. e Faleiros Jr., "não pode o Poder Público admitir a exposição de suas bases de dados a parceiros privados que não demonstrem possuir estruturas suficientes de atuação íntegra quanto à governança de dados", uma vez que os tratamentos de dados realizados pelas OSs e outros parceiros privados acarretam riscos, mesmo que necessários para a execução de suas atividades[44]. Dessa forma, ainda que não se possa falar estritamente em uma exigência de que as OSs estruturem programas próprios completos de governança de dados, é necessário que essas instituições se apresentem como capazes de se adequar aos programas de integridade que o Poder Público estabelece para si nessa matéria.

Essa obrigação de adequação à governança de dados por parte das Organizações Sociais apresenta um aspecto interessante no que se refere à obrigação de designar um encarregado de dados (ou, como apontado no GDPR, o *data protection officer* – DPO, na sigla em inglês).

O artigo 41 da LGPD determina as obrigações do encarregado de dados – entre elas, "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências" (parágrafo 2º). No tocante ao Poder Público, a obrigação de contar com o encarregado de dados é bem delimitada no artigo 23, inciso III da LGPD, como condição para o tratamento de dados pessoais pela União, Estados, Distrito Federal e Municípios. No entanto, o mencionado artigo 41 da LGPD inclui uma possibilidade de exceção à obrigação de designação de um encarregado de dados:

42. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1709, 2021.

43. "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais". BRASIL. Lei no 13.709, de 14 de agosto de 2019. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 jun. 2023.

44. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1709, 2021.

> § 3º: A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados [45].

A matéria permaneceu pendente por algum tempo, gerando um cenário de insegurança jurídica quanto à possibilidade de dispensa de encarregado de dados[46]. Finalmente, em 27 de janeiro de 2022, foi publicada a Resolução CD/ANPD nº 2, que estabelece regulamento da aplicação da LGPD para agentes de tratamento de pequeno porte[47].

A definição de agente de pequeno porte, contida no artigo 2º, inciso I da Resolução, poderia, em princípio, contemplar diversas Organizações Sociais, por incluir "pessoas jurídicas de direito privado, inclusive sem fins lucrativos". No entanto, já no artigo 3º, são excluídos do tratamento diferenciado previsto na resolução os agentes de tratamento de pequeno porte que "realizem tratamento de alto risco para os titulares". Essa exclusão abarca a maior parte das atividades das OSs, uma vez que, na definição de tratamento de alto risco, estão incluídos a utilização de dados pessoais sensíveis ou de crianças, adolescentes e idosos (art. 4º, inciso II, d). Como analisado no item 1.2 deste trabalho, a natureza das atividades das OSs frequentemente implica no tratamento de dados sensíveis e de populações hipervulneráveis.

Outras definições da Resolução, como tratamento de dados pessoais em larga escala ou o tratamento que possa afetar significativamente interesses e direitos fundamentais (parágrafos 1º e 2º do artigo 4º, inciso I), têm também o potencial de excluir as OSs do tratamento diferenciado. No entanto, é importante notar que a resolução não determina critérios objetivos para nenhum dos pontos apresentados – não é definido quantitativamente, por exemplo, o que configuraria o tratamento em larga escala. Dessa forma, mesmo que a resolução tenha trazido clareza e definição para as possíveis exceções apresentadas na LGPD, ainda assim será necessário averiguar as decisões concretas produzidas pela ANPD para que maior segurança jurídica sobre o tema seja

45. BRASIL. Lei no 13.709, de 14 de agosto de 2019. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 jun. 2023.

46. EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, p. 1712, 2021.

47. CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Resolução CD/ANPD nº 2*. Aprova o Regulamento de aplicação da Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial da União, 28 de janeiro de 2022, Edição 20, Seção 1, p. 6.

estabelecida. De toda forma, a Resolução nº 2 reforça que mesmo a dispensa ou flexibilização de obrigações não isenta qualquer agente de tratamento de cumprimento dos demais dispositivos da LGPD, incluindo aí todas as suas bases legais e princípios (art. 6º).

Considerações finais

Este trabalho buscou analisar os impactos da Lei Geral de Proteção de Dados para a atuação das Organizações Sociais, especificamente no que se refere às bases legais de tratamento de dados por essas entidades e à aplicação das determinações da LGPD (incluindo temas como governança e encarregado de dados). A análise buscou observar a origem do modelo das Organizações Sociais e a sua natureza jurídica enquanto pessoas de direito privado que, no entanto, executam atividades delegadas pelo Poder Público para a efetivação de serviços públicos e acesso da população a direitos básicos.

Para tanto, foi necessário buscar um entendimento mais profundo acerca das bases legais de tratamento de dados pelo próprio Poder Público, explorando os pontos de insegurança jurídica na legislação atual, bem como os mais recentes avanços pela Autoridade Nacional de Proteção de Dados (ANPD) em consolidar os entendimentos que vinham sendo desenvolvidos e debatidos pela doutrina.

Nesse sentido, foi possível determinar que, quanto à base legal para o tratamento de dados pelo Poder Público, prevalece atualmente o entendimento de que esta decorre do cumprimento de obrigação legal, a partir do artigo 7º, inciso II, e do artigo 11, inciso II, da LGPD. Por sua vez, para que as Organizações Sociais tratem dados compartilhados pelo Poder Público, a base legal adequada é encontrada no artigo 26, parágrafo 1º inciso IV da LGPD, considerando que os contratos de gestão constituem a relação dessas instituições com a Administração Pública e são instrumentos congêneres, que justificam o tratamento dos dados necessários para a finalidade de efetiva realização da política pública delegada à OS. Esse entendimento deriva do desenvolvimento da doutrina e da publicação de guias e resoluções pela ANPD, que representam o constante refinamento das disposições da LGPD de forma a suprir suas lacunas e permitir sua aplicação, levando em consideração as especificidades de diferentes agentes de tratamento na sociedade brasileira. Dentre esses agentes, o Poder Público se destaca, devendo cumprir com as

definições adicionais do artigo 23 da legislação – que, por consequência, devem também ser cumpridos pelas OSs na situação de compartilhamento de dados com o Poder Público.

Também foi possível concluir que, no cenário regulatório atual, embora não seja possível determinar a obrigação das Organizações Sociais de elaborar programas complexos de governança de dados, é absolutamente necessário que estas se adequem inteiramente aos programas de governança determinados pela Administração Pública, em todos os níveis aplicáveis a sua atuação. Ao mesmo tempo, foi possível observar que, ainda que a ANPD venha avançando na tarefa de determinar o espaço regulatório infralegal, prevalecem dúvidas sobre algumas disposições; quanto à obrigação de determinar encarregado de dados, não é seguro determinar que a Resolução nº 2/2022 isente ou dispense as OSs dessa responsabilidade, por sua própria natureza jurídica, sendo importante que a análise seja executada caso a caso e que se acompanhe futuras determinações do órgão em casos práticos.

O intuito do trabalho aqui empreendido foi investigar como as Organizações Sociais se encaixam e se refletem nos paradigmas da Lei Geral de Proteção de Dados, considerando que, ainda que sejam pessoas jurídicas de direito privado, essas entidades exercem papel híbrido na sociedade brasileira e na efetivação de direitos da população, e faz-se necessário iluminar e continuar a investigação dos pontos de dúvida e ambiguidade, em consonância com o objetivo da própria LGPD de trazer regulação e garantia de direitos aos titulares de dados.

Referências

ALVES, Fabrício e VALADÃO, Rodrigo. Regime jurídico do tratamento secundário de dados pessoais pelo poder público. *In*: LIMA, Ana Paula e ALVES, Fabrício (coord). *Comentários aos regulamentos e orientações da ANPD*. São Paulo: Thomson Reuters, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo – tratamento de dados pessoais pelo Poder Público*. Brasília, DF: 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 30 jun. 2023. p. 10.

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 30 jun. 2023.

BRASIL. *Decreto nº 10.046*, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 30 jun. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2019. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 30 jun. 2023.

CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Resolução CD/ANPD* nº 2. Aprova o Regulamento de aplicação da Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial da República Federativa do Brasil, Brasília, DF, 28 jan. 2022, Edição 20, Seção 1.

EHRHARDT JR., Marcos e FALEIROS JR., José Luiz. Reflexões sobre os impactos da Lei Geral De Proteção De Dados Pessoais para o "Sistema S", organizações sociais e OSCIPs. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 7, n. 6, 2021.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: FRAZÃO, Ana, TEPEDINO, Gustavo e OLIVA, Milena. *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, 2018.

MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo Poder Público. *In*: MULHOLLAND, Caitlin (Coord.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago Editorial, 2020.

NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*, Goiânia, v. 5, n. 1, jan/jun 2019.

RESENDE, Tomáz de Aquino. *Roteiro do Terceiro Setor, Associações e fundações*: o que são, como instituir, administrar e prestar contas. Belo Horizonte: Prax, 2006.

ROCHA, Sílvio Luís Ferreira da. *Terceiro Setor*. São Paulo: Malheiros Editores, 2003.

TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. *In*: SCHREIBER, Anderson *et. al.* (org). *Problemas de direito civil*: homenagem aos 30 anos de cátedra do professor Gustavo Tepedino por seus orientandos e ex-orientandos. Rio de Janeiro: Editora Forense, 2021.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. *In*: MENDES, Laura Schertel *et. al* (coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Editora Forense, 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

5

Importância dos instrumentos de governança de proteção de dados pessoais para cumprimento da função social pela empresa pública

CAROLINA SCHABBACH OLIVEIRA RIBEIRO

CAROLINA SCHABBACH OLIVEIRA RIBEIRO[1]

Sumário: Introdução. 1. Aspectos gerais do regulamento jurídico aplicável às empresas públicas na Lei Geral de Proteção de Dados Pessoais (LGPD): o hibridismo jurídico. 2. Instrumentos de *compliance* e governança de proteção de dados pessoais como sistemas autorreferenciais de autorregulação regulada e seu papel de indução à função social da empresa pública 3. Contrato como instrumento de governança de proteção de dados pessoais. Considerações finais. Referências.

Introdução

As empresas públicas são atores importantes na concretização do interesse público, nesse sentido a Constituição determina que o Estado somente pode exercer a atividade econômica de forma direta quando existir "relevante interesse coletivo" ou "imperativo de segurança nacional" (art. 173 da CRFB/88). A importância e a complexidade na gestão dessa pessoa jurídica de direito privado, controlada por um ente federativo, cresceu no que Alexandre Aragão denominou de Administração Pública gerencial ou de resultados, em que o desempenho da função pública se aproxima do regime de direito privado[2].

Dessa forma, essa instituição não poderia ficar de fora das mudanças ocasionadas na era do *big data* e da "modernidade líquida"[3], em que se exige um constante estado de adaptação (fluidez) e mostra-se vital o uso massivo de dados, inclusive pessoais, para o exercício da empresa.

Sob qualquer ótica que se queira estudar o exercício de atividade econômica por parte das empresas públicas, o hibridismo característico do regime jurídico a elas aplicável desponta como um elemento de complexidade. No que se refere ao regramento atinente ao tratamento de dados pessoais, a Lei Geral de Proteção de Dados Pessoais (LGPD) e outros normativos como a Lei de Acesso à Informação (LAI) possuem dispositivos específicos para o tratamen-

1. Mestre pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Advogada do Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e pós-graduada pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) na área de Engenharia, na especialização MBA em Transformação Digital e Futuro dos Negócios. As opiniões exaradas neste artigo não representam opiniões institucionais.

2. ARAGÃO, Alexandre Santos de. *Regime jurídico das empresas estatais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/44/edicao-2/regime-juridico-das-empresas-estatais>. Acesso em 14 jul. 2023.

3. BAUMAN, Zygmunt. Modernidade Líquida. Traduzido por Plínio Dentzien. 1ª edição. Rio de Janeiro: Zahar, 2001. ASIN B008PD6V4I. Disponível em: <https://amz.onl/2Zflhhl> . Acesso em 20 jul. 2023.

to de dados pessoais pelo setor público, mas as regras não são suficientes no caso concreto.

Apesar de existirem diversos autores que elaboraram estudos relevantes sobre o tratamento de dados pessoais pelas empresas públicas, foram raros os trabalhos que buscaram trazer uma visão holística sobre a importância dos instrumentos de compliance e governança de proteção de dados pessoais na função social e alcance da finalidade pública por essas pessoas jurídicas.

Nesse artigo, busca-se demonstrar que os instrumentos de compliance e governança de proteção de dados pessoais, ao caracterizarem-se como sistemas autorreferenciais de autorregulação das pessoas jurídicas de direito privado, induzem comportamentos desejados e auxiliam na criação de uma cultura de boas práticas e por isso são fundamentais para o cumprimento da função social pelas empresas públicas, que pressupõe o atendimento das melhores práticas de responsabilidade social (art. 27 da Lei nº 13.303/2016).

Na primeira seção, serão abordados os conceitos de empresa pública e o regime jurídico aplicáveis ao tratamento de dados pessoais, para demonstrar que os conceitos e regras trazidas pela LGPD devem considerar o hibridismo jurídico das empresas estatais, de forma que se considere a finalidade no tratamento de dados e o interesse público inerente à função social da empresa pública.

Configurou-se necessário, ao longo da mencionada seção, em termos de revisão bibliográfica, aprofundar a doutrina de direito administrativo, tendo em vista a importância do conceito de empresa pública e a definição de seu regime jurídico. Adotou-se como referência a doutrina de Alexandre Aragão sobre o hibridismo jurídico que envolve as empresas públicas. Além disso, estudou-se a doutrina de proteção de dados pessoais no setor público, essenciais para extrair as funcionalidades nos instrumentos de governança à luz da legislação brasileira sobre a tutela da informação pessoal, em especial a LGPD.

Partindo da premissa de que a interpretação das regras sobre as atividades da empresa pública deve sempre considerar o hibridismo entre regulação do setor público e do privado de forma única, na segunda seção serão vistos os conceitos de boa governança e de boas práticas de compliance, de forma a averiguar quais são os instrumentos que facilitam o seu alcance e como se relacionam com o cumprimento da função social pela empresa pública. Para definir esses mecanismos de indução de comportamentos positivos, foi

utilizada doutrina especializada em proteção de dados pessoais, *compliance* digital e governança.

No tocante à terceira seção, objetivou-se comprovar, por meio da análise de cláusulas contratuais da minuta de contrato de financiamento de uma empresa pública, que esse arranjo de governança, ao funcionar como diretriz de indução de bom comportamento (sistemas autorreferenciais de autorregulação), auxiliam para que a empresa pública atenda sua função social, o que engloba a concretização do direito fundamental à proteção de dados pessoais.

Como na terceira seção, essa análise dos arranjos de governança utilizará ferramentais das teorias de abordagem de risco (*risk approach*), avaliou-se a doutrina de quem enxerga utilidade no uso dessa teoria, como Rafael Augusto Ferreira Zanatta e Claudia Quelle, e daqueles críticos a ela, como Ricardo Villas Bôas Cueva, de forma a concluir que mostra-se um importante parâmetro de implementação prática das regras de autorregulação.

A seção considerações finais, por fim, conterá as conclusões da autora, de forma a registrar o entendimento de que os instrumentos de compliance e governança de proteção de dados pessoais, ao caracterizarem-se como sistemas autorreferenciais de autorregulação das pessoas jurídicas de direito privado, induzem comportamentos desejados e auxiliam na criação de uma cultura de boas práticas em proteção de dados pessoais e por isso são fundamentais para o exercício do dever funcional das empresas públicas.

1. Aspectos gerais do regulamento jurídico aplicável às empresas públicas na LGPD: o hibridismo jurídico.

O regime jurídico aplicável às empresas públicas sempre foi objeto de controvérsias, normalmente relacionadas a sua natureza híbrida, como pessoa jurídica de direito privado e pertencente à Administração Pública, em virtude de suas funções associadas ao “relevante interesse coletivo” ou aos “imperativos de segurança nacional” (art. 173 da CRFB/1988).

No presente artigo, apoiado nas lições de Alexandre Aragão, entende-se que um regime não deve prevalecer, mas sim existir a integração em prol de uma solução única, que considere o tipo de atividade a ser exercido pela empresa pública e a finalidade específica da atividade, no caso, a finalidade do tratamento de dados pessoais. Entende-se que quanto mais o exercício da atividade pela empresa pública depender de dispêndio de recursos públicos ou

estiver associada à execução de prerrogativas estatais, mais elementos de regras associadas ao direito público serão utilizadas.

Corroborando com essa interpretação, transcreve-se trecho da doutrina de Alexandre Aragão[4]:

> Sob essa perspectiva, o mais correto em relação ao regime jurídico das empresas estatais é afirmar que não é propriamente nem de Direito Privado, nem de Direito Público,11 nem tampouco de direito privado com derrogações de direito público:12 trata-se de outro regime jurídico, híbrido e atípico, decorrente da junção de elementos de ambos,13 (...) E mais, esse diálogo de soma de elementos do direito privado e do direito público e a subsequente alteração qualitativa deles não é homogênea para todas as estatais, dependendo de uma série de fatores próprios de cada empresa estatal individualmente considerada. Ou seja, mesmo falando de um regime híbrido e atípico das empresas estatais brasileiras, esse regime sequer é uniforme para todas elas, possuindo variações bem importantes de acordo, por exemplo, com a natureza da atividade econômica exercida e com a sua maior ou menor dependência das verbas do orçamento público.

No caso do tratamento de dados pessoais pela empresa pública, nas situações em que a finalidade específica para o tratamento estiver legitimada em bases legais mais próximas da atuação exclusiva da administração pública direta, como no caso de execução de política pública, de prestação de contas aos órgãos de controle na aplicação de recursos públicos e da promoção da transparência ativa no tocante ao acesso à informação, incidirão com maior força regras para pessoas de direito público.

Vistos as bases teóricas interpretativas, passa-se a uma análise das regras gerais sobre tratamento de dados pessoais pela empresa pública. É importante mencionar que para esse artigo o foco serão as empresas públicas que prestam atividade econômica ou em uma das nomenclaturas utilizada pela LGPD, que exerçam atividades concorrenciais na forma do art. 173 da CRFB/1988 (art. 24, parágrafo único da LGPD).

4. ARAGÃO, Alexandre Santos de. *Regime jurídico das empresas estatais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/44/edicao-2/regime-juridico-das-empresas-estatais>. Acesso em 14 jul. 2023.

Adotar-se-á como referencial o Decreto Lei nº 200/1967[5] que dispõe que será empresa pública a entidade dotada de personalidade jurídica de direito privado, com patrimônio próprio e capital exclusivo de algum ente federativo. Por atividade econômica ou "atividade concorrencial" entende-se aqui a intervenção direta do estado na economia em setor econômico reservado à livre iniciativa, em virtude de necessidade ou de conveniência[6].

Como alertava Fabrício da Mota Alves, a LGPD utiliza uma nomenclatura excessivamente plural para tratar do Poder Público[7], o que torna a regulação sobre o tratamento de dados pessoais mais complexa. No tocante à empresa pública objeto do presente estudo, vale destacar o artigo 24 da LGPD.

> Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Assim, a exegese do dispositivo é que em situações associadas às atividades típicas de livre mercado, cuja realização é admitida ao particular mas que por conveniência ou necessidade a administração atua diretamente, o regime será o mesmo das pessoas de direito privado, evitando prejuízo à livre concorrência, como, por exemplo, com o uso dos dados pessoais não disponibilizados para os concorrentes.

Apesar da aparente simplicidade do artigo, mostra-se na prática insuficiente, pois, como nos lembra Fernando Menegat, o termo "políticas públicas" por ser um conceito muito aberto gera dúvidas interpretativas[8]. Ademais, as

5. Art. 5º Para os fins desta lei, considera-se: (...) II - Empresa Pública - a entidade dotada de personalidade jurídica de direito privado, com patrimônio próprio e capital exclusivo da União, criado por lei para a exploração de atividade econômica que o Governo seja levado a exercer por força de contingência ou de conveniência administrativa podendo revestir-se de qualquer das formas admitidas em direito.

6. SILVA, Américo Luís Martins da. Introdução ao direito econômico. Rio de Janeiro: Forense, 2002.

7. ALVES, Fabrício da Mota. Desafios da adequação do Poder Público à LGPD. In: PALHARES, Felipe. Temas Atuais de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

8. Lembra o autor que o legislador pretendeu não entrar na controvérsia sobre estatais que prestam serviço público ou atividade econômica, mas acabou causando outra imprecisão terminológica. Ver em: MENEGAT, Fernando. Tratamento de dados por empresas estatais no regime da LGPD: incertezas, desafios práticos e soluções possíveis. In: MARTINS, Ricardo Marcondes; POZZO, Augusto Neves Dal. LGPD & Administração Pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, RB-32.2.

estatais dependendo de seu objeto social terão que observar dois regimes distintos, o que pode ocasionar problemas práticos e uma complexidade grande no tratamento dos dados pessoais[9].

Esse é o caso do Banco Nacional de Desenvolvimento Econômico Social (BNDES), que em suas atividades exerce, por exemplo, serviços bancários típicos, como concessão de crédito por meio de financiamento, mas também executa políticas públicas, tal como a execução dos Programas Agropecuários do Governo Federal (PAGF).

Definido o regime a ser seguido, aquele conferido às pessoas de direito público ou às de direito privado, para o correto tratamento de dados pessoais serão aplicadas as regras da LGPD sem muitas diferenças. No caso do regime associado às pessoas de direito público (parágrafo único do art. 24 da LGPD), serão seguidas as regras relacionadas ao setor público, em especial o Capítulo IV da LGPD. Assim, a principal questão para o gestor de dados pessoais da empresa pública será definir se suas atividades estão associadas à execução de política pública ou não, o que na prática pode trazer alguns desafios.

2. Instrumentos de *compliance* e governança de proteção de dados pessoais como sistemas autorreferenciais de autorregulação regulada e seu papel de indução à função social da empresa pública.

A preocupação com os temas governança e compliance tem sido crescente, principalmente no âmbito da Administração Pública. Entende-se por governança corporativa os mecanismos de organização, direção, monitoramento e incentivo que envolvem o relacionamento com e entre todos aqueles relacionados à instituição (*stakeholders*). Por sua vez, boas práticas de governança, significa adotar arranjos de governança capazes de recomendar objetivamente medidas responsáveis por promover a longevidade da empresa e o bem comum[10].

9. Fernando Menegat entende que nesses casos deve existir mecanismos rígidos de barreiras de informação, recomendando a adoção das seguintes medidas: (i) criação de banco de dados segregados, específicos para cada modalidade de atuação da empresa; (ii) consolidação de mecanismos de chinese wall e semelhantes, mediante definição de operadores e encarregados (*data protection officers* – DPO) para cada banco de dados, com garantia de que cada uma das bases seja acessível apenas pelos empregados que laboram no respectivo setor da empresa; (iii) em caso de compartilhamento de dados entre diferentes setores da empresa, realização do tratamento por *clean teams* ou figuras semelhantes, coordenados pelos DPOs, de modo a evitar vazamentos ou apropriação indevida de dados (MENEGAT, 2020). Apesar de entender a preocupação com o mau uso dos dados pessoais, essas medidas muitas vezes parecem extremamente rígidas e poderiam culminar em inviabilizar o exercício da atividade econômica de forma eficiente.

10. Essa definição está em linha com o Código das Melhores Práticas de Governança Corporativa, no seguinte trecho: *"sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos*

A boa governança, no âmbito do setor público, possui o objetivo de contribuir para tomadas de decisão e para o uso mais eficiente de recursos tão caros à sociedade, os direcionando para atos que cumpram com os valores da empresa, no caso da empresa pública o objetivo para qual foi criada (função social). Por sua vez, os mecanismos de compliance são instrumentos que promovem atos de adequação à conformidade com a lei, o que engloba práticas que direcionam a empresa ao cumprimento de seus deveres legais e éticos. Nesse sentido são sistemas autorreferenciais de autorregulação regulada. Corroborando com esse entendimento, mostram-se pertinentes as lições de Ana Frazão[11]:

> Compliance diz respeito ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade. Trata-se de sistemas autorreferenciais de autorregulação regulada, capazes de fornecer as diretrizes adequadas à estrutura interna das empresas para que os ilícitos sejam prevenidos de maneira mais adequada, muitas vezes antes de projetarem seus efeitos

Destacando os instrumentos de integridade como indutores de comportamentos desejados, transcreve-se o seguinte trecho da doutrina:[12]

> Em outras palavras, o gerenciamento dos riscos ESG deixou de ser utilizado apenas para estabelecer “como não agir”, passando a direcionar a tomada de decisão sobre “onde investir” (novas tecnologias com baixas emissões de carbono, por exemplo) e “onde não investir” (empreendimentos de alto risco socioambiental). No âmbito da estrutura da companhia, isso passa a se refletir na integração ESG à tomada de decisão e na criação de estruturas inter-

entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. (...) As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum”. Ver em: IBGC. Código de Melhores Práticas de Governança Corporativa. 5ª Ed. São Paulo: IBGC, 2015. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4382648/mod_resource/content/1/Livro_Codigo_Melhores_Praticas_GC.pdf. Acesso em 20 jul 2023.

11. FRAZÃO, Ana. Direito antitruste e direito anticorrupção: pontes para um necessário diálogo. *In*: FRAZÃO, Ana (org.). Constituição, Empresa e Mercado. Brasília: FD/UnB, 2017, p. 18.

12. PEREIRA, M. S. P; GOULBERG, C. ESG na pauta corporativa e financeira: um caminho sem volta para uma economia sustentável. In: Finanças sustentáveis [livro eletrônico]: ESG, Compliance, gestão de riscos e ODS / epílogo Consuelo Yatsuda Moromizato Yoshida, Marcelo Drügg Barreto Vianna, Sandra Akemi Shimada Kishi. Belo Horizonte: Abrampa, 2021. Disponível em: <https://abrampa.org.br/abrampa /uploads/images/conteudo/Financas_sustentaveis_final.pdf#page=265>. Acesso em 15 jul 2023

> nas próprias de análise e conformidade ESG, que não se limitam a mecanismos de exclusão (*screening out*) ou de mera validação de decisões já tomadas. As estruturas de conformidade costumam estar intrinsecamente ligadas às práticas de governança corporativa da empresa. A inclusão de critérios ESG, nesse contexto, acaba por permitir que as estruturas de conformidade também sejam engajadas nos aspectos ambientais e sociais da empresa, além de governança.

Em relação ao *compliance* de proteção de dados, mostra-se um importante instrumento ao atendimento dos requisitos legais, visto que a LGPD exige a adoção de boas práticas de governança, como dispõe o artigo 50 daquela legislação. Ademais, estar em conformidade com a lei também significa que todo tratamento deve possuir uma finalidade específica, estar legitimado em uma das bases de tratamento de dados pessoais e respeitar os princípios previstos na legislação, como o da necessidade, adequação e segurança. Ademais, o uso de dados pessoais não pode ser utilizado para fins discriminatórios e antiéticos.

Estar em *compliance* com a legislação de proteção de dados pessoais ganha relevância na sociedade de informação, pois as decisões estratégicas na economia do big data passam pela análise em massa de dados, cujo dilema de imposições de limitações éticas está intimamente relacionado à proteção de dados pessoais. Explorando um pouco mais o assunto, transcrevemos a doutrina de Juliana Oliveira Nascimento[13]:

> No aspecto de governança de dados, como vimos nos tópicos supra, muito se fala no papel das organizações em relação à proteção de dados e privacidade, desde sua coleta e manuseio, de forma a garantir a legitimidade, a responsabilidade e o respeito aos princípios fundamentais da privacidade e dos direitos dos titulares de dados. Ponto fundamental do ESG em relação à LGPD será o atendimento ao pilar S – Social, e as considerações éticas no tratamento de dados pessoais, uma vez que podem ser utilizados ao prejuízo do desenvolvimento social e democrático. Notadamente, para garantir o desenvolvimento sustentável, o fluxo livre e útil de informações sem colocar em riscos à privacidade e os direitos fundamentais, teremos que em breve acrescentar ao ESG no mínimo

13. NASCIMENTO, Juliana Oliveira. ESG e Proteção de Dados. In: ESG: O Cisne Verde e o Capitalismo de Stakeholders: a tríade regenerativa do futuro global. 1ª Ed. São Paulo: Thomson Reuters. 2021. ISBN 978-5-5991-703-7. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/274075462/v1/page/RB-19.4. Acesso em 20 jul 2023, RB-19.6.

> mais 2 (dois) pilares: o T, Technology, e o P, Privacy, os quais serão relevantes para as métricas de Compliance e de sustentabilidade quanto à aderência dos princípios e direitos fundamentais dos cidadãos no que se refere ao Technology ESG e ao Privacy ESG. (...) Assim, o artigo 50 da LGPD esculpe o princípio das boas práticas e da governança, que poderão em breve serem considerados para os índices ESG nas bolsas de valores.

Assim, toda empresa que se quer manter longeva e em conformidade com as práticas ASG, deve se preocupar em adotar mecanismos de *compliance* e governança adequados à proteção de dados pessoais. Isso ganha relevância com as empresas públicas que sempre devem se pautar pelos princípios éticos em sua atuação, pois assim conseguirão cumprir a sua função social de forma integral, como preconiza o artigo 27 da Lei das Estatais, que exige que as empresas estatais devem adotar práticas de responsabilidade social.

> Art. 27. A empresa pública e a sociedade de economia mista terão a função social de realização do interesse coletivo ou de atendimento a imperativo da segurança nacional expressa no instrumento de autorização legal para a sua criação. § 1º A realização do interesse coletivo de que trata este artigo deverá ser orientada para o alcance do bem-estar econômico e para a alocação socialmente eficiente dos recursos geridos pela empresa pública e pela sociedade de economia mista, bem como para o seguinte: (...) § 2º A empresa pública e a sociedade de economia mista deverão, nos termos da lei, adotar práticas de sustentabilidade ambiental e de responsabilidade social corporativa compatíveis com o mercado em que atuam (grifos nossos).

Sobre o tema, vale destacar a Resolução nº 4.943/2021 do Conselho Monetário Nacional e do Banco Central do Brasil, que trouxe de forma mais clara a LGPD para o espectro das boas práticas de ESG para as instituições financeiras, ao inserir na estrutura de gerenciamento de risco de uma instituição, o risco social relativo ao tratamento irregular de dados pessoais, entendidos esses como "possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à violação de direitos e garantias fundamentais", como pode-se notar da leitura do artigo 38-A da resolução, abaixo transcrito.

> Art. 38-A. Para fins desta Resolução, define-se o risco social como a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à violação de direitos e garantias fundamentais ou a atos lesivos ao interesse comum. (..) § 2º São

> exemplos de eventos de RISCO SOCIAL a ocorrência ou, conforme o caso, os indícios da ocorrência de: (...) X - tratamento irregular, ilegal ou criminoso de dados pessoais, sem prejuízo do disposto no art. 32.

A autorregulação privada, portanto, mostra-se um diferencial no cumprimento da legislação de proteção de dados pessoais, caracterizando-se como importante ativo na adequação aos preceitos ASG. Também se caracteriza como indutor no atendimento à obrigação de possuir melhores práticas de responsabilidade social corporativa, o que é previsto como um dos requisitos para o atendimento da função social da empresa pública.

3. Contrato como instrumento de governança de proteção de dados pessoais.

Nessa seção serão apontados parâmetros para o alcance da boa governança e existirá a análise de um desses mecanismos, o contrato, de forma a demonstrar que estão aptos a cooperar com a concretização do direito fundamental à proteção de dados pessoais.

O melhor parâmetro para avaliar a adequação de um mecanismo de governança (autorregulação), na percepção aqui adotada, é a abordagem baseada em riscos. Tradicionalmente, o direito à proteção de dados pessoais é compreendido apenas por seu viés de direito à privacidade e dignidade humana, como liberdade fundamental do indivíduo de controlar os seus dados, o que reflete no conceito de autodeterminação informacional. Mais recentemente, somada a essa visão, surgiram estudos que utilizam uma matriz baseada em risco para analisar a proteção de dados pessoais. Essa abordagem influenciou legisladores tanto na Europa como no Brasil, como se percebe com a exigência de apresentação de Relatório de Impacto sempre que existir risco elevado ao titular de dados pessoais na LGPD.

O uso da matriz de risco não é imune a críticas, muitos entendem, como Ricardo Villas Bôas Cueva, que ao se buscar uma metrificação, pode-se proteger de forma insuficiente um direito fundamental e facilitar a captura do legislador (normatização para interesses privados). Nesse sentido, transcrevemos as lições desse doutrinador:[14]

14. CUEVA, Ricardo Villas Bôas. Segurança da informação e proteção de dados pessoais. *In*: FRANCOSKI, D. S. L.; TASSO, F. A. (Coord.). A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 546.

> O direito de proteção de dados pessoais, na Europa, pressupõe modelo baseado em direitos, isto é, em normas e procedimentos que tendem a tutelar, com a máxima eficácia possível, os direitos subjetivos dos titulares de dados pessoais. A ideia de gestão ou controle de risco ao revés, não se funda na certeza da incidência da norma protetiva de situações fáticas, mas é associada a cálculos probabilísticos de eventos futuros. O RGPD, embora tenha preservado o modelo de proteção de dados pessoais baseado em direitos, passou a contar com ferramentas de controle de risco, o que tem suscitado críticas ao que se percebe como rendição a interesses empresariais, em abordagem desviante da pureza do modelo até então vigente.

Apesar das críticas, a própria legislação confere mecanismos para mitigar a proteção insuficiente, quando exige o cumprimento de princípios como necessidade, finalidade, segurança e não discriminação.. Claudia Quelle[15], rebatendo a crítica, afirma que a sociedade torna-se inviável caso se presuma que o titular de direitos a proteção de dados pessoais possui direito de não sofrer riscos, pois toda atividade econômica pressupõe correr riscos. Entende-se importante que o legislador ou regulador imponha limites ao uso dessas ferramentas, utilizando-se quando necessário, inclusive, do princípio da precaução, para limitar modelos de negócios arriscados e prejudiciais.

De forma a esclarecer a dinâmica da abordagem baseada em risco, transcreve-se abaixo as explicações de Rafael Augusto Ferreira Zanatta[16] sobre a mudança de percepção em relação ao tema proteção de dados pessoais.

> Para Doneda, a proteção de dados pessoais transforma a concepção contemporânea de proteção da privacidade, deixando de “dar vazão somente a um imperativo de ordem individualista” – o direito de ser deixado sozinho e a não intrusão –, passando a “ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana” (DONEDA, 2006, p. 30). Bruno Bioni afirma que “historicamente, a proteção de dados pessoais tem sido compreendida como o direito do indivíduo autodeterminar as suas informações pessoais”, fazendo com que, “por meio do consentimento, o cidadão emita autorizações sobre o flu-

15. QUELLE, Claudia. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? In: Tilburg Law School Research Paper, 1-36, 2015. Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2726073_code2482176.pdf?abstractid=2726073&mirid=1. Acesso em 23 jul 2023.

16. ZANATTA, Rafael Augusto Ferreira. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. In: ANAIS REDE 2017 – I Encontro da Rede de pesquisa em Governança da Internet. São Paulo, ago. 2018. p.175-193.

xo dos seus dados pessoais, controlando-os" (BIONI, 2018, p. 18). Tanto para Doneda quanto para Bioni, a proteção de dados pessoais relaciona-se com a capacidade do cidadão de controlar suas informações, em um contexto de expansão das técnicas de uso de informações pessoais, metadados, e fracasso dos modelos de notice-and-consent.6 Essa concepção de autodeterminação informacional, muito conectada com o pensamento europeu sobre dignidade e privacidade (WHITMAN, 2004) (...) Em Privacy and Freedom, Westin teorizou a privacidade como a "capacidade de controlar o que é coletado sobre você" (WESTIN, 1967).(...) No final da década de 1980, uma importante distinção entre privacidade e proteção de dados pessoais foi feita pela Corte Constitucional alemã. O direito alemão, como notou um acadêmico na época, "mostra que a regulação da informação pessoal em computadores não pode depender da ideia jurídica de privacidade" (SCHWARTZ, 1989, p. 675). Ao invés de uma abordagem concentrada no "segredo", o direito alemão prestou "atenção aos possíveis efeitos do processamento de informações para a autonomia humana" (SCHWARTZ, 1989, p. 676). Com os debates constitucionais em torno de um polêmico censo de 1983 – boicotado e acusado de intrusivo pela sociedade – a Corte alemã determinou que "o direito à autodeterminação informativa protege o indivíduo de coletas irrestritas, armazenamento, aplicação e transmissão dos dados pessoais" (SCHWARTZ, 1989, p. 689). (...) De forma sintética e tipológica em sentido weberiano,14 a formação de modelo teórico dominante se caracteriza pelos seguintes elementos: (i) a positivação de direitos individuais relacionados ao controle dos processos de coleta e tratamento de dados pessoais, (ii) a crença na conexão entre aumento do "poder de controle" e autonomia política em sociedades democráticas, a (iii) contratualização do consentimento, garantindo-se os direitos de informação clara, finalidade específica, prevenção de riscos e segurança das informações, e (iv) o reconhecimento da vulnerabilidade dos cidadãos, com a possibilidade de autoridades independentes para aplicação desses direitos.15 É esse modelo teórico que está sendo friccionado por uma nova abordagem da proteção de dados pessoais centrada na regulação do risco.16 Trata-se menos de um processo de ruptura normativa na proteção de dados pessoais e mais como um processo de intensificação da regulação ex ante a partir de um ferramental teórico incorporado de outros campos. (...) A ideia de risquificação também é assumida por Claudia Quelle, doutoranda na Universidade de Tilburg. Em um ensaio sobre o potencial conflito entre uma abordagem baseada em risco e a teoria dos direitos fundamentais, Quelle argumenta "a proteção de dados pode ser caracterizada como regulação do risco" (QUELLE, 2015). Para Quelle, o direito da proteção de dados "foi desenvolvido para regular o

> possível dano de tecnologias da informação bem como proteger os direitos fundamentais dos indivíduos" e "acima disso, a proteção de dados pessoais também é baseada no risco: o conceito de risco, em termos de severidade e probabilidade, é utilizado para calibrar obrigações jurídicas" (QUELLE, 2015, p. 1).

Percebe-se que a abordagem baseada em riscos serve para calibrar a obrigação de um contrato, por exemplo, de forma a usar mecanismos mais adequados ao risco ou, ainda, estabelecer diretrizes para a política de governança. Considerando essas reflexões, passa-se a análise concreta, estudo de cláusulas de minuta de contrato de financiamento do BNDES[17].

O contrato em sua perspectiva funcional preceptiva ou normativa, configura-se um dos instrumentos de autorregulação privada, por meio do qual as partes regulam seus interesses e o comportamento que desejam, também permite o controle ou supervisão proporcional ao risco.

Com intuito de esclarecer o nosso ponto de vista, destaca-se a doutrina de Gustavo Tepedino, Carlos Nelson Konder e Paula Greco[18]:

> Na experiência brasileira, ao contrário de outros ordenamentos, as codificações não definiram o contrato, o que, em certa medida, favorece a evolução conceitual a partir de constante releitura e reinterpretação histórica do conceito pela doutrina, adaptando-o aos valores fundantes do ordenamento. Nesse processo evolutivo, fala-se da passagem da visão subjetiva do contrato, concebido como acordo de vontades, para a visão objetiva, tomando-se o contrato como norma de comportamento. (...) Ao dar prioridade à perspectiva funcional do contrato (" para que serve") sobre sua análise estrutural (" como é"), sobressai na concepção desse instituto sua função preceptiva ou normativa: o contrato como instrumento de autorregulação de interesses. (...) A definição de contrato, tal como outras categorias jurídicas (próprias do contato social, como os negócios unilaterais e os atos jurídicos stricto sensu), destina-se à função normativa: determinar a quais suportes fáticos se aplica a disciplina legal prevista para a relação contratual, assim como excluir de seu âmbito de incidência os demais fenômenos, aos quais as normas em questão somente poderiam ser aplicáveis por interpretação analógica ou extensiva, devidamente fundamentada.

17. Cabe destacar que a análise neste trabalho não representa a opinião institucional do BNDES.

18. TEPEDINO, G.; KONDER, C. N.; GRECO, P. Fundamentos do Direito Civil: Contratos - Vol. 3. ISBN 978-85-309-9241-5. 2ª Ed. Rio de Janeiro: Editora Forense Ltda, 2021. Disponível em: https://amz.onl/59PoVIW. Acesso em 20 jul 2023.

> Busca-se delimitar o que é contrato para identificar sobre quais situações devem incidir as normas de direito contratual. Igualmente, a definição de contrato também serve, a contrario sensu, para determinar o que não pode ser compreendido como contrato e, dessa forma, indicar as situações que restam excluídas, a princípio, da incidência dessas normas.

Assim, por meio da inclusão das cláusulas contratuais em seus negócios jurídicos, a empresa pública pode estimular os comportamentos que estão em conformidade com a LGPD e alinhados a sua governança corporativa, bem como alocar responsabilidades de cada parte. Ademais, pode ressaltar comportamentos de obediência às exigências legais, caso de cláusulas que reforcem a transparência com o titular dos dados pessoais, especificando como podem exercer seus direitos, quais são os dados tratados e as finalidades, por exemplo.

No caso da relação jurídica do BNDES, para celebração de um contrato de financiamento, esta instituição caracteriza-se, ao tomar as principais decisões sobre o tratamento de dados pessoais, como Controlador. Ademais, ao longo da vigência da relação contratual não são coletados dados sensíveis ou de crianças e adolescentes. Além disso, não foi encontrado caso de decisões totalmente automatizadas para a concessão do crédito. Dessa forma, optou-se pela adoção de cláusulas contratuais mais genéricas e em regra mais brandas.

Por tratar-se de empresa pública, na política de governança de dados do BNDES está expresso que deve-se compatibilizar a proteção de dados pessoais com as obrigações de transparência e prestações de contas da LAI e da Política de Dados Abertos. Tal medida mostra-se necessária em razão do regime jurídico híbrido, que obriga a adoção de regras associadas ao setor público. Em razão disso, foi incluído no contrato que as Partes autorizam a divulgação de algum de seus dados para atendimento do princípio da transparência ativa (nome, CPF e cargo). Tal autorização é apenas para controle de ciência do cliente, visto que a base legal em regra para o tratamento é a obrigação legal.

Ademais, como forma de atender às obrigações de transparência com o titular de dados pessoais, são mencionadas algumas pessoas que o BNDES pode compartilhar os dados pessoais coletados com terceiros, não muito usuais no caso de agente de tratamento ser pessoa jurídica de direito privado, mais uma especificidade em razão da natureza jurídica de empresa pública.

De forma a ilustrar a inserção dessas obrigações, abaixo transcreve-se duas cláusulas da minuta de contrato de financiamento.

ACESSO E PROTEÇÃO DE DADOS PESSOAIS

As PARTES, em observância ao disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), na legislação vigente sobre proteção de dados pessoais e em eventuais determinações de órgãos/entidades reguladores, obrigam-se a proteger os direitos relativos ao tratamento de dados pessoais, devendo, para tanto, adotar medidas de boa governança sob o aspecto técnico, inclusive de segurança, jurídico e administrativo, observando principalmente o seguinte: I. os dados pessoais tratados em decorrência do presente contrato deverão ser precisos e atualizados. Os tratamentos devem observar os parâmetros previstos na legislação, especialmente na LGPD, bem como devem estar em conformidade com as finalidades expressas nesse CONTRATO, ressalvada, esta última exigência, nas hipóteses em que as PARTES forem consideradas controladoras independentes; II. cada uma das PARTES será controladora independente, para fins desse CONTRATO, cabendo definir individualmente as bases legais apropriadas e diretrizes para as operações de tratamento, em relação aos seguintes dados pessoais: (i) que vierem a coletar diretamente junto aos respectivos titulares, desde que essa operação de tratamento se dê com base em suas próprias decisões; (ii) oriundos de suas próprias bases de dados; e (iii) relativos ao seu corpo de colaboradores, funcionários e/ou prepostos envolvidos para a regular execução deste CONTRATO.; III. o s dados pessoais recebidos da outra PARTE em razão deste Contrato devem ser eliminados ao término de seu tratamento, salvo quando a Lei permitir a manutenção de tais dados após esse evento.

PARÁGRAFO PRIMEIRO: As PARTES autorizam a divulgação dos dados pessoais expressamente contidos neste Contrato, tais como nome, CPF, cargo dos representantes legais que subscreveram esse instrumento e daqueles mencionados como responsáveis pelo recebimento de
eventuais notificações, para fins de publicidade das operações de crédito em seu site institucional, comprometendo-se a informar a respeito da utilização desses dados pessoais, quando for o caso, aos seus respectivos titulares, bem como se comprometem a coletar o consentimento, quando necessário, conforme previsto na LGPD.

PARÁGRAFO SEGUNDO: O Incidente de Segurança, bem como o acesso indevido não autorizado e o vazamento ou perda de dados pessoais, serão de inteira responsabilidade da PARTE que a ele der causa, não cabendo solidariedade ou subsidiariedade caso a outra PARTE não tenha realizado o tratamento de dados pessoais objeto do incidente e não tenha violado a legislação de proteção de dados pessoais.

DO TRATAMENTO DE DADOS PESSOAIS PELO BNDES

O BNDES, sempre que se caracterizar como controlador dos dados pessoais, em conformidade com a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e com a Política Corporativa de Segurança da Informação do Sistema BNDES (PCSI), somente poderá tratar os dados pessoais compartilhados com fundamento nas hipóteses previstas na LGPD (base legal), seguindo os princípios previstos nessa legislação, em especial o da adequação, segurança, prevenção e minimização.

PARÁGRAFO PRIMEIRO: O tratamento dos dados pessoais, inclusive dos administradores, sócios, prestadores de garantias pessoas físicas, poderá ocorrer nas hipóteses evidenciadas nos Termos de Uso e Aviso de Privacidade do Portal do Cliente. Entre as finalidades previstas destacamos as seguintes: a) execução das obrigações contratuais (ex: dados dos colaboradores da empresa para possibilitar a realização de notificações, dados de contatos de representantes legais, administradores ou contatos comerciais para possibilitar o envio de cobrança e a liberação de recursos financeiros), b) para o cumprimento de obrigação legal ou regulatória (ex: dados dos sócios, administradores e prestadores de garantia para realizar as diligências necessárias para o cumprimento das normas relativas a prevenção à lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa); c) para a proteção do crédito concedido (ex: dados dos sócios e prestadores de garantia para realizar consultas e compartilhamento com instituições que prestam os serviços atinentes à análise de crédito, incluindo o Sistema de Informações de Crédito - SCR); e d) para a melhoria e otimização da experiência do cliente (ex: dados de contato de colaboradores da empresa para envio de ofertas de produtos similares ao contratado).

PARÁGRAFO SEGUNDO: Os dados pessoais tratados, inclusive os relacionados a operações de financiamento/empréstimo ou outra forma de apoio financeiro, poderão ser compartilhados com as pessoas elencadas nos Termos de Uso e Aviso de Privacidade do Portal do Cliente, as quais destacamos as seguintes: a) organismos internacionais, com os quais o BNDES capta recursos, tais como o Banco Interamericano de Desenvolvimento (BID) e o Banco Mundial, para a finalidade de demonstrar a correta aplicação dos recursos, observado o disposto na LGPD acerca do tema; b) com entidades e órgãos de controle, tais como Banco Central do Brasil, Tribunal de Contas da União, Controladoria Geral da União, Ministério Público Federal e Polícia Federal, sempre que solicitados por estas entidades; e c) com entidades e
órgãos integrantes da Administração Pública Direta e Indireta (tais como Ministérios, autarquias e empresas públicas), para fins de prestação de contas e execução/formulação de políticas públicas, para o cumprimento de outras obrigações legais ou regulatórias ou, ainda, de acordo com as demais bases legais previstas na LGPD.

> **PARÁGRAFO TERCEIRO**: Os titulares de dados pessoais tratados poderão tirar dúvidas relacionadas à legislação sobre proteção de dados pessoais por meio de e-mail a ser enviado a seguinte caixa de e-mail: dpo_encarregado@bndes.gov.br, e exercer os direitos abaixo mencionados por meio do Canal Fala.BR - Plataforma Integrada de Ouvidoria e Acesso à Informação, disponível em XXXXX, conforme informado nos Termos de Uso e Aviso de Privacidade: a) acesso a dados; b) confirmação da existência de tratamento; c) correção de dados incompletos, incorretos ou desatualizados; d) revogação do consentimento, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado; e) ser informado sobre as entidades públicas e privadas com as quais o BNDES realizou eventual uso compartilhado de dados; e f) pedido de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD)

Dos exemplos acima, nota-se que o instrumento de governança reflete as peculiaridades da natureza jurídica da empresa pública, quando por exemplo confere ciência sobre a possibilidade de divulgação dos dados pessoais por meio de transparência ativa ou confere ciência ao cliente que seus dados pessoais podem ser compartilhados com órgãos de controle. Tem também a função de induzir comportamentos positivos, como a adequada comunicação ao titular de dados pessoais sobre a finalidade do tratamento e os agentes de compartilhamento, o que é uma das condições para garantia à autodeterminação informativa por parte do titular de dados pessoais. Nesse sentido, facilita o cumprimento da obrigação de adoção de boas práticas de responsabilidade social (elemento necessário ao cumprimento da função social).

Considerações finais

Na sociedade da informação e líquida, mostra-se cada vez mais relevante o tratamento de dados pessoais de forma adequada e ética, isso porque as bases de dados pessoais integram hoje o conceito de estabelecimento e, portanto, as regras atinentes ao tratamento de dados pessoais afetam de forma direta o modelo de negócio.

Também cresce, como demonstrado ao longo deste artigo, em virtude de demandas de investidores e da própria sociedade, a cobrança pela adoção do exercício da sociedade empresária de forma sustentável. A sustentabilidade, inclusive em parâmetros estabelecidos em diversas bolsas de valores, é medida pelo atendimento de obrigações e critérios relativos aos aspectos ambientais, sociais e de governança. Nesse sentido, a proteção de dados pessoais,

tendo em vista o valor da exploração econômica dessa informação pessoal, caracteriza-se como importante instrumento ao exercício de diversos direitos fundamentais.

Para a empresa pública que exerce a atividade econômica, o uso adequado e ético dos dados pessoais mostra-se além de um comportamento desejável, uma exigência legal, por tratar-se de imperativo necessário para o cumprimento da sua função social, por relacionar-se diretamente à adoção de boas práticas de responsabilidade social.

Contudo, diante da natureza jurídica peculiar da empresa pública, cujo regime jurídico configura-se híbrido, por estar associado a elementos de direito público e privado, a interpretação das regras sobre o tratamento de dados pessoais, inclusive àquelas expressas na LGPD, por vezes mostra-se uma tarefa árdua. Contribuem, como explicado anteriormente, a ausência de uniformidade de nomenclatura para abordar o termo Poder Público e de regulação de alguns pontos pela Agência Nacional de Proteção de Dados (ANPD), além da conceituação vaga de alguns termos como as expressões “atividades concorrenciais” e “políticas públicas”.

Para interpretar a legislação e completar as lacunas, a autorregulação mostra-se extremamente importante para o alcance do interesse público e da função social da empresa pública. Conforme disposto no art. 170 da CRFB/1988, o objetivo da ordem jurídica não se esgota no atendimento da função econômica. Como nos lembra Gregory Mankiw, existem dois motivos genéricos para que um governo intervenha na economia - promover a eficiência e promover a igualdade, ou seja: “a maioria das políticas visa aumentar o bolo econômico e mudar a forma como ele é dividido”[19].

O grande desafio é conferir oportunidade para que os diferentes agentes econômicos tomem decisões maximizadoras do bem-estar social, atuem nos locais em que a mão invisível, na visão de Adam Smith[20] não é capaz de atuar. Nesse sentido, como lembra Amartya Sen,[21] para a promoção do desenvolvimento é necessário prestar atenção simultaneamente na eficiência e na equidade. Isso claramente impacta na regulação, pois é por meio desse instrumento, segundo o estabelecido na própria Constituição (art. 174 da

19. MANKIW, Gregory. Introdução à Economia. São Paulo: Cengage Learning, 2014, p. 11.

20. SMITH, Adam. A Riqueza das Nações: investigação sobre sua e suas causas. São Paulo: Editora Nova Cultural Ltda, 1996.

21. SEN, Amartya. Desenvolvimento como liberdade. Tradução de Laura Teixeira Motta. São Paulo: Companhia das Letras, 2010.

CRFB), que o Estado deve atuar na economia.

Em virtude disso, o Direito, por meio de regras contratuais ou legais, deve ser estrutural e não meramente compensatório, na visão trazida por Calixto Salomão Filho[22]. Para o referido autor, qualquer solução jurídica precisa ter o interesse e o instrumental de intervir nas estruturas econômicas de forma reorganizadora.

Assim, os instrumentos de governança de proteção de dados pessoais, como o contrato, em razão de causarem impacto no modelos de negócio e na atividade empresarial, são verdadeiras ferramentas de gerenciamento de riscos e de promoção de padrões de integridade e, por isso, são instrumentos para o desenvolvimento de forma equitativa. Por isso, são fundamentais para o exercício pleno da função social pela empresa pública.

22. SALOMÃO FILHO, Calixto. Regulação e Desenvolvimento: Novos Temas. São Paulo: Malheiros. 2012.

Referências

ALVES, Fabrício da Mota. Desafios da adequação do Poder Público à LGPD. In: PALHARES, Felipe. *Temas Atuais de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2020.

ARAGÃO, Alexandre Santos de. *Regime jurídico das empresas estatais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Administrativo e Constitucional. Vidal Serrano Nunes Jr., Maurício Zockun, Carolina Zancaner Zockun, André Luiz Freire (coord. de tomo). 2. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/44/edicao-2/regime-juridico-das-empresas-estatais>. Acesso em 14 jul. 2023.

BAUMAN, Zygmunt. *Modernidade Líquida*. Traduzido por Plínio Dentzien. 1ª edição. Rio de Janeiro: Zahar, 2001. ASIN B008PD6V4I. Disponível em: <https://amz.onl/2Zflhhl> . Acesso em 20 jul. 2023.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: Acesso em: 12 mar. 2023.

BRASIL. Banco Central. Conselho Monetário Nacional. Resolução 4.943, de 15 de setembro de 2021. *Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações*. Brasília, DF: 16 set 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo =Resolu%C3%A7%C3%A3o%20CMN&numero=4943>. Acesso em 6 jul. 2023.

BRASIL. Presidência da República. Decreto-lei 200, de 25 de fevereiro de 1967. *Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências*. Brasília, DF: 27 fev 1967. Disponível em <https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm>. Acesso em 6 jul. 2023.

BRASIL. Presidência da República. Lei 13.303, de 30 de junho de 2016. *Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios*. Brasília, DF: 1º jul. 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm>. Acesso em: 4 jul. 2023.

BRASIL. Presidência da República. Lei 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: 18 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 4 jul. 2023.

CUEVA, Ricardo Villas Bôas. Segurança da informação e proteção de dados pessoais. *In*: FRANCOSKI, D. S. L.; TASSO, F. A. (Coord.). *A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado*. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 539-550.

FRAZÃO, Ana. Direito antitruste e direito anticorrupção: pontes para um necessário diálogo. In: FRAZÃO, Ana (org.). *Constituição, Empresa e Mercado*. Brasília: FD/UnB, 2017.

GARTNER Information Technology. Gartner Glossary. Big Data. Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data. Acesso 04 jul 2023.

IBGC. Código de Melhores Práticas de Governança Corporativa. 5ª Ed. São Paulo: IBGC, 2015. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4382648/mod_resource/content/1/Livro_Codigo_Melhores_Praticas_GC.pdf. Acesso em 20 jul 2023.

MANKIW, Gregory. *Introdução à Economia*. São Paulo: Cengage Learning, 2014.

MENEGAT, Fernando. Tratamento de dados por empresas estatais no regime da LGPD: incertezas, desafios práticos e soluções possíveis. In: MARTINS, Ricardo Marcondes; POZZO, Au-

gusto Neves Dal. *LGPD & Administração Pública: uma análise ampla dos impactos*. São Paulo: Thomson Reuters Brasil, 2020.

NASCIMENTO, Juliana Oliveira. ESG e Proteção de Dados. *In: ESG: O Cisne Verde e o Capitalismo de Stakeholders: a tríade regenerativa do futuro global*. 1ª Ed. São Paulo: Thomson Reuters. 2021. ISBN 978-5-5991-703-7. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/274075462/v1/page/RB-19.4. Acesso em 20 jul 2023.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance digital e LGPD*. Coleção Compliance. v. 5. São Paulo: Thomson Reuters Brasil, 2021.

PEREIRA, M. S. P; GOULBERG, C. ESG na pauta corporativa e financeira: um caminho sem volta para uma economia sustentável. *In: Finanças sustentáveis* [livro eletrônico]: ESG, Compliance, gestão de riscos e ODS / epílogo Consuelo Yatsuda Moromizato Yoshida, Marcelo Drügg Barreto Vianna, Sandra Akemi Shimada Kishi. Belo Horizonte: Abrampa, 2021. Disponível em: <https://abrampa.org.br/abrampa/uploads/images/conteudo/Financas_sustentaveis_final.pdf#page=265>. Acesso em 15 jul 2023

QUELLE, Claudia. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? *In: Tilburg Law School Research Paper*, 1-36, 2015. Disponível em https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2726073_code2482176.pdf?abstractid=2726073&mirid=1. Acesso em 23 jul 2023.

SALOMÃO FILHO, Calixto. *Regulação e Desenvolvimento: Novos Temas*. São Paulo: Malheiros. 2012.

SEN, Amartya. Desenvolvimento como liberdade. Tradução de Laura Teixeira Motta. São Paulo: Companhia das Letras, 2010.

SMITH, Adam. *A Riqueza das Nações: investigação sobre sua e suas causas*. São Paulo: Editora Nova Cultural Ltda, 1996.

SILVA, Américo Luís Martins da. *Introdução ao direito econômico*. Rio de Janeiro: Forense, 2002.

TEPEDINO, G.; KONDER, C. N.; GRECO, P. Fundamentos do Direito Civil: Contratos - Vol. 3. ISBN 978-85-309-9241-5. 2ª Ed. Rio de Janeiro: Editora Forense Ltda, 2021. Disponível em: https://amz.onl/59PoVIW. Acesso em 20 jul 2023.

ZANATTA, Rafael Augusto Ferreira. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. *In: ANAIS REDE 2017 – I Encontro da Rede de pesquisa em Governança da Internet*. São Paulo, ago. 2018. p.175-193.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

6

Compatibilização entre a LAI e a LGPD: adequação dos contratos administrativos publicados pelas empresas estatais em seus portais de transparência

ANDREA PAULA PONTES DOS SANTOS

ANDREA PAULA PONTES DOS SANTOS[1]

Sumário: Introdução. 1. Compatibilização entre o dever de transparência, o direito à privacidade e à proteção de dados pessoais. 2. Fundamentos para a publicação dos contratos administrativos e documentos referentes às licitações realizadas pelas estatais. 3. Requisitos para que o tratamento de dados pessoais seja legítimo, conforme as disposições da LGPD. 4. Análise de decisões e guias orientativos sobre o tema. 5. Adequação à LGPD dos contratos administrativos publicados na internet pelas estatais. Considerações finais. Referências.

Introdução

As empresas públicas e as sociedades de economia mista[2], integrantes da Administração Pública indireta, são dotadas de personalidade jurídica de direito privado, conforme arts. 2º, 3º e 4º da Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais)[3]. Possuem, no entanto, um regime jurídico híbrido, sofrendo influência de normas de direito público e privado. Segundo Alexandre Aragão, esse diálogo entre o público e o privado não é homogêneo para todas as estatais, variando a depender de suas características, como, por exemplo, a natureza da atividade exercida e sua maior ou menor dependência do orçamento público[4].

Quanto à incidência do direito público, o art. 37 da Constituição Federal - CRFB estabelece a aplicação dos princípios administrativos a toda Administração Pública direta e indireta, sem distinção, incluindo-se, portanto, as empresas estatais. Dentre esses princípios, destaca-se no presente estudo o da publicidade, o qual foi contemplado em diversos aspectos na Lei das Estatais. Nessa linha, ressalta-se, ainda, a aplicação de forma expressa às estatais da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI).

1. Mestre em Direito e Políticas Públicas pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO), Pós Graduanda em Direito Digital pela Instituto de Tecnologia e Sociedade (ITS) e Universidade do Estado do Rio de Janeiro (UERJ)

2. O presente estudo se limitará à análise das empresas públicas e as sociedades de economia mista no âmbito federal, tendo em vista a impossibilidade de exame de todas as normas e pronunciamentos de órgãos de controle estaduais e municipais sobre o tema objeto desta pesquisa. As empresas públicas e as sociedades de economia mista são também denominadas de "empresas estatais", conforme art. 2º, I, do Decreto nº 8.945, de 27 de dezembro de 2016, que regulamenta no âmbito federal a Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais).

3. Explica Alexandre Aragão que as estatais foram pensadas para serem instrumentos mais ágeis de ação do Estado, a partir da premissa de que as pessoas jurídicas de direito público estavam submetidas a amarras e controles que obstavam uma atuação eficiente, em especial no âmbito econômico em que as dinâmicas de mercado impõem uma atuação mais célere e flexível. ARAGÃO, Alexandre Santos de. Regime jurídico das empresas estatais. *In: Enciclopédia jurídica da PUC SP*, tomo II (recurso eletrônico): direito administrativo e constitucional / coord. Vidal Serrano Nunes Jr. [*et al.*] - São Paulo: Pontifícia Universidade Católica de São Paulo, 2017

4. ARAGÃO, *op. cit*.

Especificamente quanto à licitação e contratos administrativos, as estatais possuem o dever de publicar informações para permitir o respectivo controle social, conforme disposto no art. 39 da Lei das Estatais, art. 8º da LAI, art. 7º do Decreto 7.724/2012 e arts. 10 e 11 da Portaria Interministerial nº 140/2006.

Em atenção à mencionada legislação, bem como determinações do Tribunal de Contas da União - TCU e Secretaria de Coordenação das Estatais - SEST, as empresas estatais passaram a divulgar em seus sítios eletrônicos diversos documentos relacionados aos procedimentos licitatórios e contratos administrativos, os quais contém dados pessoais.

Com o advento da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) e a inclusão do direito à proteção dos dados pessoais no inciso LXXIX, da CRFB[5], surge o questionamento a respeito da disponibilização dessas informações ao público em geral, inclusive em relação à adequação do legado de documentos publicados nos respectivos Portais da Transparência[6]. A partir da análise da legislação, dos Guias orientativos disponíveis sobre o tema, bem como de decisões proferidas pelos órgãos de controle, busca-se apontar algumas medidas possíveis para adequação desse acervo, visando compatibilizar o direito à intimidade e proteção de dados pessoais com o princípio da publicidade e transparência.

1. Compatibilização entre o dever de transparência, o direito à privacidade e à proteção de dados pessoais

A Constituição Federal de 1988 – CRFB dispõe em seus arts. 5º, XXXII, e 37, § 3º, II, sobre o direito fundamental de acesso à informação de interesse particular, de interesse coletivo ou geral. Em consonância com os aludidos dispositivos constitucionais, foi publicada, em 18 de novembro de 2011, a LAI, a qual tem por objetivo garantir o direito de acesso dos cidadãos às informações públicas. No âmbito do Poder Executivo federal, a LAI é regulamentada pelo

5. Incluído pela Emenda Constitucional nº 115, de 2022.

6. Em relação à aplicação da LGPD às empresas estatais, prevê o artigo 24 da Lei que quando estiverem atuando em regime de concorrência, sujeitas ao art. 173 da CRFB, terão o mesmo tratamento conferido às pessoas jurídicas de direito privado particulares. Já quando estiverem operacionalizando e executando políticas públicas terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, conforme Capítulo IV. André Carvalho e Elizabeth Bannwart fazem uma análise crítica desse dispositivo. Segundo os autores, "persiste a dificuldade em se estabelecer a distinção proposta pela lei, tendo em vista que, no limite, todas as empresas estatais baseiam-se em políticas públicas". CARVALHO, André Castro; BANNWART, Elizabeth. Marques. *A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD)*: adequando-as aos programas de governança em privacidade das empresas estatais. *In:* CARVALHOSA, Modesto; KUYVEN, Fernando. (Org.). Compliance no direito empresarial. 1ed. São Paulo: Thomson Reuters Brasil, 2020, v. 4, p. 239-253.

Decreto nº 7.724 de 16 de maio de 2012[7]. Dentre as diretrizes previstas na LAI, destaca-se a observância da publicidade como preceito geral e do sigilo como exceção, bem como o dever de divulgar informações de interesse público, independentemente de solicitações, conforme incisos I e II do art. 3º.

Já com relação à proteção de dados pessoais, o Supremo Tribunal Federal – STF, em maio de 2020, no julgamento das Ações Diretas de Inconstitucionalidade - ADIs nº 6.387[8], 6.388, 6.389, 6.390 e 6.393, que impugnaram a constitucionalidade da Medida Provisória nº 954, de 17 de abril de 2020[9], entendeu que a proteção de dados pessoais e a autodeterminação informativa constituem direitos fundamentais autônomos[10].

Posteriormente, em setembro de 2020, entrou em vigor a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), a qual, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais. Em 10 de fevereiro de 2022, foi publicada a Emenda Constitucional nº 115, por meio da qual a proteção de dados pessoais foi incluída entre os direitos e garantias fundamentais (art. 5º, LXXIX, da CRFB).

A LAI e a LGPD, como visto, asseguram direitos fundamentais distintos e podem parecer, em um primeiro momento, antagônicas entre si, porém, a partir da análise dos dispositivos das aludidas Leis, é possível inferir que ambas dialogam entre si[11].

Nesse diapasão, a LAI também resguarda a proteção à informação sigilosa, bem como à informação pessoal, conforme previsto em seu art. 6º. Ade-

7. As empresas estatais também devem observar as disposições da LAI, conforme expressamente dispõe o art. 2º, II.

8. Conforme explicado no voto da Ministra relatora Rosa Weber, a ADI nº 6387 proposta pelo Conselho Federal da Ordem dos Advogados do Brasil - OAB, é a mais abrangente, contendo o objeto das demais. Na mencionada ADI são alegados vícios de inconstitucionalidade formal, atinentes ao não atendimento dos requisitos da relevância e urgência previstos no art. 62 da CRFB, para a edição de medida provisória, e de inconstitucionalidade material, relativos à violação das regras constitucionais da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa, constante dos arts. 1º, inciso III, e 5º, incisos X e XII da CRFB.

9. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

10. Bruno Bioni destaca que "trata-se de decisão de suma importância que reconhece o caráter autônomo do direito à proteção de dados pessoais, enquadrando-o como um novo direito fundamental. Até então, a Suprema Corte vinha decidindo casos sobre proteção de dados pessoais baseando-se na lógica do direito à privacidade. (...) Tal lógica tem uma consequência importante: significa dizer que a Constituição Federal não protege apenas os dados sigilosos (...) mas todo dado que tenha por característica ser um atributo da personalidade humana". BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

11. André Carvalho e Elizabeth Bannwart ao comparar o texto da LGPD e da LAI apontam aspectos de convergência, porém destacam pontos de atenção na conjugação das leis. CARVALHO, André Castro; BANNWART, Elizabeth. *op. cit*.

mais, dispõe de uma Seção específica para tratar da proteção às informações pessoais, assim como o seu Decreto regulamentador possui um capítulo sobre o tema[12].

Da mesma forma, a LGPD prevê a liberdade de informação como um de seus princípios norteadores, conforme art. 2º, III. Além disso, ressalva que o tratamento de dados pessoais cujo acesso é público deve levar em consideração a finalidade, a boa-fé e o interesse público que justificaram sua divulgação, art. 7º, § 3º. Em seu art. 23, constante do Capítulo IV "Do Tratamento de Dados Pessoais pelo Poder Público", é mencionada expressamente a LAI.

A respeito da compatibilização entre a LAI e a LGPD, a Controladoria-Geral da União – CGU[13] editou o Enunciado nº 4, de 10 de março de 2022,[14] e o Conselho da Justiça Federal (CJF), na IX Jornada de Direito Civil, realizada em maio de 2022, aprovou o Enunciado nº 688.[15]

No entanto, conforme destacado pela Autoridade Nacional de Proteção de Dados Pessoais – ANPD,[16] o processo de adequação à LGPD, no setor público, tem gerado dúvidas sobre os parâmetros a serem adotados para a disponibilização pública de informações pessoais, cabendo ao intérprete compatibilizar de forma harmônica e sistemática o direito à privacidade e à proteção de dados pessoais com o direito à obtenção de informações sobre as atividades do Poder Público pelos cidadãos.

12. Nos termos do art. 31 da mencionada Lei e do art. 55 do citado Decreto, as informações pessoais relativas à intimidade, vida privada, honra e imagem serão de acesso restrito aos agentes públicos legalmente autorizados e à pessoa a que elas se referirem, e sua divulgação ou acesso por terceiros somente será autorizada se houver previsão legal ou consentimento expresso do seu titular.

13. De acordo com os arts. 23 e 24 do Decreto nº 7.724, de 16 de maio de 2012, compete à Controladoria-Geral da União e à Comissão Mista de Reavaliação de Informações, no âmbito da administração pública federal, apreciar sobre recursos interpostos em casos de negativa de acesso à informação determinada por órgão ou entidade pública federal, com fundamento na LAI.

14. "Nos pedidos de acesso à informação e respectivo recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), vez que: A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos". Disponível em: https://repositorio.cgu.gov.br/bitstream/1/67735/3/Enunciado_4_2022.pdf

15. "A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelecem sistemas compatíveis de gestão e proteção de dados. A LGPD não afasta a publicidade e o acesso à informação nos termos da LAI, amparando-se nas bases legais do art. 7º, II ou III, e art. 11, II, a ou b, da Lei Geral de Proteção de Dados". Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf

16. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Tratamento de dados pessoais pelo poder público*. versão 2.0, Brasília, DF, jun. 2023 Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf Acesso em 15 jul. 2023

2.Fundamentos para a publicação dos contratos administrativos e documentos referentes às licitações realizadas pelas estatais

Especificamente em relação a informações sobre licitações e contratos,[17] estas devem ser fornecidas independentemente de requerimentos através da divulgação nos sítios oficiais das estatais na rede mundial de computadores (internet), conforme art. 8º da LAI, art. 7º do Decreto 7.724/2012, art. 39 da Lei das Estatais e arts. 10 e 11 da Portaria Interministerial nº 140, de 16 de março de 2006

O Tribunal de Contas da União – TCU, conforme Acórdão nº 1832/2018, expediu determinação para que as organizações fiscalizadas, dentre elas, 62 (sessenta e duas) empresas estatais, adotassem providências para publicar em suas páginas de transparência as informações exigidas pela legislação, inclusive, as relativas a licitações e contratos. Cabe ressaltar que dentre os aspectos avaliados pelo TCU, destaca-se a verificação da publicação de contratos na íntegra pelas fiscalizadas em seus portais[18].

Cumpre mencionar, ainda, que a Secretaria de Coordenação e Governança das Empresas Estatais - SEST elaborou o guia[19] com o propósito de orientar as empresas estatais federais na implementação de páginas de transparência em seus portais da internet, abordando inclusive o dever de divulgação de documentos e informações, contendo, no mínimo, o disposto no art. 8º, §1º, da LAI.

Em atenção a legislação mencionada acima, bem como determinações do TCU e SEST, as empresas estatais passaram a divulgar em seus sítios eletrônicos diversos documentos relacionados aos procedimentos licitatórios (instru-

17. A mencionada Portaria disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da internet, entre outras providências. Em seu art. 10 elenca as informações referentes às licitações que devem ser publicadas nos portais da transparência, tais como, objeto, modalidade, situação, número da licitação e número do processo. Em seu art. 11 estão previstas as informações relativas aos contratos firmados e notas de empenho que devem ser disponibilizadas no mesmo canal, dentre elas número do contrato, o número do processo, a modalidade, o nome do contratado, o objeto, a vigência, o valor, a situação e os aditivos.

18. BRASIL. Tribunal de Contas da União Disponível. *Acórdão nº 1832/2018 – TCU – Plenário*. 08 ago. 2018. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A1832%2520ANOACORDAO%253A2018%2520COLEGIADO%253A%2522Plen%25C3%25A1rio%2522/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/sinonimos%253Dfalse Acesso em 01 jun. 2023.

19. _____ Ministério da Economia, Secretaria Especial de Desestatização, Desinvestimento e Mercados, Secretaria de Coordenação e Governança das Empresas Estatais / Secretaria de Coordenação e Governança das Empresas Estatais. Guia de padronização de informações das empresas estatais federais nos portais da internet. 3ª ed. dez. 2022 – elaborado e revisado conforme recomendações dos Acórdãos nº1832/2018-TCU-Plenário, 2647/2020-TCU-Plenário e 2726/2021-TCU-Plenário. Brasília: Sest/ME, 2022. Brasília-DF. Disponível em: https://www.gov.br/economia/pt-br/assuntos/empresas-estatais-federais/central-de-conteudo/guias-e-manuais/guia_padronizacao_informacoes_portais_internet_edicao_3_versao_9.pdf Acesso 10 jul. 2023.

mento contratual, proposta de preços, declarações, termos de confidencialidade, entre outros), os quais contêm dados pessoais, como nome, número de inscrição no CPF, endereço, e-mail, telefone, assinaturas físicas e rubricas dos representantes legais das estatais e das empresas contratadas.

Com o advento da LGPD e a inclusão do direito à proteção dos dados pessoais no inciso LXXIX, da CRFB[20], surge o questionamento a respeito da disponibilização dessas informações ao público em geral, inclusive em relação à adequação do legado de contratos administrativos publicados nos portais, conforme será desenvolvido a seguir.

3. Requisitos para que o tratamento de dados pessoais seja legítimo, conforme as disposições da LGPD

Como se infere da leitura de seu artigo inaugural, a LGPD versa sobre o tratamento de dados pessoais[21], os quais, nos moldes do inciso I de seu art. 5º, consistem na "informação relacionada a pessoa natural identificada ou identificável". Não estão abrangidos, no âmbito de proteção do aludido diploma legal, os dados relacionados a pessoas jurídicas[22], assim entendidas as entidades elencadas nos artigos 41, 42 e 44 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil Brasileiro).

O conceito de "tratamento" trazido pela LGPD, importa salientar, é o mais amplo possível, abrangendo, nos termos de seu art. 5°, X, toda operação realizada com dados pessoais.

Dessa forma, pode-se inferir que a divulgação de dados pessoais pelas estatais quando da publicação de contratos administrativos e documentos relacionados na internet, deve ser enquadrado como tratamento para fins de incidência da Lei em análise.

Diante disso, cabe observar que a LGPD prevê uma série de requisitos a serem atendidos no tratamento de dados pessoais pelos agentes de tratamento, fixando dentre as diretrizes principais o necessário enquadramento do

20. Incluído pela Emenda Constitucional nº 115, de 2022.

21. São considerados dados pessoais diretos aqueles que identificam diretamente uma pessoa natural, independentemente de outras informações, como, por exemplo, o nome, número de inscrição no CPF, título de eleitor, dentre outros. Por sua vez, são dados pessoais indiretos aqueles que, associados a outros dados, permitem identificar a pessoa natural correlata, tais como geolocalização, idade, profissão, dentre outros. VAINZOF, Rony. Capítulo I disposições preliminares. *In: LGPD: Lei Geral de Proteção de Dados comentada* / coord. MALDONADO, Viviane Nobrega e BLUM, Renato Opice. – 2. ed. Ver, atual. E ampl. – São Paulo: Thompson Reuters Brasil, 2019, p.91.

22. Conforme Enunciado nº 693 da IX Jornada de Direito Civil promovida pelo Conselho da Justiça Federal (CJF).

tratamento de dados em bases legais[23] definidas no art. 7º, no caso de dados pessoais, e no art. 11, no caso de dados pessoais sensíveis[24], e a observância dos princípios nela fixados, previstos em seu art. 6°.

O rol de bases legais é taxativo, o que significa dizer que não há outras hipóteses permissivas além das previstas nos dispositivos mencionados acima[25]. Além disso, basta o enquadramento em uma das citadas bases legais para legitimar o tratamento de dados[26], de forma que não há hierarquia entre elas, conforme Enunciado nº 689 da IX Jornada de Direito Civil promovida pelo Conselho da Justiça Federal (CJF).

No caso específico da publicação de contratos administrativos contendo dados pessoais, trata-se de cumprimento de obrigação legal, decorrente do disposto no art. 39 da Lei das Estatais, art. 8º da LAI, art. 7º do Decreto 7.724/2012 e arts. 10 e 11 da Portaria Interministerial nº 140/ 2006, como visto anteriormente, enquadrando-se o tratamento no art. 7º, II (no caso de dados pessoais) ou art. 11, II, "a" (quando se tratar de dados pessoais sensíveis), ambos da LGPD.

Além da adequação em alguma das bases legais definidas nos arts. 7° e 11, o tratamento de dados pessoais, para ser legítimo, deve observar os princípios previstos no art. 6° da LGPD[27], no qual é elencado, além da boa-fé, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas[28].

23. A doutrina recomenda que as bases legais sejam verificadas e documentadas antes do tratamento dos dados, pois cada uma delas pode acarretar alguns efeitos específicos, que exijam a realização de ajustes nas atividades e providências a serem adotadas pelos agentes de tratamento. PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance digital e LGPD. São* Paulo: Thomson Reuters, 2021, p. 149

24. De acordo com o art. 5°, II, da LGPD, considera-se 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*".

25. LIMA, Caio César Carvalho. Seção I dos requisitos para o tratamento de dados pessoais. *In LGPD: Lei Geral de Proteção de Dados comentada* / coord. MALDONADO, Viviane Nobrega e BLUM, Renato Opice. – 2. Ed. Ver, atual. E ampl. – São Paulo: Thomson Reuters Brasil, 2019, p. 180

26. Segundo Chiara Teffé e Mario Viola "deve o agente fundamentar a sua escolha e buscar a base mais segura e adequada para a relação, sendo possível inclusive – em certos casos – cumular as hipóteses assim como no GDPR". (...) "A possibilidade de identificação de mais de uma base legal para determinada operação de tratamento de dados tem encontrado respaldo tanto nas autoridades de proteção de dados quanto na doutrina europeia". DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In:* BIONI, Bruno *et al*. *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2021. p. 116 e 117

27. Devido ao enfoque do estudo, teceremos comentários apenas em relação aos princípios da finalidade, adequação e necessidade.

28. "A principiologia da LGPD impede a redução dos dados pessoais ao aspecto meramente patrimonial, uma vez que priorizou claramente a sua dimensão existencial e impôs uma série de cuidados e restrições aos tratamentos de dados". FRAZÃO, Ana. *Direitos Básicos dos titulares de dados pessoais*, Revista do Advogado, n. 144, p. 33-47, nov. 2019.

Dentre os mencionados princípios, o da finalidade determina que o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular. Ademais, conforme princípio da adequação, o tratamento de dados deve ser compatível com as finalidades explicitadas ao titular, de acordo com o contexto do tratamento. Na hipótese em análise, objetiva-se com a publicação na internet dos contratos administrativos e demais documentos pertinentes aos procedimentos licitatórios assegurar a transparência pública e permitir o controle social.

Conforme princípio da necessidade, o tratamento de dados deve se limitar ao mínimo necessário para a realização de suas finalidades, abrangendo somente os dados pertinentes, proporcionais e não excessivos. Neste aspecto deve ser avaliado se a publicação de todos os dados pessoais constantes dos documentos em análise é imprescindível à transparência das contratações e ao controle social, caso contrário, não devem ser divulgados[29].

4. Análise de decisões e guias orientativos sobre o tema

Como visto, as estatais possuem o dever de divulgar informações decorrentes das licitações e contratações administrativas, incluindo-se aqui dados pessoais de interesse público. No entanto, deve-se analisar, à luz da LGPD, em especial os princípios da finalidade, adequação e necessidade, quais dados pessoais contidos nesses documentos são efetivamente imprescindíveis ao atingimento da finalidade pretendida, que é viabilizar o controle social.

A ANPD, autarquia responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional[30], ainda não se pronunciou, de forma institucional, diante de situações concretas a respeito de quais dados devem ou não ser divulgados em sede de transparência ativa e passiva pela Administração Pública[31]. No guia Tratamento de Dados Pessoais pelo Poder Público a autoridade aborda o tema de forma mais genérica trazendo orientações sobre como proceder diante de um caso concreto.

29. Nesse sentido, destaca a ANPD que "Uma possível salvaguarda a ser adotada é a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares". Autoridade Nacional de Proteção de Dados Pessoais, *op. cit*.

30. Conforme art. 5º, XIX, da LGPD.

31. A transparência ativa ocorre quando há divulgação de informações pela Administração Pública independentemente de requerimento. Já a transparência passiva ocorre quando há disponibilização de informações mediante solicitação do cidadão. A esse respeito, consultar os arts. 7º e 9º do Decreto nº 7724/2012.

Em consulta realizada à página da transparência da ANPD, verifica-se que todos os contratos administrativos publicados apresentam os números de CPF e identidade dos representantes legais dos signatários de forma descaracterizada[32].

Cabe destacar que a ANPD e a CGU assinaram o Acordo de Cooperação Técnica nº 01/2023, em 17 de maio de 2023[33], o qual, prevê, dentre os seus objetivos, conforme, Cláusula Primeira, a elaboração em conjunto de normas, guias e materiais informativos sobre a aplicação harmônica entre a LAI e a LGPD[34].

Por sua vez, a CGU, no âmbito de sua competência para apreciar recursos interpostos em casos de negativa de acesso à informação determinada por órgão ou entidade pública federal, com fundamento na LAI, possui diversas decisões a respeito de quais dados pessoais devem ou não ser divulgados via transparência passiva[35].

A CGU já se manifestou no sentido de que nomes de empregados públicos responsáveis pela assinatura de contrato celebrado por empresa pública federal devem ser divulgados, pois eles assinam o instrumento na qualidade de agentes públicos, sendo tal informação relevante para o efetivo controle social, conforme Parecer nº 598/2020[36]:

> [...] tem-se que o empregado público, com vínculo jurídico com a Administração Pública Indireta, é regido em alguns pontos por normas de direito público e em outros por normas de direito privado. Nesse caso específico, restou demonstrado que os empregados do SERPRO somente assinaram o contrato em questão por estarem na função de agentes públicos, conferindo a execução de certas atribuições legais, voltadas para o atendimento das necessidades coletivas, em estrito cumprimento aos princípios da legalidade, da indisponibilidade do interesse público e demais princípios que norteiam a Administração Pública e, em especial, ao efetivo controle social a ser exercido pela sociedade. [...] opina-se pelo co-

32. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/licitacoes-e-contratos-1/contratos Acesso em 03 dez. 2023

33. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *ANPD assina acordo de cooperação técnica com a CGU*. 17 maio 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-acordo-de-cooperacao-tecnica-com-a-cgu Acesso em 26 jul. 2023

34. BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Acordo de cooperação técnica entre a Autoridade Nacional de Proteção de Dados Pessoais e a Controladoria Geral da União*. Brasília, DF, 2023 Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/act-anpd-cgu.pdf Acesso em 27 jul. 2023

35. Sem a pretensão de esgotar a análise dessas determinações, serão comentadas algumas delas neste estudo.

36. BRASIL. Controladoria Geral da União. *Parecer nº 598*: NUP 99928.000062/2020-89. 12 maio 2020. Disponível em: https://buscaprecedentes.cgu.gov.br/BuscaAvancada/BuscaAvancada?handler=Busca Acesso em 02 jun. 2023.

> nhecimento e provimento do recurso, com fundamento no art. 4º e 7º, incisos II e V, da Lei nº 12.527/2011, visto tratar-se de informação pública, para que seja disponibilizada a identificação dos empregados públicos responsáveis pela assinatura do Contrato nº 73.353/2020 [...]

Quanto aos números de inscrição no CPF de agentes públicos, a CGU possui decisões no sentido de que a referida numeração deve ser descaracterizada para evitar o seu uso indevido por terceiros. Tal medida permite o controle social e evita equívocos em casos de homonímia, como, por exemplo foi decidido no âmbito da Nota Técnica Nº 739/2019/CGUNE/CRG[37]. Já por meio do Parecer nº 00001/2021/CONJUR-CGU/CGU/AGU, a CGU se manifestou no sentido de que os números de CPF dos representantes legais de contratadas deveriam ser descaracterizados ao passo que, no caso de servidores públicos, deveria ser fornecido alternativamente o número de sua matrícula[38].

> [...] a CGU orienta os órgãos e entidades do Poder Executivo Federal para que, ao divulgarem a listagem com o nome e CPF de seus servidores, oculte os três primeiros dígitos e os dois dígitos verificadores do CPF, nos mesmos parâmetros adotados pela Lei de Diretrizes Orçamentárias da União (LDO de 2013 - Lei 12.708/2012 - Art. 107, Parágrafo único): ***.999.999-**.
>
> [...] quando se tratar de representante legal de pessoa jurídica da contratada, o número de CPF deve ser divulgado de forma descaracterizada, de modo a evitar, ao mesmo tempo, os homônimos e o uso desautorizado de tal dado por terceiros;[...] Com relação ao representante legal da pessoa jurídica de direito público (contratante), é possível a substituição do número do CPF pelo número de matrícula - que no âmbito federal é o número SIAPE [...], visto que se mostra suficiente para conseguir identificar o servidor responsável pelo ato (afastando-se os homônimos) e evitar o uso indevido do número de CPF por terceiros.

A respeito da divulgação de números do CPF e matrícula do servidor, assim como endereço residencial, cumpre mencionar que o STF, quando se pronun-

37. BRASIL. Controladoria Geral da União. *Nota Técnica Nº 739/2019/CGUNE/CRG*. 23 abr. 2019 Disponível em: https://repositorio.cgu.gov.br/handle/1/44434?locale=pt_BR Acesso em 05 jul. 2023.

38. BRASIL. Controladoria Geral da União. *Parecer nº 00001/2021/CONJUR-CGU/CGU/AGU*. 07 de mar. 2022. Disponível em: https://repositorio.cgu.gov.br/handle/1/67796 Acesso em 05 jul. 2023.

ciou a respeito da necessidade de divulgação da remuneração individualizada de servidores públicos federais, entendeu que não deveriam ser disponibilizados os referidos números e endereço, para atenuar os riscos pessoais decorrentes da aludida publicação[39].

Ademais, a CGU já entendeu que as assinaturas de agentes públicos deveriam ser tarjadas quando do fornecimento de documentos via transparência passiva por considerá-las dados biométricos, e, consequentemente, dados pessoais sensíveis, conforme art. 5º, inciso II LGPD, a exemplo do Parecer nº 482/2021/CGRAI/OGU/CGU[40].

> Com fundamento nas normas sobre a privacidade, admite-se a restrição de acesso apenas sobre as assinaturas dos referidos agentes públicos, por se tratarem de dados biométricos vinculados a seus titulares, constituindo assim dados pessoais sensíveis de terceiras pessoas, conforme definido pelo artigo 5º, inciso I da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

Em relação a rubricas, assinaturas, endereços de e-mail ou telefones de funcionários públicos que não se destinam ao atendimento do público em geral, a CGU manifestou-se no sentido de que não seria razoável a sua divulgação ao público em geral, conforme Parecer CGU nº 107/2015[41].

> Após a avaliação conjunta do caso concreto e as correlatas explicações apresentadas pela PREVIC, a CGU constatou a existência de informações amparadas por exceções de publicidade, a saber:
>
> [...] c) informações cuja publicidade é desarrazoada: rubricas, assinaturas; endereços de e-mails ou telefones de funcionários públicos que não se destinam especificamente ao atendimento do público em geral, porque a divulgação dessas informações

39. BRASIL. Supremo Tribunal Federal. *Suspensão de liminar 623. Brasília*, DF. 10 jul 2012. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/SL_623.pdf Acesso em 07 jun. 2023.

40. BRASIL. Controladoria Geral da União. *Parecer n° 482/2021/CGRAI/OGU/CGU*. 31 maio 2021 Disponível em: https://buscaprecedentes.cgu.gov.br/?handler=search&ConsultaBasica.TermoPesquisa=482%2F2021%2FCGRAI%2FOGU%2FCGU&ConsultaBasica.IdOuvidoriaSelecionada=&ConsultaBasica.OuvidoriaSelecionada=&ConsultaBasica.IdTipoDecisaoSelecionada=&ConsultaBasica.TipoDecisaoSelecionada=&ConsultaBasica.IdInstanciaSelecionada=&ConsultaBasica.InstanciaSelecionada=&numPagina=0&maximoRegistrosPorPagina=30 Acesso em 07 jun. 2023.

41. BRASIL. Controladoria Geral da União. *Parecer CGU nº 107: ref. 00700.000929/2016-17*. 28 de jan. 2015 Disponível em: https://buscaprecedentes.cgu.gov.br/?handler=search&ConsultaBasica.TermoPesquisa=37400.005157%2F2014-32&ConsultaBasica.IdOuvidoriaSelecionada=&ConsultaBasica.OuvidoriaSelecionada=Selecione+o+item&ConsultaBasica.IdTipoDecisaoSelecionada=&ConsultaBasica.TipoDecisaoSelecionada=Selecione+o+item&ConsultaBasica.IdInstanciaSelecionada=&ConsultaBasica.InstanciaSelecionada=Selecione+o+item&estados-simples=0&numPagina=0&maximoRegistrosPorPagina=30 Acesso em 07 jun. 2023.

> poderia em tese prejudicar o funcionamento normal do serviço público ao desviar servidores de suas respectivas competências precípuas em detrimento aos canais de atendimento;

Cumpre mencionar ainda que no Tutorial Tarjamento de Documentos no SEI[42] (Sistema Eletrônico de Informações) a CGU orienta os órgãos e entidades da Administração Pública Federal que utilizam a referida plataforma eletrônica para assinar documentos, a convertê-los em versões com tarjamento dos dados pessoais/sigilosos para que possam ser divulgados ao cidadão[43].

5. Adequação à LGPD dos contratos administrativos publicados na internet pelas estatais

A partir da análise do princípio da necessidade previsto no art. 6º, III, da LGPD[44] e, ainda, com base em decisões proferidas pelo STF e pela CGU, conforme visto acima, é recomendável que as estatais ao divulgarem os contratos administrativos e demais documentos relativos a licitações efetuem a descaracterização dos números de CPF e o tarjamento de dados como endereços, e-mails, telefones, assinaturas físicas e rubricas, pois não são informações imprescindíveis à transparência administrativa e ao controle social[45].

De fato, será um desafio a ser enfrentado, pois o volume de contratos atualmente disponibilizados na internet é elevado e o tarjamento na maioria das hipóteses é realizado manualmente. Dessa forma, a eficiência do procedimento dependerá da tecnologia e softwares detidos pela estatal e do número de funcionários disponíveis para realizar a atividade.

42. BRASIL. Controladoria Geral da União. *Tutorial tarjamento de documentos no SEI*. 1ª Ed. Jun. 2021. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/66379/1/Briefing_tarjamento_SEI_PRO.pdf Acesso em 07 jun. 2023.

43. No Guia para Tratamento de Informações com Restrição de Acesso no SEI/CGU, a CGU classifica como nível de acesso "restrito – unidade" a informação pessoal nos termos do art. 31, da LAI, quais sejam, aquelas que tragam elementos que identificam ou podem identificar determinada pessoa e se refere a sua intimidade, vida privada, honra e imagem. Ademais, classifica como nível de acesso "restrito-usuário" , a informação pessoal sensível, nos termos do art. 31 da Lei nº12.527/2011, a saber, aquelas que além de identificarem a pessoa natural, dizem respeito a aspectos mais profundos de sua personalidade, como posição política, ideológica, religiosa, sexual ou relacionadas à saúde, origem racial, étnica e genética. _____. Controladoria Geral da União. *Restrição de acesso: guia para tratamento de informações com restrição de acesso no SEI/CGU*. Versão 1.0, Brasília, DF. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/38789/5/GUIA_HIPOTESE_LEGAL_SEI.pdf Acesso 05 jul. 2023.

44. "(...)a administração pública deve realizar um juízo de necessidade acerca de quais dados pessoais deverão ser disponibilizados para o atendimento de um pedido de acesso à informação. Isso não significa, contudo, que não se pode disponibilizar nenhum dado pessoal. O princípio da necessidade, conforme se vem argumentando, não é uma fechadura, mas sim um filtro para equalizar o tratamento de dados pessoais".
BIONI, Bruno Ricardo; DA SILVA, Paula Guedes Fernandes; MARTINS, Pedro Bastos Lobo. *Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI)*: análise contextual pela lente do direito de acesso *In:* Cadernos Técnicos da CGU / Controladoria-Geral da União, v. 1, 2022.

45. No mesmo sentido já se manifestou André Castro Carvalho. LGPD e a transparência ativa no contexto da Lei de Acesso à Informação CARVALHO, André Castro. LGPD e a transparência ativa no contexto da Lei de Acesso à Informação. *Jota*, 23 jul. 2023. Disponivel em: https://www.conjur.com.br/2023-jul-23/publico-pragmatico-lgpd-transparencia-ativa-ambito-lei-12527#_ftnref5 Acesso em 25 jul. 2023.

Cumpre mencionar que o art. 63 da citada Lei preconiza que a ANPD estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data da entrada em vigor da sobredita Lei, considerada a complexidade das operações de tratamento e a natureza dos dados. Em que pese não ser possível assegurar que os contratos administrativos e demais documentos correlatos se enquadram no conceito de banco de dados, por ausência de definição na LGPD, ao menos de forma analógica é possível inferir que sua adequação deve ocorrer de forma progressiva.

Assim, para adequação desse acervo, algumas medidas são possíveis, cabendo a análise do impacto aos titulares dos dados bem como à transparência pública em cada uma delas. A seguir, serão analisadas algumas alternativas, sem a pretensão de esgotar o tema.

Uma das possibilidades consiste na retirada de todos os contratos para adequação. Tal medida foi adotada pela Petrobras, conforme se verifica de seu Portal da Transparência[46]. Nesse caso, foi prestigiado o direito à intimidade e à proteção de dados pessoais em detrimento à transparência pública e ao controle social, não sendo, portanto, o mais recomendado.

Outra medida, diametralmente oposta, é a manutenção de todos os contratos administrativos e demais documentos até que advenha orientação expressa da ANPD sobre o tema ou mudança de entendimento do TCU após a LGPD. Contudo, nesse caso, em que pese ser assegurada a transparência, o direito à intimidade e à proteção de dados pessoais não são resguardados.

No caso do Banco do Brasil, em seu da Transparência Portal, apenas é possível pesquisar contratações realizadas após 2019. Os contratos consultados apresentam nomes, número de inscrição no CPF e identidade do representante legal da contratada (preâmbulo) e as partes assinam eletronicamente, com informação sobre o nome e número do CPF.

Outra possibilidade, é a manutenção de todos os contratos e documentos nos Portais e o tarjamento ser realizado progressivamente. Nessa hipótese,a transparência pública é prestigiada e o direito à intimidade e proteção de dados vai sendo resguardado paulatinamente conforme a adequação é efetua-

46. Consta a seguinte mensagem no Portal da Transparência da Petrobrás: “Para que possamos realizar as adaptações necessárias ao cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a disponibilização de arquivos contratuais para download em nosso Portal de Transparência ficará temporariamente suspensa”. Disponível em: https://transparencia.petrobras.com.br/contratos

da. No Portal da Transparência da CGU, os contratos administrativos mais recentes não apresentam dados como CPF e identidade ou essas informações constam tarjadas[47].

Outra solução, seria a retirada dos documentos do site para adequação à LGPD, sendo disponibilizado extrato contendo todas as informações exigidas pela legislação e ainda as minutas contratuais sem assinaturas e sem preenchimento de dados pessoais. Deve haver informação no site sobre a adoção de tal medida e sobre a possibilidade de solicitação dos documentos em tela via Serviço de Informação ao Cidadão – SIC. Deve-se ponderar, no entanto, o risco de tal conduta ser considerada descumprimento às determinações do TCU comentadas anteriormente.

Adicionalmente, antes da adoção de alguma medida, é recomendável aferir os riscos envolvidos. Recomenda-se verificar o número de acessos e downloads dos contratos e documentos disponíveis, se já ocorreu algum incidente de segurança ou reporte de uso indevido dos dados publicados e, ainda, se já houve solicitação de titular de retirada de seus dados dos Portais. É indicado, ainda, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais - RIPD[48] descrevendo as medidas, salvaguardas e mecanismos de mitigação de riscos adotadas para resguardar os direitos dos titulares, conforme art. 5º, XVII e 38, da LGPD.

Considerações finais

Com a celebração do Acordo de Cooperação Técnica nº 01/2023, firmado entre a ANPD e a CGU espera-se que as entidades expeçam orientações em conjunto a respeito da divulgação de dados pessoais constantes de contratos administrativos e demais documentos relacionados às licitações publicados nos Portais da Transparência.

Enquanto não advém manifestações conjuntas dessas entidades sobre o tema, para trazer maior segurança jurídica, a interpretação que parece mais adequada aos princípios da finalidade, necessidade e adequação previstos na LGPD, é o tarjamento de dados pessoais constantes dos mencionados docu-

47. Como por exemplo: contratos administrativos nº 03/2023, 04/2023, 05/2023 e 06/2023. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/licitacoes-e-contratos/contratos-e-outras-avencas/2023

48. De acordo com o Enunciado 679 da IX Jornada de Direito Civil promovida pelo Conselho da Justiça Federal (CJF): "O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de accountability para qualquer operação de tratamento de dados considerada de alto risco, tendo sempre como parâmetro o risco aos direitos dos titulares".

mentos que não são imprescindíveis à transparência pública e ao controle social. Tal medida resguarda a intimidade e a proteção de dados pessoais, sem prejuízo à transparência e ao controle social.

Como parâmetro, recomenda-se a análise das decisões proferidas pela CGU, conforme comentado no tópico "Análise de decisões e guias orientativos sobre o tema" deste estudo. Como visto, a CGU possui decisões no sentido de que o número de inscrição no CPF deve ser descaracterizado, bem como devem ser tarjados dados pessoais como assinaturas, rubricas, endereços de e-mails e telefones que não se destinam ao atendimento do público em geral.

Ademais, diante do cenário atual, conforme comentado ao longo do presente artigo, parece mais acertado manter todos os contratos e documentos publicados nos Portais da Transparência e realizar o tarjamento dos aludidos dados pessoais progressivamente, conforme se infere do art. 63 da LGPD, de acordo com a disponibilidade de pessoal e possibilidades operacionais da estatal. Dessa forma, não haverá descumprimento das decisões proferidas pelo TCU e estará resguardada a transparência pública. Adicionalmente, conforme já ressaltado, recomenda-se a elaboração de RIPD descrevendo as medidas, salvaguardas e mecanismos de mitigação de riscos adotadas para resguardar os direitos dos titulares.

Referências

ARAGÃO, Alexandre Santos de. Regime jurídico das empresas estatais. *In: Enciclopédia jurídica da PUCSP*, tomo II (recurso eletrônico): direito administrativo e constitucional / coord. Vidal Serrano Nunes Jr. [*et al.*] - São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

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

BIONI, Bruno Ricardo; DA SILVA, Paula Guedes Fernandes; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso *In: Cadernos Técnicos da CGU* / Controladoria-Geral da União, v. 1, 2022.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *ANPD assina acordo de cooperação técnica com a CGU*. 17 maio 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-acordo-de-cooperacao-tecnica-com-a-cgu Acesso em 26 jul. 2023.

_____ Autoridade Nacional de Proteção de Dados Pessoais. *Acordo de cooperação técnica entre a Autoridade Nacional de Proteção de Dados Pessoais e a Controladoria Geral da União*. Brasília, DF, 2023 Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/act-anpd-cgu.pdf 27 Acesso em jul. 2023.

_____. Autoridade Nacional de Proteção de Dados Pessoais. *Tratamento de dados pessoais pelo poder público*. versão 2.0, Brasília, DF, jun. 2023 Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf Acesso em 15 jul. 2023.

_____. Controladoria Geral da União. *Enunciado nº 4*. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, n. 10 març. 2022. Seção I, p. 152.

_____. Controladoria Geral da União. *Tutorial tarjamento de documentos no SEI*. 1 ed. Brasília, DF, jun. 2021. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/66379/1/Briefing_tarjamento_SEI_PRO.pdf Acesso em 07 jun. 2023.

_____. Controladoria Geral da União. *Restrição de acesso*: guia para tratamento de informações com restrição de acesso no SEI/CGU. Versão 1.0, Brasília, DF. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/38789/5/GUIA_HIPOTESE_LEGAL_SEI.pdf Acesso em 05 jul. 2023

_____ Ministério da Economia, Secretaria Especial de Desestatização, Desinvestimento e Mercados, Secretaria de Coordenação e Governança das Empresas Estatais / Secretaria de Coordenação e Governança das Empresas Estatais. *Guia de padronização de informações das empresas estatais federais nos portais da internet*. 3ª ed. dez. 2022 – elaborado e revisado conforme recomendações dos Acórdãos nº1832/2018-TCU-Plenário, 2647/2020-TCU-Plenário e 2726/2021-TCU-Plenário. Brasília: Sest/ME, 2022. Brasília-DF. Disponível em: https://www.gov.br/economia/pt-br/assuntos/empresas-estatais-federais/central-de-conteudo/guias-e-manuais/guia_padronizacao_informacoes_portais_internet_edicao_3_versao_9.pdf Acesso em 10 jul. 2023.

CARVALHO, André Castro. LGPD e a transparência ativa no contexto da Lei de Acesso à Informação. *Jota*, 23 jul. 2023. Disponivel em: https://www.conjur.com.br/2023-jul-23/publico-pragmatico-lgpd-transparencia-ativa-ambito-lei-12527#_ftnref5 Acesso em 25 jul. 2023.

CARVALHO, André Castro; BANNWART, Elizabeth. Marques. A Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados (LGPD): adequando-as aos programas de governança em privacidade das empresas estatais. *In:* CARVALHOSA, Modesto; KUYVEN, Fernando. (Org.). *Compliance no direito empresarial*. 1ed. São Paulo: Thomson Reuters Brasil, 2020, v. 4, p. 239-253.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. *Tratamento de dados pessoais na LGPD*: estudo sobre as bases legais dos artigos 7º e 11. *In:* BI-

ONI, Bruno *et al*. *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2021. p. 116 e 117.

FRAZÃO, Ana. Direitos Básicos dos titulares de dados pessoais, *Revista do Advogado*, n. 144, p. 33-47, nov. 2019.

IX Jornada Direito Civil: comemoração dos 20 anos da Lei n. 10.406/2022 e da instituição da Jornada de Direito Civil : enunciados aprovados. – Brasília : Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022. Disponível em https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf Acesso em 1° jul. 2023.

LIMA, Caio César Carvalho. Seção I dos requisitos para o tratamento de dados pessoais. *In LGPD: lei geral de proteção de dados comentada* / coord. MALDONADO, Viviane Nobrega e BLUM, Renato Opice. –2. Ed. Ver, atual. E ampl. –São Paulo: Thomson Reuters Brasil, 2019.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. *Compliance digital e LGPD*. São Paulo: Thomson Reuters, 2021.

VAINZOF, Rony. Capítulo I - Disposições preliminares. *In: LGPD: lei geral de proteção de dados comentada* / coord. MALDONADO, Viviane Nóbrega e BLUM, Renato Opice. – 2. ed. Ver, atual. E ampl. – São Paulo: Thomson Reuters Brasil, 2019.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

Privacy by design e abordagem de risco

IZABELLA DE REZENDE ZUCCARI

IZABELLA DE REZENDE ZUCCARI[1]

Sumário: Introdução. 1. Sociedade da informação e a vulnerabilidade digital. 2. *Dark patterns* e manipulação de decisões. 2.1. Obstrução, dissimulação e o caso Amazon Prime. 2.2. Preços personalizados e estudo da Comissão Europeia sobre mercado consumidor e segmentação de mercado online. 3. *Privacy by design and by default*. 3.1. Princípios do *privacy by design*. 3.2. Instrumentos legais. 4. Abordagem de risco como forma de prevenção. Considerações finais. Referências.

Introdução

O atual panorama pós-pandemia traz desafios que são alavancados pela velocidade com que a tecnologia se desenvolve e a informação (e desinformação) se propagam. Este pensamento pode desembocar no senso comum como uma afirmação imprecisa e genérica. Por essa razão, é imperioso trazer um olhar crítico e educacional para a construção de um entendimento básico sobre a privacidade como parte dos direitos digitais fundamentais.

A construção da privacidade como liberdade negativa carrega como essência, ao longo do tempo, uma calibração de aspecto cultural. Vale dizer que, a compreensão sobre o conceito de privacidade e sua tutela variam e dependem da perspectiva adotada. Em determinados momentos pode ser visto como uma busca de isolamento, tranquilidade ou refúgio. Ao passo que, por outra perspectiva, a privacidade alberga necessidades diversas como a busca da igualdade, da liberdade de escolha e da não discriminação. Dessa forma, a privacidade está fortemente ligada ao livre desenvolvimento da personalidade e uma complexa teia de relações a serem ainda vislumbradas pelo direito[2] e a sociedade da informação.

O tema que irá conduzir o trabalho está relacionado com a liberdade de escolha do indivíduo e as influências que podem ameaçar sua autonomia e privacidade nas relações de consumo. Como uma destas influências, será discutido o conceito e a identificação de designs deceptivos, também chamados de dark patterns. Este tema ainda é pouco conhecido pelos titulares de dados no Brasil e, por essa razão, será o cerne debatido neste texto.

1. Advogada, pós-graduanda em Direito Digital na UERJ em parceria com Instituto de Tecnologia e Sociedade (ITS) e pós-graduada em processo civil pela Escola Damásio. Experiência profissional como Data Protection Officer em empresa de tecnologia com atuação conjunta na área de Segurança da Informação, gerente de projeto na implementação e renovação de ISO 27001:2022, certificação de DPO pela EXIN, e certificação CPC-A pela Legal, Ethics and Compliance (LEC).

2. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

O tema é de extrema relevância pela característica complexa de detecção e identificação de práticas que utilizam o design deceptivo. A ausência de transparência dessas interfaces são capazes de conduzir o titular de dados a comportamentos não consentidos e, por consequência, a exposição excessiva de dados pessoais.

Do outro lado desta vertente, observa-se a privacidade desde a concepção e por padrão (tradução livre de *privacy by design and by default*), conceitos já previstos no ordenamento jurídico brasileiro. Estas nomenclaturas adotam uma abordagem preventiva de risco para combater ameaças à liberdade de escolha e privacidade do indivíduo.

Com o objetivo de conectar estes dois pontos, quais sejam, o uso de designs deceptivos e a ameaça à liberdade de escolha e privacidade do indivíduo, pretende-se no presente artigo realizar a análise de conceitos e exemplos a fim de trazer solidez para a característica da abordagem de risco presente na Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709 de 14 de agosto de 2018).

Sendo assim, pretende-se ventilar a visão de abordagem de risco presente no conceito de privacidade desde a concepção como instrumento de cunho preventivo e potencialmente capaz de prevenir práticas e interfaces maliciosas. Através desta ideia, a proteção dos direitos dos titulares de dados vai além do âmbito individual e alcança verdadeira perspectiva coletiva.

1. Sociedade da informação e a vulnerabilidade digital

O avanço da internet e da tecnologia vem transformando a sociedade e os ambientes que proporcionam experiências para os indivíduos, bem como as próprias formas de organização social. Ao analisar as etapas de desenvolvimento da história, é possível observar a presença de um elemento central que estrutura cada período. Este raciocínio auxiliará na compreensão do cenário no qual atualmente estamos inseridos.

Ao imaginar uma linha do tempo, é possível visualizar a era da sociedade agrícola, que se estruturou com as riquezas provindas da terra; a era da sociedade industrial, que se organizou com a criação das máquinas à vapor e a eletricidade; e a era da sociedade pós-industrial, constituída pela prestação de serviços, como os casos dos setores bancário, educacional, da assistência médica e da consultoria jurídica. No momento presente, o contexto da so-

ciedade tem como elemento central a informação para o desenvolvimento da economia. Por essa razão, fala-se na chamada sociedade da informação[3].

Esta nova organização social tem como conjuntura a evolução tecnológica, que proporciona um fluxo informacional de alta velocidade que, por consequência, fomenta ainda mais os relacionamentos sociais e econômicos. Entretanto, isso ocorre de forma dissonante e desproporcional, principalmente quando analisamos a acessibilidade de internet e da educação digital.

Os reflexos desse movimento são característicos e diversos, como o caso do analfabetismo digital e vulnerabilidade informacional. Gerado nos trabalhadores, o efeito político-social do analfabetismo digital[4] afeta a aptidão da mão de obra para o uso de novas tecnologias e acentua a marginalização social. Entretanto, para trabalhar o enfoque deste presente artigo no tema acima apontado, será necessário compreender sobre o conceito de vulnerabilidade informacional e os efeitos que podem ser atenuados com a abordagem de risco.

Para tanto, vale destacar que o próprio Código de Defesa do Consumidor (Lei nº 8.078 de 11 de setembro de 1990), em seu artigo 4º, parágrafo segundo, reconhece como princípio a vulnerabilidade do consumidor no mercado de consumo. Esta vulnerabilidade é identificada em três classificações clássicas: técnica, jurídica e fática. Não obstante, novas classificações são necessárias para a atualidade.

Nos dias de hoje, considerando as novas tecnologias da informação, fica evidente a denominada vulnerabilidade informacional[5]. A assimetria informacional é um dos critérios mais significativos que caracterizam o desequilíbrio entre o consumidor e fornecedor. Uma das ferramentas que corrobora com este déficit no ambiente digital é o design deceptivo, presente em sites, aplicativos, ações de marketing e comércio eletrônico. O uso deste tipo de design pode afetar os comportamentos e decisões do indivíduo, ocasionando a realização de coleta de dados pessoais sem que o titular, que está do outro lado do dispositivo, possa questionar ou perceber. Dessa forma, há uma flagrante desproporcionalidade na ação dos fornecedores e agentes de tratamento de dados pessoais.

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

4. PINHEIRO, Patrícia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva Jur, 2021.

5. MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. In: MIRAGEM, Bruno; MARQUES, Claudia Lima; MAGALHÃES, Lucia Ancona Lopez de. (Orgs). *Direito do consumidor*: 30 anos do CDC. São Paulo: Forense, 2020, p. 233-261..

A partir deste raciocínio, vale apontar o conceito de vulnerabilidade digital. Trata-se de um estado universal de indefesa e suscetibilidade em razão do desequilíbrio de poder, este que é resultado do aumento da automação do comércio, das relações consumidor-fornecedor regidas por dados e mercados digitais bem arquitetados. Nesta perspectiva, a arquitetura de escolha disponível é desenhada de forma a organizar o contexto com que as pessoas tomam decisões, antecipando vieses cognitivos e afetivos através de designs projetados para alterar comportamentos[6].

Dessa forma, o poder de afetar a autonomia do consumidor e titular de dados é feito de forma direcionada e intencional. Saber identificar esses padrões de arquitetura e conscientizar a sociedade com educação digital são possibilidades de trazer força na prestação de contas das organizações públicas e particulares. Seja qual for o interesse do agente ao utilizar práticas com designs deceptivos, já existem instrumentos disponíveis nas legislações para mitigar os riscos desse tipo e moldar novos padrões de arquitetura pautados na transparência e na privacidade desde a concepção.

2. *Dark patterns* e manipulação de decisões

A identificação dos designs deceptivos no ambiente digital é desafiadora, o que reflete, inclusive, na diversidade de nomenclaturas encontradas na literatura. Dentre as publicações das autoridades nacionais e estudiosos da área, são encontrados nomes como padrões obscuros (tradução livre de *dark patterns*), padrões enganosos, interfaces maliciosas e design deceptivo.

O fundador da Iniciativa Padrões Deceptivos (tradução livre de *Deceptive Patterns Initiative*), Harry Brignull[7], conceitua a expressão como os truques usados em sites e aplicativos que levam o indivíduo a fazer coisas que não pretendia, como, por exemplo, comprar ou se inscrever em algo. Se considerarmos o estudo da Comissão Europeia[8] sobre o tema, acrescenta-se nessa definição que essas interfaces orientam, enganam, coagem e manipulam os consumidores a fazerem escolhas que, muitas vezes, não são de seus interesses, favorecendo empresas que prestam determinados serviços.

6. HELBERGER, Natali. *et al*. *EU Consumer Protection 2.0*: structural asymmetries in digital consumer markets. Brussels: BEUC (The European Consumer Organisation), 2021. Disponível em: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf. Acesso em: 03 dez 2023.

7. BRIGNULL, Harry. *et al*. *Deceptive patterns*: user interfaces designed to trick you. Eastbourne: Testimonium Ltd, 2013.

8. LUPIÁÑEZ-VILLANUEVA, Francisco. *et al*. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/. Acesso em: 17 jul 2023.

Se a análise partir da perspectiva do uso nas plataformas de mídia social, a Diretriz 03/2022 do Comitê Europeu de Proteção de Dados considera padrões obscuros aqueles que levam o usuário a fazer ações não intencionais, involuntárias e decisões potencialmente prejudiciais relativas ao tratamento de seus dados pessoais. O objetivo é influenciar o comportamento dos utilizadores e pode prejudicar a sua capacidade de proteger eficazmente os seus dados pessoais e fazer escolhas conscientes[9].

A Diretriz de Práticas Comerciais Desleais europeia de 2021 (tradução livre de *Unfair Commercial Practices Directive*[10] - UCPD), regulação voltada para práticas das empresas face aos consumidores, traz um item para debates sobre as práticas baseadas em dados e padrões obscuros no setor digital. O documento define o padrão escuro como um tipo de encorajamento malicioso, geralmente integrado nas interfaces digitais, que se apoia nos dados coletados e personalizados dos consumidores, ou ainda que pode ser aplicado de forma mais geral, explorando a heurística e as tendências comportamentais, como aceitar por defeito ou pelo enviesamento por escassez.

A possibilidade de influenciar no julgamento e causar erros sistemáticos sobre o que está sendo oferecido demonstra uma influência na autonomia do indivíduo. Esta manipulação comportamental evidencia riscos no consentimento, bem como uma ameaça no que tange a privacidade e coleta massiva de dados pessoais para ataques a vulnerabilidades dos titulares de dados e consumidores.

A combinação da coleta de dados com design deceptivo converge para a possibilidade de ações direcionadas, utilizando técnicas de personalização. Informações sociodemográficas combinadas com características psicológicas, como interesses e preferências, se tornam munição para manipular os consumidores. Por exemplo, um profissional consegue identificar que um

9. Tradução nossa. No original: "*in the context of these Guidelines, 'dark patterns' are considered as interfaces and user experiences implemented on social media platforms tha lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices*. EUROPEAN DATA PROTECTION BOARD. *Guidelines 3/2022 on dark patterns in social media platforms interfaces*: how to recognise and avoid then. May 2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Acesso em: 03 dez. 2023.

10. EUROPEAN COMMISSION. *Unfair commercial practices directive*. Disponível em: https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en. Acesso em: 17 jul 2023.

adolescente se encontra em situação vulnerável devido aos acontecimentos na sua vida pessoal, e estas informações são usadas posteriormente, através de anúncios baseados na emoção de determinado momento[11].

Para analisar o objeto deste tópico a partir da perspectiva de defesa de direitos, é imprescindível trazer pelo menos duas diretrizes: direitos de proteção do consumidor e proteção de dados. Os designs deceptivos atacam diretamente esses direitos, influenciando e manipulando, com a finalidade de trazer mais ativos[12] para uma organização e aumentar ainda mais as práticas de concorrência desleal, ignorando a autonomia das pessoas.

Na literatura, em prol da defesa de direitos, há também apontamentos sobre práticas denominadas como *nudges*[13]. Trata-se de uma intervenção suave que visa influenciar o comportamento de pessoas de maneira previsível e não intrusiva. A ideia é que os nudges são projetados para ajudar as pessoas a tomar decisões melhores e mais benéficas em relação à privacidade e segurança, sem coagir a realizar determinada ação. Esta ferramenta vem sendo utilizada para superar barreiras de informação, mitigar vieses comportamentais e de tomada de decisão, e aumentar a conscientização sobre riscos e ameaças à privacidade e à segurança. Um exemplo de uso de nudges seria tornar opções de privacidade e segurança mais destacadas e fáceis de entender, ou o oferecimento de incentivos para usuários tomarem decisões mais seguras.

As autoridades de proteção de dados vêm em busca de identificar, classificar e responsabilizar agentes de tratamento que realizam práticas ligadas ao uso dos padrões enganosos. Vale dizer, a intenção deste trabalho não é adentrar na taxonomia dos designs obscuros e mencionar cada classificação. Entretanto, no intuito de ilustrar as ações de alguns países na identificação deste tipo de interface maliciosa, vislumbra-se a seguir alguns casos já levantados publicamente.

11. Ibidem

12. *Ativo* é considerado qualquer coisa que tenha valor para uma organização. Desde o sentido amplo como instalações, hardware, software, serviços, pessoas, como também as informações. HINTZBERGEN, Jule. *et al*. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. p. 12.

13. ACQUISTI, Alessandro. *et al*. Nudges for privacy and security: understanding and assisting users' choices online. *ACM Comput*. Surv. v. 50, n. 3, p. 44-85, 2017. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3054926. Acesso em: 03 dez. 2023.

2.1. Obstrução, dissimulação e o caso Amazon Prime

Esta categoria de design deceptivo ocorre quando o usuário se depara com barreiras ou obstáculos que dificultam a conclusão de sua tarefa ou o acesso às informações[14]. Um exemplo seria a dificuldade de cancelamento de um serviço, na qual fica clara a demonstração de uma assimetria entre cadastro fácil e cancelamento difícil[15] -esta tática também é conhecida como *roach motel* ou dificuldade de cancelamento. Paralela a esta categoria há a assinatura forçada, que também é denominada como dissimular (tradução livre de *sneaking*).

O recente processo aberto pela *Federal Trade Commission* (FTC) contra a Amazon nos Estados Unidos, examina o uso de design deceptivo nos serviços de assinatura *prime*, ocorrido em junho de 2023[16]. O órgão americano, cuja missão é proteger os consumidores e evitar práticas de fraudes e concorrência desleal, destaca que a empresa em debate usou interfaces manipuladoras, coercitivas ou enganosas para induzir os consumidores a se inscreverem em assinaturas do serviço, cuja renovação é automática. Este uso foi intencional e consciente a fim de dificultar ao máximo o cancelamento dos assinantes.

Além disso, a liderança da empresa teria desacelerado ou rejeitado mudanças que tornariam mais fácil para os usuários cancelarem o serviço, isto porque, tal decisão afetaria os resultados financeiros da Amazon. Vale dizer que esta não é a primeira vez que a multinacional passa por este tipo de apontamento.

Em 2021, o Conselho Norueguês do Consumidor[17] fez uma reclamação formal, solicitando uma avaliação da Autoridade Norueguesa do Consumidor sobre o procedimento de rescisão da assinatura do serviço e apontou que o procedimento teria sido desenvolvido de forma obscura, com a empresa atuando com práticas comerciais desleais. O documento aponta o uso de design manipulativo de maneiras que estão em desacordo com a lei de privacidade e proteção de dados do consumidor, violando principalmente os princípios do consentimento legalmente válido.

14. BRIGNULL, Harry. *et al*. *Types of deceptive pattern*. Disponível em: https://www.deceptive.design/types. Acesso em: 24 jul 2023.

15. BENTES, Anna. *Dossiê*: taxonomia e regulação de *dark patterns* a partir do estudo da União Europeia. São Paulo: Data Privacy Brasil, 2022.

16. FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS. *FTC takes action against Amazon for enrolling consumers in Amazon Prime without consent and sabotaging their attempts to cancel*. Jun. 2023. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their. Acesso em: 24 jul 2023.

17. FORBRUKERRÅDET. *Complaint against Amazon Prime*. Disponível em: https://fil.forbrukerradet.no/wp-content/uploads/2021/01/complaint-against-amazon-prime.pdf. Acesso em: 24 jul 2023.

2.2. Preços personalizados e estudo da Comissão Europeia sobre mercado consumidor e segmentação de mercado online

A cobrança de preços diferenciados para os mesmos bens e serviços baseada nas informações coletadas dos consumidores também configura um tipo de prática considerada como design deceptivo[18]. A *Unfair Commercial Practices Directive* (UCPD)[19], mencionada anteriormente, possui uma seção destinada ao esclarecimento das práticas de fixação de preços e traz à título de exemplo o seguinte caso:

> Um consumidor classificado como tendo um «poder de compra mais elevado» pode ser reconhecido pelo endereço IP do computador ou por outros meios, sempre que o consumidor visite o sítio Web do profissional através do seu computador pessoal. Os preços propostos a este consumidor poderiam ser, por exemplo, 10 % mais elevados, em média, do que os propostos a um novo cliente ou a um consumidor classificado como tendo um «poder de compra mais reduzido».

O caso acima claramente se ajustaria no artigo 22 do Regulamento Geral sobre a Proteção de Dados da Europa (RGPD)[20], o qual prevê o direito de o titular de dados não ficar sujeito a tomada de decisão com base em tratamentos automatizados que produzam efeitos na sua esfera jurídica ou que o afete significativamente de forma singular.

O estudo de mercado consumidor sobre segmentação online através de preços/ofertas personalizadas na União Europeia (tradução livre de *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*), realizado em junho de 2018[21], traz indicadores e explora os tipos de publicidades direcionadas, a ausência de transparência sobre a personalização online e os efeitos desta personalização de ofertas.

18. BENTES, Anna. *Dossiê*: taxonomia e regulação de *dark patterns* a partir do estudo da União Europeia. São Paulo: Data Privacy Brasil, 2022. p. 29.

19. EUROPEAN COMMISSION. Unfair commercial practices directive. Disponível em: https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en. Acesso em: 24 jul 2023.

20. EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Regulamento geral sobre a proteção de dados*. Disponível em https://gdprinfo.eu/pt-pt. Acesso em: 26 jul 2023.

21. EUROPEAN COMMISSION. *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*. Jun. 2018. Disponível em https://commission.europa.eu/system/files/2018-07/exec_summary_online_personalisation_study_en.pdf. Acesso em: 24 jul 2023.

Esta análise da Comissão Europeia relata as técnicas usadas para coletar dados pessoais dos consumidores, como nos casos de criação de contas online, interação com mídias sociais, rastreamento de atividades de navegação através de *cookies*, entre outros. O uso de anúncios direcionados sem a devida transparência baseado na coleta de dados e informações ilustra, mais uma vez, o presente contexto da sociedade da informação e a vulnerabilidade digital.

Percebe-se que o design deceptivo contribui negativamente para a falta de transparência, bem como viabiliza a aplicação destas técnicas nocivas ao consumidor. Estes mecanismos maliciosos também já foram denominados como geo-pricing no setor de viagens e de transporte, a partir de uma ação civil pública do Ministério Público do Rio de Janeiro contra a empresa Decolar.com[22].

3. *Privacy by design and by default*

Uma das ferramentas para confrontar os *designs* deceptivos é a chamada privacidade por padrão e desde a concepção, ou conforme a nomenclatura em inglês *privacy by design and privacy by default*. O conceito foi desenvolvido com o objetivo de abordar os efeitos sistêmicos, cada vez maiores, de tecnologias de informação e comunicação e de sistemas de dados de larga escala[23].

A ideia foi concebida por Ann Cavoukian, que fez parte como Comissária de Informação e Privacidade da província canadense de Ontário, e se baseia em sete princípios fundamentais que direcionam a base de medidas a serem tomadas para manter a privacidade e proteção de dados dos indivíduos desde o início e de forma preventiva.

3.1. Princípios do *privacy by design*

O primeiro princípio possui uma conexão grande com o cerne deste artigo: (i) proativo não reativo (tradução livre de *Proactive not Reactive; Preventative not Remedial*). A proposta é sobre a privacidade por padrão ser caracterizada por medidas proativas, ao invés de reativas, pois teria como premissa anteci-

22. MARCHETTI, Brunno. *Como Decolar.com e outras empresas mudam preços de acordo com seus dados*. Mar 2018. Disponível em: https://nic.br/noticia/na-midia/como-decolar-com-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados/. Acesso em: 02 dez 2023.

23. CAVOUKIAN, Ann. *Privacy by design:* the 7 foundational principles. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 24 jul 2023.

par e evitar eventos invasivos de privacidade antes que eles se materializem. Esta ideia corresponde a uma abordagem de risco que será ventilada no tópico adiante.

O princípio da (ii) privacidade como configuração padrão elabora a premissa de que os dados pessoais devem ser protegidos automaticamente em qualquer negócio ou sistema de tecnologia da informação. Ou seja, a privacidade deverá ser uma configuração padrão. Ainda existem os princípios da (iii) privacidade incorporada ao design, princípio da (iv) funcionalidade total (soma positiva, não soma zero), princípio da (v) proteção completa do ciclo de vida (segurança de ponta a ponta), princípio da (vi) visibilidade e transparência e a ideia de (vii) manutenção dos interesses do usuário em primeiro lugar.

Esta visão se tornou recentemente um modelo elegido pela *International Organization for Standards* (ISO), organização internacional não-governamental independente, responsável por desenvolver padrões internacionais relevantes para o mercado. A ISO/DIS 31.700[24] será a norma sobre privacidade desde a concepção para bens e serviços de consumo, e fará parte do conjunto ISO 31.000 que aborda as diretrizes de Gestão de Riscos. Este novo modelo terá como base os princípios mencionados anteriormente, trazendo diretrizes de medidas técnicas e administrativas para equilibrar os interesses legítimos da organização e a privacidade do usuário. A ideia central é desenvolver produtos e serviços *privacy-friendly*, com mecanismos eficientes como, por exemplo, a criação de painéis de controle de privacidade para o usuário gerenciar o uso de seus dados de forma granular, criação de mecanismos de transparência ativa durante a jornada do usuário e disponibilização de mecanismos eficientes para os titulares exercerem seus direitos previstos na legislação.

A normatização da ideia da privacidade desde a concepção e por padrão vem ao encontro de proteger os titulares de dados e consumidores em meio a economia digital e sociedade da informação. Para além da visão de conformidade e combate aos designs deceptivos, trazer um modelo que tira a subjetividade do processo de adequação também auxilia na mudança de narrativa das empresas. Ter privacidade desde a concepção pode gerar valor para os negócios, com estímulos para rever os aspectos de responsabilidade sobre a

24. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO/DIS 31700*: consumer protection: privacy by design for consumer goods and services. Disponível em: https://www.iso.org/standard/76772.html. Acesso em: 25 jul 2023.

gestão de fornecedores, como até mesmo desembocar em futuros incentivos fiscais para as empresas que adotam práticas de conformidade com a proteção de dados.

3.2. Instrumentos legais

A previsão legal de *privacy by design and by default* analisada no presente trabalho será o artigo 25 do Regulamento Geral sobre a Proteção de Dados da Europa (RGPD)[25], bem como o parágrafo segundo do artigo 46 da Lei Geral de Proteção de Dados (LGPD)[26]. A escolha deste contorno legal observa a influência europeia sobre a legislação nacional de proteção de dados e o contexto dos materiais coletados e apresentados até o momento.

Vale ressaltar que as práticas de *dark patterns* que têm como característica a coleta de dados pessoais devem ser discutidas dentro de um macro sistema de leis que inclui: direito do consumidor, normas de proteção de dados pessoais, práticas do comércio eletrônico e leis que combatam a concorrência desleal. O entrelace entre normas setoriais, leis e tratados de organismos internacionais fortalece a cultura e a influência destes temas.

O artigo do RGPD, instrumento legal europeu, requer que o agente responsável pelo tratamento dos dados aplique medidas técnicas e organizacionais, tanto no momento de definição do projeto como no próprio tratamento dos dados. Tais medidas, como a pseudonimização, são destinadas a aplicar com eficácia os princípios de proteção de dados, como o próprio princípio da minimização, e a incluir as garantias necessárias no tratamento e proteção dos direitos dos titulares de dados.

25. Artigo 25º. Proteção de dados desde a conceção e por defeito. 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. 3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos nº 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42º.

26. Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei.
§ 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Estudo do Fórum Futuro da Privacidade (tradução livre de *Future of Privacy Forum*), publicado em maio de 2023[27], comenta sobre as lições de aplicação da previsão legal da RGPD. O relatório conta com 92 autoridades de proteção de dados, análise de decisões judiciais e diretrizes dos países que participaram do escopo do estudo. O principal objetivo foi explorar a eficácia das obrigações de privacidade desde a concepção e por padrão, verificar se as violações existentes possuem conexão com outras violações do regulamento europeu e quais são os requisitos mínimos de segurança necessários.

Nota-se dificuldades diversas, como mensurar quais medidas seriam suficientes para trazer eficácia ao instituto da privacidade desde a concepção e por padrão e quais condições técnicas seriam mais apropriadas. A vagueza da redação legislativa europeia (RGPD) desembocaria em uma flexibilidade aos controladores de dados, resultando, por muitas vezes, na ineficácia do cumprimento das obrigações.

Este estudo acima mencionado também inclui uma discussão acerca das tecnologias de aprimoramento de privacidade (tradução livre de *Privacy-Enhancing Technologies*, mais conhecida como PETs). As autoridades nacionais de proteção de dados da Europa encontram inconsistências em especificar e delimitar o papel destas ferramentas. Estas tecnologias têm como característica a incorporação de princípios fundamentais de proteção de dados como minimização do uso e maximização de segurança. Vale dizer que, o estudo destaca que a aplicação de PETs por si só não cobre necessariamente todas as obrigações do artigo 25 da RGPD, mas é visto como um dos meios que podem contribuir para a correta implementação da privacidade desde a concepção[28].

Vale destacar que as PETs representam um conjunto de ferramentas que podem auxiliar a maximizar o uso dos dados reduzindo os riscos inerentes ao uso de dados. É visto como um conjunto emergente de tecnologias e abordagens que permitem a obtenção de resultados úteis a partir de dados sem fornecer o acesso completo, reduzindo as ameaças normalmente associadas ao compartilhamento de dados e motivando novas parcerias. Uma ilustração de PET é a denominada criptografia homomórfica, que possibilita que operações matemáticas sejam realizadas em dados criptografados sem a necessidade

27. FUTURE OF PRIVACY FORUM. *New FPF report*: unlocking data protection by design and by default: lessons from the enforcement of article 25 GDPR. May. 2023. Disponível em: https://fpf.org/blog/new-fpf-report-unlocking-data-protection--by-design-and-by-default-lessons-from-the-enforcement-of-article-25-gdpr/. Acesso em: 19 maio 2023.

28. INFORMATION COMMISSIONER'S OFFICE (ICO). *ICO publishes guidance on privacy enhancing Technologies*. Sep. 2022. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/. Acesso em: 13 jul 2023.

de descriptografá-los primeiro - isso significa que os dados permanecem criptografados durante todo o processo de análise, o que ajuda no âmbito da proteção de dados[29].

A previsão na LGPD possui a mesma característica de adoção de medidas de segurança, técnicas e administrativas destinadas à proteção de dados pessoais, conforme a linha adotada também pela legislação europeia. A própria localização deste artigo, no capítulo de segurança e boas práticas da LGPD, evidencia a importância de uma abordagem preventiva, conectando de maneira clara com os princípios elencados no artigo 6º, em específico o da prestação de contas e responsabilização - no qual o agente deverá demonstrar a adoção de medidas eficazes para comprovar a observância da norma.

Vale ressaltar que, observando os instrumentos legais em tela, ambos evidenciam a necessidade de observar a natureza das informações tratadas. A circunstância do tratamento e o tipo de dado tratado deverão ser usados como referências no momento da mensuração do risco e das definições das técnicas e tecnologias. Este raciocínio segue representado nos princípios definidos por Ann Cavoukian[30], quando menciona sobre o especial rigor a ser aplicado quanto ao tratamento de dados pessoais sensíveis, como informações médicas e dados financeiros.

A crítica quanto a eventual vagueza das redações das leis é cabível no que tange ao grau de efetividade dos dispositivos. Entretanto, é certa a existência de ferramentas já existentes para contestar o uso de designs deceptivos. A aplicabilidade do conceito de privacidade desde a concepção e por padrão, seja por força de lei ou pelo uso de modelos de normatização em padrões internacionais como a ISO, promove o início de um processo de instrumentalização no combate à manipulação e ameaça da autonomia e privacidade dos indivíduos.

A função de trazer luz às práticas de padrões obscuros empodera os titulares de direito e fortalece a ação das autoridades nacionais, contribuindo

29. THE ROYAL SOCIETY. *Privacy Enhancing Technologies*. Jan. 2023. Disponível em: royalsociety.org/privacy-enhancing-technologies. Acesso em: 10 set. 23.

30. CAVOUKIAN, Ann. *Privacy by design*: the 7 foundational principles. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 24 jul 2023.

com os princípios de transparência, previstos na maior parte das leis que protegem os consumidores e os dados pessoais. O esclarecimento sobre estas arquiteturas evita o uso do viés cognitivo para erros sistemáticos de julgamento, vícios no consentimento e manipulação comportamental.

3. Abordagem de risco como forma de prevenção

Diante do debate apresentado, fica claro que os conceitos de privacidade desde a concepção e por padrão, institutos já previstos no recorte legal usado neste artigo, possuem uma qualidade de ação preventiva. O exame das características e referências legais demonstra que a análise sobre a natureza dos dados e as circunstâncias do tratamento leva em consideração o risco para os titulares de dados. Ou seja, a intenção é prevenir a ocorrência de dano ao titular de dados pessoais a partir de uma leitura sobre os riscos de determinado tratamento.

Este desenvolvimento de abordagem se modificou através dos anos, considerando os progressivos avanços tecnológicos que impulsionaram a criação de leis gerais de proteção de dados pessoais mais modernas, como a própria RGPD, mencionada anteriormente. A tutela do direito de proteção de dados pessoais enfrentou um processo de transformação baseado na prevenção e mitigação de riscos, o que diferenciou a legislação atual europeia da lógica regulatória anterior conhecida como Diretiva 95/46/CE. No novo modelo, a salvaguarda dos direitos fundamentais é complementada pela implementação de análises de risco, licenças, processos de documentação, registro de processos e prestação de contas (*accountability*) por parte dos agentes de tratamento de dados pessoais[31].

O cálculo do risco é formado pela equação entre dois fatores: probabilidade e impacto. O raciocínio é baseado no cálculo entre a probabilidade de materialização de uma ameaça e a dimensão do impacto considerando os danos[32]. A identificação do risco em si trata-se de um processo investigativo para reconhecer quais seriam as fontes, eventos, causas e potenciais consequências da ocorrência de um determinado evento. Este tipo de estudo pode envolver

31. ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro. *Anais...* Rio de Janeiro: Comitê Gestor da Internet no Brasil, 2017. p. 176. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 25 jul 2023.

32. SILVA, Paula Guedes Fernandes. O risco como elemento do sistema normativo de proteção de dados pessoais. In: BENTES, Anna. *et al*. *Para além da proteção de dados*: uma coletânea. São Paulo: Data Privacy Brasil Ensino, 2023.

análise de dados históricos, opiniões, pareceres fundamentados, necessidades das partes envolvidas, entre outros fatores[33].

Uma vez mapeado e tratado através de metodologia e métricas, o risco poderá estar diretamente ligado com a tomada de decisões do agente de tratamento. Este esforço torna-se fundamental como auxílio na tomada de decisões de uma organização, seja no setor público ou no setor privado. A avaliação e a gestão dos riscos viabilizam a escolha do tratamento e as medidas de mitigação, inclusive considerando o risco residual.

Os benefícios envolvidos nesta visão têm a potência de orientar a privacidade e a proteção de dados no sentido de prevenir danos em uma perspectiva coletiva. O desenvolvimento da Lei Geral de Proteção de Dados denota outros instrumentos na mesma linha de raciocínio. Se não é possível reduzir o risco a zero, é fundamental utilizar das ferramentas previstas na LGPD para adotar medidas que visem o gerenciamento de riscos, como elaboração de códigos de conduta, certificações, elaboração de Relatórios de Impacto à Proteção de Dados Pessoais, uso de privacidade por padrão e desde a concepção, estruturação de programa de governança, entre outros. Portanto, o gerenciamento de riscos se resume a método e procedimento[34].

Vale frisar que o risco em discussão tem como enfoque o titular de dados pessoais em primeiro lugar, e não o risco regulatório e sancionatório das organizações perante a autoridade de proteção de dados[35]. Para que a abordagem de risco proposta pela LGPD alcance sua finalidade, a análise sobre as ameaças e danos deverá ter como ponto final o titular de dados pessoais.

O conceito de *privacy by design* acompanha uma lógica preventiva no sentido de desenvolver o projeto ou negócio pensando na preservação dos dados pessoais dos titulares desde o início. Inclusive para tornar o atributo da proteção e privacidade como parte do produto ou serviço, que poderá agregar valor de mercado. É preciso observar as práticas de *privacy by pressure*[36] com senso

33. HINTZBERGEN, Jule. *et al*. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. p. 14.

34. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (Coord). *Temas atuais de proteção de dados*. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

35. GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (Coord). *Temas atuais de proteção de dados*. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

36. JAROVSKY, Luiza. *OpenAI's Unacceptable "Privacy by Pressure" Approach*. Abr. 2023 Disponível em: https://www.thepriva-

crítico, conforme sinalizou Luiza Jarovsky - a fim de evitar que a legislação perca sua força e seja somente seguida após reação pública, ou quando instruída a fazer por autoridade competente.

Considerações finais

Privacidade por padrão e desde a concepção é uma abordagem de risco e, por essa razão, tem característica de uma atuação essencialmente preventiva, principalmente se considerada a potencialidade do risco de causar dano coletivo. A legislação brasileira de proteção de dados demonstra a escolha desta estratégia como diretriz, sobretudo quando observada a previsão do princípio da prevenção em seu artigo 6º da LGPD.

A ideia de privacidade está ligada à existência de uma arquitetura e infraestrutura. Desde o exemplo de uma simples cortina colocada em uma janela, que instrumentaliza a preservação da intimidade; até o desenho de um produto, serviço ou negócio considerando a proteção dos dados do indivíduo como ponto central. A privacidade, por assim dizer, é um direito condicionado a instrumentos para ser materializado e efetivado. Observar as ferramentas disponíveis hoje, como o *privacy by design*, é instrumentalizar a proteção dos indivíduos não só no âmbito dos dados pessoais, mas além: prevenindo práticas abusivas e desleais com o cidadão no ambiente digital.

O despertar tardio acerca dos ativos que estão movimentando a sociedade e a economia da informação pode trazer como consequência a banalização de situações alarmantes e prejudiciais. O lançamento de novas tecnologias realizado por grandes empresas da área de tecnologia utilizando de estratégias como a "privacidade por pressão" é apenas um dos quadros ilustrativos deste cenário. Uma estratégia como esta proporciona dados e informações de forma ilegal e antiética, enquanto alimentam e treinam novos sistemas, como no caso de Inteligências Artificiais Generativas.

Há, sem dúvida, a necessidade de um avanço regulatório sobre o tema com diretrizes específicas. A identificação dos padrões de design deceptivos em determinados segmentos de mercado deve auxiliar e aquecer o formato regulatório vigente, e trazer mais força para a privacidade desde a concepção

---

cywhisperer.com/p/openais-unacceptable-privacy-by-pressure?utm_source=%2Fsearch%2Fprivacy%2520by%2520pressure&utm_medium=reader2. Acesso em: 26 jul 2023.

a fim de se tornar realmente um padrão – assim como o cinto de segurança nos meios de transporte.

Portanto, a abordagem de risco como forma de prevenção de danos é imprescindível no setor digital. A manipulação de comportamentos e a influência na autonomia da pessoa é apenas uma das vertentes dos direitos de personalidade potencialmente atingidos. Direitos digitais como direitos fundamentais são o cerne para operacionalizar garantias na sociedade da informação.

Referências

ACQUISTI, Alessandro. *et al*. Nudges for privacy and security: understanding and assisting users' choices online. *ACM Comput*. Surv. v. 50, n. 3, p. 44-85, 2017. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3054926. Acesso em: 03 dez. 2023.

BENTES, Anna. *Dossiê*: taxonomia e regulação de *dark patterns* a partir do estudo da União Europeia. São Paulo: Data Privacy Brasil, 2022.

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

BRIGNULL, Harry. *et al. Deceptive patterns*: user interfaces designed to trick you. Eastbourne: Testimonium Ltd, 2013.

BRIGNULL, Harry. *et al*. *Types of deceptive pattern*. Disponível em: https://www.deceptive.design/types. Acesso em: 24 jul 2023.

CAVOUKIAN, Ann. *Privacy by design*: the 7 foundational principles. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 24 jul 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

EUROPEAN COMMISSION. *Consumer market study on online market segmentation through personalized pricing/offers in the European Union*. Jun. 2018. Disponível em https://commission.europa.eu/system/files/2018-07/exec_summary_online_personalisation_study_en.pdf. Acesso em: 24 jul 2023.

EUROPEAN COMMISSION. *Unfair commercial practices directive*. Disponível em: https://commission.europa.eu/law/law-topic/consumer-protection-law/unfair-commercial-practices-law/unfair-commercial-practices-directive_en. Acesso em: 17 jul 2023.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 3/2022 on dark patterns in social media platforms interfaces*: how to recognise and avoid then. May 2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. Acesso em: 03 dez. 2023.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Regulamento geral sobre a proteção de dados*. Disponível em https://gdprinfo.eu/pt-pt. Acesso em: 26 jul 2023.

FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS. *FTC takes action against Amazon for enrolling consumers in Amazon Prime without consent and sabotaging their attempts to cancel*. Jun. 2023. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their. Acesso em: 24 jul 2023.

FORBRUKERRÅDET. *Complaint against Amazon Prime*. Disponível em: https://fil.forbrukerradet.no/wp-content/uploads/2021/01/complaint-against-amazon-prime.pdf. Acesso em: 24 jul 2023.

FUTURE OF PRIVACY FORUM. *New FPF report*: unlocking data protection by design and by default: lessons from the enforcement of article 25 GDPR. May. 2023. Disponível em: https://fpf.org/blog/new-fpf-report-unlocking-data-protection-by-design-and-by-default-lessons-from-the-enforcement-of-article-25-gdpr/. Acesso em: 19 maio 2023.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In: PALHARES, Felipe (Coord). *Temas atuais de proteção de dados*. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

HELBERGER, Natali. *et al*. *EU Consumer Protection 2.0*: structural asymmetries in digital consumer markets. Brussels: BEUC (The European Consumer Organisation), 2021. Disponível em: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf. Acesso em: 03 nov 2023.

HINTZBERGEN, Jule. *et al*. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

INFORMATION COMMISSIONER'S OFFICE (ICO). *ICO publishes guidance on privacy enhancing Technologies*. Sep. 2022. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/. Acesso em: 13 jul 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *ISO/DIS 31700*: consumer protection: privacy by design for consumer goods and services. Disponível em: https://www.iso.org/standard/76772.html. Acesso em: 25 jul 2023.

JAROVSKY, Luiza. *OpenAI's Unacceptable "Privacy by Pressure" Approach*. Abr. 2023 Disponível em: https://www.theprivacywhisperer.com/p/openais-unacceptable-privacy-by-pressure?utm_source=%2Fsearch%2Fprivacy%2520by%2520pressure&utm_medium=reader2. Acesso em: 26 jul 2023.

LUPIÁÑEZ-VILLANUEVA, Francisco. *et al*. *Behavioural study on unfair commercial practices in the digital environment*: dark patterns and manipulative personalisation. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/. Acesso em: 17 jul 2023.

MARCHETTI, Brunno. *Como Decolar.com e outras empresas mudam preços de acordo com seus dados*. Mar 2018. Disponível em: https://nic.br/noticia/na-midia/como-decolar-com-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados/. Acesso em: 02 dez 2023.

MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. *In*: MIRAGEM, Bruno; MARQUES, Claudia Lima; MAGALHÃES, Lucia Ancona Lopez de. (Orgs). *Direito do consumidor*: 30 anos do CDC. São Paulo: Forense, 2020.

PINHEIRO, Patrícia Peck. *Direito digital*. 7. ed. São Paulo: Saraiva Jur, 2021. p. 63.

SILVA, Paula Guedes Fernandes. O risco como elemento do sistema normativo de proteção de dados pessoais. *In*: BENTES, Anna. *et al*. *Para além da proteção de dados*: uma coletânea. São Paulo: Data Privacy Brasil Ensino, 2023.

THE ROYAL SOCIETY. *Privacy Enhancing Technologies*. Jan. 2023. Disponível em: royalsociety.org/privacy-enhancing-technologies. Acesso em: 10 set. 23.

ZANATTA, Rafael A. F. *Proteção de dados pessoais como regulação de risco*: uma nova moldura teórica? I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica. Acesso em: 25 jul 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

Requisição de dados para investigação de ilícitos: reflexões e perspectivas após o julgamento da Ação Declaratória de Constitucionalidade n. 51

MARIA AUGUSTA PERES CATELLI

MARIA AUGUSTA PERES CATELLI[1]

Introdução

A coleta de dados dos usuários é um elemento fundamental para impulsionar o desenvolvimento dos modelos de negócios das grandes empresas de tecnologia (*big techs*), que desempenham um papel de inegável importância no cenário atual. Além disso, os dados armazenados por essas empresas, geralmente distribuídos em servidores espalhados pelo mundo, têm relevância significativa para a investigação dos ilícitos praticados na internet, que se mostram cada vez mais frequentes e complexos.

Nesse contexto, as requisições de dados para fins de investigação podem atrair legislações de diferentes Estados nacionais com disposições contraditórias entre si e trazer desafios sobre jurisdição e soberania, especialmente considerando que países vêm adotando estratégias para aumentar seu controle sobre a internet por meio de soluções unilaterais em leis nacionais.

No Brasil, o Supremo Tribunal Federal se debruçou sobre esse tema no julgamento da Ação Declaratória de Constitucionalidade (ADC) n. 51, finalizado em 23 de fevereiro de 2023, que tratou sobre a (im)possibilidade de requisição direta de dados às subsidiárias localizadas no país *versus* a utilização de mecanismos de cooperação internacional para obtenção dos dados perante a empresa-mãe.

O presente artigo objetiva propor reflexões sobre os dilemas identificados e os desafios que perduram para todos os atores envolvidos mesmo após a decisão do Supremo Tribunal Federal. Para chegar às conclusões apontadas, analisar-se-á o contexto brasileiro que antecedeu o julgamento da ADC n. 51,

1. Advogada na área de Contencioso Estratégico, com temas envolvendo Direito Digital, Tecnologia e Proteção de Dados. Pós-graduada em Processo Civil pela FGV Direito SP (FGV LAW). Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Graduada em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Contato: mapcatelli@gmail.com.

os principais argumentos em debate, os fundamentos utilizados pelo Supremo Tribunal Federal, além de questões atreladas às estratégias de territorialização do ciberespaço e ao protagonismo assumido pelas *big techs* no cenário atual.

1. Internet, anonimato e investigação de ilícitos

Em 2022, a população mundial atingiu a marca de 8 bilhões de pessoas[2], sendo que 64,4% (ou 5,16 bilhões de pessoas) são usuários da internet[3]. Há significativas variações no uso da internet ao redor do mundo – desde os próprios índices de adoção da internet nos países[4] até os hábitos dos usuários nas redes sociais[5] – mas é inegável que, de uma forma geral, a internet assumiu papel central na vida dos indivíduos e que a sociedade deve estar preparada para lidar com os desafios decorrentes desse cenário.

O uso da internet comumente propicia a sensação de anonimato, ou seja, de que a pessoa por trás do equipamento eletrônico pode se expressar sem que sua verdadeira identidade seja conhecida. Ao navegar pelas redes sociais, por exemplo, não é raro se deparar com perfis falsos ou com poucas informações que viabilizem, aos demais usuários da plataforma, a pronta identificação do responsável pelo conteúdo. Ainda, há ferramentas disponíveis para mascarar a origem do usuário, como é o caso de *proxy* e VPN (sigla para virtual private network ou rede privada virtual)[6].

Com isso, ao mesmo tempo em que a internet proporciona a concretização de direitos fundamentais, intensifica os riscos de violação de direitos, que en-

2. NAÇÕES UNIDAS. *População mundial atinge 8 bilhões de pessoas*. ONU News – Perspectiva Global Reportagens Humanas. 15 nov. 2022. Disponível em: https://news.un.org/pt/story/2022/11/1805342. Acesso em 10 jul. 2023.

3. WE ARE SOCIAL. *The changing world of digital in 2023*. 26 jan. 2023. Disponível em: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Acesso em 10 jul. 2023.

4. Em 8 países, os índices de adoção da internet são iguais ou superiores a 99% e, em 55 países, os índices excedem 90%. Por outro lado, 9 países possuem índices de internet inferiores a 20%. Em termos absolutos, a Índia possui o maior número de pessoas "desconectadas" (730 milhões de pessoas). Ver: WE ARE SOCIAL. *The changing world of digital in 2023*. 26 jan. 2023. Disponível em: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Acesso em 10 jul. 2023.

5. O relatório detalha que há variações, por exemplo, nos motivos pelos quais as pessoas usam a internet, nos tipos de sites visitados e aplicativos utilizados, e nos tipos de conteúdos adquiridos. Ver: WE ARE SOCIAL. *The changing world of digital in 2023*. 26 jan. 2023. Disponível em: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Acesso em 10 jul. 2023.

6. Um *proxy* atua como um intermediário entre o usuário e a internet, de modo que o endereço IP registrado na requisição de acesso é do *proxy*, ocultando o real endereço IP e localização do usuário. Há usuários que se valem do mecanismo para acessar conteúdos, como séries e filmes, que não estariam disponíveis ao país em que está localizado, por exemplo. Uma VPN possui proteção mais abrangente, criando rede criptografada que blinda amplamente o dispositivo. Ver: https://tecnoblog.net/responde/o-que-e-proxy-e-qual-a-diferenca-para-a-vpn/ e https://www.hostinger.com.br/tutoriais/servidor-proxy. Acesso em 14 jul. 2023.

volvem, mas não se limitam, a discurso de ódio, desinformação, *cyberbullying* e pornografia infantil[7].

A sensação de anonimato, no entanto, não é absolutamente verdadeira, na medida em que os usuários deixam rastros digitais e que tais rastros podem ser utilizados para identificar os responsáveis pela prática de ilícitos e submetê-los às medidas jurídicas cabíveis.

Ademais, a evolução tecnológica e o avanço da hiperconexão[8] viabilizam o desenvolvimento de modelos econômicos baseados na coleta, armazenamento e processamento de informações em larga escala, incluindo dados pessoais[9], e geram preocupações relativas a potenciais violações a direitos da personalidade[10].

No que tange especificamente aos dados, que possuem papel central na prestação dos serviços de internet, é sabido que as gigantes do mercado de tecnologia[11] possuem atuação internacional e optam por distribuir o armazenamento em servidores espalhados ao redor do mundo.

A Google, por exemplo informa operar vinte e quatro unidades de *data center*, espalhadas pela América do Norte (Estados Unidos), América do Sul (Chile), Europa (Irlanda, Países Baixos, Dinamarca, Finlândia, Bélgica) e Ásia (Japão, Singapura, Taiwan)[12]; a Meta cita vinte e uma unidades, sendo dezesse-

7. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional*: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, Janeiro-Abril, 2020, pp. 6-7. Disponível em: http://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em 25 jun. 2023.

8. "O termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento e tem desdobramentos importantes. Podemos citar alguns: o estado em que as pessoas estão conectadas a todo momento (always-on); a possibilidade de estar prontamente acessível (*readily accessible*); a riqueza de informações; a interatividade; o armazenamento ininterrupto de dados (*always recording*). O termo hiperconectividade está hoje atrelado às comunicações entre indivíduos (*person-to-person,* P2P), indivíduos e máquina (*human-to-machine,* H2M) e entre máquinas (*machine-to-machine,* M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, nesse contexto, um fluxo contínuo de informações e massiva produção de dados". MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018, p. 21. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/23898. Acesso em 12 jul. 2023.

9. BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em 26 jun. 2023.

10. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional*: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, Janeiro-Abril, 2020, p. 7. Disponível em: http://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em 25 jun. 2023.

11. As gigantes que dominam o mercado de tecnologia são Google, Apple, Meta (anteriormente denominada Facebook), Amazon e Microsoft, também conhecidas pelo acrônimo "GAFAM". Na China, as maiores empresas de tecnologia são referenciadas pelo acrônimo "BATX" (Baidu, Alibaba, Tencent e Xiaomi).

12. Disponível em: https://www.google.com/intl/pt-BR/about/datacenters/locations/. Acesso em 12 jul. 2023.

te na América do Norte (Estados Unidos), três na Europa (Irlanda, Dinamarca, Suécia) e uma na Ásia (Singapura)[13].

A definição dos locais de armazenamento está abarcada pela livre iniciativa, de acordo com o modelo de negócios escolhido[14]. Comumente, a decisão é orientada por questões financeiras (custos para manutenção, que variam inclusive em razão do clima do país[15]) e regulatórias (especialmente normas relativas à proteção de dados pessoais e sistemas tributários)[16].

No entanto, esse cenário traz consigo dilemas relacionados aos fluxos de dados que são ínsitos ao funcionamento da internet. Afinal, embora a internet tenha conceito aberto, imaterial e transfronteiriço, é certo que os Estados nacionais possuem fronteiras e regramentos próprios, que podem entrar em conflito e gerar consequências em termos de jurisdição e soberania. Guilherme Guidi e Francisco Rezek assim pontuam:

> Nosso Direito é contido, como o são também nossas instituições e procedimentos; nossa maneira de endereçar a realidade com um comando legal está intrinsecamente ligada ao território. Estados dividem-se em suas fronteiras, jurisdições se pretendem universais, mas são limitadas por outras igualmente vocacionadas, a "comunidade" internacional, conglomerado de Estados e Organizações aferradas a suas soberanias, tem um largo caminho a percorrer até atingir a mesma integração mundial que a Internet nos deu em pouco mais de duas décadas.[17]

Como ponderado por Paulo Brancher[18], há uma tendência global de regulação da proteção de dados pessoais e observa-se certo consenso sobre os

13. Disponível em: https://datacenters.atmeta.com/all-locations/. Acesso em 15 jul. 2023.

14. VAINZOF, Rony. *ADC 51 (STF) - Investigações cibernéticas transfronteiriças*. São Paulo, 28 set. 2022. LinkedIn: Rony Vainzof. Disponível em: https://www.linkedin.com/pulse/adc-51-stf-investiga%C3%A7%C3%B5es-cibern%C3%A9ticas-rony-vainzof/. Acesso em 25 jun. 2023.

15. Quanto maior a temperatura do local, maior a dificuldade (e, consequentemente, o custo) para resfriar os servidores. Por isso, a preferência por situar data centers em locais com clima ameno.

16. SANTA ROSA, Giovanni. *O que significa arquivar na nuvem? Onde ficam os principais servidores?* Tilt UOL. São Paulo, 01 mai. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/05/01/o-que-significa-arquivar-na-nuvem-onde-ficam-os-principais-servidores.htm. Acesso em 12 jul. 2023.

17. GUIDI, Guilherme Berti de Castro; REZEK, Francisco. *Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos*. Revista Brasileira de Políticas Públicas, Brasília, v. 8, n. 1, p. 276-288, 2018, p. 278. Disponível em: https://www.academia.edu/40247906/Crimes_na_internet_e_coopera%C3%A7%C3%A3o_internacional_em_mat%C3%A9ria_penal_entre_Brasil_e_Estados_Unidos. Acesso em 26 jun. 2023.

18. BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em 26 jun. 2023.

princípios que devem reger tal proteção; não obstante, em razão dos fluxos transfronteiriços de dados, é certo que indivíduos e entes privados podem estar sujeitos a regimes distintos e conflitos de leis, criando impasses jurídicos.

Uma das questões afetadas por esse contexto é a requisição de dados armazenados pelas empresas de tecnologia para fins de investigação de atos ilícitos praticados na internet.

2. Requisição de dados para fins de investigação de ilícitos: contexto brasileiro

2.1. As diretrizes do Marco Civil da Internet sobre armazenamento e fornecimento de dados

No Brasil, o Marco Civil da Internet (Lei n. 12.965/2014), dentre outros pontos, estabelece as diretrizes relativas ao armazenamento dos dados pelos provedores de serviços de internet (referenciados na lei como "provedores de conexão" e "provedores de aplicação") e à requisição dessas informações.

Pela lei, os provedores de conexão devem armazenar os registros de conexão (entendidos como "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados", na forma do art. 5º, VI) pelo prazo de um ano[19], ao passo que os provedores de aplicação devem armazenar os registros de acesso às aplicações (entendidos como "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP", na forma do art. 5º, VIII) pelo prazo de seis meses[20].

O fornecimento dos dados deve ser necessariamente precedido por ordem judicial[21-22]. Nos termos da lei, o pedido pode ser realizado pelo interessado em âmbito judicial, cível ou penal, em caráter incidental ou autônomo. Na oportunidade, o interessado deverá necessariamente demonstrar, sem prejuízo dos

19. Art. 13, *caput*, da Lei n. 12.965/2014.

20. Art. 15, *caput*, da Lei n. 12.965/2014.

21. Art. 10, § 1º, art. 13, § 5º, e art. 15, § 3º, da Lei n. 12.965/2014.

22. O art. 10, § 3º, da Lei n. 12.965/2014 estabelece que as autoridades administrativas que detenham competência legal podem requisitar acesso a dados cadastrais que informem qualificação pessoal, filiação e endereço, observados os requisitos previstos no art. 11 do Decreto n. 8.771/2016. Para que tenham acesso a outros dados além dos cadastrais, é necessário buscar a via judicial.

demais requisitos legais: (i) fundados indícios da ocorrência do ilícito, (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e (iii) período ao qual se referem os registros[23].

Com relação à obtenção de informações que impliquem quebra de sigilo telemático, o fornecimento está restrito ao contexto de investigação criminal ou instrução processual penal, nos termos da Constituição Federal (art. 5º, XII) e da Lei n. 9.296/1996.

Desde a entrada em vigor do Marco Civil da Internet, inúmeras requisições de dados passaram pelo Poder Judiciário brasileiro e logo começaram a surgir conflitos entre os interessados na obtenção dos dados e os provedores de serviços de internet.

Um dos pontos de grande discussão diz respeito à (im)possibilidade de exigir que a empresa subsidiária, localizada no Brasil, forneça dados armazenados pelas empresas de tecnologia em servidores no exterior. Em diversos processos, ao serem instadas ao fornecimento de dados, as subsidiárias brasileiras alegaram impossibilidade técnica de cumprir a determinação e suscitaram a necessidade de adoção de mecanismos de cooperação internacional para a obtenção da prova diretamente com a empresa-mãe.

No entanto, o argumento nem sempre foi acolhido pelo Poder Judiciário e as empresas de tecnologia temem a adoção de medidas gravosas, desde a fixação de multas que alcançam altos patamares até o bloqueio de plataformas e a decretação de prisão de dirigentes[24].

2.2. Requisição direta de dados vs. utilização de mecanismos de cooperação internacional

No decorrer das deliberações sobre o então projeto do Marco Civil da Internet (Projeto de Lei n. 2.126/2011), foi inserida disposição que obrigaria as empresas de tecnologia instaladas no Brasil a manter as bases de dados de usuários brasileiros em data centers localizados fisicamente no país. A previsão gerou controvérsia e críticas, especialmente por parte de representantes das empresas de tecnologia como Google e Facebook. Ao final, optou-se por retirar a previsão de obrigatoriedade de instalação de data centers em terri-

23. Art. 22, *caput* e parágrafo único, da Lei n. 12.965/2014.

24. O aplicativo WhatsApp foi alvo de determinações de bloqueio em 2014, 2015 e 2016, e o vice-presidente do Facebook na América Latina foi preso e solto no dia seguinte (Ver: https://www.conjur.com.br/2016-mai-02/juiz-determina-bloqueio-whatsapp-partir-14h-segunda. Acesso em 15.07.2023). Em 2023, foi determinado o bloqueio do Telegram (Ver: https://www.bbc.com/portuguese/articles/c25ewyqev32o. Acesso em 15 jul. 2023).

tório nacional e ajustar a redação para prever a necessidade de as empresas respeitarem a legislação brasileira[25].

A redação final do dispositivo, vigente até o momento atual, é a seguinte:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Como se vê, o art. 11 do Marco Civil da Internet estabelece que a legislação brasileira é aplicável quando ao menos uma operação de coleta, armazenamento, guarda e tratamento de dados ocorrer em território nacional. Note-se que o § 2º do dispositivo determina que a previsão do *caput* se aplica "mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil".

A redação do aludido dispositivo revela expressamente a lei aplicável aos dados, e não cria ou indica o procedimento adequado para acesso a tais dados. Não obstante, o dispositivo é comumente suscitado para embasar a possibi-

25. CANALTECH. *Marco Civil: Governo derruba obrigatoriedade de data centers no Brasil*. 19 mar. 2014. Disponível em: https://arquivo.canaltech.com.br/internet/Marco-Civil-governo-derruba-obrigatoriedade-de-data-centers-no-Brasil/. Acesso em 15 jul. 2023.

lidade de requisição direta das informações à empresa subsidiária brasileira, independentemente da localização do *data center*, em conjunto com argumentos relativos à soberania nacional.

Aos argumentos sobre a interpretação do art. 11 do Marco Civil da Internet e o respeito à soberania nacional, soma-se a importância de se ter agilidade nas investigações de atos ilícitos, em especial nos casos que envolvem provas digitais, dada a volatilidade e o risco de perecimento. Nesse contexto, a demora na obtenção das informações necessárias à evolução da investigação pode ser determinante para impossibilitar a identificação do autor do ilícito, e, consequentemente, obstaculizar a sua responsabilização (civil e/ou criminal).

De outro lado, argumenta-se que a requisição direta dos dados pode sujeitar as empresas de tecnologia a violações das leis vigentes no local de sua sede, notadamente as leis de proteção de dados, e que esse cenário afetaria os modelos de negócio das *big techs*[26]. Ademais, há o risco de criação de tensões entre os Estados nacionais e de competição entre sistemas normativos, além de potencialmente violar garantias processuais de titulares de dados e afastar investimentos ao país que não segue o caminho da cooperação[27].

As vozes contrárias à requisição direta dos dados pontuam a necessidade de utilização dos mecanismos de cooperação jurídica internacional, como as cartas rogatórias e acordos de assistência jurídica mútua, e que tais instrumentos são frequentemente desconsiderados em decisões judiciais.

Foi nesse contexto que a Federação das Associações das Empresas de Tecnologia da Informação – Assespro Nacional ajuizou Ação Declaratória de Constitucionalidade, objetivando o reconhecimento da constitucionalidade do Decreto n. 3.810/2001, que promulgou o Acordo de Assistência Judiciária em Matéria Penal (*Mutual Legal Assistance Treaty* – MLAT) entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, do art. 237, II, do Código de Processo Civil, e dos arts. 780 e 783 do Código de Processo Penal, e, como consequência, a aplicabilidade dos mecanismos de cooperação internacional previstos em tais dispositivos para a obtenção de conteúdo de comunicação privada sob o controle de provedores de aplicação sediados no exterior.

26. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional*: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, Janeiro-Abril, 2020, p. 24. Disponível em: http://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em 25 jun. 2023.

27. SOUZA, Carlos Affonso. *STF deve reconhecer acordo para acesso a dados no exterior*. JOTA. 13 abr. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/stf-deve-reconhecer-acordo-para-acesso-a-dados-no-exterior-13042021. Acesso em 30 nov. 2023.

Note-se que a discussão da ação envolvia primordialmente o procedimento para (i) obtenção de conteúdo de comunicações (ii) em âmbito de investigação penal[28]. No entanto, o debate sobre a requisição direta e a utilização de mecanismos de cooperação internacional também aparece no contexto da busca por dados cadastrais e registros eletrônicos (ou *logs*, entendidos como endereços IP, datas, horários e fusos horários de acessos de usuários a aplicações de internet), em âmbito cível, como se verifica em julgados do Tribunal de Justiça do Estado de São Paulo[29].

2.3. O julgamento da Ação Declaratória de Constitucionalidade n. 51

Com o ajuizamento da Ação Declaratória de Constitucionalidade, a Assespro Nacional objetivava o reconhecimento da constitucionalidade dos mecanismos de cooperação internacional previstos na legislação brasileira e, como consequência, a impossibilidade de requisição direta de dados, por parte das autoridades brasileiras, às subsidiárias das empresas de tecnologia localizadas no Brasil.

No decorrer do processo, foi admitida a inclusão de partes interessadas na qualidade de *amici curiae*: Facebook Serviços Online do Brasil Ltda., Yahoo do Brasil Internet Ltda., Instituto de Referência em Internet e Sociedade – Iris e

28. Na petição inicial, inclusive, a Assespro Nacional fez ponderações sobre o objeto da controvérsia, no seguinte sentido:
"A controvérsia judicial relevante está na discussão sobre a constitucionalidade e consequente aplicabilidade do Decreto nº 3.810/2001 e dos artigos 237, II do CPC, bem como dos artigos 780 e 783 do CPP, para a obtenção de conteúdo de comunicações que esteja sob controle de entidade localizada fora do território nacional.
53. Dessa forma, importante esclarecer que não se discute na presente ação a constitucionalidade e aplicação do referido complexo normativo nas seguintes hipóteses: a) obtenção de dados públicos; b) possibilidade de imposição de restrições, pela autoridade estrangeira, ao compartilhamento dos dados entregues para outras autoridades ou em outras investigações; e c) para a obtenção de dados cadastrais e registros de acesso ("IP logs") de usuários de serviços de provedoras de aplicativos de internet estabelecidas fora do Brasil, mediante requisição judicial."

29. BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2019215-93.2021.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravados: Engtelco Engenharia De Telecomunicações Ltda. e Anova Sistemas Ltda. – ME. São Paulo, SP, 13 de abril de 2021. Diário de Justiça Eletrônico, São Paulo-SP, 20 de abril de 2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14539761&cdForo=0. Acesso em 16 jul. 2023.
BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2047875-29.2023.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravada: U. S. V. I., C. e E. L. São Paulo, SP, 27 de junho de 2023. São Paulo-SP, Diário de Justiça Eletrônico, São Paulo-SP, 03 de julho de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16900023&cdForo=0. Acesso em 16 jul. 2023.
BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2270635-27.2019.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravada: Sule Ölmez. São Paulo, SP, 02 de junho de 2023. Diário de Justiça Eletrônico, São Paulo-SP, 09 de junho de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=13611389&cdForo=0. Acesso em 20 jul. 2023.
BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação nº 1015097-82.2021.8.26.0100. Apelante: Google Brasil Internet Ltda. Apeladas P. A. B. e outra. São Paulo, SP, 25 de outubro de 2022. Diário de Justiça Eletrônico, São Paulo-SP, 26 de outubro de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16181640&cdForo=0. Acesso em 20 jul. 2023.
BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação nº 1023988-53.2020.8.26.0577. Apelante: Google Brasil Internet Ltda. Apelados: Engtelco Engenharia De Telecomunicações Ltda. e Anova Sistemas Ltda. – ME. São Paulo, SP, 28 de setembro de 2021. Diário de Justiça Eletrônico, São Paulo-SP, 04 de outubro de 2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15058551&cdForo=0. Acesso em 20.07.2023.

Sociedade de Usuários de Tecnologia – Sucesu Nacional. Ainda, foi convocada audiência pública, que permitiu a manifestação de representantes de diversos entes, com diferentes pontos de vista, contribuindo amplamente com o debate[30].

Em 23 de fevereiro de 2023, o Supremo Tribunal Federal finalizou o julgamento da Ação Declaratória de Constitucionalidade n. 51. Os Ministros, por unanimidade, julgaram parcialmente procedente o pedido para declarar a constitucionalidade dos dispositivos indicados, bem como da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional.

No decorrer de seu voto[31], o Relator Ministro Gilmar Mendes fez referência ao movimento estratégico dos Estados nacionais de criar leis domésticas que pretendem obrigar as empresas de tecnologia a obedecer às determinações de seus Tribunais e considerou que o objeto intrínseco do art. 11 do Marco Civil da Internet é o de resguardar a soberania nacional.

Ainda, pontuou que o procedimento dos mecanismos de cooperação internacional é naturalmente moroso e costuma demorar meses ou anos, o que é especialmente preocupante quando se objetiva o fornecimento de dados, que podem não estar mais disponíveis quando do cumprimento da assistência mútua, conforme demonstram as estatísticas apresentadas pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça.

Note-se que as tensões entre Estados nacionais e a sujeição das empresas a possíveis violações de leis de proteção de dados no local da sede foram objeto de ponderações no decorrer do voto, assim como a relevância do sistema de cooperação jurídica internacional, o qual funciona adequadamente para outras matérias.

30. BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade n. 51. Ata de audiência pública sobre controle de dados de usuários por provedores de internet no exterior. Brasília, DF, 10 de fevereiro de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf. Acesso em 04 jul. 2023.

31. BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade n. 51. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - Assespro Nacional. Interessado: Presidente da República. Rel. Min. Gilmar Mendes. Brasília, DF, 23 de fevereiro de 2023. Diário da Justiça Eletrônico, Brasília-DF, 28 de abril de 2023. Pp. 16-50. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em 25 jun. 2023.

No entanto, pontuou-se que os baixos índices de efetividade – demonstrados nas estatísticas do DRCI/MJ – trazem graves consequências à apuração de crimes cometidos em ambiente virtual e ao dever do Estado e direito dos cidadãos brasileiros à segurança pública e à proteção de direitos fundamentais (arts. 5º e 144 da Constituição Federal).

Observa-se que, no decorrer do voto, o Ministro Relator considerou que o art. 11 do Marco Civil da Internet, que encontra respaldo no art. 18 da Convenção de Budapeste[32]-[33], constitui norma específica em relação às regras do MLAT, das cartas rogatórias e da cooperação jurídica internacional, e está em consonância com atuais diplomas normativos sobre o tema.

Assim, concluiu-se que (i) o art. 11 do Marco Civil da Internet e o art. 18 da Convenção de Budapeste podem ser aplicados para a solicitação de dados, registros e comunicações eletrônicas relativas a atos praticados em território nacional, e (ii) fora das hipóteses previstas no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste, o instrumento cabível é o da cooperação jurídica internacional e pelas regras das cartas rogatórias, reconhecendo-se a constitucionalidade dos dispositivos do MLAT, do Código de Processo Civil e do Código de Processo Penal.

3. Estratégias de territorialização do ciberespaço e perspectivas para a matéria

No contexto da Ação Declaratória de Constitucionalidade n. 51, o próprio Relator Ministro Gilmar Mendes ponderou que a decisão do Supremo Tribunal Federal não encerraria definitivamente os debates sobre a legitimidade da jurisdição brasileira nos casos de compartilhamento transnacional de dados,

32. Convenção promulgada pelo Decreto n. 11.491, de 12 de abril de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em 25 jun. 2023.

33. Artigo 18 - Ordem de exibição
1. Cada Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a autoridades competentes para ordenar:
a. a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador;
b. a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor.
2. Os poderes e procedimentos referidos neste artigo estão sujeitos aos Artigos 14 e 15.
3. Paras os fins deste Artigo, o termo "informações cadastrais do assinante" indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:
a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço;
b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço.
c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.

especialmente considerando o crescimento exponencial dos crimes cibernéticos nos últimos anos[34].

Com isso, determinou-se o envio da decisão ao Poder Legislativo e ao Poder Executivo, para a adoção das providências necessárias ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal) e de novos acordos bilaterais ou multilaterais para a obtenção de dados e comunicações eletrônicas.

Embora estratégias de territorialização da rede com edição de leis nacionais sejam observadas[35], bem como a aplicação de medidas coercitivas gravosas para pressionar o cumprimento de ordens judiciais por parte de *big techs*, verifica-se que tais medidas individualizadas não são capazes de resolver os dilemas; pelo contrário, contribuem para o aumento dos desafios jurídicos.

Do ponto de vista das grandes empresas de tecnologia, comumente há situação de impasse sobre qual legislação ou decisão judicial cumprir, ensejando potencial cumprimento seletivo de obrigações. Do ponto de vista dos interessados na obtenção de dados, a investigação de ilícitos é prejudicada e, com isso, as vítimas dos ilícitos têm seus direitos (inclusive fundamentais) afetados.

Nesse sentido, o relatório de status global “Internet e Jurisdição”:

> Os comentários apresentados pelos especialistas consultados salientaram uma opinião amplamente defendida segundo a qual a combinação de três fatores tornará cada vez mais graves os desafios jurídicos transfronteiriços na Internet:
> 1. O mundo está cada vez mais interligado através da Internet, aumentando, assim, a diversidade on-line;
> 2. A Internet está afetando profundamente as sociedades e as economias, o que significa que as apostas são altas; e
> 3. Os Estados-nações com visões diferentes procuram aumentar seu controle sobre a Internet, principalmente através da utilização de instrumentos nacionais, em vez de cooperação e coordenação transnacionais.

34. BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade n. 51. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - Assespro Nacional. Interessado: Presidente da República. Rel. Min. Gilmar Mendes. Brasília, DF, 23 de fevereiro de 2023. Diário da Justiça Eletrônico, Brasília-DF, 28 de abril de 2023. P. 31. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em 25 jun. 2023.

35. BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em 26 jun. 2023.

> Como apontou um especialista consultado, nisso tudo, a Internet não é o problema nem a causa do problema. Ao contrário, a Internet é a vítima.[36]

Nesse sentido, Guilherme Guidi e Francisco Rezek apontam como sugestões o refino de práticas e a abrangência da cooperação jurídica internacional, como forma de favorecer a integração entre os Estados e a distribuição de justiça pelo Poder Judiciário[37].

Para Paulo Brancher, mostra-se crucial que os modelos de proteção de dados se articulem entre si, e que a cooperação internacional – do ponto de vista prático (por meio de novos mecanismos) e do ponto de vista teórico (por meio de grupos de estudo e trocas de informações) – tende a contribuir para a padronização de legislações de proteção de dados ao redor do mundo e a diminuição de conflitos entre leis com previsões incompatíveis[38].

Cumpre observar que, recentemente, a Convenção de Budapeste foi promulgada no Brasil por meio do Decreto n. 11.491, de 12 de abril de 2023, incorporando-a ao ordenamento jurídico pátrio. A referida Convenção inaugura novas previsões sobre a cooperação jurídica internacional para a obtenção de provas digitais e tem o potencial de tornar o procedimento mais ágil e eficiente[39].

Enquanto o cenário de baixo grau de alinhamento entre as legislações nacionais se perpetua, nota-se que as *big techs* não se limitam a meros sujeitos passivos de comandos estabelecidos em leis e decisões judiciais ao redor do mundo, e acabam assumindo verdadeiras funções de legislar e decidir.

36. COMITÊ GESTOR DA INTERNET NO BRASIL. Internet & jurisdição: relatório de status global 2019 [livro eletrônico] / Dan Jerker B. Svantesson; [editor] Núcleo de Informação e Coordenação do Ponto BR; tradução Ana Zuleika Pinheiro Machado. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020, pp. 75-76. Disponível em: https://www.cgi.br/publicacao/cadernos-cgi-br-internet-jurisdicao-6-1/. Acesso em 15 jul. 2023.

37. GUIDI, Guilherme Berti de Castro; REZEK, Francisco. *Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos*. Revista Brasileira de Políticas Públicas, Brasília, v. 8, n. 1, p. 276-288, 2018, p. 287. Disponível em: https://www.academia.edu/40247906/Crimes_na_internet_e_coopera%C3%A7%C3%A3o_internacional_em_mat%C3%A9ria_penal_entre_Brasil_e_Estados_Unidos. Acesso em 26 jun. 2023.

38. BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em 26 jun. 2023.

39. MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. *A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?*. Boletim IBCCRIM, 31(368), julho de 2023, pp. 15-16. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em 20 jul. 2023.

O desenvolvimento tecnológico é muito mais veloz do que qualquer debate legislativo e consolidação de interpretações pelos tribunais. Com isso, os termos de uso e políticas das plataformas assumem função normativa, e as decisões tomadas com base nesses regulamentos geram impactos diretos no exercício de direitos de seus usuários[40]-[41].

Considerações finais

O julgamento da Ação Declaratória de Constitucionalidade n. 51 representa um importante marco para a discussão sobre a requisição de dados para fins de investigação de ilícitos. No entanto, não é suficiente, por si só, para resolver os dilemas sobre a matéria de forma definitiva.

A temática da requisição de dados para investigação de ilícitos revela-se complexa e abrangente. Há a perspectiva de que autoridades e vítimas de ilícitos continuem a enfrentar empecilhos à obtenção de provas digitais – desde dados cadastrais e registros eletrônicos até conteúdos de comunicações.

Para alcançar melhorias nesse cenário, vê-se que as estratégias de territorialização da rede com edição de leis nacionais e a aplicação de medidas coercitivas gravosas para pressionar o cumprimento de ordens judiciais por parte de *big techs* não são eficientes.

Assim, é crucial que haja (i) evolução no diálogo e engajamento colaborativo entre os atores envolvidos, com ações coordenadas entre Estados nacionais, empresas de tecnologia e a sociedade civil; (ii) cooperação internacional eficaz; e (iii) aprimoramento constante das legislações, buscando a coordenação e coerência entre elas. Tais providências são relevantes para assegurar a proteção dos direitos dos usuários sem comprometer investigações legítimas e repressão de práticas ilícitas online, fomentando o equilíbrio entre a proteção da privacidade dos usuários e a efetivação da justiça.

40. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional*: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, Janeiro-Abril, 2020, pp. 14-15. Disponível em: http://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em 25 jun. 2023.

41. Com relação à temática de requisições e fornecimento de dados, a partir dos relatórios de transparência, verifica-se o seguinte: a Google indica que as solicitações são analisadas com cautela e que podem restringir ou contestar a divulgação dos dados, a depender do caso. No período de julho de 2022 a dezembro de 2022, registrou 12.773 solicitações oriundas do Brasil, relacionadas a 50.103 contas, sendo que 68% das solicitações teriam resultado em fornecimento de dados (Disponível em: https://transparencyreport.google.com/user-data/overview?hl=pt_BR&user_requests_report_period=series:requests,accounts;authority:BR;time:2022H2&lu=dlr_requests&dlr_requests=authority:BR;assisting_country:;time. Acesso em 16 jul. 2023.). A Meta afirma possuir equipe dedicada a analisar os requerimentos, de modo a garantir que são consistentes com a lei aplicável e com suas políticas. No período de julho de 2022 a dezembro de 2022, registrou 17.421 requerimentos oriundos do Brasil, relacionados a 63.355 usuários/contas, sendo que em 78,57% foram apresentados alguns dados (Disponível em: https://transparency.fb.com/data/government-data-requests/country/BR/. Acesso em 16 jul. 2023.).

Referências

BRANCHER, Paulo Marcos Rodrigues. *Proteção internacional de dados pessoais*. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em 26 jun. 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 15 jul. 2023.

BRASIL. *Decreto n. 3.810, de 2 de maio de 2001*. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em 04 jul. 2023.

BRASIL. *Decreto n. 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em 14 jul. 2023.

BRASIL. *Decreto n. 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em 25 jun. 2023.

BRASIL. *Lei n. 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em 15 jul. 2023.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 24 jun. 2023.

BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade n. 51. Ata de audiência pública sobre controle de dados de usuários por provedores de internet no exterior. Brasília, DF, 10 de fevereiro de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf. Acesso em 04 jul. 2023.

BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade n. 51. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - Assespro Nacional. Interessado: Presidente da República. Rel. Min. Gilmar Mendes. Brasília, DF, 23 de fevereiro de 2023. Diário da Justiça Eletrônico, Brasília-DF, 28 de abril de 2023. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em 25 jun. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2019215-93.2021.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravados: Engtelco Engenharia De Telecomunicações Ltda. e Anova Sistemas Ltda. – ME. São Paulo, SP, 13 de abril de 2021. Diário de Justiça Eletrônico, São Paulo-SP, 20 de abril de 2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14539761&cdForo=0. Acesso em 16 jul. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2047875-29.2023.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravada: U. S. V. I., C. e E. L. São

Paulo, SP, 27 de junho de 2023. São Paulo-SP, Diário de Justiça Eletrônico, São Paulo-SP, 03 de julho de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16900023&cdForo=0. Acesso em 16 jul. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Agravo de Instrumento nº 2270635-27.2019.8.26.0000. Agravante: Google Brasil Internet Ltda. Agravada: Sule Ölmez. São Paulo, SP, 02 de junho de 2023. Diário de Justiça Eletrônico, São Paulo-SP, 09 de junho de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=13611389&cdForo=0. Acesso em 20 jul. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação nº 1015097-82.2021.8.26.0100. Apelante: Google Brasil Internet Ltda. Apeladas P. A. B. e outra. São Paulo, SP, 25 de outubro de 2022. Diário de Justiça Eletrônico, São Paulo-SP, 26 de outubro de 2023. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16181640&cdForo=0. Acesso em 20 jul. 2023.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Apelação nº 1023988-53.2020.8.26.0577. Apelante: Google Brasil Internet Ltda. Apelados: Engtelco Engenharia De Telecomunicações Ltda. e Anova Sistemas Ltda. – ME. São Paulo, SP, 28 de setembro de 2021. Diário de Justiça Eletrônico, São Paulo-SP, 04 de outubro de 2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15058551&cdForo=0. Acesso em 20.07.2023.

CANALTECH. *Marco Civil: Governo derruba obrigatoriedade de data centers no Brasil*. Franca, 19 mar. 2014. Disponível em: https://arquivo.canaltech.com.br/internet/Marco-Civil-governo-derruba-obrigatoriedade-de-data-centers-no-Brasil/. Acesso em 15 jul. 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL. *Internet & jurisdição*: relatório de status global 2019 [livro eletrônico] / Dan Jerker B. Svantesson; [editor] Núcleo de Informação e Coordenação do Ponto BR; tradução Ana Zuleika Pinheiro Machado. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://www.cgi.br/publicacao/cadernos-cgi-br-internet-jurisdicao-6-1/. Acesso em 15 jul. 2023.

GUIDI, Guilherme Berti de Castro; REZEK, Francisco. *Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos*. Revista Brasileira de Políticas Públicas, Brasília, v. 8, n. 1, p. 276-288, 2018. Disponível em: https://www.academia.edu/40247906/Crimes_na_internet_e_cooperа%C3%A7%C3%A3o_internacional_em_mat%C3%A9ria_penal_entre_Brasil_e_Estados_Unidos. Acesso em 26 jun. 2023.

MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/23898. Acesso em 12 jul. 2023.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. *Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro*. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, Janeiro-Abril, 2020. Disponível em: http://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103/2571. Acesso em 25 jun. 2023.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. *A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?*. Boletim IBCCRIM, 31(368), julho de 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em 20 jul. 2023.

SANTA ROSA, Giovanni. *O que significa arquivar na nuvem? Onde ficam os principais servidores?* Tilt UOL. São Paulo, 01 mai. 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/05/01/o-que-significa-arquivar-na-nuvem-onde-ficam-os-principais-servidores.htm. Acesso em 12 jul. 2023.

SOUZA, Carlos Affonso. *STF deve reconhecer acordo para acesso a dados no exterior*. Jota. São Paulo, 13 abr. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/stf-deve-reconhecer-acordo-para-acesso-a-dados-no-exterior-13042021. Acesso em 30 nov. 2023.

VAINZOF, Rony. *ADC 51 (STF) - Investigações cibernéticas transfronteiriças*. São Paulo, 28 set. 2022. LinkedIn: Rony Vainzof. Disponível em: https://www.linkedin.com/pulse/adc-51-stf-investiga%C3%A7%C3%B5es-cibern%C3%A9ticas-rony-vainzof/. Acesso em 25 jun. 2023.

WE ARE SOCIAL. *The changing world of digital in 2023*. 26 jan. 2023. Disponível em: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Acesso em 10 jul. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

A proteção e transferência internacional de dados nos tratados de livre comércio

JULIANA ADÃO ALVES

JULIANA ADÃO ALVES[1]

Sumário: Introdução. 1. A globalização e a necessidade da proteção de dados. 2. Modelos de regulação de transferências internacionais de dados. 3.1 Os fluxos de dados no comércio internacional. 3.2 Tipos de cláusulas sobre proteção e transferência de dados em acordos comerciais. 3.3 O alcance da interoperabilidade com a inserção das cláusulas. Considerações finais. Referências.

Introdução

Na última década, vimos o fluxo de informação transfronteiriço aumentar significativamente. Entre 2010 e 2020, o volume de dados a nível mundial cresceu quase 5.000%[2], sendo grande parte desses dados transferidos entre os países. O aumento da fluidez nas comunicações e no comércio tem impactos positivos no desenvolvimento econômico, mas também pode ter consequências prejudiciais, devendo ser regulado.

Essa regulação ocorre principalmente de forma interna, com cada país promulgando leis e normativas sobre a regulação da internet e proteção de dados. Contudo, questiona-se: de que forma os países poderão controlar os fluxos de importação e exportação de dados, se suas legislações não tiverem um alcance extraterritorial?

O presente estudo pretende analisar uma das opções de regulação internacional da proteção e transferência de dados: os acordos de comércio. No primeiro capítulo, busca-se relacionar a globalização com o aumento dos fluxos transfronteiriços de dados para a operabilidade de negócios oferecidos mundialmente e analisar a necessidade de uma uniformidade legal sobre o tema.

No segundo capítulo, serão abordados os diferentes modelos de regulação de transferência internacional de dados, com uma análise mais profunda de duas perspectivas: da primazia dos fluxos de dados em prol do comércio internacional e da proteção de dados como um direito fundamental que não pode ser prejudicado.

1. Advogada. Graduada em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Mestranda em Integração e Comércio Internacional pela Universidade de Montevidéu, Uruguai. Pós-graduanda em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ. Atualmente, é assessora jurídica na *fintech* dLocal.

2. PRESS, Gil. *54 Predictions About The State Of Data In 2021*. Forbes, 30 Dez. 2020. Disponível em <https://www.forbes.com/sites/gilpress/2021/12/30/54-predictions-about-the-state-of-data-in-2021/?sh=68be34ef397d>. Acesso em 23 jul. 2023.

No terceiro capítulo, será analisado o aspecto regulatório do comércio internacional, através de instrumentos como os Tratados de Livre Comércio (TLC). Nos TLC foram inseridas cláusulas que mencionam a proteção e transferência de dados entre as partes do acordo, podendo ser mais amplas ou específicas e restringir o fluxo de dados ou permiti-lo. Neste capítulo, serão exploradas também as perspectivas de importantes atores da economia digital, como os Estados Unidos, União Europeia e China, além de incluir uma análise do caso do Brasil. Também será ponderado se a inclusão desses dispositivos em acordos comerciais cumpre uma função de uniformizar e harmonizar a proteção de dados.

1. A globalização e a necessidade da proteção de dados pessoais.

No mundo interconectado em que vivemos, a coleta de dados pessoais é muitas vezes essencial para o funcionamento de diversos serviços públicos e privados. Embora o titular dos dados possa negar seu uso, essa recusa o colocaria à margem, criando barreiras na dinâmica social[3]. Em outras palavras, é impraticável evitar de forma completa a coleta e o tratamento de dados pessoais, já que impossibilitaria a realização de transações financeiras, o comércio *online* e até mesmo determinados serviços médicos, para citar alguns exemplos.

Ademais, deve-se agregar à fórmula a dimensão extraterritorial da proteção de dados. Na maioria dos casos, os servidores destinados ao armazenamento desses dados estão localizados no exterior, e não no país em que os dados são coletados, sendo necessário o seu deslocamento[4]. Nesse processo se abre uma lacuna: a proteção recebida no país de origem é garantida no destino?

Apesar de ser tratada pelos ordenamentos jurídicos internos – em alguns de forma mais exaustiva do que outros –, não é possível lidar com a proteção de dados apenas de uma perspectiva local, não sendo suficiente o anteparo muitas vezes limitado das legislações nacionais[5]. A eficácia da proteção dos

3. DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*. p. 182.

4. FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. *E-book*. p. 632.

5. DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*. p. 257.

dados pessoais depende de uma reciprocidade existente entre os países de origem e destino.

A criação de um padrão internacional de regulação da proteção de dados é uma resposta rápida a essa questão, mas acaba entrando em conflito com o desenvolvimento econômico e tecnológico, fundamento previsto no art. 2º, V, da Lei Geral de Proteção de Dados brasileira (LGPD). Esse conflito ocorre porque tampouco se almeja uma restrição às transferências internacionais de dados, visto que o comércio mundial depende desse processo[6].

Nota-se uma confluência das diferentes legislações existentes sobre regulação e proteção de dados[7], principalmente entre países do norte global, que possuem grande interesse em manter firmes os fluxos comerciais.

2. Modelos de regulação de transferências internacionais de dados

É possível identificar três modelos de transferência internacional de dados: fluxo livre, em que a transmissão é ilimitada (podendo haver exceções); quando o país obriga o outro a manter os padrões domésticos de proteção, através de disposições contratuais; e o modelo híbrido, que funciona com um fluxo livre condicionado, em que a transferência de dados é liberada apenas para outros países considerados com um nível adequado de regulação.

Contudo, dois importantes *players* no cenário internacional chamam a atenção por se encontrarem diametralmente opostos no plano dos modelos de regulação: Estados Unidos (EUA) e União Europeia. Enquanto no modelo americano há a predominância da livre circulação de bens e serviços, devendo ser a proteção de dados pessoais adaptável a esse fim, e restrições consideradas prejudiciais, para a União Europeia a concepção do direito a proteção de dados como um direito humano fundamental prevalece e é condição substancial para a existência de fluxos comerciais[8].

Os EUA permitem um fluxo livre de dados, porque consideram o direito à proteção de dados como um direito do consumidor, podendo a Agência de

6. FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. *E-book*. p. 633.

7. DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*. p. 257.

8. GUEIROS, Pedro. Tratados e Acordos para Transferências Internacionais de Dados. Rio de Janeiro: ITS, 2023. Disponível em <https://itsrio.org/pt/publicacoes/tratados-e-acordos-para-transferencias-internacionais-de-dados/>. Acesso em 18 jul. 2023.

Segurança Nacional (NSA) solicitar os dados de nacionais e estrangeiros. Já a União Europeia permite transferências internacionais "com base em uma decisão de adequação"[9], ou seja, apenas com países considerados apropriados pela Comissão Europeia, que tem a competência de determinar, revisar ou revogar decisões sobre a adequação de um país para transacionar dados.

Quando ocorre o fluxo livre entre dois países estes consideram que os dados de seus nacionais estarão protegidos da mesma forma. Em seu art. 45, o RGPD se utiliza de três parâmetros básicos para que um país seja considerado adequado: o primado do Estado de Direito; a existência de autoridade independente de proteção de dados; e a assunção de compromissos internacionais quanto à proteção de dados.

Apesar de haver uma decisão da Comissão Europeia que considerava os Estados Unidos como um país adequado, datada de 2000, dentro do escopo da Diretiva 95/46/CE e do acordo *Safe Harbour*, essa decisão foi invalidada em 2015 pela Corte de Justiça da União Europeia (CJUE), após ação judicial movida pelo austríaco Maximillian Schrems. O caso, conhecido como *Schrems I*[10], demonstrou que os dados dos nacionais europeus não recebiam a mesma proteção garantida pela legislação europeia ao serem tratados nos EUA.

No ano seguinte, em 2016, foi celebrado um novo acordo sobre proteção de dados, o *EU-US Privacy Shield*. Contudo, em 2020, a decisão de adequação da Comissão Europeia foi invalidada pela CJUE, em caso nomeado *Schrems II*[11], e fundamentado de forma similar ao anterior. Em 2022 foi anunciado o *Trans-Atlantic Data Privacy Framework*[12] como o novo esforço entre a União Europeia e os EUA de dirimir as preocupações levantadas pela CJUE nos julgamentos antecedentes. Em 10 de julho de 2023, a Comissão Europeia adotou uma decisão de adequação para esse último acordo, permitindo novamente o fluxo livre de dados entre UE e EUA[13].

9. União Europeia, art. 45, Regulamento Geral de Proteção de Dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em 18 jul. 2023.

10. Corte de Justiça da União Europeia, Decisão de 6 de outubro de 2015. Disponível em <https://curia.europa.eu/jcms/jcms/P_180250/>. Acesso em 18 jul. 2023.

11. Corte de Justiça da União Europeia, Decisão de 16 de julho de 2020. Disponível em <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>. Acesso em 23 jul. 2023.

12. *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*. The White House, 25 mar. 2022. Disponível em <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>. Acesso em 18 jul. 2023.

13. Comissão Europeia. *Commercial sector: adequacy decision on the EU-US Data Privacy Framework*. 10 jul. 2023. Disponível em <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en>. Acesso em 18 jul. 2023.

Em virtude das interrupções causadas pelas revogações das decisões de adequação, o fluxo comercial entre os países é afetado, já que muitos serviços dos Estados Unidos dependem da transferência dos dados europeus, e acabam sofrendo restrições ou proibições. Quando não há decisão de adequação, devem ser inseridas cláusulas contratuais para garantir a proteção dos dados europeus. Portanto, ao ocorrer uma decisão negativa, os contratos devem ser revistos, gerando uma pausa no fluxo comercial.

É possível também perceber com a trajetória de acordos entre EUA e UE que há certa maleabilidade nos padrões de proteção, dependendo de quem for a outra parte contratante. Os critérios europeus de proteção, notoriamente mais rígidos que os norte-americanos, acabaram sendo flexibilizados, devido às pressões econômicas[14]. Contudo, tal flexibilização acaba não sendo aplicável a acordos com outros países, já que os acordos mencionados são bilaterais, e não envolvem terceiros.

O Uruguai, país incluído na lista de adequação da Comissão Europeia, também estabelece que transferências internacionais de dados apenas poderão ocorrer a países considerados adequados pela Unidade Reguladora e de Controle de Dados Pessoais (URCDP)[15]. A URCDP vinculou sua lista de países considerados adequados à lista da União Europeia ao determinar que "se encontram compreendidos os países membros da União Europeia e aqueles que a Comissão Europeia considere que garantem as condições [antes] indicadas"[16].

Essa regra se repetiu nas resoluções de adequação da URCDP posteriores[17], que também acompanharam a inclusão e exclusão dos EUA da lista europeia, fazendo com que a última resolução, No. 23/021[18], estabelecesse um período de seis meses para a adequação de empresas norte-americanas aos critérios de exceção da lei uruguaia[19] (i.e., verificação de alguma exceção da lista do art. 23 da lei de proteção de dados uruguaia; obtenção de uma auto-

14. FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. *E-book*. p. 648.

15. Uruguai. Art. 23, Lei 18.331 de 2008. Disponível em <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em 18 jul. 2023.

16. Tradução livre. URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 17/009. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-17009>. Acesso em 18 jul. 2023.

17. URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 04/019. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-4019>. Acesso em 18 jul. 2023.

18. URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 23/021. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021>. Acesso em 18 jul. 2023.

19. ORDIOZOLA, José Miguel. *Las transferencias internacionales de datos personales desde Uruguay, tras la resolución No. 23/021 de la URCDP*. Revista CADE No. 60, 2022. pp. 83-89.

rização da URCDP ao oferecer garantias contratuais apropriadas; ou realizar uma Avaliação de Impacto[20]). A URCDP ainda não emitiu uma nova resolução que considere a última decisão de adequação dos EUA pela Comissão Europeia.

A LGPD adota um modelo similar ao europeu, mas com algumas diferenças significativas. Em seu art. 33, inciso I, estão permitidas as transferências internacionais de dados "para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei", devendo a Autoridade Nacional determinar essa adequação através de parâmetros previstos na própria lei. Contudo, também é possível identificar outros dois regimes: através de garantias privadas de cumprimento, como, por exemplo, cláusulas contratuais, normas corporativas globais, ou selos[21]; e um regime autorizativo, com derrogações específicas, listadas nos incisos III a IX do art. 33, a fim de promover algum interesse público. A existência desses três regimes aponta a proteção de dados também como a proteção de um direito fundamental, o que requere uma ponderação mais acentuada ao tema e sua aplicação[22].

Ao levar a proteção de dados a esse patamar, a LGPD prioriza que seus princípios de proteção devam ser encontrados no ordenamento jurídico do outro país, não sendo necessária a existência de regulação similar[23]. Dessa forma, a lei brasileira busca um efeito extraterritorial de forma mais flexível e ampla, sem a necessidade de uma análise minuciosa, tentando garantir um equilíbrio entre a proteção de dados e a facilitação de serviços e do comércio internacional. A existência de salvaguardas adicionais evidencia um empenho por uma "assimilação funcional" entre a lei brasileira e os ordenamentos estrangeiros, podendo ser considerada uma abordagem mais eficaz de aplicação[24].

A busca por uma eficácia transnacional da LGPD evidencia o ponto de conflito encontrado entre a proteção de direitos fundamentais e o fluxo comercial, sendo o principal objetivo a interoperabilidade dos mecanismos de proteção

20. URUGUAI. Art. 6, Decreto No. 64/020. Disponível em <https://www.impo.com.uy/bases/decretos/64-2020>. Acesso em 18 jul. 2023.

21. Art. 33, II, LGPD.

22. PRATA DE CARVALHO, Angelo. Transferência internacional de dados na Lei geral de proteção de dados – Força normativa e efetividade diante do cenário transnacional. p. 621-645. In: FRAZÃO, Ana. TEPEDINO, Gustavo. DONATO OLIVA, Milena. A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2019.

23. *Ibidem*.

24. POLIDO, Fabrício B. P. Transferência internacional de dados e 'lei aplicável mais favorável'. JOTA, 14 Ago. 2022. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/transferencia-internacional-de-dados-e-lei-aplicavel-mais-favoravel-14082022>. Acesso em 18 jul. 2023.

dos diversos ordenamentos jurídicos[25], a fim de que as ferramentas internas tenham alcance em outras jurisdições. Em vista da existência de países com graus de proteção diferentes, a regulação das transferências internacionais de dados tem se afastado de regulamentos específicos sobre proteção de dados, como os celebrados entre EUA e UE, por exemplo, e encontrado espaço em acordos comerciais[26].

No próximo capítulo será analisado como as transferências internacionais de dados são reguladas nos acordos comerciais, os tipos de cláusulas, e, por fim, se essas cláusulas garantem que os dados dos titulares sejam protegidos ao mesmo tempo que sejam oferecidos serviços e produtos ao redor do globo.

3.1 Os fluxos de dados no comércio internacional

Assim como ocorre com as transferências internacionais de dados, para que o comércio mundial tenha impactos positivos e estimule o desenvolvimento econômico, mostra-se necessária uma regulação a nível internacional[27]. Uma das formas de regular o comércio internacional é através de acordos de comércio, sejam bilaterais, regionais ou multilaterais. Esses acordos fornecem segurança e previsibilidade aos participantes dos fluxos comerciais.

Com o aumento da complexidade dos negócios, acordos que originalmente regulavam o livre comércio de produtos e serviços começaram a regular também a propriedade intelectual, o desenvolvimento sustentável, a migração e a proteção de dados, dentre outras matérias. Na economia digital, o oferecimento de um serviço internacionalmente depende do acesso a dados. O desequilíbrio entre a proteção e o fluxo de dados podem gerar impactos sérios tanto para a defesa de um direito fundamental quanto para o desenvolvimento do comércio, conforme explicitado anteriormente.

A Organização Mundial do Comércio (OMC) primeiro mencionou o comércio eletrônico em 1998, com a Declaração Mundial de Comércio Eletrônico[28], e em seguida com a criação de um Grupo de Trabalho[29] sobre o tema. Contudo,

25. GUEIROS, Pedro. Tratados e Acordos para Transferências Internacionais de Dados. Rio de Janeiro: ITS, 2023. Disponível em <https://itsrio.org/pt/publicacoes/tratados-e-acordos-para-transferencias-internacionais-de-dados/>. Acesso em 18 jul. 2023.

26. *Ibidem*.

27. VAN DEN BOSSCHE, Peter. PRÉVOST, Denise. *WTO Law in a nutshell*. Maastricht University, 2008. p. 3.

28. OMC. Declaração Ministerial. *The Geneva Ministerial Declaration on global electronic commerce*. 25 maio. 1998. Disponível em <https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm>. Acesso em 18 jul. 2023.

29. OMC. Grupo de Trabalho. *Work Programme on E-Commerce*. Disponível em <https://www.wto.org/english/tratop_e/

não houve avanços significativos e as regras do sistema multilateral de comércio foram consideradas ultrapassadas para tratar a matéria[30]. Apenas em 2019 o tópico foi retomado, com a Iniciativa Conjunta de Comércio Eletrônico[31].

Por outro lado, a estagnação das regras do sistema multilateral trouxe as temáticas do comércio eletrônico, como a proteção de dados, aos acordos bilaterais e regionais de comércio, que tem demonstrado maior capacidade para inovação[32]. As restrições ao fluxo de dados geram muitos conflitos comerciais, e esses acordos são uma forma de harmonizar as medidas e estabelecer princípios comuns entre membros da OMC[33].

3.2 Tipos de cláusulas sobre proteção e transferência de dados em acordos comerciais.

As cláusulas sobre proteção e transferência de dados presentes em Tratados de Livre Comércio (TLC) tentam combater dois tipos de obstáculos ao comércio digital: as restrições no fluxo de dados e as obrigações de localização forçada. As restrições aos fluxos de dados seriam medidas que impedem tanto a importação quanto a exportação de dados, sendo prejudiciais tanto às empresas nacionais quanto estrangeiras. Já as obrigações de localização forçada condicionam a operação a ter um estabelecimento ou instalação no país, o que gera um custo maior às empresas estrangeiras, que teriam que se domiciliar, para estarem submetidas às leis locais de proteção de dados.

Como as restrições no fluxo de dados seriam direcionadas a determinados países em que não seria permitido o fluxo, esse controle estaria infringindo o Princípio da Nação Mais Favorecida[34] do Acordo Geral de Tarifas e Comércio da OMC (conhecido por sua sigla em inglês, GATT), enquanto as obrigações de localização forçada violariam o Princípio do Tratamento Nacional[35], já que

---

ecom_e/ecom_work_programme_e.htm>. Acesso em 18 jul. 2023.

30. WU, M. Digital *Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*. RTA Exchange. Genebra: *International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB)*, 2017. Disponível em <https://unov.tind.io/record/67136?ln=es>. Acesso em 18 jul. 2023.

31. OMC. *Joint Initiative on E-commerce*. Disponível em <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm>. Acesso em 18 jul. 2023.

32. WU, M. *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB)*, 2017. Disponível em <https://unov.tind.io/record/67136?ln=es>. Acesso em 18 jul. 2023.

33. *Ibidem*.

34. Art. I, GATT.

35. Art. III, GATT.

acabariam afetando mais as empresas estrangeiras que desejam operar no país[36].

Os TLC podem mencionar a proteção e transferência de dados de forma mais simples ou complexa, abordando além destes dois temas a obrigatoriedade da localização forçada das empresas e a inovação no setor. O Tratado de Livre Comércio entre os Estados Unidos e a Coreia do Sul, por exemplo, apesar de ter um capítulo inteiro dedicado ao comércio eletrônico, possui apenas uma cláusula breve sobre o fluxo internacional de informação. Nesta cláusula, é reconhecida a importância do fluxo livre para o comércio e da proteção de dados pessoais, mas determina – de forma não vinculante – que ambos os países não imponham barreiras desnecessárias ao fluxo comercial[37].

Já o TLC celebrado entre o México e Panamá, apesar de também tratar a transferência internacional de dados em uma única cláusula, o faz de forma vinculante, determinando que a transferência deverá ser realizada "de acordo com a legislação aplicável sobre a proteção de dados pessoais e levando em conta as práticas internacionais"[38].

É importante mencionar também as disposições do Tratado de Associação Transpacífico (TPP), o maior acordo regional realizado de forma independente da OMC. Apesar dos Estados Unidos terem se retirado em 2017, o acordo, agora conhecido como CPTPP[39], em seu capítulo sobre o comércio eletrônico possui uma garantia à transferência de dados, permitindo que as partes regulem o fluxo com "um objetivo legítimo de política pública"[40], desde que não seja de forma arbitrária. Da mesma forma, o acordo veda, em cláusula separada, a localização forçada de instalações de computação de empresas para que possam atuar no país, também permitindo exceções não discriminatórias[41].

O TLC entre Singapura e Austrália possui um capítulo intitulado "Economia Digital", com duas cláusulas muito similares às de transferência de dados

36. GAO, H. *Data regulation in trade agreements: different models and options ahead*. p. 326. In: *Adapting to the digital trade era: challenges and opportunities*. OMC, 2021. Disponível em <https://www.wto.org/english/res_e/publications_e/adtera_e.htm>. Acesso em 18 jul. 2023.

37. Art. 15.8, Tratado de Livre Comércio entre Estados Unidos e Coreia do Sul. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta>.

38. Tradução livre. Art. 14.10, Tratado de Livre Comércio entre México e Panamá. Disponível em <https://www.gob.mx/cms/uploads/attachment/file/224510/2.4.11_Mx-Panam_.pdf>.

39. *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*. Disponível em <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>.

40. Tradução livre. Art. 14.11, Trans-Pacific Partnership Agreement. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text>.

41. *Ibidem*. Art. 14.13.

e localização forçada do TPP[42]. Em outro artigo, o acordo submete as partes a desenvolver legislações internas de proteção de dados[43], usando como parâmetro os princípios e diretrizes de organismos internacionais como a OCDE[44] e a APEC (Cooperação Econômica Ásia-Pacífico)[45].

Esse TLC também trouxe uma nova perspectiva, incluindo uma cláusula chamada "Inovação de dados", em que as partes se comprometem a realizar sandboxes regulatórios para fomentar a transferência internacional de dados e a inovação na economia digital, buscando cooperar em pesquisas sobre essa temática[46]. Também instaura uma política aberta de dados entre ambos os governos, de forma a torná-los mais acessíveis ao público geral[47].

O USMCA, acordo celebrado fora do âmbito da OMC entre Estados Unidos, México, e Canadá, trouxe um capítulo sobre o comércio eletrônico, algo que não havia no NAFTA[48]. Este acordo possui cláusulas similares ao TLC de Singapura e Austrália[49]: uma cláusula sobre proteção de dados indicando como instrumentos adequados às diretrizes da OCDE e da APEC; outra cláusula que garante a transferência internacional; e uma terceira vedando a localização forçada de instalações de computação, porém mais restritiva, sem incluir nenhum tipo de exceção.

Embora o Brasil não adote um modelo de regulação mais próximo do norte-americano, que prioriza o fluxo comercial à proteção de dados, no Acordo sobre Comércio Eletrônico do Mercosul[50] e em seu TLC com o Chile[51], as disposições sobre proteção de dados, transferências internacionais, e de localização forçada são semelhantes às cláusulas do USMCA, permitindo essas medidas com exceções vinculadas às políticas públicas.

42. Arts. 23 e 24, Tratado de Livre Comércio entre Singapura e Austrália. Disponível em <https://www.dfat.gov.au/trade/agreements/in-force/safta/singapore-australia-fta>.

43. *Ibidem*. Art. 17.

44. OCDE. Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em <https://www.oecd.org/sti/ieconomy/15590254.pdf>.

45. APEC. *Cross-Border Privacy Rules*. Disponível em <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>.

46. Art. 26, Tratado de Livre Comércio entre Singapura e Austrália. Disponível em <https://www.dfat.gov.au/trade/agreements/in-force/safta/singapore-australia-fta>.

47. *Ibidem*. Art. 27.

48. O NAFTA (Tratado de Livre Comércio da América do Norte), implementado em 1994, foi substituído pelo USMCA (Estados Unidos-México-Canadá) em 2020.

49. Arts. 19.8, 19.11 e 19.12, Acordo Estados Unidos-México-Canadá. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

50. Arts. 6, 7 e 8, Acordo sobre Comércio Eletrônico do Mercosul. Disponível em <https://www.mercosur.int/documento/acordo-sobre-o-comercio-eletronico-do-mercosul/>.

51. Arts. 10.8, 10.12 e 10.13, Acordo de Livre Comércio entre Brasil e Chile. Disponível em <https://www12.senado.leg.br/noticias/materias/2021/09/28/aprovado-acordo-de-livre-comercio-entre-brasil-e-chile>.

No caso dos países do Mercosul, há uma grande convergência entre o Acordo celebrado para esse fim e as legislações internas dos países-membros, com decisões similares de adequação pelas autoridades de proteção de dados. Esses países estão caminhando rumo a uma lógica equilibrada de proteção e um fluxo livre de dados, importante para fomentar o comércio regional e o próprio Mercosul.

No caso da União Europeia, como a proteção de dados é um direito fundamental não aberto a negociações, em 2018 foram transmitidas as "Disposições horizontais para fluxos de dados transfronteiriços e para a proteção de dados pessoais"[52], que seriam cláusulas prontas a serem inseridas em acordos comerciais e de investimentos. Essas cláusulas embora tenham como finalidade a facilitação do comércio reforçam a proteção como um direito humano ("Cada Parte reconhece que a proteção dos dados pessoais e da privacidade é um direito fundamental e que altos padrões nesse sentido contribuem para a confiança na economia digital e para o desenvolvimento do comércio"[53]) e a aplicação do RGPD, proibindo expressamente requerimentos de localização forçada.

Essas disposições visam garantir que os princípios do RGPD não seriam prejudicados, além de excluir os acordos de comércio e investimentos do Sistema de Tribunais de Investimento[54], submetendo qualquer disputa à jurisdição da Corte de Justiça da União Europeia. Essas medidas buscam proporcionar uma proibição direta de barreiras protecionistas aos fluxos de dados transfronteiriços, sempre em conformidade com a legislação europeia sobre o assunto[55].

Contudo, cabe a reflexão de até que ponto não seriam medidas que favorecem nacionais europeus em detrimento de estrangeiros, gerando um desequilíbrio no fluxo, já que as Disposições Horizontais garantem que cada parte do acordo poderá garantir a proteção de dados conforme sua legislação interna[56].

52. Comissão Europeia. *Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)*. Disponível em <https://ec.europa.eu/newsroom/just/items/627665>. Acesso em 18 jul. 2023.

53. *Ibidem*. Art. B.1

54. Sistema sugerido pela União Europeia para dirimir disputas sobre investimentos através da criação de um tribunal multilateral permanente. Comissão Europeia. *Multilateral Investment Court Project*. Disponível em <https://policy.trade.ec.europa.eu/enforcement-and-protection/multilateral-investment-court-project_en>. Acesso em 18 jul. 2023.

55. *European Commission approves provisions for cross-border data flows while consultation on GDPR Article 49 guidance closes*. Technology Law Dispatch, 04 abr. 2018. Disponível em <https://www.technologylawdispatch.com/2018/04/privacy-data-protection/european-commission-approves-provisions-for-cross-border-data-flows-while-consultation-on-gdpr-article-49-guidance-closes/>. Acesso em 18 jul. 2023.

56. GAO, H. *Data regulation in trade agreements: different models and options ahead. p. 331. In: Adapting to the digital trade era: challenges and opportunities*. OMC, 2021. Disponível em <https://www.wto.org/english/res_e/publications_e/adtera_e.htm>. Acesso em 18 jul. 2023.

Essas disposições foram implementadas no Acordo de Comércio e Cooperação entre a União Europeia e o Reino Unido[57], celebrado pós-Brexit. Também foram aceitas pelo Chile na atualização do Acordo de Associação entre as partes, além de terem sido submetidas nas negociações entre o bloco e países como Japão, Nova Zelândia, Indonésia e Índia[58]. É interessante ressaltar que acordos com países que tiveram decisões positivas de adequação pela Comissão Europeia são substituídos pela referida decisão, sendo o fluxo de dados livre entre a UE e o país, como foi o caso do TLC pactuado com a Coreia do Sul[59].

Embora a China controle o comércio eletrônico junto com os EUA, sua abordagem quanto a acordos comerciais é diferente. A regulação da internet na China é altamente controlada pelo governo, que em 2017 adotou uma lei de segurança cibernética[60] que exige que os operadores armazenem localmente informações coletadas e geradas no país, indo em contra as medidas dos EUA ou da União Europeia, além da proteção à privacidade contar com muitas exceções relacionadas ao controle governamental.

Até 2015 os acordos celebrados pela China não contavam com disposições sobre o comércio eletrônico, sendo os primeiros os celebrados com a Austrália e a Coreia do Sul[61]. Ademais, esses acordos possuem medidas focadas na facilitação do comércio, como, por exemplo, que os consumidores do comércio eletrônico tenham o mesmo nível de proteção que aqueles do comércio tradicional.

A falta de medidas mais aprofundadas pode ser motivada pelo modelo de regulação chinês, mas também pelo fato de que as principais empresas chinesas líderes no comércio mundial são de venda de produtos físicos[62], diferente das empresas norte-americanas, que fornecem serviços totalmente digitais.

57. Art. 201, Acordo de Comércio e Cooperação entre a União Europeia e o Reino Unido. Disponível em <https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en>.

58. Comissão Europeia. COM (2022) 336 final. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=-CELEX:52022PC0336>. Acesso em 18 jul. 2023.

59. Comissão Europeia. *Decision on the adequate protection of personal data by the Republic of Korea with annexes*. Disponível em <https://commission.europa.eu/document/e9453177-f192-4416-a147-3c57adc468c4_en>. Acesso em 18 jul. 2023.

60. *Cybersecurity Law of the People's Republic of China*. Disponível em <https://digichina.stanford.edu/work/translation--cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>. Acesso em 18 jul. 2023.

61. GAO, H. *Data regulation in trade agreements: different models and options ahead*. p. 329. *In: Adapting to the digital trade era: challenges and opportunities*. OMC, 2021. Disponível em <https://www.wto.org/english/res_e/publications_e/adtera_e.htm>. Acesso em 18 jul. 2023.

62. Das 5 maiores empresas chinesas, 3 são de comércio eletrônico, enquanto das 5 norte-americanas, apenas 1 envolve o comércio de produtos físicos. *List of Largest Internet Companies*. Wikipedia. Disponível em <https://en.wikipedia.org/wiki/List_of_largest_Internet_companies>. Acesso em 18 jul. 2023.

Por esse motivo a China possui um foco maior em acordos de comércio tradicional de mercadorias possibilitado pela Internet[63].

3.3 O alcance da interoperabilidade com a inserção das cláusulas

Ao incluir a proteção e transferência de dados nos TLC se busca regular a livre circulação de dados de forma a permitir o livre comércio. Majoritariamente, as cláusulas inseridas permitem o fluxo livre de dados, com restrições justificadas, e não o caminho contrário, que seria de transmissão justificada.

Essas cláusulas também reconhecem que cada país parte do acordo deve ter uma regulação interna, a ser respeitada, e que juntos encontrem mecanismos de cooperação para o fluxo internacional. Caso exista uma harmonização entre as legislações internas, que pode ser com nível adequado ou equivalente de proteção, o fluxo seguramente será livre, e, em diferentes circunstâncias, será aplicado algum grau de restrição, permitindo que os serviços funcionem, mas não necessariamente que os dados circulem de forma desimpedida.

Conforme foi analisado, no âmbito do sistema multilateral da OMC não houve grande inovação em relação à economia digital. Apesar de seu potencial como fórum multilateral institucionalizado, esse sistema ainda possui uma natureza física e analógica, presa ao comércio de mercadorias[64]. Com isso, os TLC lograram melhores soluções e compromissos no âmbito da proteção de dados, fora do sistema multilateral.

Não obstante, os TLC criam uma espécie de colcha de retalhos regulatória de acordos múltiplos e sobrepostos, que não contribuem para o fluxo de informações em escala global[65]. Mesmo que os objetivos seja uma interoperabilidade entre os sistemas jurídicos, acabam levando a uma fragmentação legal, prejudicando o multilateralismo e o direito internacional. A interoperabilidade e uniformidade requeridas pela economia digital seriam melhor encontradas em normativas de aplicação mais ampla, sem preferencialismos[66].

63. GAO, H. *Data regulation in trade agreements: different models and options ahead*. p. 330. In*: Adapting to the digital trade era: challenges and opportunities*. OMC, 2021. Disponível em <https://www.wto.org/english/res_e/publications_e/adtera_e.htm>. Acesso em 18 jul. 2023.

64. BURRI, M. *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. UC Davis Law Review*, Vol. 51, 2017, p. 129.. Disponível em <https://ssrn.com/abstract=3067973>. Acesso em 23 jul. 2023.

65. *Ibidem*.

66. *Ibidem*.

A falta de coerência normativa gerada pelos TLC, que acabam não levando em consideração a complexa natureza dos dados, que são ao mesmo tempo bens públicos e ativos comerciais, também fortalecem as grandes plataformas que controlam enormes bases de dados[67]. Como nos TLC é favorecido o fluxo comercial, as empresas, principalmente as *big techs*[68], tem um controle praticamente de oligopólio sobre os dados que detém.

Essas empresas através da realização de *lobby* durante as negociações dos acordos comerciais, conseguem substituir os interesses nacionais com os seus próprios[69]. Sobretudo no caso dos EUA, país onde estão instaladas a maioria das *big techs*, que vem impulsionando sua agenda digital fragmentada, e levando a uma desejada desregulação do setor[70].

Ao mesmo tempo, é importante questionar se os acordos de comércio no geral, principalmente no âmbito da OMC, são realmente o instrumento apropriado para regular as temáticas de proteção e transferências de dados mundial. A economia digital possui questões complexas e multidimensionais, e talvez algumas cláusulas em acordos comerciais não sejam suficientes para tratar desses temas. Qualquer que seja o instrumento escolhido, terá fortes impactos na inovação digital, e em direitos fundamentais como privacidade, liberdade de expressão, equidade e justiça[71].

Contudo, tampouco se deve descartar os TLC e acordos multilaterais dentro do escopo da OMC como forma de regular ao menos parte da economia digital. Esses dispositivos se mostraram eficazes em disciplinar o protecionismo, aspecto importante da regulação de proteção e fluxo de dados para o comércio[72]. A satisfação parcial das demandas do comércio eletrônico, através do aprimoramento da cooperação regulatória, é essencial para o avanço nas questões de dados, que implicam a necessidade de conciliar diferentes interesses.

67. POURMALEK, P.; TWOREK, H.; TIBERGHIEN, Y. *As Digital Trade Expands, Data Governance Fragments*. CIGI, 2023. Disponível em <https://www.cigionline.org/articles/as-digital-trade-expands-data-governance-fragments/?utm_campaign=-thinktech_44&utm_medium=email&utm_source=RD+Station>. Acesso em 23 jul. 2023.

68. As maiores empresas de tecnologia da informação, como Google, Apple, Meta, Amazon e Microsoft.

69. BURRI, M. *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*. UC Davis Law Review, Vol. 51, 2017, p. 129. Disponível em <https://ssrn.com/abstract=3067973>. Acesso em 23 jul. 2023.

70. FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. *E-book*. p. 651.

71. BURRI, M. *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*. UC Davis Law Review, Vol. 51, 2017, pp. 130, 131. Disponível em <https://ssrn.com/abstract=3067973>. Acesso em 23 jul. 2023.

72. *Ibidem*.

Embora preferencialmente a cooperação regulatória deveria ser tratada de forma multilateral, seja no âmbito da OMC ou de uma nova organização mundial, os acordos bilaterais e TLC podem servir como laboratórios de governança[73] no assunto. Enquanto os países enquadrarem os dados como um "ativo soberano" para alcançar uma economia de escala, e não reconhecerem a dualidade dos dados como um direito humano e um ativo comercial, estaremos longe de esforços mais globalizados[74].

No entanto, a criação de uma nova organização internacional que pudesse oferecer incentivos adequados e pagar às empresas globais para que compartilhem dados, através de uma normativa vinculante, poderia gerar a interoperabilidade desejada[75]. Isso seria conquistado através de discussões técnicas sobre fluxos de dados, governança e regras para o comércio digital que fossem contextualizadas dentro de cuidados fundamentais sobre a natureza dos dados e o papel dos direitos humanos.

Considerações finais

Além da convergência textual existente em diversas leis nacionais sobre proteção de dados, outro aspecto comum entre os países pode ser ressaltado: a busca por uma soberania digital. Essa soberania, que envolve a proteção dos dados de seus nacionais, motivo mais do que respeitável, está sendo refletida nas cláusulas sobre proteção e transferência de dados negociadas em acordos comerciais. O espelhamento dessa soberania nos acordos ocorre de forma muito menos complexa que o tratamento dado às legislações nacionais, visto que são cláusulas mais breves.

O resultado disso, como pode-se perceber no presente estudo, são cláusulas amplas e sem aprofundamento, mais básicas que a lei brasileira ou da União Europeia, por exemplo. A proliferação desses acordos, apesar de mencionar o comércio e a economia digital, não examinam o tema da proteção de dados com o empenho necessário, e, portanto, ainda estamos distantes de uma harmonização eficaz sobre a matéria.

73. *Ibidem*.

74. POURMALEK, P.; TWOREK, H.; TIBERGHIEN, Y. *As Digital Trade Expands, Data Governance Fragments*. CIGI, 2023. Disponível em <https://www.cigionline.org/articles/as-digital-trade-expands-data-governance-fragments/?utm_campaign=-thinktech_44&utm_medium=email&utm_source=RD+Station>. Acesso em 23 jul. 2023.

75. *Ibidem*.

É importante ressaltar, também, que muitos países não participam de acordos internacionais com previsões sobre a proteção de dados, e se quer possuem uma legislação nacional, estando completamente à margem.

Esses aspectos fortalecem os interesses de *players* como a União Europeia, que busca impor a sua legislação interna através dos acordos comerciais com outros países, que acabam internalizando os parâmetros europeus para serem considerados adequados. Por mais que a normativa europeia seja avançada no tratamento da proteção de dados como um direito humano, não deveria ser a única referência no assunto, e tampouco deveria condicionar os países do sul global. Não obstante, é notável a tolerância no tratamento dado aos Estados Unidos, que ainda se encontram em um patamar distante em matéria de proteção de dados, , devido a um certo protencionismo em relação às empresas norte-americanas de tecnologia.

Com tantas dificuldades apresentadas, o caminho da proteção internacional de dados continuará tortuoso. Apesar dos acordos comerciais não serem os instrumentos ideais para regular a matéria, é preferível tê-los, enquanto esforços mais globais não são realizados. Embora seja necessário um mecanismo internacional que entenda a complexidade envolvida, desde a óptica do comércio e dos direitos humanos, o estabelecimento de um padrão mínimo global, que abarque todos os países, já seria um passo vantajoso.

Referências

Acordo de Comércio e Cooperação entre a União Europeia e o Reino Unido. Disponível em <https://commission.europa.eu/strategy-and-policy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en>.

Acordo de Livre Comércio entre Brasil e Chile. Disponível em <https://www12.senado.leg.br/noticias/materias/2021/09/28/aprovado-acordo-de-livre-comercio-entre-brasil-e-chile>.

Acordo Estados Unidos-México-Canadá. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>.

Acordo Geral de Tarifas e Comércio (GATT), OMC. Disponível em <https://www.wto.org/english/docs_e/legal_e/gatt47.pdf>.

Acordo sobre Comércio Eletrônico do Mercosul. Disponível em <https://www.mercosur.int/documento/acordo-sobre-o-comercio-eletronico-do-mercosul/>.

APEC. *Cross-Border Privacy Rules*. Disponível em <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>.

BURRI, M. *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*. UC Davis Law Review, Vol. 51, 2017, pp. 65-133. Disponível em <https://ssrn.com/abstract=3067973>. Acesso em 23 jul. 2023.

BRASIL. Lei Geral de Proteção de Dados (LGPD). Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

Comissão Europeia. COM (2022) 336 final. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0336>. Acesso em 18 jul. 2023.

Comissão Europeia. *Commercial sector: adequacy decision on the EU-US Data Privacy Framework*. 10 jul. 2023. Disponível em <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en>. Acesso em 18 jul. 2023.

Comissão Europeia. *Decision on the adequate protection of personal data by the Republic of Korea with annexes*. Disponível em <https://commission.europa.eu/document/e9453177-f192-4416-a147-3c57adc468c4_en>. Acesso em 18 jul. 2023.

Comissão Europeia. *Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)*. Disponível em <https://ec.europa.eu/newsroom/just/items/627665>. Acesso em 18 jul. 2023.

Comissão Europeia. *Multilateral Investment Court Project*. Disponível em <https://policy.trade.ec.europa.eu/enforcement-and-protection/multilateral-investment-court-project_en>. Acesso em 18 jul. 2023.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Disponível em <https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>.

Cybersecurity Law of the People's Republic of China. Disponível em <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>. Acesso em 18 jul. 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019. E-book.

European Commission approves provisions for cross-border data flows while consultation on GDPR Article 49 guidance closes. Technology Law Dispatch, 04 abr. 2018. Disponível em <https://www.technologylawdispatch.com/2018/04/privacy-data-protection/european-commission-approves-provisions-for-cross-bor-

der-data-flows-while-consultation-on-gdpr-article-49-guidance-closes/>. Acesso em 18 jul. 2023.

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. The White House, 25 mar. 2022. Disponível em <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>. Acesso em 18 jul. 2023.

FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. Curso de proteção de dados pessoais: fundamentos da LGPD. 1. ed. Rio de Janeiro: Forense, 2022. E-book.

GAO, H. *Data regulation in trade agreements: different models and options ahead. In: Adapting to the digital trade era: challenges and opportunities*. OMC, 2021. Disponível em <https://www.wto.org/english/res_e/publications_e/adtera_e.htm>. Acesso em 18 jul. 2023.

GUEIROS, Pedro. Tratados e Acordos para Transferências Internacionais de Dados. Rio de Janeiro: ITS, 2023. Disponível em <https://itsrio.org/pt/publicacoes/tratados-e-acordos-para-transferencias-internacionais-de-dados/>. Acesso em 18 jul. 2023.

List of Largest Internet Companies. Wikipedia. Disponível em <https://en.wikipedia.org/wiki/List_of_largest_Internet_companies>. Acesso em 18 jul. 2023.

OCDE. Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em <https://www.oecd.org/sti/ieconomy/15590254.pdf>.

OMC. Declaração Ministerial. *The Geneva Ministerial Declaration on global electronic commerce*. 25 maio. 1998. Disponível em <https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm>. Acesso em 18 jul. 2023.

OMC. Grupo de Trabalho. *Work Programme on E-Commerce*. Disponível em <https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm>. Acesso em 18 jul. 2023.

OMC. Joint *Initiative on E-commerce*. Disponível em <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm>. Acesso em 18 jul. 2023.

ORDIOZOLA, José Miguel. *Las transferencias internacionales de datos personales desde Uruguay, tras la resolución No. 23/021 de la URCDP*. Revista CADE No. 60, 2022.

POLIDO, Fabrício B. P. Transferência internacional de dados e 'lei aplicável mais favorável'. JOTA, 14 ago. 2022. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/transferencia-internacional-de-dados-e-lei-aplicavel-mais-favoravel-14082022>. Acesso em 18 jul. 2023.

POURMALEK, P.; TWOREK, H.; TIBERGHIEN, Y. *As Digital Trade Expands, Data Governance Fragments*. CIGI, 2023. Disponível em <https://www.cigionline.org/articles/as-digital-trade-expands-data-governance-fragments/?utm_campaign=thinktech_44&utm_medium=e-mail&utm_source=RD+Station>. Acesso em 23 jul. 2023.

PRATA DE CARVALHO, Angelo. Transferência internacional de dados na Lei geral de proteção de dados – Força normativa e efetividade diante do cenário transnacional. In: FRAZÃO, Ana. TEPEDINO, Gustavo. DONATO OLIVA, Milena. A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2019.

PRESS, Gil. *54 Predictions About The State Of Data In 2021*. Forbes, 30 Dez. 2020. Disponível em <https://www.forbes.com/sites/gilpress/2021/12/30/54-predictions-about-the-state-of-data-in-2021/?sh=68be34ef397d>. Acesso em 23 jul. 2023.

Trans-Pacific Partnership Agreement. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text>.

Tratado de Livre Comércio entre Estados Unidos e Coreia do Sul. Disponível em <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta>.

Tratado de Livre Comércio entre México e Panamá. Disponível em <https://www.gob.mx/cms/uploads/attachment/file/224510/2.4.11_Mx-Panam_.pdf>.

Tratado de Livre Comércio entre Singapura e Austrália. Disponível em <https://www.dfat.gov.au/trade/agreements/in-force/safta/singapore-australia-fta>.

UNIÃO EUROPEIA. Regulamento Geral de Proteção de Dados (RGPD). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>.

URUGUAI. Decreto No. 64/020. Disponível em <https://www.impo.com.uy/bases/decretos/64-2020>.

URUGUAI. Lei 18.331/2008. Disponível em <https://www.impo.com.uy/bases/leyes/18331-2008>.

URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 04/019. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-4019>.

URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 17/009. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-17009>.

URUGUAI. Unidade Reguladora e de Controle de Dados Pessoais. Resolução No. 23/021. Disponível em <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021>.

VAN DEN BOSSCHE, Peter. PRÉVOST, Denise. WTO *Law in a nutshell*. Maastricht University, 2008.

WU, M. *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB)*, 2017. Disponível em <https://unov.tind.io/record/67136?ln=es>. Acesso em 18 jul. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Marketing e proteção de dados: análise acerca das bases legais mais adequadas para a utilização de *cookies* de publicidade no tratamento de dados pessoais

BEATRIZ CORRÊA PEIXOTO

Introdução

Com a alteração do mundo físico pelo digital, houve um crescimento exponencial do comércio eletrônico, no qual os usuários da internet transformaram-se rapidamente em consumidores ou possíveis consumidores[2]. Diante desse novo cenário, os setores de marketing (segmentação dos bens de consumo) e de publicidade (promoção da atividade)[3], passaram por vitais transformações nos últimos anos.

Esses setores tiveram que se adaptar ao novo sistema econômico e ao novo modelo operacional, marcado pela era digital, e precisaram abandonar a publicidade de massa[4;5], abrindo as portas para a publicidade digital e direcionada, o marketing de precisão e preditivo, como também para o setor de mídia programática. Tal mudança de perspectiva sucedeu-se devido ao avanço tecnológico e à utilização em larga escala dos meios de comunicações digitais, que proporcionaram a coleta de uma ampla gama de dados pessoais, permitindo que as empresas identifiquem os seus consumidores e seus interesses.

Não por outra razão o surgimento da publicidade direcionada tornou os dados pessoais um *commodity* valioso para as empresas, sendo o principal in-

1. Advogada de Propriedade Intelectual e Direito Digital. Pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ), em parceria com o Instituto de Tecnologia e Sociedade (ITS) e Centro de Estudos e Pesquisas no Ensino do Direito (CEPED-UERJ). Bacharel em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).

2. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. *E-book* Kindle.

3. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. E-book Kindle.

4. Até então, as empresas, no intuito de promover suas atividades e expandir suas operações, utilizavam-se da comunicação em massa, abordando diversos públicos de uma só vez (*e.g.* por meios televisivos, em que não se sabia ao certo quem era o indivíduo do outro lado da tela).

5. Os resultados obtidos pela ciência mercadológica, mostraram que a comunicação em massa era ineficiente, pois não atingiam o consumidor em si, mas sim diversos indivíduos que não teriam propensão a consumir o bem anunciado.BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. E-book Kindle.

sumo atual das relações de consumo[6]. As empresas, munidas das informações fornecidas por seus consumidores, para que obtenham determinados produtos ou serviços, começaram a utilizar esses dados pessoais para uma série de usos secundários, notadamente lucrativos para os gestores dos sistemas interativos[7].

Conforme adverte Stefano Rodotà, as companhias, elaborando as informações obtidas quando do fornecimento dos serviços, podem "criar" informações novas (perfis de consumo individual ou familiar)[8], com o objetivo de direcionar a publicidade digital, por exemplo.

Dentre as ferramentas mais expressivas utilizadas pelo setor de marketing, para esquematizar o direcionamento de publicidade e o funcionamento de seu ecossistema lucrativo, estão os *cookies*, - sobretudo os cookies de publicidade, que, de uma maneira geral, permitem o rastreamento da atividade virtual do indivíduo; a construção de perfil (*profiling*) baseado nos interesses do usuário; e, principalmente, a personalização de anúncios e o direcionamento de publicidade[9].

Contudo, é comum notar que a possibilidade de monitorar e rastrear o comportamento humano no ambiente virtual vem favorecendo casos de abusividade e de discriminação na utilização dessas informações. Basta ver os casos envolvendo a rede social Tik Tok, que foi acusada de promover anúncios sobre perda de peso para portadores de transtorno alimentar[10], como também de rastrear as emoções dos usuários para vender slots de publicidade[11].

Com efeito, não é incomum observar o fomento de discussões sobre a utilização de rastreadores digitais, a coleta de dados pessoais, o seu uso indiscriminado e o direcionamento abusivo de publicidade. Tais discussões ganharam ainda mais destaque com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). Isso pois, a LGPD, inaugurando um microssistema específico,

6. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 609.

7. RODOTÁ, Stefano. *A vida na sociedade de vigilância – a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 46.

8. RODOTÁ, Stefano. *A vida na sociedade de vigilância – a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 46.

9. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

10. DAWSON, Brit. *Eating disorder sufferers on the danger of weight loss ads on TikTok*. Dazed, 2020. Disponível em: https://www.dazeddigital.com/life-culture/article/50566/1/eating-disorder-sufferers-on-the-danger-of-weight-loss-ads-on-tiktok. Acesso em: 15 jun. 2023

11. BLACK, Damien. *TikTok accused by privacy watchdog of tracking user emotions to sell advertising slots*. Cybernews, 2023. Disponível em: https://cybernews.com/privacy/tiktok-privacy-tracking-emotions-advertising/. Acesso em: 15 jun. 2023.

determinou uma série de deveres imputados aos agentes de tratamento e estabeleceu as hipóteses em que o tratamento de dados pessoais é autorizado e lícito (bases legais).

Quanto aos cookies de publicidade, observa-se, todavia, que a promulgação da LGPD veio com a carência de previsão e regulamentação dessa ferramenta e qual enquadramento de base legal seria atribuído a esses rastreadores digitais. Justamente por isso, ainda há grande divergência doutrinária sobre essa temática.

Nesse contexto, o presente artigo visa discutir qual, ou quais, bases legais podem ser aplicáveis à publicidade digital, especialmente no que tange a utilização dos cookies de publicidade. Busca-se enfrentar as discussões doutrinárias sobre o enquadramento dos *cookies* de publicidade, quando diante da coleta, utilização, e rastreamento de dados pessoais[12].

Para enfrentar esses pontos, este artigo abordará a definição jurídica de cookies, e suas respectivas modalidades, as consequências da utilização de cookies de publicidade, assim como buscará elaborar as discussões e controvérsias existentes acerca das bases legais dos cookies de publicidade, passando pela base legal do consentimento e do legítimo interesse. Para mais, analisar-se-á a recomendação emitida pela ANPD, em seu Guia Orientativo sobre Cookies e Proteção de Dados Pessoais, suas falhas e consequências.

1. Cookies

Em sua acepção prática, os cookies podem ser compreendidos como pequenos arquivos de texto depositados no dispositivo eletrônico enquanto um indivíduo navega pelas páginas virtuais[13]. Basicamente, os *cookies*, -contendo uma cadeia de números que pode ser usada para identificar um computador -, possibilitam que "uma vez feito o registro de dados pelo usuário no site, a ele regresse em outra oportunidade sem que precise (re)inserir tais informações"[14].

12. Devido à complexidade do tema, o presente artigo visa abordar apenas as bases legais aplicáveis ao tratamento de dados pessoais, e não dados pessoais sensíveis.

13. KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 4 jul. 2023.

14. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

Também chamados de testemunhos de conexão, ou simplesmente rastreadores, os cookies foram concebidos para otimizar a experiência na rede[15], assim como viabilizar a experiência do usuário[16]. Os *cookies* desempenham funções cruciais para o funcionamento do site e, a priori, são inofensivos[17].

Ocorre que, a despeito de serem essenciais para o funcionamento dos sites e possibilitarem o comércio virtual[18], os *cookies* podem ser subdivididos em variadas categorias, com finalidades diversas, e, a depender de sua classe, podem armazenar uma grande quantidade de dados pessoais de forma suficiente a identificar um indivíduo específico, sem o seu consentimento[19]. Tamanha é a possibilidade de utilização de *cookies* para a identificação e especificação de uma pessoa natural, que, na União Europeia, os *cookies* podem ser enquadrados, em alguns casos, como dados pessoais[20];[21].

Usualmente, os *cookies* podem ser divididos segundo a entidade responsável pela sua gestão (*cookies* primários ou de terceiros); de acordo com a sua necessidade (*cookies* necessários e não necessários); conforme a sua finalidade (*cookies* analíticos, de funcionalidade, de publicidade); e de acordo com o período de retenção das informações (de sessão ou persistentes)[22].

Nota-se que os *cookies*, a depender de sua categoria, são responsáveis por possibilitar a coleta de dados pessoais para diversas finalidades. Inclusive, para identificação de uma pessoa natural e direcionamento de anúncios. Como será visto em detalhes a seguir, as definições de *cookies* necessários e não necessários, e suas respectivas distinções, são imprescindíveis para a

15. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

16. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

17. KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 4 jul. 2023.

18. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

19. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

20. *How do the cookie rules relate to the GDPR?* Ico.org.uk. Disponível em: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/#:~:text=The%20UK%20GDPR%20classes%20cookie,account%20at%20an%20online%20service. Acesso em: 4 jul. 2023.

21. KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 4 jul. 2023.

22. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

definição da hipótese legal que autoriza o uso de *cookies* e a coleta de dados pessoais[23].

1.1. Cookies necessários e não necessários

Os cookies necessários, ou também chamados de obrigatórios e essenciais, são aqueles indispensáveis para o regular funcionamento das páginas eletrônicas. Sem estes *cookies*, os *sites* não poderiam realizar suas funções básicas, como abrir a página e navegar virtualmente naquele endereço eletrônico. Para ilustrar o que se diz, vale dizer que, na ausência dos *cookies* necessários, os usuários não conseguiriam comprar qualquer produto em um site de compras, pois "ao incluir o produto no carrinho e em seguida clicar no ícone referente ao pagamento, o carrinho apareceria vazio"[24].

Em contrapartida, os *cookies* não necessários correspondem aqueles que, ao serem desabilitados, não impedem o funcionamento do site[25]. Como se pode extrair da definição da ANPD, os *cookies* não necessários "estão relacionados com funcionalidades não essenciais do serviço, da aplicação ou da página eletrônica"[26]. Ou seja, esses cookies podem englobar tanto aqueles *cookies* utilizados para rastrear comportamento e exibir anúncios direcionados[27], a exemplo dos cookies de publicidade e marketing, quanto para medir o desempenho das páginas eletrônicas.

1.2. *Cookies* de publicidade e suas implicações (*profiling* e rastreamento)

Os *cookies* de publicidade podem de antemão ser pré-definidos como *cookies* não necessários, pois esses cookies não são responsáveis por possibilitar o funcionamento da página eletrônica. Isto significa dizer que os cookies

23. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

24. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 604.

25. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

26. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

27. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

de publicidade são cookies não essenciais, sem os quais a página eletrônica poderia funcionar perfeitamente.

Pode-se, então, defini-los como aqueles que rastreiam a atividade online do usuário para auxiliar os anunciantes a fornecerem publicidades mais relevantes (direcionada) ou para limitar a quantidades de vezes que o indivíduo vê cada anúncio[28]. Além disso, os cookies de publicidade são utilizados para o rastreamento de preferências e para a criação de perfis comportamentais (*profiling*), para fins de marketing direito e preditivo, possibilitando a identificação específica do usuário[29]. Para isso, em diversos casos, os cookies de publicidade implicam no tratamento de dados pessoais.

Possibilitando a coleta e o processamento de dados pessoais, os cookies de publicidade tornaram-se o principal instrumento de segmentação utilizado pelo mercado para o direcionamento publicitário. Ao coletar os dados pessoais sobre uma determinada pessoa natural, as empresas, utilizando-se de técnicas de inteligência artificial atrelada ao processamento de grandes bancos de dados (*Big Data*), são capazes de conduzir análises probabilísticas que promovem informações sobre os interesses de certo nicho do mercado, incrementando e personalizando a venda de produtos e serviços[30].

No entanto, tal prática, que, em princípio, poderia ser uma utilidade positiva, traz consigo também dilemas de abusividade e arbitrariedade. A coleta de dados pessoais e a produção de perfis comportamentais, pode aumentar o controle sobre a pessoa, mitigando a sua autonomia e o seu direito de livre acesso ao consumo de bens e serviços, e dificultar sua participação no processo decisório relativo ao tratamento de seus dados pessoais[31].

Por certo, as consequências da utilização de *cookies* de publicidade são inúmeras. Analisar a base legal aplicada a essa ferramenta é fundamental para compreender os deveres dos anunciantes e os direitos dos usuários. Não só isso, mas a identificação da base legal é imprescindível para a eficaz fiscalização e aplicação de sanções, pela ANPD, tal como para o ajustamento das

28. KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 17 jul. 2023.

29. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

30. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 607.

31. TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. São Paulo: Thomson Reuters, 2020. p. 607.

pessoas jurídicas, e principalmente das empresas anunciantes, em promoverem a correta adequação, a perfeita transparência de informações para com seus usuários, a prestação de contas (*accountability*), a utilização de *banners* de *cookies* de consentimento ou informativos e, igualmente, para investigar se os *cookies* não necessários podem, ou não, estar ativados por padrão.

2. Controvérsia acerca das hipóteses legais dos *cookies* de publicidade

Para investigar qual enquadramento será dado aos cookies de publicidade, é necessário, antes de qualquer coisa, entender a definição legal de dados pessoais, conferida pela LGPD. Em seu artigo 5°, I, a normativa adotou o conceito amplo de dado pessoal[32], definindo-o como qualquer informação relacionada a pessoa natural identificada ou identificável.

Devido à sensibilidade do tema, e para se evitar usos abusivos e ilegítimos dos dados, o sistema legal, inaugurado pela LGPD, estabeleceu que qualquer tratamento de dados pessoais, inclusive aquele realizado nos meios digitais, deverá ter uma base legal que o autorize (art. 1º da LGPD)[33].

Isto é dizer que, ao realizar o tratamento de dados pessoais deverá operar-se o devido encaixe do tratamento realizado em pelo menos uma das hipóteses legais previstas na lei para que o tratamento seja considerado legítimo e lícito[34]. Em relação aos dados pessoais, o legislador previu 10 (dez) hipóteses legais, chamadas de bases legais, nas quais será autorizado realizar o tratamento de dados.

Por implicar na utilização, coleta e armazenamento de dados pessoais, a utilização de *cookies* de publicidade necessita, portanto, enquadrar-se em uma das bases legais, disponíveis no artigo 7º, da LGPD. É a partir disso que surgem os questionamentos sobre qual base legal seria aplicável aos cookies

32. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 115.

33. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 116.

34. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 116.

de publicidade. Ganham destaque duas bases legais focais sobre o tema: o consentimento (art. 7º, I, da LGPD) e o legítimo interesse (art. 7°, IX, da LGPD).

2.1. Base legal do consentimento do titular (art. 7°, I, da LGPD)

O artigo 7º, I, da LGPD, determina que o tratamento de dados pessoais poderá ser realizado mediante o fornecimento de consentimento pelo titular. Entende-se que o consentimento, sendo a primeira hipótese prevista pelo legislador para autorizar o tratamento de dados pessoais, recebeu tutela destacada na LGPD, ainda que não seja hierarquicamente superior às demais previsões contidas no rol do referido artigo[35].

Essa base legal traduz um dos principais fundamentos da LGPD, materializado na autodeterminação informativa, e confere ao titular dos dados o direito de controlar e proteger as suas informações. Nas palavras de Chiara de Teffé e Mario Viola, o consentimento "revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações"[36].

A fim de que seja considerado válido, o consentimento deve preencher certos requisitos, previstos no artigo 5º, XII, da LGPD. Para tal, determina-se que o consentimento deve representar a manifestação livre, informada e inequívoca pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Observa-se, desse modo, que a base legal do consentimento vislumbra-se numa hipótese procedimental, no qual se é requerido, pelo menos, 4 (quatro) condições.

O consentimento deve ser (i) livre, o titular deve poder escolher entre aceitar ou recusar o tratamento de seus dados[37]; (ii) informado, oferecendo-se informações necessárias, suficientes e transparentes para o titular dos dados[38]; (iii) inequívoco, carecendo de ação afirmativa e clara, não podendo ser extraído da omissão do titular, mas tão somente de atos que revelem claramente

35. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 119.

36. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 119.

37. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023 p. 120.

38. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023p. 122.

sua vontade”[39]; e, por fim, (iv) destinado a uma finalidade específica, isto é, o titular deve ser informado sobre o objetivo final do tratamento, sendo vedado o tratamento para finalidade diversa daquela que foi explicitada ao titular no momento da coleta do aceite[40].

Vale mencionar também que o consentimento deve ocorrer de forma granular. O usuário deve emitir autorizações fragmentadas no tocante ao fluxo de seus dados[41]. Dessa maneira, afasta-se a lógica binária[42] do tudo ou nada (*take it or leave it*)[43], na qual o usuário só tem a opção de aceitar todos os termos de uso e de serviço ou não poderá utilizá-lo[44].

À luz do exposto, e voltando-se a discussão aos *cookies*, muitos entendem que o consentimento é a base legal mais adequada a ser aplicada aos cookies não necessários, especialmente no que diz respeito aos *cookies* de publicidade, requerendo-se o aceite do usuário. Argumenta-se, para tanto, que essa base legal conferiria ao titular dos dados o poder de decidir sobre quais assuntos, matérias e anúncios ele será influenciado e, portanto, representaria o seu direito à autodeterminação informativa, na mesma medida que aumentaria o seu acesso a ofertas mais diversas de produtos e serviços, pois os anúncios não estariam direcionados apenas às suas preferências primárias.

Enquadrando-se os cookies de publicidade na base legal do consentimento, os banners de cookies, por exemplo, não poderiam vir com os cookies de marketing pré-selecionados e pré-ativados, o consentimento não poderia partir da lógica de “aceitar todos os *cookies*” de uma só vez, ou do consentimento por omissão (“ao navegar nesta página você concorda com o uso de *cookies*”) e tampouco poderia ser aceito o consentimento vago e genérico. Não obstan-

39. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 123.

40. MIRAGEM, Bruno, MADALENA, Juliano. Comentários ao artigo 7º, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 72.

41. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. E-book Kindle.

42. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 121.

43. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). Tratado de Proteção de Dados Pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 121. e MIRAGEM, Bruno, MADALENA, Juliano. Comentários ao artigo 7º, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 71.

44. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 121.

te, a opção de consentir para com os *cookies* de publicidade deve vir de forma separada e destacada do texto principal, que mostre a sua relevância para o titular dos dados[45].

O que ocorre, na prática, é que muitas páginas eletrônicas não seguem esses critérios, mesmo quando enquadram, em seus termos de uso, os *cookies* de publicidade na base legal do consentimento. As empresas acabam por apresentar *banners* de *cookies* de primeiro nível extremamente vagos e com opções genéricas de "aceitar todos os *cookies*". Nos termos do Guia Orientativo da ANPD[46], ao se aplicar o consentimento na utilização de cookies não necessários:

> não é recomendável a utilização de *banners* de *cookies* com opções de autorização pré-selecionadas ou a adoção de mecanismos de consentimento tácito, como a pressuposição de que, ao continuar a navegação em uma página, o titular forneceria consentimento para o tratamento de seus dados pessoais.

Como se pode perceber, o processo de obtenção de um consentimento válido é bastante específico e rigoroso, sendo muito difícil de ser aplicado na prática. Tal processo mostra-se ainda mais árduo em situações de desigualdade entre as partes, - usuários *versus* agentes de tratamento -, na qual, em muitos casos, o usuário encontra-se em uma posição de vulnerabilidade. Conforme expõe Bruno Bioni e Maria Luciano, ao mesmo tempo que busca-se um consentimento extremamente qualificado, corre-se o risco de limitar o terreno por ele ocupado, ocasionando a sua evasão e fuga para as demais bases legais no tratamento de dados pessoais[47].

A título exemplificativo, basta ver que, muito embora cookies seja um termo difundido atualmente, o seu significado técnico e sua aplicação prática ainda é de difícil compreensão pelo homem médio brasileiro, assim como as implicações das escolhas de *cookies* ainda não são totalmente compreendidas pelo usuário comum[48].

45. MARTINS, Pedro; SANTOS, Pedro Henrique. *Relatório de Inteligência: Proteção de Dados e Marketing – Da captação ao lead ao fechamento do negócio*. Data Privacy BR e Clube Data.

46. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

47. BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 151.

48. BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. E-book Kindle.

Para mais, a possibilidade de não consentir e de revogar o consentimento anteriormente fornecido, faz com que as empresas tenham acesso a um público menor e, consequentemente, resta-se dificultado o direcionamento de anúncios com base na inferência dos usuários.

Posto isso, na tentativa de se resguardarem e se protegerem quanto ao consentimento considerado inválido e de atingirem um maior público, as pessoas jurídicas de direito público e privado, especialmente as empresas, que utilizam-se de *cookies* de publicidade para segmentar os seus anúncios, vêm buscando outros meios de fundamentar a utilização dessa modalidade de cookies, visando enquadrá-los em outras bases. Com a ausência de legislação sobre o tema, e as possibilidades interpretativas da LGPD, há quem defenda a utilização dos cookies de publicidade pela base legal do legítimo interesse, na qual é dispensado o consentimento, conforme será exposto a seguir.

2.2. Base legal do legítimo interesse (art. 7, XI c/c art. 10, I, da LGPD)

Observando-se o artigo 2º da LGPD, que prevê os fundamentos da disciplina de proteção de dados, é possível notar que o legislador não focou apenas em garantir o direito do titular em poder dispor e controlar os seus dados pessoais, mas também determinou que a LGPD tem como objetivos o desenvolvimento econômico, tecnológico, a livre iniciativa, a livre concorrência e a promoção da inovação[49].

Nesse cenário, o legítimo interesse nasce com uma dupla premissa de valores[50], passando, a um, pela necessidade de se assegurar o direito à privacidade e a autodeterminação informativa, para o livre desenvolvimento da personalidade[51] e, a dois, pela promoção de um livre fluxo de dados que incentive o desenvolvimento econômico[52].

49. BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. Thomson Reuters, 2020. p. 461.

50. BIONI, Bruno Ricardo; RIELLI, Mariana; KITAYAMA, Marina. *O Legítimo Interesse na LGPD: Quadro Geral e Exemplos de Aplicação*. Observatório da privacidade e proteção de dados e Data Privacy Brasil Research, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf. Acesso em: 17 jun. 2023.

51. BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. Thomson Reuters, 2020. p. 461.

52. BIONI, Bruno Ricardo; RIELLI, Mariana; KITAYAMA, Marina. *O Legítimo Interesse na LGPD: Quadro Geral e Exemplos de Aplicação*. Observatório da privacidade e proteção de dados e Data Privacy Brasil Research, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf. Acesso em: 17 jun. 2023.

O artigo 7º, XI, da LGPD, traz consigo um conceito abstrato e, como muitos chamam, uma cláusula aberta[53] (*i.e.*, cláusula geral e indeterminada[54]), que autoriza o tratamento de dados pessoais. Por conseguinte, a conformidade dessa hipótese legal se desenvolverá no caso concreto pelo correto uso do ônus argumentativo[55].

Na tentativa de delimitar o que se configuraria como legítimo interesse, a LGPD trouxe, no artigo 10, situações em que o interesse poderá ser considerado como legítimo. Os incisos I e II, do referido artigo, preveem que 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 o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei[56].

Ao informar que o interesse será considerado legítimo quando a finalidade do tratamento de dados for destinada ao apoio e promoção de atividade do controlador, a figura do legítimo interesse ganha um destaque bastante significativo para o setor de marketing e publicidade. Isso devido ao fato de tais áreas, especialmente a publicidade, serem setores destinados, quase exclusivamente, ao apoio e promoção de atividades.

A possibilidade de enquadramento da publicidade na base legal do legítimo interesse encontra, inclusive, amparo doutrinário. Ao elencarem exemplos de aplicação do legítimo interesse, Chiara de Teffé e Mario Viola afirmam que tal base legal poderia ser aplicada às seguintes situações:

53. BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. Thomson Reuters, 2020. p. 469.

54. MIRAGEM, Bruno, MADALENA, Juliano. Comentários ao artigo 7º, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 87.

55. BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. 2. ed. Thomson Reuters, 2020. p. 467.

56. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018.

> e) no caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando dados estritamente necessários para tal; f) envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compra, tomando como base seu histórico de compras"[57].

Corroborando com tal possibilidade, Bruno Miragem e Juliano Madalena expõem que, as atividades de apoio e promoção de atividades do controlador poderão ser concretizadas na hipótese de divulgação e promoção negocial (e.g. para direcionamento e oferta publicitária)[58].

Veja-se que, usualmente, a doutrina entende que as atividades de marketing e de publicidade possuem a possibilidade de se enquadrarem na base legal do legítimo interesse, autorizando-se o tratamento de dados pessoais para esse fim. Sobre isso, vale mencionar que esse enquadramento encontra berço também no considerando n° 47, do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), dispondo que "*the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest*"[59].

Com isso, é comum notar o enquadramento do marketing e da publicidade como hipótese em que o interesse é considerado legítimo. Até mesmo porque, além de promover e incentivar o consumo de bens e serviços, tais atividades são (i) essenciais para o desenvolvimento dos negócios; e (ii) possuem uma finalidade lícita, legítima e concreta[60].

Justamente por essa razão, e por uma consequência lógica, sendo os cookies de publicidade uma das ferramentas utilizadas pelo setor de marketing, para direcionar os anúncios e baratear a oferta de publicidade, o controlador desse dispositivo poderia facilmente valer-se da base legal do legítimo interesse para aplicação de *cookies* nos aparelhos de seus consumidores,

57. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 127.

58. MIRAGEM, Bruno, MADALENA, Juliano. Comentários ao artigo 7º, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 88.

59. Tradução livre: "O tratamento de dados pessoais para fins de marketing direto podem ser considerados como realizados por um interesse legítimo". EUROPA, Regulation 2016/679: General Data Protection Regulation (GDPR), 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 1 jul. 2023.

60. BIONI, Bruno Ricardo; RIELLI, Mariana; KITAYAMA, Marina. *O Legítimo Interesse na LGPD: Quadro Geral e Exemplos de Aplicação*. Observatório da privacidade e proteção de dados e Data Privacy Brasil Research, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf. Acesso em: 17 jun. 2023.

quando do ingresso em uma página eletrônica. Caso assim seja feito, a base legal do legítimo interesse poderia ser muito bem aproveitada pelas empresas, tendo em vista as suas diversas vantagens para o setor de marketing, como facilitar a arquitetura da operação e atingir um maior público.

Ao utilizar a base legal do legítimo interesse, as empresas anunciantes e os agentes controladores não precisariam pedir autorização dos usuários para a aplicação dos cookies de publicidade. Ilustrativamente, os banners de *cookies* poderiam vir com os *cookies* de publicidade pré-ativados e, em caso de não oposição pelo usuário (*opt-out*), as empresas poderiam seguir tratando os seus dados.

Como se pretendeu demonstrar, diante da ausência de legislação, e aplicando uma investigação orgânica sobre o tema, é factível afirmar que ambas as bases legais, do consentimento e do legítimo interesse, poderiam ser utilizadas para fundamentar a utilização dos *cookies* de publicidade pelas empresas. Trata-se, em verdade, de uma arquitetura de escolha, na qual deve-se sopesar os pontos positivos e negativos de cada base legal.

3. Estudo do Guia Orientativo da ANPD: *cookies* e proteção de dados pessoais

O presente trabalho se propôs, até aqui, a apresentar a lacuna legislativa existente sobre o tema ora em debate, elaborando observações sobre as posições doutrinárias paradoxais quanto a melhor e mais adequada base legal aplicada aos cookies de publicidade.

Em face da falta de previsão normativa sobre a questão, e na tentativa de harmonizar as questões suscitadas, a ANPD, em outubro de 2022, publicou o Guia Orientativo sobre Cookies e Proteção de Dados Pessoais, com o objetivo de examinar as hipóteses legais aplicáveis aos cookies, os requisitos a serem observados em caso de sua utilização e, também, identificar as práticas positivas e negativas na elaboração de políticas de *cookies*.

Embora não possua força normativa[61], o Guia Orientativo veio como uma antecipação do entendimento que poderá vir a ser adotado como padrão pela ANPD, sendo relevante analisar as conclusões defendidas pela autoridade. Em resumo, a ANPD orienta que a base legal do consentimento pode ser considerada a mais apropriada para o uso de *cookies* de publicidade.

61. Art. 55-J, inciso III, da LGPD.

A Autoridade afirma que, tratando-se de cookies não necessários, seria de suma importância respeitar as legítimas expectativas dos titulares, conferindo-lhes maior controle sobre o uso de seus dados pessoais no ambiente digital[62]. Dessa forma, defende que o legítimo interesse dificilmente será a base legal mais apropriada nas hipóteses em que os dados coletados por meio de cookies são utilizados para fins de publicidade. Chamando atenção, inclusive, para os casos em que a coleta dos dados pessoais é efetuada por *cookies* de terceiros (*i.e.*, por outro agente que não o titular da página eletrônica).

Para a ANPD, a coleta de dados pessoais, associada a formação de perfis, análise e previsão de preferências e comportamentos, podem implicar em maior risco à privacidade e aos direitos fundamentais dos titulares[63], e, por essa razão, conclui que, em geral, devem-se prevalecer os direitos e liberdades fundamentais dos titulares sobre os interesses legítimos do controlador ou de terceiros[64].

O posicionamento da ANPD teve como norte as discussões da União Europeia sobre o assunto, e a prevalência da base legal do consentimento nos casos de utilização de *cookies* de publicidade[65]. Entretanto, deve-se atentar que o transpasse das conclusões adotadas pela União Europeia sem o devido olhar para a legislação nacional, pode levar a conclusões inadequadas. Como informa Lucas Piveto, apesar da influência do GDPR "o ordenamento jurídico brasileiro possui uma redação completamente distante do prisma europeu e, por consequência, desperta uma série de controvérsias a respeito do seu escopo de aplicação"[66].

Diferentemente da GDPR e da Diretiva de Privacidade Eletrônica, a LGPD e as demais leis esparsas brasileiras carecem da regulamentação dos *cookies*.

62. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

63. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

64. Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022.

65. Em recentíssima decisão, no caso da Meta Platforms Inc., o Tribunal de Justiça da União Europeia entendeu que, para fins de publicidade direcionada, é necessário requerer o consentimento livre dos usuários, afastando-se à aplicabilidade das demais bases legais. Pontualmente, o Tribunal concluiu que a hipótese legal de execução de um contrato poderá tratar apenas os dados indispensáveis à execução daquele respectivo termo, necessitando requerer o consentimento para o tratamento de dados pessoais que não são necessários para a execução do respectivo negócio, como, por exemplo, para o direcionamento de anúncios. Além disso, vale mencionar também que o Tribunal de Justiça da União Europeia também não reconheceu o legítimo interesse como a hipótese mais adequada para fundamentar o tratamento de dados pessoais para publicidade. *CJEU Declares Meta/Facebook's Gdpr Approach Largely Illegal*. Noyb, 2023. Disponível em: https://noyb.eu/en/cjeu-declares-metafacebooks-gdpr-approach-largely-illegal. Acesso em: 04 jul. 2023.

66. PIVETO, Lucas Colombera Vaiano. Comentários ao artigo 10, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 115.

No ordenamento jurídico nacional, não há qualquer normativa que discipline a utilização de *cookies* e a operacionalização dessa ferramenta digital, podendo ser impróprio entender o posicionamento da ANPD como absoluto, posto que nem sempre o consentimento pode-se mostrar o melhor fundamento para o tratamento de dados pessoais no contexto nacional.

As bases legais do consentimento e do legítimo interesse podem ser aplicadas aos cookies de publicidade, tratando-se de uma arquitetura de escolha, na qual o agente de tratamento deve assumir os bônus e os ônus de cada uma das hipóteses legais. No contexto brasileiro, onde o conhecimento sobre proteção de dados ainda não é totalmente difundido na sociedade, para os usuários comuns, o consentimento seria uma vantagem competitiva apenas para algumas empresas e uma desvantagem para os pequenos negócios.

Explica-se: as empresas que já estão bem estabelecidas no mercado, que possuem anos de atuação e uma boa reputação, terão mais facilidade em obter o consentimento do usuário para a utilização de *cookies* de publicidade e, consequentemente, para o tratamento dos dados pessoais para esse fim, pois o consumidor ou possível consumidor deposita naquela empresa alta confiança. Por outro lado, empresas pequenas e iniciantes não terão essa facilidade, vez que a confiança do usuário ainda não foi conquistada.

Dito isso, considerando que, em muitos casos, "a receita publicitária é a própria base de sustentação de muitos modelos de negócios"[67], principalmente dos pequenos negócios, que conseguem distribuir suas mensagens de forma direcionada, atingindo seu público-alvo com menos custos, atribuir-lhe os ônus do consentimento como a única forma de fundamentar o tratamento de dados pessoais para a publicidade direcionada seria extremamente danoso a longo prazo. Dificultando, por exemplo, a livre concorrência, o desenvolvimento tecnológico e a inovação, - fundamentos basilares da LGPD.

Outrossim, é válido assinalar que a ANPD parece ter se olvidado do fato de que, na prática, o legítimo interesse poderia evitar, em grande escala, os casos de fraude e de insuficiência do consentimento.

Conforme expõem Laura Schertel Mendes e Gabriel Campos Soares da Fonseca, existem 3 (três) pontos principais que elucidam as insuficiências do consentimento como foco regulatório, sendo eles: (i) as limitações cognitivas

67. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 165.

do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações de vulnerabilidade, marcadas pela assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento, nas quais não há uma real liberdade de escolha do titular (*e.g.*, nas hipóteses de *take it or leave it*, em que não consentir é sinônimo de não desfrutar o serviço almejado, - uso de uma rede social ou de um aplicativo online); e (iii) as modernas técnicas de tratamento de dados a partir de *Big Data* que fazem com que a totalidade do valor e a possibilidade de uso dos dados pessoais não sejam completamente mensuráveis no momento em que o consentimento é requerido[68].

Certamente, limitar o tratamento de dados pessoais para fins de publicidade ao consentimento traria certos prejuízos para os pequenos negócios, que precisam reduzir gastos com a publicidade e ganham dela a sua maior receita, e, de outro lado, traria uma vantagem competitiva às grandes empresas já consolidadas no mercado.

Além disso tudo, a ANPD aparentemente também omitiu o fato de que, na prática, fundamentar o legítimo interesse, de forma adequada, pode ser muito mais difícil do que o consentimento, levando os agentes de tratamento a resguardar, com mais força, os direitos e liberdades fundamentais do titular dos dados pessoais. Isso porque, para se considerar um interesse como legítimo, é necessário aplicar um teste ainda mais rigoroso do que o consentimento, chamado de teste multifatorial de balanceamento (*legitimate interests assessment* – LIA)[69].

3.1. *Legitimate Interests Assessment* (LIA)

O LIA surgiu a partir da proposta realizada pelo antigo Grupo de Trabalho do Artigo 29 (*Working Party 29*)[70], por meio do qual foi sugerido um teste de ponderação, com o objetivo de balancear os direitos dos titulares de dados e de quem faz o uso das suas informações[71], investigando se há um interesse le-

68. MENDES, Laura Schertel Mendes; FONSECA, Gabriel Campos Soares da. Proteção para além do consentimento: tendências de materialização. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 78-81.

69. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 162.

70. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 127.

71. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bru-

gítimo do agente de tratamento e se estão sendo respeitadas as legítimas expectativas do titular dos dados e os seus direitos e liberdades fundamentais[72]. Em síntese, conforme expõe Chiara de Teffé e Mario Viola, o LIA apresenta quatro fases que devem ser cumpridas de modo a se verificar o preenchimento do requisito do legítimo interesse:

> (i) avaliação dos interesses legítimos; (ii) o impacto sobre o titular dos dados; (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado[73].

O artigo 10º da LGPD materializa bem essas fases, de forma exemplificativa[74], buscando sopesar o legítimo interesse do controlador ou de terceiro e a legítima expectativa do titular. Para isso, o dispositivo estabelece, assim com leciona Bruno Bioni, o próprio teste, passando pelos seguintes critérios: (i) verificação de uma situação concreta e finalidade legítima e articulada (art. 10, *caput* e I, da LGPD); (ii) verificação se os dados coletados são realmente aqueles necessário (minimização) para se atingir a finalidade pretendida (art. 10, §1º, da LGPD); (iii) balanceamento dos impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD); e (iv) salvaguardas: transparência e minimização dos riscos ao titular dos dados (art. 10, §§2º e 3º, da LGPD)[75].

No que tange à publicidade direcionada e à utilização de *cookies* de publicidade, os itens (iii) e (iv) demonstram-se os mais relevantes. Diante disso, mostra-se necessário que o titular dos dados pessoais realmente tenha a expectativa de que seus dados estão sendo utilizados para esse fim, inclusive, nos casos em que forem utilizados por terceiros. É necessário que haja a total transparência do agente controlador em promover o acesso às informações

---

no (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 127.

72. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 127.

73. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 128.

74. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 128.

75. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 161-164.

sobre o tratamento realizado, permitindo ao titular dos dados se opor a tal tipo de tratamento (*opt-out*)[76]. Como ensina Bruno Bioni, "quanto mais visível for tal prática e mais fácil for o exercício do *opt-out*, maiores serão as chances de a aplicação do legítimo interesse ser considerada como uma base legal válida"[77].

O posicionamento adotado pela ANPD, com fortes influências das discussões europeias, pode restar ultrapassado diante das diferenças significativas existentes na LGPD quanto à solidez do legítimo interesse, reduzindo sua subjetividade e seu enquadramento como uma "cláusula aberta". Como defendido até aqui, é necessário que o tratamento de dados pessoais para a publicidade direcionada, utilizando-se de *cookies* de publicidade, seja analisado caso a caso, observando-se os critérios definidos em lei, assim como os outros deveres e princípios estabelecidos na LGPD. É uma questão de escolha de arquitetura atrelada ao ônus argumentativo dos agentes de tratamento, circunscrevendo principalmente o princípio da transparência para com o usuário e titular dos dados pessoais.

Por exemplo, se restar evidente que ao titular dos dados foi informado claramente as implicações do tratamento dos dados pessoais, e preenchidos os demais requisitos, não haveria motivo para negar a aplicação do legítimo interesse. Até mesmo porque, a aplicação do legítimo interesse seria mais interessante, inclusive, do que o consentimento, uma vez que não adianta prever que o consentimento será a única hipótese para fundamentar o tratamento de dados para publicidade se o consentimento dado pelo titular tiver sido insuficiente ou viciado, devido à falta de informação, à posição de vulnerabilidade que se encontrava o titular dos dados ou devido às posições de *take it or leave it*, em que o usuário sentiu-se obrigado a consentir para utilizar alguma aplicação eletrônica.

Por fim, mais uma forma de mitigar os riscos do legítimo interesse, é propriamente reforçar a necessidade de uma documentação especial[78] do tratamento de dados realizado sob esse fundamento. Nos moldes do artigo 37, da

76. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 167-168.

77. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 168.

78. BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 170.

LGPD, o controlador e o operador devem manter registros das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Nesse contexto, não se pode esquecer, tal como defende Chiara de Teffé e Mario Viola, que a utilização adequada e inteligente do legítimo interesse pode proporcionar e incrementar novos modelos de negócios e diversas estratégias comerciais, de segurança e inovação[79].

Considerações Finais

Pela interpretação do microssistema da LGPD, não existem óbices legislativos que impeçam a aplicação do consentimento ou do legítimo interesse para fundamentar a utilização dos cookies de publicidade. O agente de tratamento poderia fundamentar a utilização desses *cookies* em ambas as bases legais.

Nessa conjuntura, não seria de todo o errado entender que os *cookies* de publicidade poderiam enquadrar-se em mais de uma base legal, levando os agentes de tratamento e as empresas anunciantes (muitas vezes, confundidos na mesma pessoa) a utilizarem mais de uma hipótese autorizadora para fundamentar o tratamento de dados pessoais com o objetivo de segmentar, direcionar anúncios e criar perfis comportamentais de consumidores.

Sucede-se, todavia, que a cumulação de bases legais seria extremamente difícil de ser aplicada aos *cookies* de publicidade. Conforme visto nos tópicos supra, a escolha e adoção de uma base legal pelas empresas anunciantes e controladoras das páginas eletrônicas influenciará diretamente a condução dos banners e a redação das políticas de *cookies*. Pode ser que a cumulação da base legal não seja clara para o consumidor e, consequentemente, as empresas não cumprirão com o seu dever de transparência.

Por isso, entende-se que não havendo hierarquia entre as hipóteses legais, cabe ao agente de tratamento escolher e buscar a base mais segura e adequada[80] para fundamentar o tratamento de dados para fins de publicidade, visto que preza-se pelo princípio da melhor adequação (*i.e.*, a compatibilidade do tratamento com as finalidades informados ao titular, de acordo com o contex-

79. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023. p. 130.

80. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023 p. 131.

to do tratamento de dados).

Por fim, muito embora a tendência regulatória da ANPD volte-se para a prevalência do consentimento em detrimento da base legal do legítimo interesse no que tange à fundamentação da utilização de *cookies* de publicidade, tal entendimento pode-se restar ultrapassado diante do cenário legislativo brasileiro. Ainda que muitos a chamem de cláusula aberta e indeterminada, o artigo 10º da LGPD traz consigo critérios mais objetivos para dirimir as controvérsias do legítimo interesse e, por essa razão, deve-se começar a dar luz para as inúmeras vantagens dessa base legal, para promoção de novos modelos de negócios e novos modelos de operação, considerando, especialmente, o rápido desenvolvimento tecnológico e o aparecimento de tecnologias de inteligências artificiais cada vez mais autônomas.

Referências

Autoridade Nacional de Proteção de Dados Pessoais. *Guia orientativo: Cookies e proteção de dados pessoais*. [S.l.]. out 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 17 mai. 2023.

BIONI, Bruno Ricardo. Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. 3. ed. Rio de Janeiro: Forense, 2021. E-book Kindle.

BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

BIONI, Bruno Ricardo; RIELLI, Mariana; KITAYAMA, Marina. *O Legítimo Interesse na LGPD: Quadro Geral e Exemplos de Aplicação. Observatório da privacidade e proteção de dados e Data Privacy Brasil Research, 2021*. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf. Acesso em: 17 jun. 2023.

BLACK, Damien. *TikTok accused by privacy watchdog of tracking user emotions to sell advertising slots*. Cybernews, 2023. Disponível em: https://cybernews.com/privacy/tiktok-privacy-tracking-emotions-advertising/. Acesso em: 15 jun. 2023.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018.

BUCAR, Daniel; VIOLA, Mario. Tratamento de Dados Pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. 2. ed. Thomson Reuters, 2020.

CJEU Declares Meta/Facebook's Gdpr Approach Largely Illegal. Noyb, 2023. Disponível em: https://noyb.eu/en/cjeu-declares-metafacebooks-gdpr-approach-largely-illegal. Acesso em: 04 jul. 2023.

DAWSON, Brit. *Eating disorder sufferers on the danger of weight loss ads on TikTok*. Dazed, 2020. Disponível em: https://www.dazeddigital.com/life-culture/article/50566/1/eating-disorder-sufferers-on-the-danger-of-weight-loss-ads-on-tiktok. Acesso em: 15 jun. 2023.

EUROPA, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 1 jul. 2023.

How do the cookie rules relate to the GDPR? Ico.org.uk. Disponível em: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/#:~:text=The%20UK%20GDPR%20classes%20cookie,account%20at%20an%20online%20service. Acesso em: 4 jul. 2023

KOCH, Richie. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.EU. Disponível em: https://gdpr.eu/cookies/. Acesso em: 4 jul. 2023.

MARTINS, Pedro; SANTOS, Pedro Henrique. Relatório de Inteligência: Proteção de Dados e Marketing – D*a captação ao lead ao fechamento do negócio*. Data Privacy BR e Clube Data.

MENDES, Laura Schertel Mendes; FONSECA, Gabriel Campos Soares da. Proteção para além

do consentimento: tendências de materialização. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023

MIRAGEM, Bruno, MADALENA, Juliano. Comentários ao artigo 7º, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022.

PIVETO, Lucas Colombera Vaiano. Comentários ao artigo 10, da LGPD. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros (coords.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. Indaiatuba, SP: Editora Foco, 2022.

RODOTÁ, Stefano. *A vida na sociedade de vigilância – a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de Dados Pessoais na LGPD: Estudo sobre as Bases Legais dos Artigos 7°, e 11. In: MENDES, Laura Schertel; DANILO, Danilo; RODRIGUES, Otávio Luiz; SARLET, Ingo Wolfgang; BIONI, Bruno (Org.). *Tratado de Proteção de Dados Pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. *A utilização econômica de rastreadores e identificadores on-line de dados pessoais*. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters, 2020.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

11

Herança Digital: a tutela dos bens digitais híbridos na transmissão *post mortem*

EMÍLIA DE FREITAS CABREIRA

Introdução

A sociedade globalizada vive um momento de intensa transformação, passando o mundo virtual a integrar a realidade do cotidiano contemporâneo. Para ilustrar o citado cenário, cabe mencionar que o número de usuários da internet ultrapassou a marca de 5,1 bilhões no ano de 2023, o que representa cerca de 64,4% da população mundial.[2]

A aludida presença on-line consequentemente acarreta intensas mudanças nas relações como as conhecemos. Passamos a interagir por meio de redes sociais e e-mails, a adquirir moedas virtuais e acumular milhas aéreas, os quais são exemplos de ativos digitais (*digital assets*) presentes em nossa rotina, e cada usuário passa a deter o que se tem chamado de patrimônio digital. Diante da nova realidade vivenciada, surge uma nova categoria de bens jurídicos: os bens digitais. Com essa novidade também se instalam conflitos inéditos, como a tutela *post mortem* de tais ativos.

O referido tema permanece sem regulamentação específica no ordenamento jurídico brasileiro, inexistindo referência expressa na Lei Geral de Proteção de Dados Pessoais (LGPD) ou no Marco Civil da Internet. Tampouco há qualquer previsão no Código Civil em vigor, embora haja Projetos de Lei em tramitação na Câmara dos Deputados que visam a incluir o direito de Herança Digital no Código Civil.

A doutrina tem se debruçado sobre a questão e desempenhado relevante papel nesse propósito, buscando estabelecer categorias para um tratamento uniforme. Os bens digitais têm sido classificados quanto à sua natureza jurídica, dividindo-se em três categorias: bens digitais patrimoniais, bens digitais

1. Pós-graduada em Processo Civil e graduada em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul (UFRGS). Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio (ITS), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED).

2. DATAREPORTAL. Digital 2023: *Global Overview Report*. Disponível em: https://datareportal.com. Acesso em 01/05/2023.

existenciais e bens digitais híbridos ou dúplices, os quais possuem conteúdo econômico e existencial simultaneamente. Nessa terceira categoria inclui-se a pergunta que deu origem ao presente trabalho: qual a tutela jurídica dos bens digitais híbridos *post mortem*?

Tal questão foi inserida em intensos debates após se observar o crescimento de seguidores em perfis de redes sociais de celebridades depois do falecimento delas. Cita-se o caso da Marília Mendonça, em que o seu perfil no Instagram ganhou 2,3 milhões de seguidores nos doze meses seguintes ao seu falecimento, enquanto no Facebook o seu número de seguidores triplicou, alcançando 15 milhões de fãs. A artista também ganhou novos admiradores na plataforma de streaming Spotify, no YoTtube e no TikTok, totalizando mais de 17,3 milhões de novos seguidores.[3]

No momento, ainda não é claro o que deve acontecer com os aludidos perfis de notório aspecto econômico que muitas vezes seguem disponíveis na rede mundial de computadores após o falecimento dos seus titulares. É possível encontrar equilíbrio entre o direito à privacidade e o conteúdo patrimonial deles? A partir desse panorama, busca-se identificar e apresentar quais as correntes doutrinárias atuais sobre a sucessão hereditária dos bens digitais existenciais de natureza híbrida.

1. A Era Digital e a Nova Categoria de Bens Jurídicos

A vida humana tem cada vez mais habitado o mundo digital, provocando intensa mudança em nossa forma de perceber a realidade. Como bem refere Bruno Zampier, “ao longo da vida bilhões de pessoas irão interagir, externar seus pensamentos e opiniões, compartilhar fotos e vídeos, adquirir bens corpóreos e incorpóreos, contratar serviços, dentre centenas de outras possíveis atividades por meio da rede mundial de computadores”.[4]

A riqueza também acompanhou essa movimentação. Antes a sociedade tinha fixação por bens corpóreos, enquanto atualmente a riqueza circula intensamente naquilo que não se enxerga, como perfis digitais, criptomoedas, cotas em startups. Para ilustrar tal cenário, importa destacar que sete das dez

3. GLOBO. *Números de Marília Mendonça crescem e impressionam um ano após sua morte*. Disponível em: https://revistaquem.globo.com/google/amp/entretenimento/musica/noticia/2022/11/numeros-de-marilia-mendonca-crescem-e-impressionam-um-ano-apos-sua-morte.ghtmla. Acesso em 26. Nov. 2023.

4. ZAMPIER, Bruno. B*ens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 61.

maiores fortunas mundiais no ano de 2022 eram associadas à tecnologia e à internet.[5]

Para adentrar ao debate, é necessário inicialmente traçar o conceito de bem digital. Segundo Bruno Zampier, bens digitais são aqueles "bens incorpóreos, os quais são progressivamente inseridos na internet por um usuário, consistindo em informações de caráter pessoal que trazem alguma utilidade àquele, tenha ou não conteúdo econômico".[6] São perfis em redes sociais, músicas, vídeos, milhas aéreas, criptomoedas, entre outros diversos bens que estão presentes em — nosso atual estilo de vida.

A transmissão dos bens digitais *post mortem* é uma grande preocupação moderna, de feição patrimonial e de proteção aos direitos de personalidade da pessoa falecida. Segundo dispõe o artigo 6º do Código Civil, a existência da pessoa natural tem fim com a morte biológica. Por outro lado, o conteúdo postado por alguém em vida pode permanecer acessível indefinidamente na rede mundial de computadores. Consoante referem Heloísa Helena Barboza e Vitor Almeida, as memórias pessoais divulgadas em suporte digital são diferentes das memórias privadas que podem ser arquivadas em meios analógicos, tais como diários, fotografias e cadernos.[7]

E os desafios devem ir além dos que já presenciamos em nossas rotinas, visto que alguns aplicativos prometem prolongar a existência da pessoa falecida por meio do uso de inteligência artificial. Têm sido criados meios de interação com uma espécie de sistema operacional, programado com base em informações coletadas através de mensagens enviadas pela pessoa que faleceu, o que certamente traz novos desafios em relação à proteção de dados.[8] É preciso ponderar sobre os efeitos da permanência indefinida de uma vida digital de uma pessoa falecida, bem como compreender os limites da autonomia privada sobre os rumos de sua "existência digital" *post mortem* e os direitos e deveres dos familiares em relação à preservação da memória e o manuseio do conteúdo presente na rede perpetuamente.[9]

5. CAHALI, Francisco José; MARZAGÃO, Silvia Felipe. Os limites à vontade do planejador para dispor sobre a transmissão ou destruição de bens digitais híbridos. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 195-211. p. 198.

6. ZAMPIER, Bruno. Op. cit. 63-64.

7. BARBOZA, Heloisa Helena; ALMEIDA, Vitor. *Tecnologia, morte e direito: em busca de uma compreensão sistemática da "herança digital"*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 1-23. p. 4.

8. LEAL, Livia Teixeira. *Tratamento Jurídico do Conteúdo Disposto na Interna Após a Morte do Usuário e a Denominada Herança Digital*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 221-236. p. 223.

9. BARBOZA, Heloisa Helena; ALMEIDA, Vitor. *Tecnologia, morte e direito: em busca de uma compreensão sistemática da*

2. A Regulamentação no Brasil da Transmissão dos Bens Digitais *Post Mortem*

Preliminarmente é necessário esclarecer que, até o presente momento, inexiste regulamentação, de forma específica, sobre a destinação dos bens e dados digitais *post mortem*.[10]

O Marco Civil da Internet (Lei nº 12.965/14) nada dispôs sobre o tema, assim como o Código Civil. Atualmente, tramita na Câmara dos Deputados o Projeto de Lei nº 3.050/2020 e seus apensados (PL 3.051/2020, 410/2021, PL 1.144/2021, PL 1.689/2021, PL 2.664/2021, PL 703/2022), que pretende incluir no Código Civil o direito de herança digital, dispondo sobre a sucessão dos bens e contas digitais do autor da herança de qualidade patrimonial.[11]

A Lei Geral de Proteção de Dados (Lei nº 13.709/18) igualmente nada abarcou sobre o tratamento de dados após a morte do usuário. Contudo, em relação ao aludido ponto, importa mencionar que a Autoridade Nacional de Proteção de Dados (ANPD), após questionamento da Polícia Rodoviária Federal, publicou Nota Técnica 3/2023/CGF/ANPD em fevereiro de 2023, posicionando-se pela não incidência da LGPD no caso de tratamento de dados pessoais de pessoas falecidas.[12]

Segundo o entendimento da Coordenação-Geral de Fiscalização da ANPD, a existência da pessoa natural termina com a morte, conforme previsto no Código Civil, pressupondo-se que a incidência da LGPD ocorre apenas no âmbito do tratamento de dados pessoais de pessoas naturais vivas. Na referida Nota Técnica ainda foi destacado que "outras normas do ordenamento brasileiro visam a proteger os direitos de pessoas falecidas, como o direito sucessório e os direitos de personalidade, que incluem o direito ao nome e à imagem (art. 16 e 20, Código Civil)".

Frente a tantas mudanças, cada vez mais rápidas e céleres, a constituição de uma legislação própria deve garantir maior segurança jurídica aos usuários da internet.[13] Ainda sem tratamento legal, persiste a insegurança jurídica

---

"herança digital". In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 1-23. p. 21.

10. NEVARES, Ana Luiza Maia. *Testamento virtual: ponderações sobre a herança digital e o futuro do testamento*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 187-205. p. 197.

11. Disponível em: https://www.camara.leg.br/noticias/674175-projeto-assegura-a-familiares-direito-a-heranca-digital. Acesso em: 18 de jul. 2023.

12. BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Nota Técnica 3/2023/CGF/ANPD*. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica3CGF.ANPD.pdf>. Acesso em: 18 de jul. 2023.

13. HONORATO, Gabriel; GODINHO, Adriano Marteleto. *Planejamento sucessório e testamento digital: a proteção dinâmica*

sobre o tema e o Poder Judiciário cada vez mais deve ser demandado a solucionar questões oriundas do descompasso entre a morte e a permanência de conteúdos inseridos pelo usuário na rede ao longo de sua vida.[14]

3. A Transmissão *mortis causa* dos Bens Digitais conforme Classificação da Natureza

Na doutrina nacional, a análise acerca da transmissibilidade ou não dos bens digitais em virtude da sucessão *mortis causa* de seu titular tem início majoritariamente a partir da discussão quanto à sua natureza. A fim de buscar uma uniformização sobre o tema, têm-se estabelecido padrões e dividido os bens digitais em três categorias: bens digitais patrimoniais, bens digitais existenciais e bens digitais patrimoniais-existenciais.

Em relação aos bens digitais patrimoniais, Bruno Zampier os define quando "a informação inserida em rede for capaz de gerar repercussões econômicas imediatas" e cita como exemplos moedas virtuais, milhas aéreas e as ferramentas que incrementam os desafios em jogos de videogame. O autor ainda ressalta bibliotecas, videotecas e discotecas no mundo virtual, afirmando que o usuário pode adquirir esses arquivos licitamente, mediante o pagamento de valores diversos, e armazená-los em componentes físicos ou remotamente em contas digitais, com acesso através de senhas.[15] Por relevante, cumpre transcrever o seguinte trecho que aborda o tema:

> Não há dúvida de que estas novas formas de aquisição, armazenamento e utilização de livros, filmes e músicas integram o patrimônio digital do indivíduo. Quanto dinheiro efetivo não se desembolsa para a aquisição destes ativos? Quanto vale um arquivo deste? Quantas horas de navegação pela Internet foram necessárias para que se pudesse chegar à formação deste patrimônio?[16]

Zampier sustenta que o direito de propriedade dos bens digitais deveria gozar das mesmas faculdades jurídicas já existentes para a propriedade de

---

do patrimônio virtual. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 171-190. p.188.

14. LEAL, Livia Teixeira. *Tratamento Jurídico do Conteúdo Disposto na Interna Após a Morte do Usuário e a Denominada Herança Digital*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 225.

15. ZAMPIER, Bruno. *Bens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 78-80.

16. Ibid., p. 80.

roupagem tradicional, conforme previsão no artigo 1.228 do Código Civil. Assim sendo, segundo o autor, deve ser garantido o direito de dispor ao proprietário, além do evidente uso e gozo.[17]

O Direito das Sucessões se ocupa com a transmissão da herança que, em sentido amplo, é o conjunto patrimonial deixado pelo morto. Importa ressaltar que o patrimônio consiste em bens materiais e imateriais, mas avaliável economicamente, pois, em princípio, os direitos da personalidade se afastam da patrimonialidade.[18]

Ensinam Heloisa Barbosa e Vitor Almeida que "a herança é uma universalidade de direito, constituída pelo complexo de relações jurídicas, dotadas de valor econômico (CC, art. 91), que passam aos sucessores, como um todo unitário, mesmo que muitos sejam os herdeiros". Mencionam, ainda, que o direito dos sucessores sobre essa universalidade será indivisível até a partilha, com regulação pelas normas do condomínio.[19]

A partir de tal contexto, os bens patrimoniais digitais, considerados unicamente em seu valor econômico, poderiam ser transmitidos imediatamente aos herdeiros, em caso de morte do titular. A exceção desta hipótese seria manifestação em vida do titular, afirmando não ter interesse na transferência do bem aos herdeiros.[20]

Para ilustrar tal cenário, cabe referir que existem decisões judiciais que já admitiram a transferência de bens digitais de conteúdo patrimonial. Cita-se, como exemplo, a decisão proferida pela 11ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo, no processo nº 2160958-57.2022.8.26.0000, que autorizou a penhora de eventuais milhas aéreas ou pontos de programas de fidelidade de companhias aéreas em nome de um devedor.[21]

Quanto aos bens digitais existenciais, Bruno Zampier os define como a informação inserida na rede mundial capaz de gerar repercussões extrapa-

17. Ibid., p. 80.

18. VENOSA, Silvio de Salvo. *Sucessões e herança digital: Reflexões*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 19-28. p. 22.

19. BARBOZA, Heloisa Helena; ALMEIDA, Vitor. *Tecnologia, morte e direito: em busca de uma compreensão sistemática da "herança digital"*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 1-23. p. 11.

20. HONORATO, Gabriel; GODINHO, Adriano Marteleto. *Planejamento sucessório e testamento digital: a proteção dinâmica do patrimônio virtual*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 171-190. p.178.

21. CONSULTOR JURÍDICO. *Milhas aéreas têm natureza patrimonial e podem ser penhoradas, diz TJ-SP*. Disponível em: https://www.conjur.com.br/2023-mar-07/milhas-aereas-natureza-patrimonial-podem-penhoradas. Acesso em: 01 mai. 2023.

trimoniais. Arquivos de fotografias pessoais armazenados em redes sociais ou nuvens, vídeos, com imagem-voz ou imagem-retrato do próprio sujeito que foram publicadas ou que estejam arquivadas, e e-mails são exemplos de bens que teriam essa natureza.[22] Novamente, por considerar a importância da abordagem do autor, cumpre colacionar o seguinte excerto da sua obra a respeito dos bens digitais existenciais:

> Cada ser humano, a partir do momento em que se tornar usuário da Internet, terá a possibilidade de titularizar ativos digitais de natureza personalíssima. E esse movimento é altamente comum nos dias atuais, com a proliferação tantas vezes demonstrada neste estudo das redes sociais. O sujeito irá realizar o upload de fotos, vídeos, externar suas emoções, seus pensamentos, suas ideias, sua intimidade, com número limitado de pessoas. Esse conjunto de atributos extrapatrimoniais digitalizado ao longo do tempo, formaria a noção de bem tecnodigital existencial.[23]

Ana Carolina Teixeira e Carlos Konder afirmam que os bens digitais com função existencial estão presentes predominantemente no âmbito dos direitos da personalidade, em razão da ligação direta e imediata com a realização da dignidade da pessoa humana.[24] Desse modo, a informação sem repercussão econômica goza da proteção aos direitos da personalidade, os quais são bens jurídicos inerentes à pessoa.[25]

A transmissão hereditária dos bens de tal categoria gera importantes debates. Imagine o caso em que seja concedido acesso irrestrito aos familiares a conversas privadas do falecido. Além de violar o direito à privacidade de terceiros que se comunicaram com aquele usuário, também poderá haver a violação da privacidade e da intimidade do próprio usuário. Não se ignora a existência dos argumentos que apontam similitudes com a transmissão de bens físicos, como cartas e diários, os quais os familiares poderão ter acesso após a morte do seu titular. Contudo, há uma expectativa de privacidade maior em relação ao conteúdo no meio digital, tendo em vista que são protegidos por senhas.[26]

22. ZAMPIER, Bruno. *Bens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 116-117.

23. Ibid., p. 117.

24. TEIXEIRA, Ana Carolina Brochado; KONDER, Carlos Nelson. *O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 25-47. p. 38.

25. ZAMPIER, Bruno. *Bens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 116-117.

26. LEAL, Livia Teixeira. *Tratamento Jurídico do Conteúdo Disposto na Interna Após a Morte do Usuário e a Denominada Heran-*

A Constituição Federal enuncia uma longa série de direitos denominados personalíssimos e garantias individuais, que devem ser protegidos e respeitados como conteúdo mínimo para assegurar a coexistência em sociedade. O Código Civil de 2022 inseriu um capítulo sobre o tema, pela primeira vez de forma expressa e ordenada na legislação brasileira, e cada vez mais cresce em nossa sociedade a importância sobre a proteção à imagem, à privacidade, ao direito ao próprio corpo, entre outros.[27]

A personalidade, entendida como aptidão genérica para titularizar direitos e contrair obrigações, é extinta com a morte, mas os direitos de personalidade são projetados para além do falecimento de seu titular.[28] Ressalta-se o teor do artigo 12, *caput*, do CC/02 ao dispor que "pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei". O teor do parágrafo único do referido artigo acrescenta que, "em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau".

Assim sendo, embora as lesões aos direitos da personalidade do falecido não possam repercutir em razão do fim da existência do indivíduo, elas podem produzir efeitos no meio social, motivo pelo qual são coibidas na legislação, tendo sido conferida legitimidade a determinadas pessoas para agir diante de violações.[29]

Segundo Livia Teixeira Leal, não há no Direito brasileiro transmissão *post mortem* dos direitos da personalidade, mas sim a tutela de um centro de interesses relacionado à personalidade, considerada como valor. Aponta que não podem ser objeto de transferência os dados pessoais dos usuários falecidos, visto que se referem ao aspecto existencial do *de cujus*.[30]

Dessa forma, os bens digitais personalíssimos poderiam, ou deveriam, ser excluídos do meio digital quando a plataforma tomasse conhecimento a res-

---

ça Digital. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 226.

27. VENOSA, Silvio de Salvo. *Sucessões e herança digital: Reflexões*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 19-28. p. 23-24.

28. TERRA, Aline de Miranda Valverde; OLIVA, Milena Donato; MEDON, Filipe. *Acervo digital: controvérsias quanto à sucessão causa mortis*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 63-86. p. 65.

29. TERRA, Aline de Miranda Valverde; OLIVA, Milena Donato; MEDON, Filipe. *Acervo digital: controvérsias quanto à sucessão causa mortis*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 63-86. p. 66.

30. LEAL, Livia Teixeira. *Tratamento Jurídico do Conteúdo Disposto na Interna Após a Morte do Usuário e a Denominada Herança Digital*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 221-236. p. 232.

peito do óbito do usuário, visto que se enquadram em uma reserva de privacidade exclusiva dos titulares. A exceção ocorreria diante de específica manifestação em vida do titular sobre a transferência dos conteúdos aos seus herdeiros ou a pessoas por ele indicadas, medida que poderia ser adotada através de técnicas e ferramentas de planejamento sucessório.[31]

Ocorre que existem bens digitais de natureza híbrida, os quais não podem ser enquadrados exclusivamente como patrimoniais ou existenciais.[32] Nesses casos, o acesso ao ambiente virtual pressupõe o pagamento para que seja possível conhecer dados de outrem. Logo, o próprio indivíduo disponibiliza seus dados, como imagem, informações sobre a idade, gostos e preferências, a fim de obter ganhos financeiros.[33]

Os perfis de redes sociais e em canais do YouTube são exemplos, quando a inserção dos dados pessoais se presta a objetivos financeiros, como é o caso de blogueiros, influenciadores digitais e *YouTubers*. Trata-se de indivíduos com perfis em redes sociais, *sites* e canais do Youtube, que têm como objetivo a divulgação de produtos de forma remunerada.[34] Assim sendo, o que a princípio era somente fruto de uma liberdade de expressão acaba por se transformar em um negócio rentável.[35]

Para atrair seguidores, usualmente essas pessoas expõem sua rotina e estilo de vida. A imagem serve como influência para os seguidores e, com o crescimento da audiência, o retorno financeiro também aumenta. As postagens podem ter maior engajamento quando membros da família também são apresentados em anúncios, por exemplo. Ana Carolina Teixeira e Carlos Konder esclarecem que imagem, estilo de vida (pessoal e familiar) e reputação são elementos determinantes para a confiança do consumidor. Portanto, em que pese essa situação jurídica tenha como elemento central os dados pes-

31. HONORATO, Gabriel; GODINHO, Adriano Marteleto. Planejamento sucessório e testamento digital: a proteção dinâmica do patrimônio virtual. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 171-190. p. 178-179.

32. ZAMPIER, Bruno. *Bens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 117.

33. TEIXEIRA, Ana Carolina Brochado; KONDER, Carlos Nelson. *O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 25-47. p. 42.

34. TEIXEIRA, Ana Carolina Brochado; KONDER, Carlos Nelson. *O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 25-47. p. 41.

35. ZAMPIER, Bruno. *Bens Digitais: cibercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª ed. Indaiatuba, SP: Editora Foco, 2021. p. 118.

soais e a privacidade dos envolvidos tem como escopo fundamental objetivos de cunho financeiro, mediante o consentimento do titular.[36]

Conforme os indivíduos têm transferido partes de sua vida para o ambiente virtual, novos desafios para a proteção dos direitos da personalidade são revelados, especialmente dos direitos à intimidade e à privacidade, provocando consequências para a sucessão legítima de seus bens digitais. Consoante salientado por Simone Tassinari e Letícia Tedesco, "ao mesmo tempo em que se deve resguardar a legítima no tocante aos bens digitais, também deve-se assegurar a tutela dos direitos da personalidade do *de cujus*".[37]

4. A Transmissão *mortis causa* dos Bens Digitais Híbridos

A respeito da transmissibilidade dos bens digitais *post mortem*, Gabriel Honorato e Livia Leal citam que existem dois posicionamentos. O primeiro entende pela transmissão de todos os conteúdos, independentemente da sua natureza, com exceção no caso de haver manifestação de vontade do próprio usuário em vida em sentido diverso. Essa corrente entende, portanto, que todo o acervo se projeta consoante o princípio da *saisine*.[38]

Terra, Oliva e Medon explicam que o "referido entendimento passou a reverberar com maior intensidade após o julgamento do *leading case* pelo *Bundesgerichtshof* (BGH), em 2018", bem como apontam que essa posição vem ganhando força.[39] Sobre o caso, Laura Schertel Mendes e Karina Nunes Fritz narram que:

> Os pais de uma adolescente de 15 anos, falecida em um acidente no metrô de Berlim, em 2012, entraram com uma ação contra o Facebook, alegando terem sido impedidos de acessar a conta da filha, que havia sido transformada em "memorial". As circunstâncias da morte não estavam esclarecidas, havendo suspeita de suicídio e mobbing no colégio. O objetivo do acesso à conta, segundo os pais, era compreender a causa do falecimento da filha, de modo a es-

36. TEIXEIRA, Ana Carolina Brochado; KONDER, Carlos Nelson. op. cit. 40-41.

37. FLEISCHMANN, Simone Tassinari Cardoso; TEDESCO, Letícia Trevizan. *Legítima e Herança Digital: um desafio quase impossível*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 165-186. p. 175-176.

38. HONORATO, Gabriel; LEAL, Livia Teixeira. *Exploração econômica de perfis de pessoas falecidas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 143-163. p. 151.

39. TERRA, Aline de Miranda Valverde; OLIVA, Milena Donato; MEDON, Filipe. *Acervo digital: controvérsias quanto à sucessão causa mortis*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 63-86. p. 68.

> clarecer se se tratou de suicídio ou de acidente. Essa questão era relevante também para a defesa dos pais em processo judicial de reparação movido pelo condutor do transporte público, que estava pleiteando danos morais pelo abalo emocional por ele sofrido em decorrência do envolvimento no suposto suicídio.[40]

Na decisão do *Bundesgerichtshof* (BGH), equivalente ao Superior Tribunal de Justiça Brasileiro, proferida em 12/07/2018, foi reconhecido o direito sucessório da conta e do seu conteúdo aos genitores. Novamente citam-se Laura Schertel Mendes e Karina Nunes Fritz, que assim detalharam a decisão:

> Em síntese, a Corte Federal alemã reconheceu a pretensão dos pais, herdeiros únicos da menor, de ter acesso à conta e a todo o conteúdo nela existente uma vez que essa pretensão decorre do contrato de consumo (contrato de utilização) existente entre a adolescente é o Facebook, o qual é transmissível aos herdeiros com a morte. Para a Corte, o direito sucessório à herança digital não se opõe aos direitos de personalidade *post mortem* da falecida, ao direito geral de personalidade do *de cujus* ou dos terceiros interlocutores, ao sigilo das comunicações, nem tampouco às regras sobre proteção de dados pessoais.[41]

As autoras, que se filiam à corrente adotada no demonstrado *leading case*, sustentam que, se o titular não decide a respeito do destino da herança digital, cabe a transmissibilidade de todo o conteúdo digital aos herdeiros, tal como ocorre no conteúdo analógico.[42] Argumentam que a tutela do caráter existencial do conteúdo, que visa a proteger a privacidade, a intimidade e a personalidade do falecido ou de terceiro, independe do meio em que se materializa tal conteúdo. Em suas palavras, Laura Schertel Mendes e Karina Nunes Fritz afirmam que "parece incoerente permitir a transmissão de cartas, diários e informações confidenciais e vedar a transmissão daquelas armazenadas em nuvens ou nos servidores de plataformas digitais, como o Facebook".[43] Apontam, ainda, que a "existencialidade não resulta da forma como tais informações estão corporificadas ou salvas, mas exclusivamente de seu próprio conteúdo".[44]

40. MENDES, Laura Schertel Ferreira; FRITZ, Karina Nunes. *Case report: corte alemã reconhece a transmissibilidade da herança digital*. RDU, Porto Alegre, v.15, n.85, 2019. p.188-211. p. 192-193.

41. Ibid.,. p. 194.

42. MENDES, Laura Schertel Ferreira; FRITZ, Karina Nunes. *Case report: corte alemã reconhece a transmissibilidade da herança digital*. RDU, Porto Alegre, v.15, n.85, 2019. p.188-211. p. 204.

43. Ibid., p. 202.

44. Ibid., p. 202.

A segunda corrente doutrinária, adotada por Gabriel Honorato e Livia Leal, já pincelada no capítulo anterior, entende que, ao menos em tese, apenas os bens de natureza patrimonial deveriam seguir a regra geral do direito sucessório. Em relação aos demais, os autores esclarecem que não estariam sujeitos à transmissão aos sucessores em razão da preservação da privacidade do falecido e de terceiros com quem houve interação. Assim sendo, nem mesmo diante da manifestação do autor da herança seria possível optar pela destinação dos ativos a herdeiros quando puderem comprometer a personalidade de outrem.[45]

Nas palavras de Gabriel Honorato e Livia Leal:

> A dignidade da pessoa humana, como princípio norteador de todo o ordenamento vigente, não poderia ser sobreposta pela autonomia privada, seja daqueles sujeitos que almejam projetar seus conteúdos para os sucessores sem a preservação dos direitos de terceiros ou seja daqueles herdeiros que objetivam acessar conteúdos restritos do falecido sem a sua prévia manifestação. Parece evidente que todo o arcabouço de valores incluídos na dignidade humana, como a imagem, a honra e a privacidade devem ter privilégio nas ponderações tanto do intérprete como do legislador.[46]

No mesmo sentido defende Ana Luiza Nevares, afirmando que "não parece conforme a dignidade humana e a necessária proteção de sua personalidade *post mortem* que haja uma transmissão hereditária *tout court* de todos os dados e bens digitais da pessoa falecida, sem que ela tenha expressamente assim consentido".[47]

A respeito dos bens digitais híbridos, Gabriel Honorato e Livia Leal mencionam a importância dos mecanismos de planejamento sucessório, os quais permitem a escolha, pelo próprio titular da conta, sobre a administração do perfil após o falecimento, podendo o titular optar pela sua exclusão ou congelamento de sua conta, dotada de aspecto personalíssimo.[48]

45. HONORATO, Gabriel; LEAL, Livia Teixeira. *Exploração econômica de perfis de pessoas falecidas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 143-163. p. 151.

46. Ibid., p. 152.

47. NEVARES, Ana Luiza Maia. *Testamento virtual: ponderações sobre a herança digital e o futuro do testamento*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 187-205. p. 198-199.

48. HONORATO, Gabriel; LEAL, Livia Teixeira. *Exploração econômica de perfis de pessoas falecidas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 143-163. p. 154.

Francisco Cahali e Silvia Marzagão igualmente sustentam a intransmissibilidade, em regra, dos bens digitais puramente existenciais.[49] Todavia, ao falarem sobre a disponibilidade de bens digitais híbridos, os autores citam duas situações hipotéticas. Na primeira o falecido determina a transferência do patrimônio a terceiro, o que os autores afirmam que, respeitados os limites da legítima e a questão relativa à privacidade do falecido e de terceiros, mostra-se factível e possível a disposição do conteúdo e planejamento.[50]

Na segunda hipótese apresentada pelos autores, o titular determina a destruição do bem quando do seu falecimento, o que alegam ser muito mais complexo, considerando o aspecto patrimonial agregado potencialmente ao bem. Argumentam que o direito à privacidade seria mitigado em relação a pessoas públicas e notórias em razão da exposição de sua imagem, especialmente as que obtiveram fama em virtude da revelação de atos deliberados.[51]

Nesse caso, referem que haverá dilema quanto à determinação de exclusão, mencionando que a herança carrega em si elementos atrelados ao princípio da solidariedade e da função social da propriedade. O direito à herança está previsto no artigo 5º, inc. XXX, da Constituição Federal, o qual possui função social, visto que valoriza a propriedade e o interesse na formação e avanço patrimonial, de modo a estimular a poupança e o desempenho no progresso econômico. Salientam que tais fatos, de forma direta ou indireta, acabam por impulsionar o desenvolvimento da própria sociedade.[52]

Assim sendo, permitir a destruição de tais bens representaria possível ofensa à função social que traz consigo o bem e a herança.[53] Para melhor elucidação os doutrinadores citam a seguinte situação:

> A questão parece mais clara ao transportarmos a situação para bens materiais. Imaginemos que Pablo Picasso, que por ocasião de sua morte deixou 45 mil obras de arte, estabelecesse em seu testamento a vontade explícita de que toda a sua produção artística fosse imediatamente queimada quando de seu passamento, afirmando que aquelas obras retratam suas angústias e aflições e, por esse motivo, têm elementos de sua personalidade nelas impressas.

49. CAHALI, Francisco José; MARZAGÃO, Silvia Felipe. *Os limites à vontade do planejador para dispor sobre a transmissão ou destruição de bens digitais híbridos*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 195-211. p. 202-203.

50. Ibid., p. 204.

51. Ibid., p. 204.

52. Ibid, p. 207-208.

53. Ibid., p. 208.

> Podemos até admitir que as obras, de alguma maneira, tenham elementos existenciais do artista, mas o relevante valor patrimonial levaria ao certeiro questionamento sobre a possibilidade ou não de destruição desse patrimônio.
> Da mesma forma ocorre com os bens digitais híbridos: ainda que contenham elementos existenciais, parece bastante complexa a permissão da destruição pura e simples, com comprometimento patrimonial do que se transmitirá aos herdeiros, especialmente pensando na obrigatoriedade de observância da legítima.[54]

Desse modo, considerando que a destruição de bens digitais híbridos pode impactar financeiramente o legado que o *de cujus* deixa para transferência aos seus herdeiros, sustentam ser legítimo aos herdeiros se oporem, tendo em vista o princípio da solidariedade, da função social da herança e da necessidade de observância da legítima. Francisco Cahali e Silvia Marzagão também ressaltam que a cindibilidade dos conteúdos de aspecto patrimonial e existencial, quando possível, pode facilitar o direcionamento da questão.[55]

Além da problemática a respeito da possibilidade de transmissibilidade dos bens digitais que contenham reflexos nos direitos da personalidade do *de cujus*, também há outra importante questão, referente à valoração do bem digital. Como será realizada a quantificação desses bens, tendo em vista o necessário cálculo da legítima?[56]

Mais um ponto a ser debatido deriva de bens digitais submetidos a termos de uso. Consideráveis bens digitais são controlados por empresas, as quais são responsáveis pela disponibilização e manutenção, enquanto os temas referentes à propriedade e à possibilidade de transferência podem ser tratados conforme as disposições de termos de uso, aceito pelo usuário quando da criação de determinada conta on-line.[57]

No caso da rede social Facebook, é permitido ao usuário a escolha de contato herdeiro para cuidar do perfil depois de ser transformado em memorial ou optar pela exclusão da conta permanentemente. Com o perfil transformado em memorial, o conteúdo que a pessoa compartilhou permanecerá na página

54. CAHALI, Francisco José; MARZAGÃO, Silvia Felipe. *Os limites à vontade do planejador para dispor sobre a transmissão ou destruição de bens digitais híbridos*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 195-211. p. 208.

55. Ibid., p. 209-210.

56. FLEISCHMANN, Simone Tassinari Cardoso; TEDESCO, Letícia Trevizan. *Legítima e Herança Digital: um desafio quase impossível*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 165-186. p. 166.

57. Ibid,. p. 181

e ficará visível para o público com o qual foi compartilhado e haverá a expressão "em memória de" ao lado do nome da pessoa do perfil. O contato herdeiro poderá aceitar solicitações de amizade em nome de um perfil transformado em memorial, além de alterar a foto do perfil e a foto de capa.[58]

O Instagram permite que outros usuários da rede social solicitem a transformação da conta de pessoa falecida em memorial, sendo necessária a prova do falecimento, como link para obituário ou artigo em jornal. A plataforma esclarece não ser possível divulgar informações de login de uma conta transformada em memorial e que a entrada na conta de outra pessoa sempre viola as políticas da rede social. Também é permitido aos familiares diretos solicitarem a remoção da conta do falecido, igualmente mediante comprovação, como envio de certidões de nascimento e óbito da pessoa falecida ou comprovação de autoridade de acordo com a legislação local de que se trata de representante legal da pessoa falecida ou do espólio.[59]

As disposições a respeito da destinação *post mortem* dos bens digitais nos termos de uso das plataformas digitais são importantes, especialmente diante da ausência de previsão legal até o momento. Contudo, importa destacar que esses termos são alterados frequentemente, além de ser comum que os usuários os aceitem sem fazer a efetiva leitura ou compreensão.[60]

Especificamente quanto à validade das aludidas disposições, Terra, Oliva e Medon apontam que se mostram de duvidosa legalidade, uma vez que retiram a autodeterminação do titular, o qual não pode escolher a destinação a ser dada aos seus bens digitais em razão de seu falecimento. Os autores apontam que as disposições contratuais não podem se sobrepor ao direito sucessório, especialmente quando são decorrentes de cláusulas-padrão inseridas em contrato de adesão.[61]

Portanto, verifica-se que a própria internet dispõe de mecanismos para auxiliar a transmissão de contas virtuais pelo titular aos seus herdeiros, mas,

58. Central de ajuda do Facebook. Disponível em: https://pt-br.facebook.com/help/103897939701143/?helpref=uf_share. Acesso em: 02 dez. 2023.

59. Central de ajuda do Instagram. Disponível em: https://help.instagram.com/264154560391256/?helpref=uf_share. Acesso em: 02 dez. 2023.

60. FLEISCHMANN, Simone Tassinari Cardoso; TEDESCO, Letícia Trevizan. *Legítima e Herança Digital: um desafio quase impossível*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 165-186. p. 182.

61. TERRA, Aline de Miranda Valverde; OLIVA, Milena Donato; MEDON, Filipe. *Acervo digital: controvérsias quanto à sucessão causa mortis*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 63-86. p. 71-72.

como bem questionam Gabriel Honorato e Livia Leal, “para além da discussão a respeito da validade destas, pergunta-se: qual manifestação deverá prevalecer em havendo conflito entre a manifestação na plataforma e aquela realizada através de um testamento público, por exemplo?”[62]

Considerações finais

Em nossa realidade, o mundo físico se mistura profundamente ao mundo digital. Passamos a interagir tanto presencialmente quanto virtualmente com outros indivíduos, e as relações se tornam complexas. Por exemplo, uma celebridade pode usar seu perfil pessoal nas redes sociais para compartilhar suas vivências e simultaneamente auferir renda a partir disso. Mas o que acontece com tal perfil quando esse usuário falece?

Até o momento inexiste regulamentação da Herança Digital no ordenamento jurídico brasileiro. Diante da omissão legislativa, o papel desempenhado pelos doutrinadores é extremamente importante para o aprofundamento da questão e apresentação de soluções possíveis.

Com as mudanças nas formas de interações atuais, uma nova categoria de bens jurídicos tem sido classificada, a dos bens digitais. Consoante a majoritária doutrina nacional, os bens digitais dividem-se em três categorias, sendo elas: bens digitais patrimoniais, bens digitais existenciais e bens digitais híbridos.

Ao abordarmos as questões atinentes à transferência dos bens digitais *post mortem*, a maior indagação reside na transferência dos bens digitais híbridos, como de perfis de celebridades em redes sociais. A dificuldade está na simultaneidade nesses casos do caráter patrimonial, que, ao considerar apenas o caráter econômico, autoriza a transmissão *mortis causa*; e do caráter existencial, que, em princípio, não a autoriza, em atenção à tutela dos direitos da personalidade, projetados para além do falecimento do seu titular.

Importa mencionar que existem dois principais posicionamentos sobre a transmissibilidade dos bens digitais após o falecimento do autor da herança. O primeiro entende que todo o acervo se projeta conforme o princípio da saisine, logo seria possível a transmissão de todos os conteúdos aos herdeiros, independentemente da sua natureza. A segunda corrente entende que, em princí-

62. HONORATO, Gabriel; LEAL, Livia Teixeira. *Exploração econômica de perfis de pessoas falecidas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 143-163. p. 157.

pio, somente os bens de natureza patrimonial deveriam seguir a regra geral do direito sucessório. Os demais, contudo, não estariam sujeitos à transmissão imediata aos sucessores, devendo-se preservar a privacidade do falecido e de terceiros com quem aquele tenha interagido.

Ademais, alguns estudiosos ponderarem sobre limitações ao autor da herança nos casos de bens digitais híbridos, especialmente quando detiverem valor patrimonial agregado, inviabilizando a determinação de sua destruição, em virtude do princípio da solidariedade, da função social da herança e da necessidade de observar à legítima. Outro aspecto relevante é a possibilidade de cindir os conteúdos, quando viável, permitindo a facilitação na busca de soluções.

Diante das intensas transformações decorrentes do estilo de vida na Era da Informação, o debate permanece aberto e em ebulição. Por enquanto, existem mais perguntas do que respostas, sendo importante o aprofundamento dos estudos sobre essa temática tão recente e presente em nossas vidas para termos respostas mais adequadas à nossa realidade.

Referências

BARBOZA, Heloisa Helena; ALMEIDA, Vitor. *Tecnologia, morte e direito: em busca de uma compreensão sistemática da "herança digital"*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 1-23.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Nota Técnica 3/2023/CGF/ANPD*. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica3CGF.ANPD.pdf>. Acesso em: 18 de jul. 2023.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 01 mai. 2023.

CAHALI, Francisco José; MARZAGÃO, Silvia Felipe. *Os limites à vontade do planejador para dispor sobre a transmissão ou destruição de bens digitais híbridos*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 195-211.

CONSULTOR JURÍDICO. *Milhas aéreas têm natureza patrimonial e podem ser penhoradas, diz TJ-SP*. Disponível em: https://www.conjur.com.br/2023-mar-07/milhas-aereas-natureza-patrimonial-podem-penhoradas. Acesso em: 01 mai. 2023.

DATAREPORTAL. *Digital 2023: Global Overview Report*. Disponível em: https://datareportal.com. Acesso em: 01 mai. 2023.

FLEISCHMANN, Simone Tassinari Cardoso; TEDESCO, Letícia Trevizan. *Legítima e Herança Digital: um desafio quase impossível*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 165-186.

GLOBO. *Números de Marília Mendonça crescem e impressionam um ano após sua morte*. Disponível em: https://revistaquem.globo.com/google/amp/entretenimento/musica/noticia/2022/11/numeros-de-marilia-mendonca-crescem-e-impressionam-um-ano-apos-sua-morte.ghtmla. Acesso em 26. Nov. 2023.

HONORATO, Gabriel; GODINHO, Adriano Marteleto. *Planejamento sucessório e testamento digital: a proteção dinâmica do patrimônio virtual*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 171-190.

HONORATO, Gabriel; LEAL, Livia Teixeira. *Exploração econômica de perfis de pessoas falecidas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 143-163.

LEAL, Livia Teixeira. *Tratamento Jurídico do Conteúdo Disposto na Interna Após a Morte do Usuário e a Denominada Herança Digital*. In: TEIXEIRA, Daniele Chaves (org.). Arquitetura do planejamento sucessório. Tomo I. 3ª ed. Belo Horizonte: Fórum, 2022. p. 221-236.

MENDES, Laura Schertel Ferreira; FRITZ, Karina Nunes. *Case report: corte alemã reconhece a transmissibilidade da herança digital*. RDU, Porto Alegre, v.15, n.85, 2019. p.188-211.

NEVARES, Ana Luiza Maia. *Testamento virtual: ponderações sobre a herança digital e o futuro do testamento*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 187-205.

TEIXEIRA, Ana Carolina Brochado; KONDER, Carlos Nelson. *O enquadramento dos bens digitais sob o perfil funcional das situações jurídicas*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança Digital: Controvérsias e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 25-47.

TERRA, Aline de Miranda Valverde; OLIVA, Milena Donato; MEDON, Filipe. *Acervo digital: controvérsias quanto à sucessão causa mortis*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Lívia Teixeira. (orgs.). Herança Digital: Controvérsias

e Alternativas. Tomo I. 2ª Ed. Indaiatuba: Foco, 2022. p. 63-86.

VENOSA, Silvio de Salvo. *Sucessões e herança digital: Reflexões*. In: TEIXEIRA, Ana Carolina Brochado; LEAL, Livia Teixeira (org.). Herança digital: controvérsias e alternativas. Tomo II. 1ª Ed. Indaiatuba: Foco, 2022. p. 19-28.

ZAMPIER, Bruno. *Bens digitais: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. 2ª Ed. Indaiatuba: Foco, 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

Blockchain e o Sistema Tributário Brasileiro: expectativa de eficiência na tributação da economia digital

AMANDA CARVALHO DOS SANTOS

Introdução

A ascensão da Quarta Revolução Industrial é uma realidade no mundo contemporâneo, traduzindo-se na integração de novas tecnologias disruptivas que vêm modificando, em larga escala, a troca de dados, as etapas de produção e os modelos de negócios, no Brasil e no mundo, como, por exemplo, a *blockchain*, que permite a realização de transações integralmente automatizadas, conferindo eficiência, segurança, agilidade, transparência e confiabilidade para seus usuários, funcionando como uma "cadeia de blocos", que permite o armazenamento dos códigos computacionais que dão origem aos *smart contracts*.[2]

Por sua vez, os contratos inteligentes baseados na blockchain, os referidos "smart contracts", são programações autoexecutáveis dos termos de um acordo quando as condições preestabelecidas são atendidas pelas partes.[3] São procedimentos armazenados nas células de banco de dados da *blockchain*.

No presente artigo será apresentada uma análise, teórica e prática, sem qualquer intuito de esgotar o tema, de como a tecnologia Blockchain pode contribuir para a simplificação no sistema de cobrança de tributos, na medida que a ferramenta poderá propiciar uma significativa redução em custos operacionais, bem como facilitará os processos de cálculo e recolhimento de tributos, além de proporcionar um ambiente essencialmente transparente e uniformizado.

A *blockchain*, assim como os *smart contracts*, serão analisadas como tecnologias passíveis de serem utilizadas como mecanismos a favor do fisco, com

1. Advogada formada pela Universidade Federal do Rio de Janeiro. Pós Graduanda em Direito Digital pela Universidade Estadual do Rio de Janeiro. E-mail: amanda.santos@ufrj.br

2. GATTESCHI, Valentina; ORCID, Fabrizio Lamberti; ORCID, Claudio Demartini; PRANTEDA, Chiara; SANTAMARÍA, Victor. *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?* Future Internet, v. 10, fev. 2018. Disponível em: <http://www.mdpi.com/1999-5903/10/2/20/htm>. Acesso em 15 de maio de 2023.

3. CAPGEMINI. *Smart Contracts in Financial Services: Getting from Hype to Reality*. 2016. Disponível em: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf. Acesso em 20 de junho de 2023.

o aumento da adesão na arrecadação e a facilitação da análise das operações tributáveis; e em benefício do contribuinte, como ferramenta apta a descomplexificar o cumprimento das obrigações tributárias e a proporcionar maior acessibilidade, transparência e segurança nas transações.

A implementação de tecnologia na sistemática de cobrança de tributos implica em uma nova lógica de funcionamento do sistema tributário nacional, que pode contribuir com um desenvolvimento exponencial da ordem econômica nacional.

1. Indústria 4.0 e novas tecnologias

O termo "Indústria 4.0" traduz-se no conjunto de soluções que integram equipamentos, serviços de alto valor agregado e *softwares* para explorar o uso de insumos na produção de bens customizados.[4] Em suma, é um conceito que engloba a crescente automação, com a integração de um extenso sistema de tecnologias como inteligência artificial, nanotecnologia, robótica avançada, IoT (*Internet of Things*), impressão 3D e *Cloud Computing*, que podem ser usadas em conjunto, propiciando o aprimoramento dos métodos de produção.

Nesse contexto, tecnologia de sistemas ciber físicos - CPS permitem que empresas tenham a oportunidade de representar a realidade do mundo físico em ambientes digitais, ou seja, conseguem fazer simulações, testes, alternativas de modelagem, design e análise de forma integrada; Internet das Coisas (IoT) conecta máquinas, objetos e pessoas em tempo real e *Cloud Computing* oferece soluções em além de possibilitar a troca e gestão de informações, permitindo combinar processos produtivos e de negócios para a criação de valor para as organizações.

A utilização de dispositivos "inteligentes" tem a capacidade de produzir impactos significativos na produtividade, uma vez que amplia a eficiência do uso de recursos e no desenvolvimento de produtos em larga escala, além de propiciar a integração do país em cadeias globais de valor.

Um forte elemento da Indústria 4.0, e uma das diversas vantagens da *blockchain*, é a rastreabilidade, característica que favorece diversos modelos de negócios, aprimora o controle e contribui para a gestão dos processos de produção com a integração de dados.

4. DE WECK, O. et al. *Trends in Advanced Manufacturing Technology Innovation*. Production in the Innovation Economy (PIE) Study. Cambridge: Massachusetts Institute of Technology (MIT), 2013.

Em síntese, as novas tecnologias se apresentam como impulsionadores e facilitadores em diversos setores econômicos, e principalmente como mecanismo de mudanças na manufatura, o que promete revolucionar os meios de produção e a sociedade como um todo.

2. *Blockchain*

A *blockchain*, em uma tradução literal do inglês, significa "cadeia de blocos". Metaforicamente, assim poderia se entender, por se tratar de um banco de dados único, em que as informações são compartilhadas e validadas entre os diferentes participantes da cadeia, em uma espécie de consenso sobre tais informações, conferindo assim, maior transparência e confiabilidade.

A tecnologia *blockchain* tem sido mencionada como solução adequada para uma nova geração de aplicações transacionais, definida como um livro razão compartilhado e imutável que tem como principal objetivo facilitar o processo de registro, identificação e localização das transações e operações envolvendo ativos – tangíveis e/ou intangíveis – e o cumprimento de obrigações ou contratos em uma rede descentralizada, visando à redução de riscos e custos, com maior garantia de segurança, eficiência e transparência.[5]

Tendo em vista a amplitude de benefícios proporcionados, a tecnologia blockchain está sendo cada vez mais implementada em diversos setores econômicos, como no bancário, imobiliário e de logística. Além disso, a ferramenta vem sendo utilizada pelo governo federal, prometendo garantir proteção aos dados, simplificação de processos, redução das fraudes e dos desperdícios e, ao mesmo tempo, aumentar a confiança e a responsabilidade, rumo a um desenvolvimento mais sustentável.

Segundo o Centro de Excelência (CoE) em *blockchain* da SERPRO[6]:

> Estas promessas se baseiam sobretudo no uso de criptografia, no compartilhamento dos registros que são gravados de forma distribuída e nos algoritmos de consenso, que garantem a segurança, rastreabilidade e auditabilidade destes registros. Tudo isso faz desta tecnologia uma forte candidata para implementar a tão desejada transformação digital dos serviços públicos.

5. GUPTA, Manav. *Blockchain For Dummies*, IBM Limited Edition. 1.ed. Hoboken – NJ; Editora John Wiley & Sons, Inc. 2017, p.3.
6. *Como o governo federal usa o blockchain?* https://www.serpro.gov.br/menu/noticias/noticias-2023/blockchain-no-governo-federal. Acessado em 23 de julho de 2023.

As negociações na *blockchain* podem envolver tanto ativos digitais como representações digitais de ativos existentes no mundo tangível, que, ao serem digitalizados, são representados por um token. Ao ser realizada, determinada operação é registrada pelo sistema, que identificará os sujeitos envolvidos, o que cada uma das partes recebeu na transação e o momento em que ela se concretizou.

Cada um dos usuários da *blockchain* possui duas "chaves": 1) uma privada, pessoal, que além de permitir o acesso à rede (uma espécie de *login* e senha), serve como uma certificação que aparecerá no registro das transações realizadas na *blockchain*; e 2) outra pública, que pode ser compartilhada com todos e identifica as transações efetuadas por determinado usuário. [7]

Em sequência, a *blockchain* utiliza como um dos mecanismos de consenso o conceito de *Proof-of-Work* (prova de trabalho) para realizar a validação das transações realizadas na rede. Este conceito é um algoritmo, um protocolo criptográfico, que requer que certa quantidade de membros de uma rede validem as transações emitidas dentro dessa rede, para provar que um consenso foi alcançado.

Após a validação, os dados referentes à operação passam a agregar a cadeia de dados referentes às transações anteriores envolvendo o mesmo ativo, formando aquilo que se denomina de "bloco". Os blocos são um conjunto de registros cronológicos de operações envolvendo o mesmo ativo ao qual se atribui uma identidade — *hash* —, de modo que passam a ser vistos como uma unidade.

Quando uma transação é finalizada, o seu armazenamento é realizado dentro de um "bloco", que está interligado em cadeia a outros blocos – relativos a transações anteriores, sendo praticamente impossível a modificação de um bloco sem a modificação de toda a cadeia.

Uma rede *blockchain* pode ainda ser caracterizada como pública ou privada. A rede pública não requer autenticação para um novo usuário fazer parte da rede, além disso, todos os dados são públicos e acessíveis. Por outro lado, na rede privada, somente os usuários que forem autorizados a ingressar podem fazer parte da rede e emitir transações. Este modelo de rede *blockchain* é mais indicado para as empresas que desejam manter um alto nível de governança sobre sua rede, e buscam a proteção de dados sensíveis institucionais.

7. MENDES, Daniele; FERREIRA, Paulo.; DE CASTRO, Douglas. *Blockchain e Agenda 2030*. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4938. Acesso em 10 de julho de 2023.

Não há dúvidas que em trocas de informações pelos governos, por exemplo, a melhor opção seria a *blockchain* privada, a fim de blindar a segurança nacional. Inclusive, a própria Receita Federal do Brasil[8] deixou claro que

> A implementação da Receita Federal utiliza a tecnologia *Blockchain*, em uma abordagem de rede permissionada em que apenas as entidades autorizadas participarão da rede. Toda a tecnologia está baseada em software livre de código fonte aberto e auditável.

Gisele Bossa e Eduardo Gomes[9] chamam atenção para formas de utilização da referida tecnologia e sua importância para a Administração Tributária:

> Em vista da dinâmica de funcionamento do *blockchain* é oportuno reconhecer sua capacidade de evitar as referidas assimetrias internas e internacionais. A *blockchain* pode sim aumentar a eficiência da Administração Tributária pois otimiza o cruzamento de informações, auxiliando na pouca uniformidade e assertividade dos campos constantes dos formulários usualmente adotados. Ao trazer informações específicas sobre contribuintes, permitiria ao fisco selecionar as operações que devem ser fiscalizadas, com maior propriedade, resultando em trabalhos fiscais mais sofisticados e com alto potencial de arrecadação. No mais, como poderia ser utilizada simultaneamente e em tempo real por Administrações Tributárias diversas, constituiria relevante ferramenta para a implementação de tratados internacionais.

Ademais, Aleksandra Bal destaca que, no âmbito tributário, a *blockchain* teria três usos em potencial: (i) segurança na cadeia de fornecedores; (ii) automatização do cálculo dos tributos, e (iii) identificação das atividades que geram valor nas operações do grupo.

A rastreabilidade e a imutabilidade são características essenciais da *blockchain*. Uma vez efetuada a transação no bloco, não há a possibilidade de mudança. As atualizações se dão por meio da criação de novas transações, as quais apontarão para a anterior e indicarão a atualização. Com dados imutáveis, tem-se a garantia da integridade do dado e sua irretratabilidade. Sendo

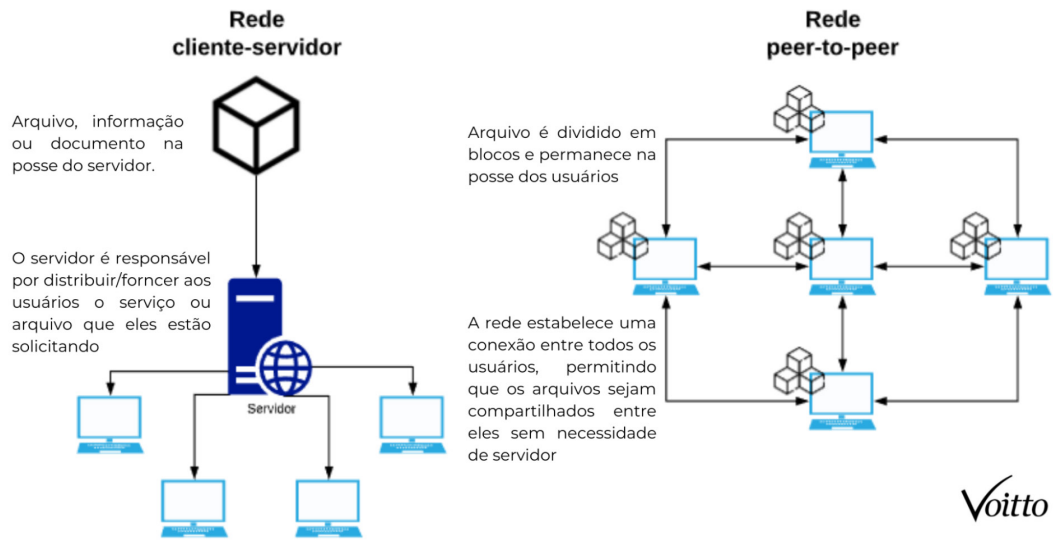
8. *Receita Federal Publica Norma Sobre Compartilhamento de Dados Utilizando Tecnologia Blockchain*, novembro, 2018. Disponível em http://idg.receita.fazenda.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobrecompartilhamento-de-dados-utilizando-tecnologia-blockchain. Acessado em 10 maio 23

9. BOSSA, G e GOMES, E. *Blockchain: Tecnologia à Serviço da Troca de Informações Fiscais ou Instrumento de Ameaça a privacidade dos Contribuintes?* In PISCITELLI, Tathiane (Coord), Tributação da Economia digital. RT. 2017, p. 375.

ponto a ponto, a *blockchain* utiliza o conceito de computação distribuída, reduzindo custos e aumentando a velocidade dos processos. [10]

A descentralização da *blockchain* se origina de uma rede denominada peer-to-peer (ponto a ponto) conforme Figura 4, "b". Essa ilustração se refere à disposição dos computadores interligados na referida rede, onde cada computador conectado faz as tarefas de cliente e servidor ao mesmo tempo, tornando o sistema independente de um único servidor centralizado que detenha todos os arquivos.[11]

O principal objetivo é a transmissão e compartilhamento de arquivos em larga escala de forma descentralizada, em que cada computador dessa rede é denominado de nó da rede. Esse nó pode compartilhar dados com vários outros nós conectados. Desse modo, os participantes são responsáveis pelo armazenamento e por manter a base de dados existentes.[12]



O sistema *blockchain* pode ser subdividido em "Blockchain 1.0", o qual emergiu a bitcoin e criptomoedas; "Blockchain 2.0", através da qual são aplicáveis os smart contracts; e, por fim, a "Blockchain 3.0", que abrange áreas governamentais, ou seja, é utilizada em áreas como a saúde, alfabetização, cultura e arte.

Nas palavras da autora Erica Abreu:[13]

10. FORTE, P., Romano, D., & Schmid, G., 2015. *Beyond Bitcoin – Part I: A critical look at blockchain-based systems*. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2015/1164. Acesso em 20 de julho de 2023.

11. OFICINA DA NET. *O que é p2p e como ela funciona*. 2022. Disponível em: https://www. oficinadanet.com.br/post/14046-o--que-e-p2p-e-como-ela-funciona. Acesso em: 28 outubro 2022.

12. MAÇOLI, F. *Blockchain Advanced: Fundamentação Tecnológica Blockchain*. 2022. Disponível em: https://on.fiap.com.br/mod/conteudospdf/view.php?c=3911&id= 174962. Acesso em: 28 maio 2023.

13. ABREU, E. *O impacto da tecnologia blockchain no combate à fraude e evasões fiscais*. 2020. 111 f. Dissertação (Mestrado em Direito Internacional e Europeu) - Nova School of Law, Lisboa, Portugal.

> ...o objetivo é de se obter um sistema novo e mais eficiente para organizar, administrar, coordenar e registrar todas as interações humanas, seja empresarial, governamental ou pessoal. Ou seja, a blockchain 3.0 pode ser utilizada por governos e pela administração pública, para modernizar e automatizar processos estatais, através de "repasses públicos por meio de criptomoedas; [...] em licitações, no pagamento e recolhimento de tributos e no registro público de empresas.

Para a pesquisadora, as características da tecnologia *blockchain* de imutabilidade, confiabilidade e segurança são atrativas aos governos e há um enorme potencial para a sua consolidação como uma das principais formas de combate à fraude e à evasão fiscal.

O uso da *blockchain* e o registro das informações compartilhadas entre o fisco e o contribuinte racionaliza processos atualmente complexos e onerosos, bem como aumenta a transparência das transações efetuadas, além de viabilizar a implementação de mecanismos de tributação em tempo real. A blockchain é uma realidade não só no Brasil, mas em diversos países do mundo, e aos poucos tem conquistado espaços cativos nas aplicações da tecnologia na administração contábil e tributária, com imensas expectativas acerca das múltiplas vantagens que tem a oferecer.

2.1 O metaverso e os impactos tributários

O Metaverso é uma realidade virtual alternativa, onde as pessoas podem interagir, se relacionar, criar conteúdo e até mesmo realizar movimentações financeiras advindas de atividades como investimentos, jogos, vendas de produtos digitais e prestação de serviços.

Apesar de estarmos ainda em um cenário de construção e aprimoramento destas novas tecnologias, o metaverso, ambiente virtualizado, traz diversas implicações econômicas, sociais, culturais, sucessórias e patrimoniais. Como não poderia ser diferente, atualmente estão em voga diversos debates acerca dos impactos tributários na economia digital e sobre as necessárias adaptações para viabilizar a tributação das relações econômicas estritamente virtuais.

Nesse contexto, surgem uma série de debates acerca das implicações tributárias nas operações realizadas no metaverso, entre os quais destacam-se: análise da aplicabilidade dos critérios de dedutibilidade do Imposto de Renda sobre Pessoas Jurídicas (IRPJ) de despesas operacionais necessárias ao desenvolvimento de atividades econômicas de empresas que funcionam

nesse ambiente; avaliação da incidência de ICMS (Imposto sobre Circulação de Mercadorias e Serviços) em operações que envolvem bens, mercadorias e produtos incorpóreos ou intangíveis; avaliação da incidência de ISS (Imposto sobre Serviços) considerando a notável evolução da robótica avançada e com a transposição da noção de prestação de serviço, anteriormente realizados exclusivamente por humanos, para uma noção que considera o exponencial crescimento da digitalização das relações fabris, sociais e de trabalho, e as inúmeras possibilidades de prestação de serviços dentro do espaço virtual.[14]

É preciso lembrar que o metaverso se propõe a ser um ambiente no qual haverá intensa atividade comercial, bem como a realização de prestação de serviços por empresas e profissionais autônomos. Serviços que hoje sofrem tributação pelo ISS no mundo físico, como terapia, estética, vestuário, poderiam atrair a tributação desses serviços pelos Municípios, no mundo virtual.

Também há margem para discussões sobre competências territoriais, a fim de se alcançar a definição de qual Estado seria competente para tributar uma determinada operação no metaverso. São apenas alguns dos desafios que a revolução tecnológica nos colocou, com a disposição de recursos de realidade aumentada e pela proliferação de bens, serviços e moedas digitais.

Estamos em um momento de construção de novas ideias e seria impossível dimensionar com precisão quais serão os reais impactos e as repercussões de um ambiente relativamente incipiente como o metaverso no âmbito tributário.

3. Sistema tributário brasileiro no século XXI

Desde a sua criação, o sistema tributário brasileiro possui uma sistemática complexa, sendo um obstáculo para a fácil compreensão do contribuinte, que foi pensada para uma economia corpórea, física, com a prestação de serviços realizada exclusivamente por humanos.

Duas universidades alemãs pesquisaram o modelo de arrecadação de tributos de cem países e, no ranking internacional *Tax Complexity Project*, o Brasil foi apontado como o país com a maior complexidade tributária do mundo.[15]

A burocracia do sistema tributário foi apontada com um dos quesitos desabonadores, fazendo o Brasil ocupar a 124ª posição de 190, na oferta de

14. *O Metaverso pode impactar a forma como cobramos tributos?* Disponível em: https://exame.com/bussola/o-metaverso-pode-impactar-a-forma-como-cobramos-tributos/. Acessado em 10 de junho de 2023.

15. HARST, S., Schanz, D., Siegel, F. & Sureth-Sloane, C. *The Tax Complexity Index – A Survey-Based Country Measure on Tax Code and Framework Complexity*, European Accounting Review. 2021. Disponível em: https://www.taxcomplexity.org/. Acesso em 12 abr. 2023.

ambientes de negócios favorável ao empreendedorismo, segundo o relatório anual Doing Business 2020. Além da burocracia, encontram-se menções sobre a complexidade das leis, requisitos fiscais complicados, incidência de vários tributos sobre o mesmo fato gerador e altas cargas tributárias como demais obstáculos. [16]

O autor Alfredo Augusto Becker, na obra "Teoria Geral do Direito Tributário", já alertava para as problemáticas encontradas na legislação tributária brasileira, as quais sempre se mostraram um obstáculo para o entendimento do contribuinte, aumentando a probabilidade de descumprimento, voluntário ou não, das obrigações tributárias principais e acessórias. Nas palavras do autor:

> Se fossem integralmente aplicadas as leis tributárias, todos os contribuintes seriam passíveis de sanções, inclusive de cárcere e isto, não tanto em virtude de fraude, mas principalmente pela desorientação que o caos da legislação tributária provoca no contribuinte. Tão defeituosas costumam ser as leis tributárias que o contribuinte nunca está seguro das obrigações a cumprir e necessita manter uma dispendiosa equipe de técnicos especializados para simplesmente saber quais as exigências do Fisco.[17]

Apesar de ser uma obra publicada há 60 anos, o trecho grifado acima traduz os exatos problemas gerados pela complexidade da legislação e dificuldade de compreensão das extensas regras tributárias, os quais são encontrados até os dias atuais no Brasil.[18]

Outrossim, apesar da alta carga de impostos cobrados – equivalentes a tributação em países desenvolvidos – o Brasil entrega serviços públicos de péssima qualidade, com defeituosa distribuição demográfica de políticas públicas, demonstrando, assim, a desastrosa gestão dos recursos públicos arrecadados.[19]

Ter um sistema tributário eficiente é fundamental para o exercício da cidadania e para aumentar a competitividade das empresas e, assim, acelerar o

16. *Entre 190 países, Brasil ocupa 124ª posição em ranking que avalia facilidade de fazer negócios*. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/iti-na-midia/entre-190-paises-brasil-ocupa-124-posicao-em-ranking-que-avalia-facilidade-de-fazer-negocios. Acesso em: 02 de Julho de 2023.

17. BECKER, Alfredo Augusto. *Teoria Geral do Direito Tributário*. 3ª ed. São Paulo: Lejus, 1998, p. 609

18. SILVA, S; D'ANDRÉA, Ribeiro. *Introdução ao Direito Constitucional Tributário*. Curitiba: Ibpex, 2012. pg. 26.

19. SOUZA, J. *Análise crítica do sistema nacional tributário vigente e propostas de mudanças em sua estrutura e de sua simplificação*. Rio de Janeiro: Revista Augustus, v. 23, n. 46, p. 10-29, jul./dez. 2018.

ritmo de crescimento econômico do país, gerando oportunidades de emprego e renda para a população. Da mesma forma, resta claro que as iniciativas nacionais para o desenvolvimento tecnológico e industrial não serão suficientes sem uma reformulação tributária que deixe o Brasil apto a concorrer com economias globais mais desenvolvidas nesse quesito.

3.1 *Blockchain* e a simplificação da arrecadação de impostos

No livro "Internet e Direito"[20], o autor Marco Aurélio Greco já discorria sobre a complexidade da aplicação das leis no mundo virtual, onde "não há paredes ou portas físicas", defendendo a globalização da população "realizando atos, celebrando negócios, transmitindo e recebendo informações de todo o mundo, e muitas vezes, sua conduta, acaba escapando do controle jurídico de cada ordenamento positivo".

Como já dito, a internet é o ambiente da criação de valor nas novas tecnologias, e elas vêm se difundindo de forma mais rápida e orgânica do que nas revoluções anteriores, justamente por serem divulgadas através de uma rede. As tecnologias que surgiram com o advento da quarta revolução industrial, em especial a *blockchain*, trazem uma transmutação em todos os setores da empresa, sendo de especial relevância as suas implicações na área fiscal, podendo torná-la mais estratégica.

Suíça, Japão, China, Canadá, El Salvador e Singapura são alguns dos países que já vêm implementando a tecnologia em seus governos e, em alguns, é possível até mesmo realizar pagamentos através de criptomoedas.

A cidade suíça de Zug, pequena área administrativa da Suíça, ficou conhecida como "Vale Cripto" e foi classificada como a comunidade de tecnologia que mais cresce na Europa. Em setembro de 2020, foi anunciado que os residentes de Zug poderiam pagar impostos utilizando criptomoedas, a partir de fevereiro de 2021. [21]

Em 09 de junho de 2021, o Congresso de El Salvador se tornou o primeiro país a adotar *Bitcoin* como moeda de circulação nacional no país. O governo de Singapura, por sua vez, lançou o projeto Ubin em 2020, um sistema de pa-

20. GRECO, M. *Internet e Direito*. São Paulo: Dialética, 2000.

21. JENKINSON, G. *Os 5 países de 2020 mais amigáveis às criptomoedas e blockchain*. Disponível em: https://br.cointelegraph.com/news/2020-s-5-countries-friendliest-to-crypto-and-blockchain. Acesso em 10 de maio de 2023.

gamento baseado em *blockchain*, além de ter sido o primeiro país a conceder licença de *tokens* digitais a uma Exchange. [22]

No Canadá, há um tímido crescimento no uso da tecnologia *blockchain* e segundo o Statistics Canada apenas 0,3% das empresas canadenses usaram *blockchain* em 2021, embora seu uso tenha aumentado substancialmente entre empresas de médio e grande porte entre 2019 e 2021.

No Brasil, foi publicada a Lei nº 14.478, em dezembro de 2022, dispondo sobre as diretrizes da prestação de serviços de ativos virtuais (criptomoedas) e da regulamentação das prestadoras de serviços de ativos virtuais. A lei considera ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento.

O decreto nº 11.563 de 2023, por sua vez, ao regulamentar a Lei nº 14.478/22, estabeleceu competências ao Banco Central do Brasil, que deverá regular a prestação de serviços de ativos virtuais, observadas as diretrizes da lei.

Em que pese seja uma tecnologia relativamente nova a título de usabilidade, a *blockchain* mostrou que chegou para abalar com as estruturas vigentes e que a internacionalização da economia já é uma realidade.

A tecnologia *blockchain*, ainda que incipiente, poderá exercer relevante função social no que diz respeito à simplificação dos processos tributários, tendo em vista que a atual complexidade afasta o contribuinte de sua autonomia enquanto cidadão, inviabilizando uma postura ativa frente ao Estado. O contribuinte precisa ao menos compreender e visualizar qual a carga tributária suportada em suas atividades, a fim de tornar viável o monitoramento e a cobrança do Estado da contraprestação pelo pagamento daquele tributo.

Segundo o professor Paulo Ayres Barreto, do Departamento Econômico, Financeiro e Tributário da Faculdade de Direito da Universidade de São Paulo (USP), ao comentar sobre o uso da tecnologia sob a perspectiva da reforma tributária: “Os desafios dessa reforma são, de um lado, a simplificação do nosso sistema, mas, de outro, o de captar a chamada ‘economia digital’ — muito pouco materializada. Então, toda tecnologia que se constrói no sistema tributário pode colaborar para a captação dessas capacidades contributivas.”[23]

22. *Cingapura lança sistema de pagamento blockchain*. Disponível em: https://guiadobitcoin.com.br/noticias/cingapura-lanca-sistema-de-pagamento-blockchain-%E2%94%82ubin/. Acesso em 10 de maio de 2023.

23. AYRES, P. T*ecnologia blockchain pode melhorar sistema tributário*. Disponível em: https://www.inovacao.usp.br/tecnologia-blockchain-pode-melhorar-sistema-tributario/. Acessado em 23 de maio de 2023.

O professor entende que há perspectivas de que a relação de comunicação com a Receita Federal seja mais centralizada, com simplificação de impostos e novas tecnologias, que defende:

> A todo instante, o fisco tem interesse em saber o que se passa na vida do contribuinte; quando ele tem que informar sobre certas relações que tenham efeitos tributários para o fisco, a existência de blockchain pode ser um caminho para centralizar, com bastante segurança, esse contato. É bom ressaltar que o fisco brasileiro é um dos mais avançados sistemas de informatização para controle de atividades de contribuintes.[24]

A revolução tecnológica trouxe uma inafastável mudança de paradigmas e de novas possibilidades em favor da sociedade, e ainda teremos muitos caminhos a trilhar a fim de garantir uma maior efetividade na sistemática de cobrança de tributos, e uma maior eficiência para a Administração Pública em seus processos internos.

Considerações finais

De forma incontestável, a superveniência de uma economia digital atrai significativos impactos ao atual Sistema Tributário Brasileiro e na forma como são tributados, arrecadados e fiscalizados os tributos. Durante o presente estudo, foi possível verificar que a tecnologia *blockchain* possui amplo potencial para se tornar uma ferramenta apta a facilitar a gestão e cobrança de impostos, através de sua acessibilidade e agilidade de validação e cruzamento de dados, possibilitando grande capacidade para evitar fraudes e sonegações, em razão da facilidade de rastreamento das operações por meio do *hashcode* e do sistema de criptografia e inviolabilidade do livro-razão (*ledger*), que possibilitam a integridade contra alterações de registros. Através da tecnologia *blockchain*, os órgãos fiscalizadores não precisariam basear-se em formulários manuais, preenchidos por contribuintes – muitas vezes de forma equívoca ou incompleta.

Para que mecanismos de soluções fiscais baseadas em *blockchain* prosperem em sua implementação, é necessário um planejamento meticuloso, cooperação mútua entre os usuários e a solução de desafios técnicos e de privacidade. Contudo, é certo que a tecnologia *blockchain* oferece muitas opor-

24. Ibidem.

tunidades para a indústria 4.0, incluindo maior eficiência, segurança e transparência, além de construir um cenário de reais expectativas de soluções tecnológicas possam cooperar cada vez mais com o desenvolvimento das nações.

Referências

GATTESCHI, Valentina; ORCID, Fabrizio Lamberti; ORCID, Claudio Demartini; PRANTEDA, Chiara; SANTAMARÍA, Victor. *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?* Future Internet, v. 10, fev. 2018. Disponível em: <http://www.mdpi.com/1999-5903/10/2/20/htm>. Acesso em 15 de maio de 2023.

CAPGEMINI. *Smart Contracts in Financial Services: Getting from Hype to Reality. 2016*. Disponível em: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf. Acesso em 20 de junho de 2023.

DE WECK, O. et al. *Trends in Advanced Manufacturing Technology Innovation*. Production in the Innovation Economy (PIE) Study. Cambridge: Massachusetts Institute of Technology (MIT), 2013.

GUPTA, Manav. *Blockchain For Dummies*, IBM Limited Edition. 1.ed. Hoboken – NJ; Editora John Wiley & Sons, Inc. 2017, p.3.

Como o governo federal usa o blockchain? https://www.serpro.gov.br/menu/noticias/noticias-2023/blockchain-no-governo-federal. Acessado em 23 de julho de 2023.

MENDES, Daniele; FERREIRA, Paulo.; DE CASTRO, Douglas. *Blockchain e Agenda 2030*. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4938. Acesso em 10 de julho de 2023.

Receita Federal Publica Norma Sobre Compartilhamento de Dados Utilizando Tecnologia Blockchain, novembro, 2018. Disponível em http://idg.receita.fazenda.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobrecompartilhamento-de-dados-utilizando-tecnologia-blockchain. Acessado em 10 maio 23

BOSSA, G e GOMES, E. *Blockchain: Tecnologia à Serviço da Troca de Informações Fiscais ou Instrumento de Ameaça a privacidade dos Contribuintes?* In PISCITELLI, Tathiane (Coord), Tributação da Economia digital. RT. 2017, p. 375.

FORTE, P., Romano, D., & Schmid, G., 2015. *Beyond Bitcoin – Part I: A critical look at blockchain-based systems*. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2015/1164. Acesso em 20 de julho de 2023.

OFICINA DA NET. *O que é p2p e como ela funciona*. 2022. Disponível em: https://www. oficinadanet.com.br/post/14046-o-que-e-p2p-e-como-ela-funciona. Acesso em: 28 outubro 2022.

MAÇOLI, F. Blockchain Advanced: Fundamentação Tecnológica Blockchain. 2022. Disponível em: https://on.fiap.com.br/mod/conteudospdf/view.php?c=3911&id= 174962. Acesso em: 28 maio 2023.

ABREU, E. *O impacto da tecnologia blockchain no combate à fraude e evasões fiscais*. 2020. 111 f. Dissertação (Mestrado em Direito Internacional e Europeu) - Nova School of Law, Lisboa, Portugal.

O Metaverso pode impactar a forma como cobramos tributos? Disponível em: https://exame.com/bussola/o-metaverso-pode-impactar-a-forma-como-cobramos-tributos/. Acessado em 10 de junho de 2023.

HARST, S., Schanz, D., Siegel, F. & Sureth-Sloane, C. *The Tax Complexity Index – A Survey-Based Country Measure on Tax Code and Framework Complexity*, European Accounting Review. 2021. Disponível em: https://www.tax-complexity.org/. Acesso em 12 abr. 2023.

Entre 190 países, Brasil ocupa 124ª posição em ranking que avalia facilidade de fazer negócios. Disponível em: https://www.gov.br/iti/pt-br/assuntos/noticias/iti-na-midia/entre-190-paises-brasil-ocupa-124-posicao-em-ranking-que-avalia-facilidade-de-fazer-negocios. Acesso em: 02 de Julho de 2023.

BECKER, Alfredo Augusto. *Teoria Geral do Direito Tributário*. 3ª ed. São Paulo: Lejus, 1998, p. 609

SILVA, S; D'ANDRÉA, Ribeiro. *Introdução ao Direito Constitucional Tributário*. Curitiba: Ibpex, 2012. pg. 26.

SOUZA, J. *Análise crítica do sistema nacional tributário vigente e propostas de mudanças em sua estrutura e de sua simplificação*. Rio de Janeiro: Revista Augustus, v. 23, n. 46, p. 10-29, jul./dez. 2018.

GRECO, M. *Internet e Direito*. São Paulo: Dialética, 2000.

JENKINSON, G. *Os 5 países de 2020 mais amigáveis às criptomoedas e blockchain*. Disponível em: https://br.cointelegraph.com/news/2020-s-5-countries-friendliest-to-crypto-and-blockchain. Acesso em 10 de maio de 2023.

Cingapura lança sistema de pagamento blockchain. Disponível em: https://guiadobitcoin.com.br/noticias/cingapura-lanca-sistema-de-pagamento-blockchain-%E2%94%82ubin/. Acesso em 10 de maio de 2023.

AYRES, P. *Tecnologia blockchain pode melhorar sistema tributário*. Disponível em: https://www.inovacao.usp.br/tecnologia-blockchain-pode-melhorar-sistema-tributario/. Acessado em 23 de maio de 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO 2

Inteligência Artificial e seus impactos

AUTORES

Rafael Affonso Cristino Sousa Barros

Julia Ferrari Oliveira Lima

Bruno Blum Fonseca

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

13

Modelos grandes de linguagem e vazamento de dados pessoais: perspectiva regulatória e PL 2338/2023

RAFAEL AFONSO CRISTINO SOUSA BARROS

RAFAEL AFONSO CRISTINO SOUSA BARROS[1]

Introdução

Os modelos grandes de linguagem ou *LLMs* (*Large Language Models*) têm recebido grande atenção midiática. Sua popularidade bateu recordes no ano de 2023, tendo o Chat GPT se estabelecido como um dos aplicativos com o crescimento mais rápido de usuários já visto. Em apenas 2 meses o aplicativo alcançou a marca de 100 milhões de usuários ativos mensais[2], o que demonstra não apenas a sua relevância temática, mas também a necessidade de melhor conhecimento e educação quanto a essa ferramenta.

A grande aceitação da ferramenta é acompanhada também de preocupações quanto aos riscos e os possíveis impactos trazidos por ela à sociedade. Tais discussões têm trazido diversos questionamentos quanto à transparência desses modelos, vieses nos processos decisórios ou até mesmo a possibilidade de substituição de profissionais por meio da utilização de modelos de inteligência artificial.

Embora não seja possível, no momento, prever o impacto dessa ferramenta em alguns anos, faz-se extremamente importante o desenvolvimento de uma estrutura de regulamentação e garantia que possa atuar diante das mais visíveis distorções e riscos trazidos por estes modelos.

O presente artigo se dedicará à exploração desses riscos na perspectiva de ataques adversariais, *i.e.*, ataques cometidos contra essas redes com o propósito de obtenção de dados pessoais, propriedade intelectual ou até mesmo a obstrução da operação dessas redes, especificamente na possibilidade de vazamento de dados pessoais e riscos associados.

1. Advogado, graduado pela Universidade Presbiteriana Mackenzie em 2021 e aluno da Pós-graduação de Direito Digital do Instituto de Tecnologia e Sociedade.

2. HU, K. *ChatGPT sets record for fastest-growing user base - analyst note*. Reuters, 2 fev. 2023. Disponível em: <https://tinyurl.com/ykj7pnfp/> Acesso em: 19 nov. 2023.

Estruturalmente, antes de se aprofundar quanto às vias de ataque, buscou-se estabelecer conceitualmente o que seriam os modelos grandes de linguagem, *LLMs*, e o que seria o processamento de linguagem natural (PLN), para então abordar as vias de ataque atualmente existentes e as vulnerabilidades relativas ao tratamento de dados pessoais. Por fim, os riscos identificados serão analisados perante a Lei Geral de Proteção de Dados, Lei nº 13.709/2018 (LGPD) e o Projeto de Regulamentação de Inteligências Artificiais -PL 2.338/2023.

Espera-se que este artigo contribua com a presente discussão de identificação de riscos envolvidos com o desenvolvimento e utilização de *LLMs*. Objetiva-se, por meio de análise aplicada, uma contribuição ao desenvolvimento de um arcabouço regulatório adequado às particularidades desses modelos e aplicações semelhantes, especificamente no que tange à proteção de dados.

1. Processamento de linguagem natural e modelos grandes de linguagem

O Processamento de Linguagem Natural é compreendido como uma subárea da computação, mais especificamente uma área multidisciplinar do desenvolvimento de Inteligências Artificiais que se preocupa com a capacidade de algoritmos compreenderem texto e fala de maneira natural, ou seja, da mesma maneira que humanos conseguem entender.

Semelhantemente, para melhor compreensão, podemos nos referir à visão computacional, outra área da computação, desta vez preocupada com a capacidade de inteligências artificiais compreenderem imagens e vídeos, da mesma maneira que humanos conseguem compreender. Nessa subárea se encaixam aplicações como reconhecimento facial, reconhecimento e buscas de imagens e afins.

O Processamento de Linguagem Natural e suas aplicações permitiram o desenvolvimento de aplicativos como os assistentes de voz, traduções automatizadas e, por meio dos *Large Language Models*, os *Chatbots*, como o *Bard*, Chat Gpt, entre outros.

Os *Large Language Models*, por sua vez, são essencialmente algoritmos de deep learning utilizados com o propósito de aplicação no processamento de Linguagem Natural. No entanto, há diferenças importantes entre *LLMs* e outros modelos de *deep learning* utilizados para o mesmo fim.

Ainda em 2017, foi proposta uma nova arquitetura de modelo que permitiu alavancar o avançar da tecnologia. Esta nova arquitetura foi proposta por

Vaswani *et al*.[3], pesquisadores da Google, em seu artigo *Attention is all you need* e foi batizada de arquitetura de "transformadores". Essa nova arquitetura permitia, de maneira sucinta, o treinamento mais rápido de modelos em comparação com a arquitetura de RNR (Redes Neurais Recorrentes) utilizada anteriormente. Essa nova arquitetura, por meio da técnica de paralelização, permitia que modelos fizessem uso de bancos de dados consideravelmente maiores para treinamento, com maior eficácia também para a realização de treinamentos semi-supervisionados, reduzindo consideravelmente a tarefa humana envolvida na classificação dos dados inclusos no banco de dados.

A introdução da nova arquitetura de transformadores permitiu a melhoria dos modelos existentes, bem como o desenvolvimento de novos modelos de linguagem como o BERT (*Bidirectional Encoder Representations from Transformers*), introduzido em 2019 novamente por pesquisadores da Google, Jacob Devlin, Ming-Wei Chang, Kenton Lee e Kristina Toutanova, representando um período de grandes avanços no desenvolvimento de soluções de PLN. [4] [5]

Inclusive, o BERT é tido para muitos como o primeiro *LLM* "verdadeiro". No entanto, antes de sua introdução havia outros modelos como o ULMFIT e ELMo, que, embora não fossem tão eficientes, já utilizavam dos avanços propostos em 2017 com a introdução da arquitetura de transformadores.

Em comum entre esses modelos elaborados a partir da arquitetura de transformadores estão a sua capacidade de serem treinados em grandes bancos de dados e a quantidade de parâmetros com os quais operam. Por exemplo, o GPT-3 utiliza por volta de 175 bilhões de parâmetro, e é estimado que o GPT-4 faz uso de por volta de 1.8 trilhões de parâmetros, esses parâmetros são equivalentes às estruturas neurais que podemos observar em redes neurais, artificiais, trazendo ao processo de treinamento certos pesos e vieses que, por meio de iteração e ajustes, levam ao aperfeiçoamento do output entregue pelo modelo. [6]

Em conclusão, Modelos Grandes de Linguagem permitem maior aproveitamento de tempo de treinamento dos modelos, o que por sua vez permite maior quantidade de parâmetros e aperfeiçoamento de output. Esse desenvol-

3. VASWANI, A. *et al*. *Attention Is All You Need*. Disponível em: <https://arxiv.org/abs/1706.03762>, Acesso em: 19 nov. 2023.

4. MENON, P. I*ntroduction to Large Language Models and the Transformer Architecture*. Disponível em: <https://tinyurl.com/3z5zbm6s>. Acesso em: 19 nov. 2023.

5. NOUROUZI, Armin. LLM *Behind the Scenes: Exploring Transformers with TensorFlow*. Disponível em: <https://tinyurl.com/49cxhuf3>. Acesso em: 19 nov. 2023.

6. DEVLIN, J. et al. BERT: *Pre-training of Deep Bidirectional Transformers for Language Understanding*. Proceedings of the 2019 Conference of the North, v. 1, 2019.

vimento permitiu nos últimos anos, desde o advento do BERT e da arquitetura de transformador, o grande crescimento dessas ferramentas e sua utilização.

No entanto, o rápido desenvolvimento dessas tecnologias não apenas levaram à maior eficiência e utilidade de modelos, mas também novas vulnerabilidades técnicas que devem ser estudadas e compreendidas para que possamos, de maneira socialmente consciente e responsável, implementar medidas remediativas e preventivas.

2. Utilização de dados pessoais para desenvolvimento e treinamento de modelos.

Como exposto, a aceleração exponencial do desenvolvimento da IA e a consequente possibilidade de sua integração a tarefas rotineiras e aos mais diversos *workflows* só foram possíveis por meio do desenvolvimento de novas arquiteturas que permitiram o treinamento mais rápido e eficaz desses modelos, permitindo a utilização de conjuntos de dados cada vez maiores.

Esses conjuntos de dados, inevitavelmente, em razão de fazerem uso das fontes mais diversas de dados, acabam por incluir dados pessoais, como números de telefone, e-mails, endereço de residência e afins. Além disso, os conjuntos de dados e, por consequência, as fontes dos dados utilizados para o treinamento dos Modelos de Inteligência Artificial, não são rotineiramente divulgados pelas companhias, aumentando a opacidade referente à que dados podem estar sendo utilizados para o treinamento desses modelos. [7]

A questão sensível não é apenas a utilização não autorizada desses dados, mas a possibilidade de seu vazamento. Ao explorar vulnerabilidades próprias dos modelos, os ataques buscam alcançar diversos objetivos. Nesse sentido, o mais relevante desses objetivos para os propósitos deste texto é a possibilidade de recuperação dos dados pessoais presentes no conjunto de dados utilizados para treinamento. [8]

No contexto do conjunto de dados utilizado para o treinamento de modelos de linguagem natural, dados pessoais são aqueles que identificam diretamente um indivíduo, como nomes, endereços de e-mail ou até mesmo endereços residenciais ou identificadores parciais que, quando analisados em conjunto,

7. LUKAS, N. et al. *Analyzing Leakage of Personally Identifiable Information in Language Models*. arXiv (Cornell University), 1 fev. 2023.

8. MORAIS, Alana. *Ameaças a Sistemas baseados em Machine Learning* – Parte 1 de 5 | *SideChannel Tempest*. Disponível em: <https://tinyurl.com/2e5wy49u>. Acesso em: 19 nov. 2023.

podem identificar um indivíduo, como gênero, aniversário, descrição de sua aparência ou até mesmo informações sobre a sua rotina e hobbies.[9]

Como exemplo da possibilidade de identificação de indivíduos a partir de identificadores parciais, em 2008 a Netflix lançou um concurso para o desenvolvimento de um método aperfeiçoado para a realização de recomendações de filmes, com base do concurso foram disponibilizados os dados referentes aos filmes assistidos pelos seus assinantes, na época, em torno de 500.000 indivíduos.[10]

Com acesso ao banco de dados, duas pesquisadoras da Universidade do Texas conseguiram desanonimizar os dados por meio de uma análise conjunta dos dados fornecidos pela Netflix e outros disponíveis publicamente, como em plataformas públicas de avaliação de filmes.

Destaca-se que esse estudo foi realizado ainda em 2008. Atualmente, as mesmas ferramentas disponíveis para o desenvolvimento de Inteligências Artificias úteis e benéficas também podem ser utilizadas de maneira adversarial, acelerando o processo de desanonimização de dados a partir de identificadores parciais.

No mesmo sentido, no contexto americano foram realizados estudos que demonstraram que a combinação desses identificadores parciais podem levar à identificação de 63 até 87% da população, utilizando-se apenas de dados como gênero, data de nascimento e código postal,[11] o que por si só destaca a relevância da matéria. A possibilidade de vazamento e compilação de dados, mesmo que apenas de identificadores parciais, oferece grande risco à privacidade de usuários desses modelos, bem como de outros indivíduos que possam até mesmo não ter ciência de que seus dados foram utilizados para o treinamento de modelos de linguagem.

Há, ainda, a possibilidade de consequências ainda mais graves quando consideramos o desenvolvimento de ferramentas de linguagem natural com o propósito de utilização em setores de risco elevado[12], havendo possibilidade de vazamento de segredos industriais, informações pessoais referentes a

9. LUKAS, Nils et al. op.cit, p. 3

10. NARAYANAN, A.; VITALY SHMATIKOV. *How To Break Anonymity of the Netflix Prize Dataset*. arXiv (Cornell University), 18 out. 2006.

11. GOLLE, P. *Revisiting the uniqueness of simple demographics in the US population*. Proceedings of the 5th ACM workshop on Privacy in electronic society - WPES '06, 2006.

12. OPREA, Alina; VASSILEV, Apostol. *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (draft). *National Institute of Standards and Technology*, 2023.

serviços de crédito, dados pessoais sensíveis utilizados para aconselhamento médico, dentre outros.[13] [14]

Tornando o olhar à LGPD, em seu artigo 4º, III, há previsão de que dado relativo ao titular que não possa ser identificado não há de ser considerado como dado pessoal. Contudo, como se verá adiante, a mera utilização do dado para treinamento de modelos não implica necessariamente a inacessibilidade dos dados ou impossibilidade de identificação.

Desse modo, para os propósitos da LGPD, o conjunto de dados que contenha dados pessoais não pode ser considerado anonimizados apenas ao ser utilizado para o treinamento de modelo de inteligência artificial, aplicando-se também ao desenvolvimento e implementação de modelos de Inteligência Artificial as previsões referentes aos requisitos para tratamento de dados pessoais e dados sensíveis, caso não anonimizado previamente o conjunto de dados utilizado.

Diante das vulnerabilidades desses modelos, desenvolveram-se diversos métodos para a sua recuperação ou extração de dados pessoais. Ao analisarmos estes métodos, podemos melhor compreender os riscos envolvidos na implementação e no desenvolvimento de sistemas de inteligência artificial, aspectos que devem também ser considerados no desenvolvimento do framework regulatório e legal atualmente em elaboração.

3. Ataques Adversariais

O campo do estudo de ataques adversariais à *machine learning* (*adversarial machine learning*) busca analisar a estrutura e capacidades reais de agentes maliciosos, visando a identificar as fraquezas dessas ferramentas para possibilitar o desenvolvimento de medidas de proteção e prevenção. O Instituto Nacional de Padrões e Tecnologia (NIST) do Departamento de Comércio do Governo dos Estados Unidos publicou em março de 2023 o documento *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, buscando estabelecer uma terminologia comum ao campo.

Abaixo, preparou-se uma tradução de visualização da taxonomia elaborada pelo NIST. Os objetivos de cada ataque estão ao centro de cada círculo, sendo eles, interrupção de **Disponibilidade**, violação de **Integridade** e viola-

13. PRICE II, W. Nicholson. *Risks and remedies for artificial intelligence in healthcare*. 2019.

14. BAK, Marieke et al. *You can't have AI both ways: balancing health data privacy and access fairly*. Frontiers in Genetics, v. 13, p. 1490, 2022.

ção de **Privacidade**. Em torno dos objetivos, há a listagem das capacidades que devem ser obtidas pelos adversários para que possam alcançar o seu objetivo. Cada categoria de ataque é destacada de maneira independente, com ligações indicando a conexão entre as às capacidades necessárias e outras vias de ataques semelhantes ou relacionadas.[15]

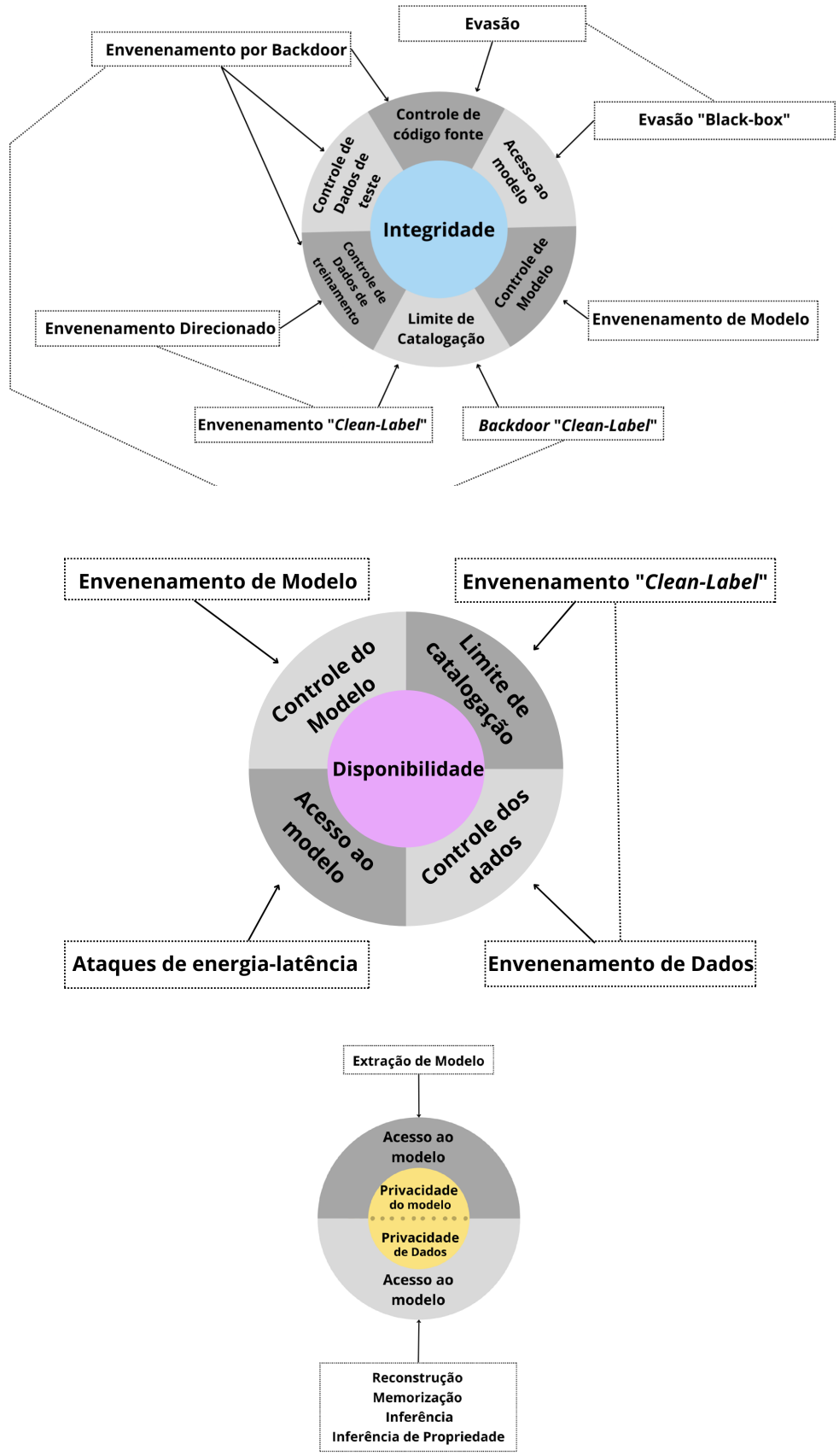


Figura 1 – Tradução de gráfico taxonômico. (tradução do autor) [16]

15. OPREA, Alina; VASSILEV, Apostol, op. cit. p. 5
16. OPREA, Alina; VASSILEV, Apostol, id. p. 6

Como pode-se verificar a partir do gráfico acima, há diversas vias de ataque as quais apresentam variedade também em relação a seus objetivos e meios. Como já exposto anteriormente, para os propósitos deste artigo, trataremos apenas dos ataques à privacidade de dados. Além disso, importante destacar que a taxonomia proposta não é universalmente adotada, havendo interseções entre diversos ataques e funcionalidades, o que demonstra a visível amplitude do tema, bem como de vias de ataque a Inteligências Artificiais.

3.1 Memorização e extração

Ataques de memorização ou ataques de extração[17] buscam a extração de dados de treinamento dos modelos de *machine learning*, como os modelos de linguagem discutidos no presente artigo. Uma das primeiras demonstrações da possibilidade de realização de extração desses dados se deu a partir do aproveitamento do que se chama de 'memorização' de dados por modelos de *machine learning*:

> Carlini et al. foram os primeiros a demonstrar na prática ataques de memorização em modelos de linguagem. Ao inserir "canários" sintéticos nos dados de treinamento, eles desenvolveram uma metodologia para extrair os canários e introduziram uma métrica chamada exposição para medir a memorização.[18]

A partir deste primeiro desenvolvimento e com o avanço de modelos com capacidades maiores para treinamento, verificou-se que modelos com capacidade maior, como modelos grandes de linguagem, possuem também a tendência de maior memorização de dados.

Como o objetivo de um ataque de extração é justamente obter o máximo de dados pessoais a partir do conjunto de dados utilizado para o treinamento de um modelo, quão mais frequente uma informação aparecer no banco de dados, espera-se também que ela será gerada com maior facilidade pelo modelo.

Desde as pesquisas iniciais de Carlini et. al, tem-se desenvolvido considerável corpo de pesquisa referente aos ataques de extração e memorização que continua a buscar metodologias alternativas e mitigações possíveis para

17. LUKAS, Nils et al. id. p. 2

18. OPREA, Alina; VASSILEV, Apostol, id. p.29. Tradução nossa.

a proteção de dados pessoais. Em pesquisa recente, datada de fevereiro de 2023, Lukas et. al alcançaram a métrica de que o modelo GPT2-Large, sem medidas de mitigação, permitia a extração de 23% de dados pessoais presentes no conjunto de dados utilizados, com 30% de precisão de extração, isso é, a confiança de que um dado pessoal gerado também aparece no conjunto de dados de treinamento[19]. Com a implementação de medidas de proteção de dados pessoais, como a privacidade diferencial, é possível reduzir essa porcentagem para apenas 3% de precisão e 3% de extratibilidade.

3.2 Reconstrução de dados

Em ataques de reconstrução, o objetivo de obtenção de dados pessoais identificáveis requer um agente informado, e se dá por meio da preparação de prompts ocultando parcialmente a informação, esperando então que o modelo de linguagem complete o prompt com a informação pessoal, semelhantemente ao que seria realizado por um programa de *autocomplete*.

Podemos exemplificar o ataque de reconstrução de dados da seguinte maneira: em razão da ausência de informações quanto ao dado que completará o contexto, um agente malicioso terá que exaustivamente buscar por soluções, o que por sua parte pode levar à menor praticidade da realização deste ataque, o que não significa dizer que se trata de um ataque ineficiente. Há razão para preocupação em referência a ataques de privacidade por sua capacidade de recuperação de dados a partir apenas de agregados de informações estatísticas obtidas a partir de interação com os modelos de linguagem grande. [20]

Novamente, em Lukas et. al., por meio de métodos melhorados na realização de ataque, verificou-se que o modelo de linguagem GPT2-Large, novamente treinado no banco de dados ECHR e sem defesas adicionais, seria consideravelmente suscetível a ataques desta natureza, tendo sido capaz de reconstruir 18.27% dos dados pessoais presentes no conjunto de dados[21].

3.3 Inferência

Semelhantemente ao ataque de reconstrução de dados, requer-se aqui novamente um agente malicioso informado, desta vez com conhecimento não

19. LUKAS, Nils et al. id. p. 9
20. LUKAS, Nils et al. id. p. 6
21. LUKAS, Nils et al. id. p. 10

apenas do contexto, mas também do conjunto de candidatos, a partir deste conjunto de informações o agente buscará inferir os dados pessoais.

Para a efetivação do ataque, é necessário, portanto, obter acesso ao conjunto de dados anonimizados utilizado para treinamento e uma lista de possíveis dados pessoais presentes no conjunto de dados utilizado para o treinamento, incluindo aquele que efetivamente se encontra presente no modelo.

Com o acesso ao modelo, pode-se, por meio de um ataque de reconstrução, obter possíveis candidatos para os dados pessoais presentes, alavancando por consequência a possibilidade da realização de ataques de inferência mais eficazes do que a simples reconstrução de dados.

A partir da inserção dos potenciais candidatos, verifica-se a 'perplexidade' do modelo diante de cada uma das possíveis 'soluções', uma baixa perplexidade indica uma maior presença no banco de dados. A partir da avaliação da perplexidade de cada resposta, retorna-se ao melhor candidato com a menos perplexidade do modelo.

Em Lukas et. al., os ataques de inferência obtiveram uma taxa de sucesso consideravelmente superior aos ataques de extração ou de reconstrução, alcançando uma taxa de precisão de 70% entre 100 candidatos em modelos treinados no banco de dados ECHR, 50% no banco de dados Enron e 28% no banco de dados YelpHealth.[22]

Mesmo em modelos que façam uso de mitigações, como a privacidade diferencial, os resultados ainda eram consideráveis, embora consideravelmente menores do que os resultados em modelos sem qualquer defesa ou mitigação para vazamentos, com precisão de 8% entre 100 candidatos e 4% entre 500 no banco de dados ECHR.

3.3.1 Inferência de propriedade e de associação

Enquanto ataques de inferência buscam extrair dados pessoais específicos, sabidamente presentes no conjunto de dados utilizado para o seu treinamento, os ataques de inferência de propriedade e de associação buscam extrair informações gerais sobre o conjunto de dados utilizado.

Em ataques de inferência de propriedade, o objetivo é inferir aspectos referentes ao conjunto do banco de dados, por exemplo, pode-se objetivar determinar qual porcentagem do banco de dados contém certo atributo sensível,

22. LUKAS, Nils et al. id. p. 10

como determinar qual grupo demográfico compõe a maioria do conjunto de dados.

Ataques de inferência de associação buscam determinar se os dados de um indivíduo estariam presentes no conjunto de dados utilizado para o treinamento, o que por si só pode ser identificado como uma violação de privacidade, como em treinamento de modelos com base em bancos de dados de pacientes de doenças raras.[23]

Essas informações então podem ser alavancadas, semelhantemente ao ataque de reconstrução, para a realização de ataques de extração e de inferência de dados pessoais mais precisos.

Destaca-se que as medidas de proteção passíveis de utilização contra outras formas de ataque são consideravelmente menos eficientes diante de ataques de inferência de propriedade e associação, em razão dos modelos de linguagem em sua implementação necessariamente revelarem certas características do conjunto de dados de treinamento.

3.4 Mitigação

É seguro dizer que atualmente as vias de ataque contra modelos de linguagem, assim como qualquer outro modelo algorítmico de *machine learning*, superam a quantidade de medidas de mitigação contra esses ataques. Esse cenário tende a continuar a se aprofundar conforme novas vias de ataque e vulnerabilidades são descobertas.

Atualmente, há duas medidas de mitigação eficientes contra a maioria dos ataques listados: a primeira é o processo de higienização e anonimização dos conjuntos de dados utilizados para treinamento. Esse '*scrubbing*' de dados pessoais é uma alternativa acessível para a remoção de dados pessoais, no entanto, a medida é apenas parcialmente eficaz em razão da possibilidade de redução da utilidade e acurácia do modelo, razão pela qual essa medida tende a ser utilizada para a remoção de dados pessoais sensíveis:

> A depuração de PII e a Privacidade Diferencial (DP) protegem a privacidade dos dados de treinamento ao custo de degradar a utilida-

23. OPREA, Alina; VASSILEV, Apostol, id. p. 29

> de do modelo. A depuração agressiva para melhorar a privacidade prejudica drasticamente a utilidade.[24]

Além disso, a remoção de dados pessoais por meio de "*scrubbing*", não remove a possibilidade de reconstrução de dados pessoais a partir do conhecimento do contexto dos dados pessoais. Portanto, embora útil, a higienização de conjunto de dados não pode ser compreendida como uma solução perfeita[25], mas sim uma medida de mitigação que deverá ser balanceada com a manutenção de utilidade do modelo.

A segunda medida de mitigação passível de utilização como mitigação de vazamentos de dados pessoais é a chamada privacidade diferencial – ao contrário da simples higienização e anonimização de dados, a privacidade diferencial busca ofuscar os dados presentes no conjunto de dados de treinamento, adicionando propositalmente ruído ao conjunto, impedindo que adversários possam inferir a presença de dados pessoais a partir dos outputs do modelo[26], por outro lado, há um correspondente prejuízo à utilidade do modelo:

> Existem novas abordagens que buscam aumentar critérios de privacidade sem que degrade muito a acurácia do modelo. Mas esta é uma questão sensível, porque invariavelmente teremos um *trade-off* entre o nível de privacidade e o desempenho do modelo. Podemos aumentar a privacidade removendo informação ou adicionando ruído ao conjunto de dados, e em ambos os casos haverá um impacto na acurácia do modelo. – (CORTIZ, 2020) [27]

As duas medidas não são capazes por si só de eliminar o risco de vazamento de dados pessoais e nem podem serem utilizadas de maneira indiscriminada, sob o prejuízo de afetar negativamente o modelo de linguagem. Elas ainda precisam ser acompanhadas de outras ferramentas de mitigação que podem inclusive se fazerem presentes no *pipeline* de implementação desses modelos de linguagem, aplicando limitações de *prompt* para usuários, restringindo respostas do modelo que contenham dados pessoais, entre outras.

24. LUKAS, Nils et al. id. p. 12 Tradução nossa.

25. CARLINI, Nicholas et al. *Quantifying memorization across neural language models*. arXiv preprint arXiv:2202.07646, 2022, p. 13.

26. YIN, Y.; HABERNAL, I. *Privacy-Preserving Models for Legal Natural Language Processing*. Disponível em: <https://arxiv.org/abs/2211.02956>. p. 4 Acesso em: 19 nov. 2023.

27. CORTIZ, Diogo. *K-ANONYMITY – PRIVACIDADE E INTELIGÊNCIA ARTIFICIAL, 2020*. Disponível em: https://tinyurl.com/3ycre4k6. Acesso em: 23 de julho de 2023

Diante disso, sabendo que não há medida preventiva perfeita e que as vias de ataque continuarão a se aperfeiçoar, faz-se necessária também uma abordagem regulatória referente aos riscos de operação de modelos de linguagem. Por exemplo, há necessidade de previsões quanto à avaliação de risco desses modelos, aos requisitos necessários de segurança para a sua implementação e utilização, à possibilidade de estabelecimento de *benchmarks* de privacidade, entre outras medidas regulatórias relevantes.

4. Perspectiva regulatória

Diante dos questionamentos trazidos, é importante analisar o texto do PL 2.338/2023, o qual estabelece as "normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil".

Em seus primeiros artigos, já é possível identificar a preocupação da proposta legislativa com a proteção de dados pessoais, bem como com a proteção das pessoas afetadas por sistemas de IA. Interpreta-se, aqui, que esses efeitos se estendem também a eventuais vazamentos de dados pessoais contidos nos conjuntos de dados utilizados para treinamento desses sistemas de IA.

> Art. 5º Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:
> VI – direito à privacidade e à proteção de dados pessoais, nos termos da legislação pertinente.
> (...)
> Art. 7º Pessoas afetadas por sistemas de inteligência artificial têm o direito de receber, previamente à contratação ou utilização do sistema, informações claras e adequadas quanto aos seguintes aspectos:
> (...)
> V – categorias de dados pessoais utilizados no contexto do funcionamento do sistema de inteligência artificial;

No entanto, é importante destacar que não há previsão quanto à informação referente à identificação ou mesmo a possibilidade de vazamentos de dados pessoais utilizados para o treinamento desses sistemas de IA. Além disso, a redação do inciso V aparenta não incluir informações referentes aos dados pessoais específicos utilizados no treinamento de conjunto de dados, apenas suas categorias.

Além disso, há de se considerar a possibilidade de compartilhamento de informações quanto às medidas tomadas para a higienização do banco de dados, sendo essa informação relevante para a tomada de decisões referente à contratação ou utilização de sistemas de inteligência artificial, tendo em vista o risco consideravelmente maior na utilização de sistemas de IA que não fazem uso de qualquer medida de mitigação.

Em continuidade, referente à utilização do conjunto de dados, o projeto de lei corretamente estabelece a necessidade da realização de uma avaliação preliminar com o propósito de avaliação de risco do sistema de inteligência artificial:

> Art. 13. Previamente a sua colocação no mercado ou utilização em serviço, todo sistema de inteligência artificial passará por avaliação preliminar realizada pelo fornecedor para classificação de seu grau de risco, cujo registro considerará os critérios previstos neste capítulo.
> (...)
> § 2º Haverá registro e documentação da avaliação preliminar realizada pelo fornecedor para fins de responsabilização e prestação de contas no caso de o sistema de inteligência artificial não ser classificado como de risco alto.
> § 3º A autoridade competente poderá determinar a reclassificação do sistema de inteligência artificial, mediante notificação prévia, bem como determinar a realização de avaliação de impacto algorítmico para instrução da investigação em curso.
> § 4º Se o resultado da reclassificação identificar o sistema de inteligência artificial como de alto risco, a realização de avaliação de impacto algorítmico e a adoção das demais medidas de governança previstas no Capítulo IV serão obrigatórias, sem prejuízo de eventuais penalidades em caso de avaliação preliminar fraudulenta, incompleta ou inverídica.

A previsão de prestação de contas no caso de o sistema não ser classificado como risco alto é fundamental para a implementação responsável de sistemas de inteligência artificial. no entanto, há de se considerar a possibilidade de incluir no processo de avaliação a realização de um *benchmark* de privacidade dos modelos de inteligência artificial, conjuntamente à avaliação preliminar de riscos.

Como explorado anteriormente, todos os modelos de linguagem estão suscetíveis a vazamento de dados pessoais, especialmente quando não implementam em seu desenvolvimento medidas de mitigação de vazamento de

dados pessoais, como higienização de conjunto de dados ou privacidade diferencial, razão pela qual se justifica a obrigatoriedade da triagem de sistemas de inteligência artificial por meio de uma avaliação específica de privacidade.

Por sua vez, a previsão do Art. 19, inciso IV, prevê a legitimação do tratamento de dados com base na legislação vigente de proteção de dados e prevê também a necessidade de implementação pelos agentes de inteligência artificial de medidas de privacidade para o desenvolvimento e implementação de sistemas de inteligência artificial.

> Art. 19. Os agentes de inteligência artificial estabelecerão estruturas de governança e processos internos aptos a garantir a segurança dos sistemas e o atendimento dos direitos de pessoas afetadas, nos termos previstos no Capítulo II desta Lei e da legislação pertinente, que incluirão, pelo menos:
> (...)
> IV – legitimação do tratamento de dados conforme a legislação de proteção de dados, inclusive por meio da adoção de medidas de privacidade desde a concepção e por padrão e da adoção de técnicas que minimizem o uso de dados pessoais;

Diante dos elementos técnicos trazidos anteriormente, tem-se destacada a importância da efetivação desta obrigação. Efetivamente, todo modelo que não implemente medidas de segurança devem ser considerados como altamente suscetíveis a vazamentos e poderão, portanto, se encaixar nas hipóteses de alto grau de identificabilidade de recuperação de dados pessoais e identificabilidade de titulares, conforme o Art. 18, inciso VIII.

Assim, embora não haja medida preventiva perfeita, propõe-se o estabelecimento da obrigatoriedade da realização de um relatório de privacidade para disponibilização no mercado ou utilização em serviço de todo sistema de inteligência artificial, este benchmark poderá ser estabelecido conjuntamente entre a autoridade responsável e a indústria, estabelecendo parâmetros aceitáveis para a operação de modelos de Inteligência Artificial, considerando o balanço entre utilidade e privacidade que deverá ser alcançado.

Dessa forma, para o propósito do treinamento de modelos de IA, deve-se atentar não apenas às previsões específicas de tratamento de dados, previstas na LGPD e aplicáveis aos conjuntos de dados utilizados para o treinamento de modelos, mas também aos padrões técnicos da autoridade para verificação da robustez do próprio modelo, para verificar a adequação quanto à tomada de medidas de mitigação.

Com a previsão explícita da necessidade de realização de não apenas uma avaliação de risco, mas também uma prévia avaliação de privacidade para todos os sistemas de IA, em razão da vulnerabilidade técnica desses modelos, elevasse-a a importância das garantias legais referente à privacidade, conjuntamente oferecendo maior eficácia às previsões da LGPD ao campo do treinamento de sistemas de inteligência artificial, simultaneamente oferecendo maior previsibilidade e clareza do framework regulatório que deseja-se alcançar.

Considerações finais

Em conclusão, a partir do levantamento de artigos recentes demonstrando a viabilidade da realização de ataques adversariais contra *LLMs*, com considerável grau de obtenção de dados pessoais, e diante das preocupações destes artigos em relação às possíveis medidas de prevenção e a sua atual incapacidade de lidar totalmente com a possibilidade de vazamentos, tem-se que o campo de estudos de ataques adversariais terá de receber atenção especial para viabilizar a continuidade do desenvolvimento sustentável e socialmente responsável de modelos de inteligência artificial.

Enquanto as atuais propostas legislativas possuem espaço para melhorias e estas devem ser continuamente discutidas e aprofundadas, a proposição dessas propostas indicam um avanço certeiro no sentido de regulamentar os critérios de desenvolvimento de inteligência artificial no Brasil e devem continuar a acompanhar o desenvolvimento não apenas dos modelos, mas também das vias adversariais.

Em razão disso é que, na esfera técnica, deverão ser buscadas maneiras de melhor implementar medidas de segurança e mitigações no treinamento de Inteligência Artificial. Apenas assim, poderemos avançar no objetivo do desenvolvimento responsável de inteligência artificial, sobrepondo as medidas regulatórias da LGPD com novo arcabouço regulatório preparado para lidar com um setor em rápido desenvolvimento.

Enquanto devemos continuar atentos quanto a novas vias de ataque, como, por exemplo, a extração de modelo[28], injeção de *prompts*[29], entre outras, deve-

28. ZANELLA-BÉGUELIN, S. et al. *Grey-box Extraction of Natural Language Models*. [s.l: s.n.]. Disponível em: <https://tinyurl.com/25yas422f>. Acesso em: 19 nov. 2023.

29. GRESHAKE, K. et al. *Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection*. Disponível em: <https://arxiv.org/abs/2302.12173>.

-se também tornar a atenção ao desenvolvimento de novas mitigações, como a utilização de outros modelos de inteligência artificial em colaboração para treinar adversariamente os modelos que se busca defender, por meio do chamado "*red-teaming*"[30]

Destaca-se novamente que a taxonomia e os ataques aqui apresentados não são definitivos e demonstram apenas um recorte do campo do estudo de ataques adversariais. Há ainda diversas perspectivas não atendidas por este artigo. Espera-se, portanto, ao menos contribuir com o desenvolvimento de pesquisas futuras sobre o tema.

Futuras perspectivas de regulação de Inteligência Artificial necessariamente terão de tornar seus olhares às medidas tomadas internacionalmente, de modo a construir por meio também da colaboração internacional um *framework* com maior robustez e sofisticação.

Em conclusão, enquanto há a necessidade de melhores *benchmarks* de privacidade não apenas para modelos grandes de linguagem, mas também para sistemas de inteligência artificial como um todo, havendo necessidade de desenvolvimento de novas medidas de mitigação, a perspectiva inicial do cenário regulatório mostra-se definitivamente positiva.

30. PEREZ, E. et al. *Red Teaming Language Models with Language Models*. arXiv:2202.03286 [cs], 7 fev. 2022. Disponível em: <https://arxiv.org/abs/2202.03286>.

Referências

CARLINI, N. et al. *Quantifying Memorization Across Neural Language Models*. Disponível em:<https://arxiv.org/abs/2202.07646>. Acesso em: 19 nov. 2023.

CORRÊA, N. K. *Artificial Intelligence Ethics and Safety: practical tools for creating "good" models*. Disponível em: <https://arxiv.org/abs/2112.11208>. Acesso em: 1 dez. 2023.

CORTIZ, Diogo *K-ANONYMITY - Privacidade e Inteligência Artificial*. Disponível em: <https://tinyurl.com/3ycre4k6>. Acesso em: 1 dez. 2023.

DEVLIN, J. et al. *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*. Proceedings of the 2019 Conference of the North, v. 1, 2019.

JAGIELSKI, M.; ULLMAN, J.; OPREA, A. *Auditing Differentially Private Machine Learning: How Private is Private SGD?* Disponível em: <https://arxiv.org/abs/2006.07709>. Acesso em: 1 dez. 2023.

LUDERMIR, Teresa Bernarda. *Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências*. Estudos Avançados, v. 35, p. 85-94, 2021.

LUKAS, N. et al. *Analyzing Leakage of Personally Identifiable Information in Language Models*. arXiv (Cornell University), 1 fev. 2023.

MORAIS, Alana. *Ameaças a Sistemas baseados em Machine Learning* – Parte 1 de 5 | *SideChannel Tempest*. Disponível em: <https://tinyurl.com/5n8nsdrs/>. Acesso em: 19 nov. 2023.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. *Robust de-anonymization of large sparse datasets*. In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008. p. 111-125.

OPREA, Alina; VASSILEV, Apostol. *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (draft). National Institute of Standards and Technology*, 2023.

POLIDO, Fabrício Bertini Pasquot. *Inteligência artificial entre estratégias nacionais e a corrida regulatória global: Rotas analíticas para uma releitura internacionalista e Comparada (Artificial Intelligence Between National Strategies and the Global Regulatory Race: Analytical Routes for an International and Comparative Reappraisal). Rev. Fac. Direito UFMG, Belo Horizonte,* n. 76, p. 229-256, 2020.

VASWANI, A. et al. *Attention is all you need in Advances in Neural Information Processing Systems*, 2017. Search PubMed, p. 5998-6008.

XU, Q. et al. *Student Surpasses Teacher: Imitation Attack for Black-Box NLP APIs*. Disponível em: <https://arxiv.org/abs/2108.13873>. Acesso em: 1 dez. 2023.

YIN, Y.; HABERNAL, I. *Privacy-Preserving Models for Legal Natural Language Processing*. Disponível em: <https://arxiv.org/abs/2211.02956>.

ZHANG, W. E. et al. *Adversarial Attacks on Deep-learning Models in Natural Language Processing. ACM Transactions on Intelligent Systems and Technology*, v. 11, n. 3, p. 1–41, 13 maio 2020.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

14

Intersecções e relações entre a Lei Geral de Proteção de Dados e o Projeto de Lei 2.338/2023: uma análise comparativa sobre *accountability*

JULIA FERRARI OLIVEIRA LIMA

JULIA FERRARI OLIVEIRA LIMA[1]

Introdução

A conexão entre a Inteligência Artificial (IA) e a proteção de dados pessoais tem sido amplamente debatida, sendo um dos destaques mais recentes a publicação, pela Autoridade Nacional de Proteção de Dados (ANPD), de sua Análise Preliminar do Projeto de Lei 2.338/2023[2] e a Nota Técnica nº 16/2023/CGTP/ANPD[3].

A intersecção entre a proteção de dados pessoais, regulada pela Lei n. 13.709/2018 ou Lei Geral de Proteção de Dados (LGPD), e questões da Inteligência Artificial, a princípio abordadas no Projeto de Lei n. 2.338/2023, é evidente devido ao inerente uso de dados - pessoais e não pessoais - por sistemas de IA, que dependem dessa "matéria-prima" essencial no seu funcionamento, treinamento, e aprimoramento contínuo. Essa relação se estreita na medida da convergência desses campos de estudo, tendo em comum, por exemplo, direitos e deveres relacionados ao processamento de dados.

Esse cenário traz à tona discussões envolvendo instrumentos para prevenção e solução de problemas que emergem dessa tecnologia, a aplicação de estatutos legais já existentes e, ainda, de futura regulação específica. Dessa forma, compreender o princípio da *accountability*, ou responsabilização e prestação de contas, torna-se chave para identificar pontos de convergência entre os possíveis instrumentos para proteção de dados no contexto do desenvolvimento e uso de IA.

A LGPD representa um marco regulatório importante para a proteção da privacidade e de dados no Brasil, enquanto o PL 2.338/23 busca regular o uso de IA de forma abrangente. Dessa forma, surgem intersecções, relações, con-

1. Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS-Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Graduada em Direito pela Universidade Presbiteriana Mackenzie. Atua como advogada nas áreas de Tecnologia, Proteção de Dados e Propriedade Intelectual.

2. ANPD. *Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial*. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 23 jul. 2023.

3. ANPD. Nota Técnica nº 16/2023/CGTP/ANPD. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 17 ou. 2023.

vergências e conflitos entre esses textos legais que devem ser debatidos. O presente artigo busca, portanto, analisar a LGPD e o PL 2.338/23, sob a ótica da *accountability* como ponto comum para nortear medidas adequadas de proteção de dados e a regulação de tecnologias emergentes.

A LGPD estabelece regras e princípios para o tratamento de dados pessoais, garantindo aos titulares dos dados o controle sobre suas informações, bem como a transparência e a responsabilidade dos agentes de tratamento. Contudo, o avanço no desenvolvimento da IA e o tratamento de dados por sistemas automatizados criam novos desafios para a proteção da privacidade e a responsabilização adequada dos agentes envolvidos, bem como para a interconexão entre as normas existentes.

A responsabilidade e prestação de contas tornam-se cruciais no contexto da IA, uma vez que o tratamento automatizado de dados pode levar a decisões que afetam significativamente os indivíduos. A *accountability* busca garantir que os agentes de tratamento de dados sejam responsabilizados por suas ações e decisões tomadas com base em IA para além de contraprestações de causa e efeito, permitindo que os titulares de dados compreendam como suas informações estão sendo utilizadas e os riscos de decisões potencialmente injustas ou discriminatórias possam ser mitigados.

A crescente aplicação da inteligência artificial em diversas esferas da sociedade tem levantado questões relevantes sobre a privacidade e proteção de dados pessoais. Tanto a LGPD quanto o PL 2.338 buscam endereçar essas preocupações, estabelecendo mecanismos de *accountability* para o tratamento de dados em sistemas de IA. A análise comparativa deste artigo visa identificar semelhanças e diferenças nestes dispositivos quanto à proteção dos direitos fundamentais dos indivíduos e os dilemas da construção de uma base regulatória sólida.

Assim, serão abordados adiante os conceitos e fundamentos da *accountability*, bem como os princípios originados pelo este conceito na legislação brasileira, com o intuito de compreender suas abordagens para assegurar o tratamento responsável de dados pessoais em sistemas de IA num contexto regulatório coeso, com segurança jurídica e eficácia plena.

1. *Accountability*: conceitos e fundamentos

O conceito de *accountability* é amplamente discutido no campo do direito e política contemporâneos. No entanto, ao contrário de ideais políticos fundamentais, como democracia, direitos humanos, constitucionalismo e Estado

de Direito, alguns entendem que ele não ocupa uma posição tão destacada quanto deveria. Danielle Rached destaca que a *accountability* é muitas vezes negligenciada e opera em um nível menos proeminente no vocabulário jurídico e político[4].

A *accountability* surgiu na proteção de dados internacional há mais de 30 anos, quando primeiro adotada nas Diretrizes da OCDE[5]. Atualmente, porém, é fato que o discurso político sobre a regulamentação da proteção de dados tem sido repleto de referências à *accountability*, desde a Opinião de 2010 do *Article 29 Data Protection Working Party*[6] até o *AI Act*[7], bem como a LGPD e PL n. 2.338/2023 no cenário brasileiro. No contexto desses documentos, a *accountability* é vista como garantia para que os controladores estabeleçam políticas eficazes para conformidade.

Seu ressurgimento no *zeitgeist* regulatório é atribuído à globalização, sendo considerada uma forma promissora de lidar com os desafios da globalização dos fluxos de informação, como a computação em nuvem[8]. No cerne, o conceito refere-se a uma relação em que uma entidade pode convocar outra para explicar sua conduta, comumente encontrada quando uma entidade tem poderes ou responsabilidades a serem verificados para mitigar riscos. A regulamentação de proteção de dados surgiu para proteger indivíduos contra riscos do tratamento de dados pessoais e, ao longo do tempo, diferentes instrumentos avançaram mecanismos de *accountability*, mas notáveis diferenças existem entre eles. Uma dessa diferenças é a transição de uma abordagem "reativa" para uma mais "proativa", em que os atores podem demonstrar conformidade sem prévia reclamação específica.

4. RACHED, Danielle Hanna. The Concept(s) of Accountability: form in search of substance. *Leiden Journal Of International Law*, [S.L.], v. 29, n. 2, p. 317-342, 29 abr. 2016. Cambridge University Press (CUP). http://dx.doi.org/10.1017/s0922156516000042. Disponível em: https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/abs/concepts-of-accountability-form-in-search-of-substance/8E481D883DC5B5E9752C3CCA9BE39884. Acesso em: 23 jul. 2023.

5. ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. 2023. OECD Legal Instruments*. Disponível em: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf. Acesso em: 27 nov. 2023.

6. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2010 on the principle of accountability*. 2010. 00062/10/EN WP 173. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 27 nov. 2023.

7. PARLAMENTO EUROPEU. *Artificial Intelligence Act (AI Act)*. 2023. 2021/0106(COD). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html. Acesso em: 27 nov. 2023.

8. ALHADEFF, Joseph; van ALSENOY, Brendan; DUMORTIER, Jos. *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*. 2011. In: GUAGNIN; Hempel; ILTEN (org.). *Managing Privacy through Accountability*. Londres: Palgrave Macmillan, 2012. p. 49-82. Disponível em: https://ssrn.com/abstract=1933731. Acesso em: 27 nov. 2023

Analogamente, de acordo com Rached, a *accountability* não se concentra em uma visão jurídica ou política abrangente, mas, em vez disso, fornece uma caixa de ferramentas para restringir o poder, permitindo diversas abordagens dependendo do papel, posição e importância da entidade ou ator que será responsabilizado.

A título de exemplo, no arcabouço jurídico brasileiro, a responsabilidade civil, especialmente na LGPD, é objeto de intenso debate. Nestas discussões, a questão central é se essa responsabilidade seria objetiva ou subjetiva, visto que a lei não o definiu expressamente. No caso de ser considerada objetiva, a atribuição do dano estaria relacionada ao risco inerente à atividade (conforme o artigo 42 da referida lei) ou ao defeito do produto/serviço (tratamento irregular - artigo 44).

Já na corrente subjetivista, dentre outros argumentos, entende-se que a LGPD cria um verdadeiro padrão de conduta para os agentes de tratamento e, portanto, a culpa do agente é fator determinante no regime de responsabilidade. Neste último caso, a eliminação da culpa levaria à exclusão da responsabilidade subjetiva, ou a real obrigação objetiva de indenizar só seria alcançada quando afastássemos a ilicitude[9].

É crucial ressaltar que essa discussão não esgota todas as múltiplas variáveis e dimensões do conceito de “responsabilidade” e suas possíveis aplicações na LGPD. Na verdade, a controvérsia se concentra principalmente na qualificação da obrigação de indenizar, visando a reparação completa de danos materiais e morais, transferindo-os da vítima para os responsáveis pelos danos. Contudo, ainda há um elemento mais abrangente da prestação de contas que se mostra útil neste fórum.

Conforme leciona Nelson Rosenvald, o termo *liability*, presente no *common law*, ajusta-se bem ao sentido do Direito Civil clássico de responsabilidade. Diversas teorias desenvolvem a liability no contexto da responsabilidade civil, sendo comum remeterem a uma indenização com base no nexo causal entre uma conduta e um dano, acrescido por outros elementos, dependendo da peculiaridade de cada jurisdição[10].

9. FERRÃO DOS SANTOS, C.; GOMES DA SILVA, J.; PADRÃO, V. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. *Revista Eletrônica da PGE-RJ, [S. l.]*, v. 4, n. 3, 2021. DOI: 10.46818/pge.v4i3.256. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 27 jul. 2023.

10. ROSENVALD, Nelson. *A polissemia da responsabilidade civil na LGPD*. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336002/a-polissemia-da-responsabilidade-civil-na-lgpd. Acesso em: 23 jul. 2023.

No entanto, "*liability*" é apenas um dos sentidos da responsabilidade. Existem outros três vocábulos que trazem mais profundidade ao conceito: "*responsibility*", "*accountability*" e "*answerability*". Embora esses três termos possam ser traduzidos diretamente para a nossa língua como responsabilidade, eles diferem do sentido monopolístico que as jurisdições da *civil law* conferem à *liability*, vista como o cerne da responsabilidade civil (artigos 927 a 954 do Código Civil). Em comum, os três termos transcendem a função judicial de reparação de danos, acrescentando novas camadas à responsabilidade para responder à complexidade e rapidez das relações sociais.

O enfoque do presente artigo será quanto à "*accountability*". Todavia, é relevante enfatizar o sentido de cada um desses termos em inglês para ampliar o entendimento sobre a responsabilidade. Desmembrar a *liability* como ponto central da responsabilidade civil, é um caminho para entendê-la como um último recurso para o que se busca na responsabilidade civil no século XXI [reparação], especialmente na proteção de dados pessoais.

O termo "*responsibility*" aborda a responsabilidade no sentido moral, voluntariamente aceita e não imposta por lei. Este conceito prospectivo torna a responsabilidade um instrumento para autogoverno e modelagem de vida. No tratamento de dados pessoais, isso implica na incorporação da ética para os agentes de tratamento e na educação digital para os titulares dos dados, permitindo um uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania.

Já a "*accountability*" amplia o espectro da responsabilidade, incluindo parâmetros regulatórios preventivos que promovem a interação entre a *liability* do Código Civil e uma regulamentação voltada à governança de dados, seja em caráter *ex ante* ou *ex post*.

Na perspectiva *ex ante*, Rosenvald destaca que a *accountability* na LGPD serve como guia para controladores e operadores, estabelecendo boas práticas, procedimentos, normas de segurança e padrões técnicos para lidar com riscos de alto impacto. Os princípios da atividade de tratamento de dados, mencionados no artigo 6 da LGPD, incluem "responsabilização e prestação de contas". Além disso, o Regulamento Geral sobre a Proteção de Dados 2016/679 (*General Data Protection Regulation* - GDPR) da União Europeia amplia a *accountability* na avaliação de impacto sobre a proteção de dados, informando os envolvidos sobre operações que podem violar direitos humanos.

Na vertente *ex post*, a *accountability* atua como guia para o juiz e autoridades na identificação de responsabilidades e estabelecimento de medidas de

reparação. Padrões objetivos são estabelecidos para avaliar o risco em comparação com outras atividades, evitando a discricionariedade do juiz. A efetividade do *compliance* pode ser considerada para redução de indenizações, seguindo o parágrafo único do artigo 944 do Código Civil[11]. Apesar da falta de um modelo jurídico semelhante aos "*punitive damages*", a Autoridade Nacional de Proteção de Dados pode utilizar a *accountability* para impor sanções punitivas e multas, conforme o artigo 52 da LGPD, em resposta a infrações de agentes de tratamento de dados.

Por fim, a "*answerability*", traduzida literalmente como "explicabilidade", é outra dimensão preventiva da responsabilidade. Esse processo de justificação de escolhas e decisões vai além do direito à informação, possibilitando uma compreensão abrangente do tratamento de dados. Na LGPD, isso se reflete na "habilidade de apelação", concedendo ao titular o direito de solicitar a revisão de decisões automatizadas que impactem seus interesses (artigo 20 da LGPD). Prioriza-se uma revisão extrajudicial por humanos em decisões de inteligência artificial. A "*liability*" surge posteriormente, caso danos ocorram devido a atividades prejudiciais que violem o perfil da pessoa ou afetem situações existenciais.

Responsibility, *accountability* e *answerability* adicionam à responsabilidade civil elementos preventivos, eventualmente complementadas pela função compensatória da *liability*. Ao contrário do que é propagado por escolas clássicas da responsabilidade, o efeito preventivo não é um mero efeito colateral de uma sentença condenatória para uma indenização. A multifuncionalidade da responsabilidade civil vai além de uma discussão acadêmica e é um exemplo legislativo da necessidade de ampliar a percepção sobre a responsabilidade civil. Não se trata apenas de um mecanismo para conter danos, mas também para conter comportamentos.

Nesse contexto, incorporam-se a pessoa do agente e a indução à conformidade por meio de uma regulação de gestão de riscos, especialmente sua mitigação, tanto por parte de desenvolvedores de tecnologias digitais emergentes, quanto por parte de agentes de tratamento e reguladores (*accountability/answerability*).

11. Art. 944, parágrafo único: "Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, eqüitativamente, a indenização". BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

Retornando à centralidade da *accountability*, segundo Bruno Bioni, o termo carrega uma carga retórica significativa, muitas vezes sendo interpretado como sinônimo de virtude. É comum utilizá-lo como um adjetivo para descrever comportamentos responsáveis em diversas situações, como políticos honestos, empresas com responsabilidade social, países que alcançam metas climáticas e parceiros de relacionamento[12].

Ao tratar especificamente da proteção de dados, o termo é frequentemente utilizado para denotar o cumprimento da lei, indicando um uso responsável dos dados. Em vez de ser considerada apenas como um fim em si mesma, a *accountability* deve ser vista como um mecanismo para alcançar virtuosidade. Bioni destaca a natureza relacional da *accountability*, estabelecendo um processo colaborativo e dialógico entre os agentes e aqueles que os julgam, promovendo uma co-deliberação para decisões sobre o fluxo informacional. Ele associa a boa-fé à *accountability*, destacando a base cooperativa e colaborativa do processo.

Já pela lente da lexicografia, o *Oxford Learner's Dictionary Of Academic English* define o termo "*accountability*" como "o fato ou estado de assumir a responsabilidade por suas decisões ou ações, para que você possa explicá-las, se necessário" (tradução nossa)[13]. Corroborando com esta definição, a LGPD interpreta o termo com a disposição sobre o princípio da "responsabilização e prestação de contas" em seu artigo 6º, inciso X: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas", destacando a importância de demonstrar o cumprimento das normas de proteção de dados[14].

Disto depreende-se, portanto, que a prestação de contas é fundamental para determinar se o uso dos dados é, de fato, responsável. A *accountability*, é um vínculo dinâmico e obrigacional, que requer cooperação entre as partes envolvidas no tratamento de dados para alcançar práticas virtuosas.

12. BIONI, Bruno. *Accountability na qualidade de um conceito relacional e de modulação do poder*. 2022. Disponível em: https://blog.grupogen.com.br/juridico/postagens/artigos/accountability-conceito-relacional/. Acesso em: 23 jul. 2023.

13. OXFORD LEARNER'S DICTIONARY OF ACADEMIC ENGLISH. *Accountability noun*. Disponível em: https://www.oxfordlearnersdictionaries.com/definition/academic/accountability. Acesso em: 23 jul. 2023.
Tradução nossa: "*the fact or state of taking responsibility for your decisions or actions, so that you can explain them if necessary*."

14. BRASIL. Lei n. 13.709 de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 jul. 2023.

Visto o acima exposto, é possível afirmar que a *accountability* é um conceito relevante, embora muitas vezes subestimado, que possui aplicação em diversos campos jurídicos. Na proteção de dados, ela desempenha um papel crucial na regulação e governança, e sua aplicação pode se estender a outros setores, como o direito do consumidor, proporcionando um processo colaborativo e dialógico para tomar decisões e controlar o poder. Nesse cenário, o desenvolvimento de tecnologias emergentes e da sociedade, em especial em relação ao uso de dados pessoais, trouxe à tona a necessidade da codificação específica da *accountability* em proteção de dados.

2. *Accountability* na LGPD

A LGPD é fruto de um processo legislativo complexo que envolveu debates, discussões e ajustes ao longo de vários anos. Sua origem pode ser rastreada até o surgimento da necessidade de se criar uma legislação específica para a proteção de dados pessoais no Brasil, em meio ao crescente uso da internet, das tecnologias da informação e datificação das atividades cotidianas, comerciais e governamentais.

A discussão sobre a proteção de dados no Brasil teve início no início dos anos 2000, quando o avanço tecnológico e a coleta massiva de informações pessoais chamaram a atenção para a necessidade de salvaguardar a privacidade e os direitos dos cidadãos. Nesse contexto, o país aprovou o Marco Civil da Internet em 2014, que tratou de alguns aspectos relacionados à privacidade e à proteção de dados, mas não era uma legislação específica sobre o tema.

A partir de então, várias propostas de lei foram apresentadas no Congresso Nacional visando a regulamentação da proteção de dados. Diversas organizações e especialistas participaram de debates e audiências públicas para discutir o tema, ressaltando a importância de garantir a proteção dos dados pessoais diante da crescente coleta e tratamento dessas informações por empresas e instituições.

Em 2010, foi apresentado um anteprojeto de lei para proteção de dados pessoais, que passou por diversas atualizações e modificações ao longo do tempo[15]. O Marco Civil da Internet, por sua vez, contribuiu para a conscientiza-

15. BRASIL. *Anteprojeto de Lei para a Proteção de Dados Pessoais de 2010*. Disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em: 23 jul. 2023.

ção da sociedade sobre a importância da proteção de dados e da necessidade de uma lei específica para tratar do assunto[16].

Em 2018, após um amplo processo de discussão e tramitação legislativa, o Projeto de Lei N. 53/2018 foi aprovado no Congresso Nacional e sancionado pelo então presidente em 14 de agosto de 2018, tornando-se a LGPD.

Em conclusão, a origem da LGPD está intrinsecamente ligada à crescente preocupação com a proteção da privacidade e dos direitos dos cidadãos diante do avanço tecnológico e a responsabilização sobre o tratamento desses dados. Seu processo legislativo envolveu um amplo debate e participação da sociedade civil, resultando em uma lei abrangente, atualizada e participativa que busca garantir maior segurança e transparência no tratamento de dados pessoais no Brasil.

Especialmente na última década, temos observado uma mudança significativa nos modelos regulatórios adotados no Brasil. Os antigos modelos rígidos e centralizados, baseados em estruturas de comando e controle, estão sendo substituídos por normas mais flexíveis, abertas e orientadas pelo princípio do compliance. A LGPD é um exemplo recente dessa tendência, marcando uma importante transição de paradigma no conceito jurídico de "responsabilidade"[17].

Essa mudança conceitual reflete-se no cenário do tratamento de dados pessoais no Brasil, em que diversos atores compõem um ecossistema complexo. Nota-se na LGPD que o legislador reconhece a necessidade de conceder aos titulares de dados o poder de autodeterminação informativa, estimulando debates sobre o controle dos fluxos de dados. Porém, o que salta aos olhos é o modo como esse poder é concedido: ao mesmo tempo, é depositada confiança nos agentes de tratamento para gerir os riscos envolvidos em suas atividades[18].

16. BRASIL. *Lei n. 12.965 de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 jul. 2023.

17. FRAZÃO, Ana; CUEVA, Ricardo. 32. *Accountability e Mitigação da Responsabilidade Civil na Lei Geral de Proteção de Dados*. In: FRAZÃO, Ana; CUEVA, Ricardo. Compliance e Políticas de Proteção de Dados. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/32-accountability-e-mitigacao-da-responsabilidade-civil-na-lei-geral-de-protecao-de-dados-pessoais-compliance-e-politicas-de-protecao-de-dados/1506551422. Acesso em: 23 jul. 2023.

18. BIONI, Bruno; LUCIANO, Maria. *O PRINCÍPIO DA PRECAUÇÃO NA REGULAÇÃO DE INTELIGÊNCIA ARTIFICIAL*: seriam as leis de proteção de dados o seu portal de entrada? 2019. Disponível em: https://brunobioni.com.br/home/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: 23 jul. 2023.

No entanto, essa confiança não é desprovida de responsabilidade. Como mencionado anteriormente, LGPD estabelece a "responsabilidade e prestação de contas" como requisitos essenciais para o contexto brasileiro do tratamento de dados pessoais, abrangendo tanto a responsabilidade (*liability*) quanto a prestação de contas (*accountability*). Essa abordagem regulatória tem implicações significativas na atuação da Autoridade Nacional de Proteção de Dados (ANPD), abrindo espaço para a aplicação de sanções administrativas e para a reconfiguração do entendimento sobre a responsabilidade civil e suas funções.

Disso depreende-se que a LGPD representa uma mudança na forma a responsabilidade no tratamento de dados pessoais é abordada, buscando um equilíbrio entre o poder de controle conferido aos titulares de dados e a confiança depositada nos agentes de tratamento. A legislação promove uma abordagem mais aberta e flexível, ou principiológica, alinhada com o princípio do *compliance*. Para tanto, estabelece a necessidade de prestação de contas e responsabilização dos envolvidos no complexo ecossistema de tratamento de dados no Brasil. Isso tem impacto nas práticas regulatórias e também na interpretação do conceito de responsabilidade civil[19].

Nesta toada, a *accountability* amplia a responsabilidade civil, incorporando parâmetros regulatórios preventivos para promover uma interação entre a responsabilidade civil do Código Civil e a governança de dados, seja de forma preventiva ou reativa[20].

Complementarmente, os sujeitos envolvidos na relação de *accountability*, não se limitando apenas aos controladores de dados, mas também abrangendo aqueles que possuem competência decisória sobre informações, como autoridades de proteção de dados e entidades certificadoras[21].

3. *Accountability* no PL 2.338/2023

O Projeto de Lei nº 2.338/2023 é uma proposta legislativa que busca regular a Inteligência Artificial no Brasil, estabelecendo normas e diretrizes para o

19. TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. RESPONSABILIDADE CIVIL E REGULAÇÃO DE NOVAS TECNOLOGIAS: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Rei - Revista Estudos Institucionais*, [S.L.], v. 6, n. 1, p. 301-333, 25 abr. 2020. Revista Estudos Institucionais. http://dx.doi.org/10.21783/rei.v6i1.383. Disponível em: https://doi.org/10.21783/rei.v6i1.383. Acesso em: 23 jul. 2023.

20. ROSENVALD, Nelson. *Conceitos de responsabilidade civil para 4ª revolução industrial e o capitalismo de vigilância*. In: EHRHARDT JÚNIOR, Marcos (coord.). Direito civil: futuros possíveis. Fórum, 2021.

21. BIONI, Bruno. *Accountability na qualidade de um conceito relacional e de modulação do poder*. 2022. Disponível em: https://blog.grupogen.com.br/juridico/postagens/artigos/accountability-conceito-relacional/. Acesso em: 23 jul. 2023.

uso dessa tecnologia no país. O PL 2.338/2023 foi apresentado com o objetivo de criar um marco legal que permita a utilização da IA de forma responsável, considerando seus impactos na sociedade, na economia e nos direitos dos cidadãos.

O PL 2.338/2023 parte do princípio de que a regulação da IA deve ser pautada em abordagens baseadas em riscos e direitos. Ou seja, busca equilibrar a proteção dos direitos e liberdades fundamentais dos cidadãos com o estímulo ao desenvolvimento econômico e tecnológico proporcionado pela IA. Essa perspectiva visa harmonizar avanços tecnológicos com a valorização do trabalho e a dignidade humana, seguindo os princípios da Constituição Federal.

A proposta do projeto é alinhada - ou até decorrente - à Lei Geral de Proteção de Dados, uma vez que esta também adota uma abordagem baseada em direitos e riscos. Isso demonstra que a regulação da IA e a proteção de dados pessoais não são mutuamente excludentes, muito pelo contrário, são complementares, considerando que a IA utiliza uma quantidade significativa de dados, incluindo dados pessoais, para seu funcionamento e desenvolvimento.

O PL 2.338/2023 contém diversas disposições relevantes para a regulação da IA no Brasil. Em relação aos riscos, o projeto proíbe o uso de sistemas de IA considerados de risco excessivo, buscando evitar potenciais danos à sociedade e aos indivíduos. Além disso, estabelece obrigações específicas para sistemas de IA de alto risco, buscando mitigar os riscos associados a esses sistemas.

Outro ponto relevante do projeto é a previsão de *sandboxes regulatórios*, ambientes de testes controlados e limitados, que permitem que as empresas e desenvolvedores testem novas tecnologias e inovações em IA, sob a supervisão e regulamentação das autoridades competentes. Essa iniciativa visa incentivar a inovação responsável, permitindo que novas soluções em IA sejam desenvolvidas de forma segura e em conformidade com a legislação aplicável.

É importante destacar que o PL 2.338/2023 está sujeito a alterações e discussões no processo legislativo antes de se tornar lei. A proposta passará por análises, debates e possíveis emendas por parte dos parlamentares e da sociedade em geral, garantindo que as diferentes perspectivas sejam consideradas e que a regulação final seja a mais adequada e equilibrada possível.

No que diz respeito ao princípio da *accountability*, ou responsabilização e prestação de contas, porém, este é um dos pilares fundamentais do PL. Tal princípio visa assegurar que os agentes envolvidos no desenvolvimento, implementação e uso de sistemas de IA sejam responsáveis por suas ações e

decisões, e que prestem contas de forma transparente sobre como a IA está sendo utilizada e quais os impactos decorrentes de suas aplicações. Dispõe o artigo 3º do PL:

> Artigo 3º O desenvolvimento, a implementação e o uso de sistemas de inteligência artificial observarão a boa-fé e os seguintes princípios:
> IX – rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica;
> X – prestação de contas, responsabilização e reparação integral de danos; (BRASIL, 2023)

O PL prevê diversas disposições relacionadas à *accountability*, buscando garantir que os agentes regulados atuem de forma ética, responsável e em conformidade com as normas estabelecidas na legislação. Uma das principais formas de promover a *accountability* é por meio da obrigatoriedade de elaboração de Relatório de Impacto à Proteção de Dados (RIPD) para sistemas de IA de alto risco.

O RIPD, de modo semelhante ao previsto na LGPD, é um documento que deve ser elaborado pelos desenvolvedores e operadores de sistemas de IA e que tem como objetivo avaliar os potenciais impactos do uso da tecnologia nos direitos fundamentais dos cidadãos, especialmente em relação à proteção de dados pessoais. Esse relatório permite que os agentes regulados identifiquem os riscos associados ao uso da IA e adotem medidas para mitigá-los.

Ademais, o PL 2.338/2023 prevê a realização de Avaliação de Impacto Algorítmico (AIA), que consiste em uma análise detalhada dos algoritmos utilizados nos sistemas de IA. Essa avaliação visa verificar se os algoritmos são justos, transparentes e não discriminatórios, garantindo que as decisões tomadas pela IA sejam baseadas em critérios objetivos e não violem direitos e princípios constitucionais. Instrumento o qual remete à avaliação do legítimo interesse (*legitimate interest assessment* – LIA) prevista pelo GDPR europeu.

A *accountability* também se manifesta na previsão de mecanismos de governança para a regulação da IA. O PL 2.338/2023 estabelece a criação de códigos de boas práticas e governança para os agentes de tratamento que utilizam sistemas de IA. Esses códigos têm o objetivo de orientar as ações dos agentes, garantindo que eles atuem de acordo com os princípios éticos e legais no uso da IA.

Outro aspecto relevante do princípio da *accountability* presente no projeto é a previsão de direitos aos titulares de dados afetados pelo funcionamento de sistemas de IA. O PL 2.338/2023 estabelece o direito de contestar e solicitar revisão de decisões tomadas com base em IA, garantindo que os cidadãos possam questionar e obter explicações sobre as decisões automatizadas que os afetem.

A responsabilização dos agentes regulados também é prevista no projeto por meio da aplicação de sanções administrativas em caso de descumprimento das normas estabelecidas. Essas sanções podem incluir advertências, multas, suspensão temporária de atividades e até mesmo a proibição do uso de sistemas de IA considerados de risco excessivo.

Em conclusão, o Projeto de Lei n. 2.338/2023 representa uma importante iniciativa para a regulamentação da IA no Brasil, visando equilibrar o desenvolvimento tecnológico com a proteção dos direitos e liberdades individuais. A proposta aborda questões relevantes, como a gestão de riscos, direitos dos cidadãos e mecanismos de governança, buscando garantir uma abordagem responsável e ética no uso da IA no país. No entanto, é fundamental que o processo legislativo seja conduzido com cautela e diálogo para que a regulação final seja efetiva e adequada aos desafios da era digital.

Desse modo, erguem-se questões quanto à definição de critérios para identificação de sistemas de IA de alto risco, o estabelecimento de padrões técnicos e éticos para a realização das avaliações de impacto, e a capacidade das autoridades de fiscalização de acompanhar o ritmo acelerado das inovações em IA. Além disso, é necessário considerar as possíveis interações entre o PL 2.338/2023 e outras legislações já existentes, como a LGPD, o Marco Civil da Internet e o Código de Defesa do Consumidor, de modo a garantir a coerência e complementaridade das normas.

A discussão sobre a regulação da IA envolve diversos atores, incluindo o setor privado, a sociedade civil, a academia e órgãos governamentais. A participação de todos é fundamental para que a legislação alcance seus objetivos, protegendo os direitos dos cidadãos, estimulando a inovação responsável e garantindo a competitividade do país no cenário internacional.

Portanto, é essencial que o debate acerca do PL 2.338/2023 seja amplo e democrático, levando em consideração os diferentes interesses e perspectivas, e garantindo a construção de uma legislação que reflita os valores e necessidades da sociedade brasileira. Somente dessa forma será possível al-

cançar uma regulação da IA que promova o desenvolvimento tecnológico de forma ética e sustentável, contribuindo para o progresso do país e o bem-estar de seus cidadãos.

4. Intersecções e relações

O PL 2.338/2023 apresenta notadas intersecções com a LGPD, adotando uma abordagem baseada em riscos e direitos. Embora tenham enfoques distintos, os objetivos de ambas as normas reforçam a importância de criar mecanismos para aplicação coesa dessas normativas.

A ANPD, abordou algumas convergências entre as áreas e suas normas, e futuras normas, regulamentadoras em um estudo preliminar sobre o PL 2.338/2023 e na Nota Técnica nº 16/2023/CGTP/ANPD. Nesses documentos expositivos, a análise da autoridade enfatiza alguns campos de correspondência entre o PL e a LGPD e possíveis coincidências e conflitos com as atribuições legais da ANPD, são estes: (i) tutela de direitos; (ii) correlação entre sistemas de IA de alto risco e o tratamento de dados pessoais; (iii) compatibilização do fomento à inovação com a proteção de direitos fundamentais; (iv) mecanismos de governança; e (v) a autoridade competente.

Examinando os pontos de conexão, percebe-se a relação entre os direitos dos titulares de dados pessoais e aqueles afetados pelos sistemas de IA. Por exemplo, o direito à informação, previsto no PL 2.338/23 (artigos 5º, I, 7º e 8º), é semelhante ao direito de acesso e ao princípio da transparência presentes na LGPD (artigos 9º e 6º, IV, respectivamente). Ambos os sistemas preveem a garantia de informações claras e acessíveis aos titulares de direitos.

Além disso, o PL 2.338/23 (artigos 5º, II e 9º) estabelece o direito do titular de contestar e solicitar revisão de decisões tomadas com base em IA, o que se relaciona diretamente com o direito de revisão e obtenção de informações sobre decisões automatizadas previsto no art. 20 da LGPD. Aqui, a ANPD aponta a tensão entre as condições estabelecidas no PL 2.338/23 para o exercício desse direito (“efeitos jurídicos relevantes” e que “impactem de maneira significativa os interesses das pessoas”) e a desnecessidade dessas condições para o exercício do direito na LGPD.

As definições de risco no espectro da IA também têm conexão direta com os dados pessoais, especialmente os sensíveis, uma vez que seu tratamento pode aumentar o risco em sistemas de IA. Portanto, a conformidade de um agente de tratamento que utiliza sistemas de IA com a LGPD é um fator necessário para mitigar riscos e demonstrar *accountability*. A classificação de risco

no tratamento de dados pessoais, como o "alto risco" previsto pela Resolução CD/ANPD 02[22] e as futuras definições, conforme previsto no item "8" da agenda regulatória da ANPD para o biênio 23-24[23], devem servir de referência para a compreensão da quantificação dos riscos relacionados aos sistemas de IA, facilitando seu entendimento e observância pelos agentes regulados.

Já no contexto da inovação, a análise preliminar da ANPD destaca a preocupação contemporânea dos reguladores em conciliar o fomento à inovação com a proteção de direitos fundamentais, e vê a União Europeia como um exemplo notável nesse esforço. O estudo da autoridade ressalta a importância de aplicar uma abordagem sistêmica semelhante no Brasil, especialmente no contexto do PL n. 2.338/2023. Nesse aspecto, a autoridade enxerga como acertada a inclusão de uma seção específica no projeto sobre *sandboxes regulatórios*, destacando a necessidade de equilibrar regras e fomentar inovações responsáveis. A análise preliminar da ANPD sugere que o PL n. 2.338/2023 siga a abordagem europeia, por exemplo, a estratégia do Mercado Único Digital de 2015[24], dando destaque à proteção de dados nos *sandboxes* de IA e atribuindo um papel central à ANPD nessas iniciativas, semelhante ao papel das Autoridades de Proteção de Dados (*Data Protection Authorities* - DPAs) na UE.

Além disso, existe uma conexão entre os mecanismos de governança da regulamentação de ambas as áreas. Enquanto o PL n. 2.338/23 prevê o programa de governança por meio de códigos de boas práticas e governança dos agentes de IA (artigo 30), a LGPD também aborda a formulação de regras de boas práticas e governança (artigo 50).

Portanto, esses pontos de contato mostram a importância de se utilizar, sempre que possível, da experiência e das práticas já existentes no mercado para a regulação da IA, aproveitando e adaptando aquilo que já é conhecido e manuseado pelos agentes regulados em outros campos, como a proteção de dados. A experiência adquirida na LGPD pode contribuir para tornar a regulamentação da IA menos turbulenta e mais efetiva, garantindo a segurança jurídica e a previsibilidade.

22. ANPD. *RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022*. 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: 23 jul. 2023.

23. ANPD. *PORTARIA ANPD Nº 35, DE 4 DE NOVEMBRO DE 2022*. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 23 jul. 2023.

24. "Estratégia fundada em pilares como acesso, segurança, proteção de dados, crescimento da economia digital e transparência das plataformas, a estratégia passou a abarcar iniciativas legislativas paradigmáticas, como, por exemplo, o Regulamento Geral de Proteção de Dados (2016)13, a Diretiva sobre Direitos Autorais e Direitos Conexos (2019)14, a Lei dos Serviços Digitais (2022)15, a Lei dos Mercados Digitais (2022)16, e, mais recentemente, a proposta de Regulamento Geral da Inteligência Artificial (AI Act) 17, que ainda está em discussão no Parlamento europeu". ANPD. *Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial*. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 23 jul. 2023.

Uma outra relevante interação entre o PL e a LGPD é a previsão de mecanismos de governança, como o Relatório de Impacto à Proteção de Dados e a Avaliação de Impacto Algorítmico, que auxiliam na promoção da conformidade com os regimes de proteção de dados e com as determinações da proposta de marco legal de IA.

Quanto ao agente regulador responsável, em publicações sobre o tema a ANPD defendeu sua posição como autoridade-chave para a regulamentação da IA no Brasil. A ANPD argumentou que a criação de um novo órgão ou a atribuição de competências a outra entidade poderiam resultar em fragmentação regulatória e sobreposição de competências.

Nesse contexto, a ANPD destaca sua posição em relação à regulação da IA e sua competência na proteção dos direitos dos titulares de dados. A autoridade afirma que a regulação da IA deve estar em harmonia com a LGPD e apresentou recomendações práticas para garantir a governança da IA e a proteção de dados pessoais, por exemplo, com sua proposta de modelo institucional e pela defesa de sandboxes regulatórios para IA[25].

O texto da Nota Técnica supramencionada da ANPD propõe um modelo institucional para a regulamentação da inteligência artificial no Brasil, estruturado em quatro instâncias. A ANPD seria designada como a autoridade competente, atuando como órgão regulador central para interpretar a lei decorrente do PL nº 2.338/2023. Nesse sentido, a autoridade teria a responsabilidade de supervisionar e fiscalizar a implementação de tal lei, proteger os direitos fundamentais relacionados e afetados pela IA, promover boas práticas e cooperar com outras autoridades. A Nota destaca, ainda, a necessidade de fortalecimento institucional da ANPD, garantindo sua independência técnica, decisória e administrativa. Além disso, propõe a criação de um "Fórum de Órgãos Reguladores Setoriais" para a coordenação entre o órgão central e os reguladores setoriais, e sugere a formação de um Conselho Consultivo para garantir a participação da sociedade nas decisões relacionadas à IA.

Na proposta da Nota Técnica, o Poder Executivo, representado por órgãos como Ministério da Ciência, Tecnologia e Inovação, teria um papel crucial na

25. Sandboxes regulatórios são ambientes regulatórios experimentais, que contam com reguladores e organizações que desenvolvem novas tecnologias e processos para testar as inovações em relação à estrutura regulatória. DATASPHERE INITIATIVE. Sandboxes for data: creating spaces for agile solutions across borders. Disponível em: https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf. Acesso em: 03 dez. 2023.
Cumpre mencionar também que a ANPD publicou, em 03 de outubro de 2023, consulta à sociedade sobre o seu programa piloto de sandbox regulatório de IA, subsidiado pelo estudo técnico "Sandbox regulatório de inteligência artificial e proteção de dados no Brasil" disponível em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/sandbox_regulatorio___estudo_tecnico__versao_publica_.pdf>.

formulação de políticas públicas relacionadas à IA, enquanto os Órgãos Reguladores Setoriais manteriam suas competências específicas. Esse modelo busca uma abordagem abrangente e coordenada para a regulamentação da IA no Brasil, buscando alinhar-se às diretrizes estabelecidas na LGPD e no Projeto de Lei n. 2.338/2023. Há ainda a proposta de criação de um Conselho Consultivo, o qual asseguraria a participação de diversos setores da sociedade nas decisões relacionadas à IA.

Portanto, o estado da arte requer atenção à importância de conciliar a regulação da IA com a proteção de direitos fundamentais, por conseguinte, com a LGPD, reforçando o papel da ANPD como autoridade-chave para proteger os direitos dos titulares de dados e promover a inovação responsável no contexto da inteligência artificial.

Dessa forma, é fundamental que a regulação da IA seja bem articulada com a LGPD, considerando a proteção dos direitos dos cidadãos, a segurança jurídica e a convergência regulatória. A proposta de modelo institucional da ANPD a respeito do PL n. 2.338/2023 desempenharia um papel importante nesse cenário, garantindo que as normas estabelecidas sejam efetivamente aplicadas pelos reguladores e cumpridas pelos agentes regulados. A busca por soluções equilibradas, que promovam a inovação responsável e a proteção dos direitos fundamentais, é essencial para o avanço seguro e ético da IA no Brasil.

Considerações finais

O presente artigo teve como propósito realizar uma análise comparativa entre a Lei Geral de Proteção de Dados e o Projeto de Lei 2.338/2023, com foco na responsabilização e prestação de contas (*accountability*) no contexto da Inteligência Artificial e proteção de dados pessoais. A convergência entre essas áreas torna-se inescapável, dado o crescente uso de dados - pessoais e não pessoais - nos sistemas de IA, essenciais para seu funcionamento e aprimoramento contínuo. Depreende-se, portanto, que compreender as intersecções e relações entre a LGPD e o PL n. 2.338/2023 é crucial para garantir uma regulação coesa e eficaz, assegurando a proteção dos direitos fundamentais dos indivíduos e o desenvolvimento responsável da IA no Brasil.

A utilização da IA representa um avanço tecnológico significativo, mas também impõe desafios à proteção de dados pessoais e à privacidade dos indivíduos. Sendo assim, a evolução tecnológica demanda a mesma evolução e sofisticação legislativa, desencadeando em novas formas de se conter ou

controlar resultados, comportamentos ou virtudes. Nesse sentido, a *accountability* surge como uma importante ferramenta para assegurar que os agentes de tratamento de dados sejam responsáveis pelo uso adequado e seguro das informações.

A LGPD e o PL n. 2.338/2023, embora apresentem abordagens distintas, têm em comum o objetivo de garantir a proteção dos direitos dos titulares de dados e a promoção de uma cultura de responsabilidade, para além da meramente indenizatória, no tratamento de informações. A análise comparativa desses marcos regulatórios permite identificar suas complementaridades e desafios, contribuindo para a evolução e aprimoramento do arcabouço legal relacionado à inteligência artificial e à proteção de dados.

Por fim, é importante destacar que a regulação da IA é uma tarefa complexa e em constante evolução, e a interação entre a LGPD e o PL 2.338/2023 é apenas um dos aspectos relevantes desse desafio. É fundamental que a sociedade, os especialistas, as autoridades reguladoras e os legisladores trabalhem em conjunto para garantir uma abordagem ética, responsável e eficaz no uso da IA, protegendo os direitos fundamentais dos indivíduos e promovendo o avanço tecnológico em benefício de toda a sociedade brasileira.

Referências

ALHADEFF, Joseph; van ALSENOY, Brendan; DUMORTIER, Jos. *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*. 2011. In: GUAGNIN; Hempel; ILTEN (org.). ***Managing Privacy through Accountability***. Londres: Palgrave Macmillan, 2012. p. 49-82. Disponível em: https://ssrn.com/abstract=1933731. Acesso em: 27 nov. 2023.

ANPD. A*nálise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. 2023*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 23 jul. 2023.

ANPD. *Nota Técnica nº 16/2023/CGTP/ANPD*. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf. Acesso em: 17 ou. 2023.

ANPD. *PORTARIA ANPD Nº 35, DE 4 DE NOVEMBRO DE 2022*. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 23 jul. 2023.

ANPD. *RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022*. 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: 23 jul. 2023.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2010 on the principle of accountability*. 2010. 00062/10/EN WP 173. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 27 nov. 2023.

BIONI, Bruno. *Accountability na qualidade de um conceito relacional e de modulação do poder*. 2022. Disponível em: https://blog.grupogen.com.br/juridico/postagens/artigos/accountability-conceito-relacional/. Acesso em: 23 jul. 2023.

BIONI, Bruno; LUCIANO, Maria. *O PRINCÍPIO DA PRECAUÇÃO NA REGULAÇÃO DE INTELIGÊNCIA ARTIFICIAL*: seriam as leis de proteção de dados o seu portal de entrada? 2019. Disponível em: https://brunobioni.com.br/home/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: 23 jul. 2023.

BRASIL. *Anteprojeto de Lei para a Proteção de Dados Pessoais de 2010*. Disponível em: http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/. Acesso em: 23 jul. 2023.

BRASIL. *Lei n. 12.965 de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 jul. 2023.

BRASIL. *Lei n. 13.709 de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 jul. 2023.

BRASIL. *Projeto de Lei n. 2.338 de 2023*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1689259290825&disposition=inline&_gl=1*92d8lo*_ga*MTQ4NzE0NzgwLjE2ODMxM.jc2MjA.*_ga_CW3ZH25XMK*MTY5MDQyNTUzMC4xMC4wLjE2OTA0MjU1MzAuMC4wLjA. Acesso em: 23 de jul. 2023.

BRASIL. *Projeto de Lei n. 4.060 de 2012*. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1630450891439&disposition=inline&_gl=1*g4277e*_ga*MTQ4NzE0NzgwLjE2ODMxMjc2MjA.*_ga_CW3ZH25XMK*MTY5MDQyMTE0Ni45LjEuMTY5MDQyMTQyMy4wLjAuMA. Acesso em: 23 jul. 2023

DATASPHERE INITIATIVE. *Sandboxes for data: creating spaces for agile solutions across borders*.

Disponível em: https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf. Acesso em: 03 dez. 2023.

FERRÃO DOS SANTOS, C. .; GOMES DA SILVA, J.; PADRÃO, V. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. *Revista Eletrônica da PGE-RJ*, [S. l.], v. 4, n. 3, 2021. DOI: 10.46818/pge.v4i3.256. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 27 jul. 2023.

FRAZÃO, Ana; CUEVA, Ricardo. 32. *Accountability e Mitigação da Responsabilidade Civil na Lei Geral de Proteção de Dados*. In: FRAZÃO, Ana; CUEVA, Ricardo. Compliance e Políticas de Proteção de Dados. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/32-accountability-e-mitigacao-da-responsabilidade-civil-na-lei-geral-de-protecao-de-dados-pessoais-compliance-e-politicas-de-protecao-de-dados/1506551422. Acesso em: 23 jul. 2023.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. 2023. OECD Legal Instruments. Disponível em: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf. Acesso em: 27 nov. 2023.

OXFORD LEARNER'S DICTIONARY OF ACADEMIC ENGLISH. *Accountability noun*. Disponível em: https://www.oxfordlearnersdictionaries.com/definition/academic/accountability. Acesso em: 23 jul. 2023.

PARLAMENTO EUROPEU. *Artificial Intelligence Act (AI Act)*. 2023. 2021/0106(COD). Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html. Acesso em: 27 nov. 2023.

RACHED, Danielle Hanna. The Concept(s) of Accountability: form in search of substance. *Leiden Journal Of International Law*, [S.L.], v. 29, n. 2, p. 317-342, 29 abr. 2016. Cambridge University Press (CUP). http://dx.doi.org/10.1017/s0922156516000042. Disponível em: https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/abs/concepts-of-accountability-form-in-search-of-substance/8E481D883DC5B5E9752C3CCA9BE39884. Acesso em: 23 jul. 2023.

ROSENVALD, Nelson. *Conceitos de responsabilidade civil para 4ª revolução industrial e o capitalismo de vigilância*. In: EHRHARDT JÚNIOR, Marcos (coord.). Direito civil: futuros possíveis. Fórum, 2021.

ROSENVALD, Nelson. *A polissemia da responsabilidade civil na LGPD*. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/336002/a-polissemia-da-responsabilidade-civil-na-lgpd. Acesso em: 23 jul. 2023.

TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. RESPONSABILIDADE CIVIL E REGULAÇÃO DE NOVAS TECNOLOGIAS: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *Rei - Revista Estudos Institucionais*, [S.L.], v. 6, n. 1, p. 301-333, 25 abr. 2020. Revista Estudos Institucionais. http://dx.doi.org/10.21783/rei.v6i1.383. Disponível em: https://doi.org/10.21783/rei.v6i1.383. Acesso em: 23 jul. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

Inteligência artificial e a proteção dos dados pessoais no recrutamento de trabalhadores: desafios e perspectivas

BRUNO BLUM FONSECA

BRUNO BLUM FONSECA[1]

Introdução

As diversas etapas que envolvem a busca, triagem e seleção de candidatos a vagas de trabalho demandam consideráveis recursos e tempo das organizações. Por isso, o recrutamento de recursos humanos foi um dos primeiros campos da sociedade civil a adotar sistemas de Inteligência Artificial ("IA") para torná-lo mais eficiente. Com o crescimento da popularidade da IA, impulsionado pelo advento de inteligências artificiais generativas como o Chat GPT no final de 2022, a tendência é a adoção ainda mais intensa dessa tecnologia nos próximos anos.

A Inteligência Artificial, principalmente quando na forma do chamado "aprendizado de máquina", é uma tecnologia com características técnicas especialmente desafiadoras, como a sua notória aptidão a produzir resultados enviesados e discriminatórios, além da condição muitas vezes "opaca" – isto é, sem transparência – do funcionamento desses sistemas. Isso coloca o candidato em uma condição particularmente vulnerável diante do risco de ter seu direito de acesso ao trabalho negado por um sistema computacional obscuro e potencialmente enviesado, sem poder compreender ou contestar a decisão automatizada.

O direito brasileiro, principalmente após a entrada em vigor da Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD"), reconhece direitos e apresenta mecanismos aptos a proteger os titulares de dados pessoais, inclusive em face de decisões automatizadas no recrutamento. Tal regime protetivo impõe uma série de obrigações às organizações públicas e privadas. Contudo, a lei não foi elaborada visando os atuais sistemas de Inteligência Artificial.

1. Advogado atuante na área de Direito Digital e Propriedade Intelectual, com foco em consultivo de tecnologia, mídia e entretenimento, apoiando empresas brasileiras e estrangeiras na implementação de novas tecnologias e modelos de negócio digital. Bacharel em Direito pela Universidade de São Paulo. Pós-graduando em Direito Digital pela Universidade do Estado do Rio de Janeiro em parceria com o Instituto de Tecnologia e Sociedade do Rio. Instrutor na Opice Blum Academy. Possui certificado EXIN Privacy and Data Protection Essentials based on LGPD. Membro da equipe da Universidade de São Paulo na 4ª Edição da Helsinki Information Moot Court Competition, na qual a equipe conquistou o prêmio de melhor memorial escrito e o segundo lugar geral.

Assim, é importante compreender como as particularidades dos sistemas de IA podem afetar a conformidade das organizações com as normas e obrigações legais que garantem o cumprimento dos direitos fundamentais dos candidatos, como o direito à proteção de dados pessoais, para que se possa pensar em medidas a serem adotadas.

Trata-se de um tema atual e relevante[2], principalmente considerando que os riscos jurídicos impostos por esses sistemas muitas vezes não são considerados adequadamente pelas organizações antes de implementá-los, colocando em xeque os direitos dos candidatos.

Este artigo analisará a legislação e a bibliografia pertinentes com o objetivo de mapear, primeiramente, os direitos dos candidatos. Em seguida, será analisado como o uso da IA pode afetar tais direitos, principalmente diante de quatro[3] pontos de atenção centrais quanto ao uso dessa tecnologia: (i) inferências e violações à proteção dos dados pessoais; (ii) discriminação e vieses; (iii) opacidade e baixa transparência; e (iv) questões éticas.

Será adotada a revisão bibliográfica e o método dedutivo de argumentação como metodologia. Pretende-se alcançar um panorama abrangente dos desafios jurídicos no uso da IA no recrutamento, considerando a legislação atual. Com isso, o objetivo é identificar caminhos e lacunas presentes na proteção dos direitos dos candidatos.

1. Inteligência Artificial e recrutamento

O uso de IA no recrutamento consiste no acoplamento de tecnologias de IA[4] a uma ou mais etapas da seleção de candidatos. Essas tecnologias incluem desde sistemas de reconhecimento de voz ou facial até sistemas mais complexos de aprendizado de máquina.

2. A importância do tema também é evidenciada pelo debate em curso no Congresso Nacional a respeito do Projeto de Lei nº 2338 de 2023, que versa sobre o uso da inteligência artificial. O projeto aborda expressamente a questão do uso de IAs para fins de recrutamento de candidatos, classificando tal uso como sendo de "alto risco", conforme o Art. 17 do texto inicial do PL.

3. Há quem proponha a existência de três riscos principais no uso de IAs em geral: "(i) de data sets viciados; (ii) da opacidade na sua forma de atuação, consequência das técnicas de *machine* e *deep learning*; (iii) da possibilidade de promoverem a discriminação ainda que bem estruturados". Optou-se por propor aqui quatro riscos, adicionando as "questões éticas" impostas pelo uso da IA, as quais são amplamente estudadas na atualidade. As questões éticas interagem diretamente com as questões jurídicas e devem ser consideradas para uma visão mais completa do cenário regulatório. Cf. FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. Arbitrium *ex machina*: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. Revista dos Tribunais, vol. 995, p. 635-655, set., 2018. p. 637.

4. Para os fins deste artigo, "Inteligência Artificial" é definida como qualquer sistema computacional capaz de interpretar dados externos e aprender com eles, usando esse aprendizado para atingir fins específicos.

De acordo com levantamento de 2021, 32% das empresas brasileiras utilizam tecnologias de Inteligência Artificial para realizar tarefas relacionadas à gestão de recursos humanos ou recrutamento.[5] A tendência é de aumento. Uma pesquisa de 2022 identificou que 55% das empresas aumentaram seus investimentos em automação do recrutamento.[6]

Dentre as etapas do recrutamento em que se adota IA, destaca-se: (i) elaborar comunicações personalizadas para captar talentos; (ii) examinar e classificar currículos; (iii) analisar entrevistas em vídeo através de reconhecimento facial; (iv) analisar respostas de candidatos para identificar traços de personalidade e competências; (v) confeccionar testes e jogos para testar habilidades dos candidatos; e (vi) facilitar o agendamento de atividades.[7]

A maioria dos sistemas de IA usados atualmente são variações do aprendizado de máquina, método através do qual os computadores adquirem a habilidade de aprender sem receber uma programação prévia explícita. Partindo apenas de um treinamento prévio realizado com dados rotulados (aprendizado supervisionado) ou dados brutos (aprendizado não supervisionado), o sistema é capaz de encontrar, por conta própria, padrões em meio à massa de dados fornecida e reconhecer padrões nos novos dados eventualmente apresentados.[8]

Essa tecnologia, associada ao *Big Data*[9], permite a computação de uma enorme quantidade de dados, resultando na extração de conclusões e inferências que não poderiam ser feitas por humanos. Diante disso, é evidente a razão do interesse das empresas em usar essa tecnologia no recrutamento, principalmente em processos envolvendo milhares de candidatos.

Geralmente, associa-se ao uso de Inteligência Artificial no recrutamento uma maior eficiência para identificar e resumir informações relevantes, supe-

5. Cf. Estudo "TIC Empresas 2021" (CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.BR). Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas Empresas Brasileiras - TIC Empresas 2021. São Paulo: Cetic.Br, 2021. p. 80).

6. Cf. Estudo patrocinado pela empresa "Predictive Hire", especializada no setor de recrutamento automatizado (LAURANO, Madeline. Automation with Humanity: putting the candidate first. Aptitude Research, patrocinado por Predictive Hire. 2022. p. 3).

7. Lista de exemplos de uso da IA no recrutamento extraída de: HUNKENSCHROER, A.L., KRIEBITZ, A. Is AI recruiting (un) ethical? A human rights perspective on the use of AI for hiring. AI Ethics 3, p. 199–213 (2023). p. 200.

8. Para mais detalhes e explicações técnicas sobre algoritmos, IA, aprendizado de máquina e Big Data, ver primeiro capítulo de: MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação Algorítmica à Luz da Lei Geral de Proteção de Dados. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 421-446. Ver também: FERRARI; BECKER; WOLKART, op. cit., p. 635-655.

9. Big Data é um termo que se refere a grandes conjuntos de dados, tanto estruturados quanto não estruturados, que são coletados, armazenados e analisados por meio de tecnologias avançadas. Esses dados são caracterizados por sua enorme quantidade, diversidade e velocidade, desafiando as abordagens tradicionais de análise. Sua importância reside na capacidade de extrair *insights* valiosos, identificar padrões e tomar decisões informadas.

rior à capacidade humana. Além disso, a tecnologia promete trazer mais objetividade, racionalidade e imparcialidade ao processo seletivo, podendo inclusive reduzir os vieses presentes nos processos conduzidos por recrutadores humanos. No entanto, diversos estudos na última década vêm desconstruindo o "mito sobre a objetividade, neutralidade, racionalidade e imparcialidade dos algoritmos"[10].

Isso ocorre porque a IA, por mais que tente emular o raciocínio humano ou tente ser estritamente racional, em última análise sempre se baseia em uma lógica matemática[11], programada por uma pessoa ou grupo para atingir determinados fins. Muitas vezes, o verniz de tecnicidade pura da IA oculta intervenções eminentemente sociais e políticas que moldam os algoritmos[12]. Ainda, esses sistemas têm a capacidade de realizar, por conta própria, novas correlações inesperadas e sem ancoragem em uma lógica causal explicável[13].

Além disso, o raciocínio baseado em padrões estatísticos dificulta a extração de uma explicação sobre como a IA chegou a um determinado resultado, tornando sua compreensão desafiadora até mesmo para especialistas. Embora as operações matemáticas que levaram ao resultado sejam visíveis, a cognição do raciocínio empregado é tão desafiadora, em termos humanos, que equivale a uma invisibilidade prática. Essa elevada abstração e adaptabilidade das IAs levou ao que se convencionou chamar de caráter "opaco" ou "*black box*" (caixa preta).

No meio de todas essas questões está o candidato. Os departamentos de recursos humanos, atraídos pela promessa de eficiência, muitas vezes adotam esses sistemas sem abordar adequadamente os desafios subjacentes, colocando em risco direitos do candidato, como o direito fundamental à proteção de dados pessoais e o direito social ao trabalho.

10. MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência artificial e a lei de proteção de dados pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (Coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. p. 265-290.

11. ABRUSIO, Juliana; ARAUJO, André Eduardo Dorster. Inteligência artificial: decisões automatizadas e discriminação nas relações de trabalho. Revista de Direito do Trabalho e Seguridade Social. vol. 223. ano 48. p. 321-343. São Paulo: Ed. RT, mai./jun. 2022.

12. CRAWFORD, Kate. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven and London: Yale University Press, 2021.

13. AFFONSO SOUZA, Carlos; PERRONE, Christian; MAGRANI, Eduardo. O Direito à Explicação entre a Experiência Europeia e a sua Positivação na LGPD. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 243-270.

2. Normas aplicáveis e direitos dos candidatos

Um dos valores centrais da ordem jurídica internacional é a igualdade em dignidade e direitos entre os seres humanos.[14] Além disso, essa ordem garante o exercício dos direitos "sem discriminação alguma", a igualdade de gozo dos direitos entre homens e mulheres e o direito de todas as pessoas a condições de trabalho justas e favoráveis.[15] A igualdade também é respaldada por convenções sobre discriminação racial e direitos das pessoas com deficiência.[16]

No âmbito trabalhista, destacam-se a Convenção 100 e a Convenção 111 da Organização Internacional do Trabalho (OIT), que tratam, respectivamente, da "Igualdade de Remuneração entre Homens e Mulheres" e da "Discriminação em Matéria de Emprego e Ocupação". Essa última define "discriminação" para fins de emprego como:

> a) toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão;
> b) qualquer outra distinção, exclusão ou preferência que tenha por efeito destruir ou alterar a igualdade de oportunidades ou tratamento em matéria de emprego ou profissão [...].[17]

No direito brasileiro, a Constituição da República se fundamenta na dignidade da pessoa humana e no valor social do trabalho (Art. 1º, III e IV), e tem como objetivo fundamental promover o bem de todos sem qualquer forma de discriminação (Art. 3º). A Constituição também garante a proteção do mercado de trabalho da mulher e proíbe a diferença de salários e critérios de admissão por motivo de sexo, idade, cor, estado civil ou porte de deficiência (Art. 7º, XX, XXX e XXXI).

A Consolidação das Leis do Trabalho (Decreto-Lei nº 5.452/1943) proíbe a recusa de emprego em razão de sexo, idade, cor, situação familiar ou estado

14. Cf. disposto logo no Artigo 1 da Declaração Universal dos Direitos Humanos, proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948: "Artigo 1 Todos os seres humanos nascem livres e iguais em dignidade e direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade."

15. Cf. Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, artigos 2º, 3º e 7º, respectivamente.

16. Merece destaque a Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial de 1968, que apresenta o conceito de "discriminação racial" e condena a sua prática, bem como a Convenção sobre os Direitos das Pessoas com Deficiência de 2007, que garante, em seu Artigo 5, a igualdade e a não-discriminação com base na deficiência.

17. Cf. Art. 1 — 1 da Convenção 111 da OIT sobre Discriminação em Matéria de Emprego e Ocupação.

de gravidez, salvo quando a natureza da atividade seja notória e publicamente incompatível (Art. 373-A, II). A Lei nº 9.029/1995 proíbe "a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção".[18]

Por sua vez, a LGPD, promulgada em 2018, complementa o regime protetivo antidiscriminação. O princípio da não-discriminação[19] determina a impossibilidade de realizar tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.[20]

Logo, há uma robusta ordem jurídica protegendo os candidatos contra qualquer forma de discriminação. A distinção entre candidatos é possível desde que devidamente justificada, como quando a função for notoriamente incompatível ou para promover ações afirmativas.

Os processos de recrutamento e seleção envolvem diversos dados pessoais dos candidatos. Assim, além de reforçar o arcabouço jurídico antidiscriminação, a LGPD disciplina de forma prática como as organizações devem tratar os dados pessoais dos candidatos a fim de evitar injustiças e violações da privacidade.

A entidade recrutadora geralmente será a controladora dos dados pessoais tratados no âmbito do recrutamento, sendo responsável por garantir e comprovar a adequação à lei.[21] Já os desenvolvedores ou fornecedores dos sistemas de IA tendem a ser operadores, focando em aspectos técnicos.[22]

A lei garante transparência sobre o tratamento, com informações claras e precisas, bem como a adoção de medidas eficazes pelos agentes de tratamento para cumprir as normas de proteção de dados.[23] Assim, ao utilizar Inteligência Artificial no recrutamento, é essencial garantir a devida transparência aos candidatos sobre o seu uso. As empresas de recrutamento e as Inteligências Artificiais escolhidas para participar do processo devem ser claramente

18. Além disso, é tipificado como crime "negar ou obstar emprego em empresa privada" devido a preconceito de raça, cor, etnia, religião ou procedência nacional (Art. 4º da Lei nº 7.716/89).

19. Cf. LGPD, Art. 6º, inciso IX.

20. Para uma explicação detalhada dos elementos "ilícito" e "não abusivo" presentes no conceito do princípio da não discriminação, ver MENDES; MATTIUZZO; FUJIMOTO, op. cit.

21. SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da Proteção de Dados nas Relações de Trabalho. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 509.

22. Uma vez que muitas empresas de tecnologia são estrangeiras e utilizam contratos de adesão para seus serviços, sem possibilidade de negociação, os recrutadores devem estar especialmente atentos aos riscos regulatórios desse tipo de contratação. Eles devem adotar medidas mitigatórias ou até mesmo optar por não contratar, dependendo de como a empresa lida com os dados pessoais ou de como funciona determinado sistema.

23. Cf. LGPD, Art. 6º, incisos VI, VII, VIII e X. Princípios da transparência, segurança, prevenção e responsabilização, respectivamente.

apresentadas, e deve ser esclarecido quais dados serão utilizados, como serão utilizados, e para qual finalidade[24].[25] Dessa forma, o candidato deve ser informado de maneira clara sobre o grau de participação de sistemas de IA no processo, antes da candidatura, ou em momento oportuno antes do início do tratamento.

Além disso, o tratamento deve estar respaldado por uma base legal, e o tratamento de dados pessoais sensíveis é revestido de mais garantias para proteger grupos historicamente perseguidos ou discriminados.[26] Ademais, deve-se respeitar os princípios da adequação e da necessidade[27], buscando-se minimizar[28] a coleta e o uso de dados.

A qualidade dos dados inseridos nos sistemas também é de suma importância. Frank Pasquale destaca que, como os algoritmos são guiados por dados, a qualidade de um algoritmo depende da qualidade dos dados que o informam. Em face disso, Pasquale defende uma governança de dados focada nos algoritmos, para (i) garantir que os dados de treinamento reflitam adequadamente a realidade e os objetivos pretendidos, e (ii) detectar e corrigir eventuais anomalias antes que causem grandes danos.[29]

Por sua vez, o Artigo 20 da LGPD se destaca por conferir ao titular o direito de solicitar a revisão de decisões "tomadas unicamente com base em tratamento automatizado[30] de dados pessoais que afetem seus interesses", incluindo decisões destinadas a definir seu "perfil profissional". Além disso, o controlador deve "fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial" (§1º). Caso as informações solicitadas não sejam fornecidas com base na proteção ao segredo comercial e industrial, o §2º prevê que a Autoridade Nacional de Proteção de Dados (ANPD) poderá realizar uma auditoria para verificar possíveis aspectos discriminatórios.

24. Art. 9º da LGPD especifica informações que sempre devem ser apresentadas ao titular.

25. SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira, op. cit., p. 510.

26. O Art. 5º, inciso II, da LGPD apresenta o rol de dados pessoais considerados sensíveis.

27. Cf. LGPD, Art. 6º, incisos II e III.

28. A minimização de dados pessoais refere-se à prática de limitar a coleta, o uso e a retenção de dados pessoais apenas ao que é necessário para uma finalidade específica, reduzindo o risco de violações.

29. PASQUALE, Frank. Data-Informed Duties in AI Development. 119 Columbia Law Review 1917, University of Maryland Legal Studies Research Paper, No. 14, 2019. p. 1928

30. A Diretiva das Decisões Automatizadas do Canadá, de 1º de abril de 2019, traz definição do que seria uma "decisão automatizada", o que não foi feito pela LGPD: "Qualquer tecnologia que auxilie ou substitua o julgamento de tomadores de decisão humanos."

Assim, a LGPD concedeu ao titular dos dados dois importantes direitos diante de uma decisão automatizada: o direito à explicação e o direito à revisão.[31] O direito à explicação decorre do princípio da transparência e do direito de acesso à informação. Além disso, é "um pressuposto para o exercício de outros direitos e, particularmente, do direito a requerer revisão de decisões automatizadas"[32]. Sem o direito à explicação, o titular não conseguiria obter e assimilar as informações necessárias para identificar possíveis erros e exercer o direito à revisão.[33]

A doutrina especializada debate a respeito da natureza exata do direito à explicação.[34] Alguns argumentam que este direito abrange explicações prévias a respeito do funcionamento geral do sistema automatizado, enquanto outros defendem que ele deve entrar em detalhes sobre uma decisão específica.[35]

Independentemente do resultado desse debate, é evidente que a explicação deve ser suficiente para que o titular possa exercer seus direitos, não sendo obrigatório entrar em detalhes técnicos.[36] A adequação da explicação deve ser avaliada casuisticamente, conforme a sua utilidade concreta para o titular, podendo ora ser necessário informações mais técnicas, ora ser mais adequado oferecer informações gerais.[37]

Quanto ao momento em que a explicação deve ser fornecida, a LGPD não especifica um prazo, permitindo que o titular solicite a qualquer momento. No entanto, é importante lembrar que o princípio da transparência exige que o controlador seja proativo ao fornecer informações relevantes.

31. Para Renato Leite: "O [...] direito à explicação diz respeito ao direito de receber informações suficientes e inteligíveis que permita ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais. Já o [...] *direito à revisão* [...] compreende o direito do titular de requisitar a revisão [...] de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses [...]" (grifo nosso). Cf.: LEITE, Renato. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. Artigo Estratégico 39. Rio de Janeiro: Instituto Igarapé, dez., 2018. p. 4.

32. AFFONSO SOUZA; PERRONE; MAGRANI, op. cit., p. 262.

33. Existe uma grande discussão no âmbito europeu sobre a existência de um direito à explicação e qual seria a sua natureza, enquanto o §1º do Art. 20 da LGPD parece não deixar dúvidas quanto à sua existência no Brasil.

34. LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: O Direito à Explicação nas Decisões Automatizadas. Revista Brasileira de Direito Civil - RBDCivil, Belo Horizonte, v. 26, p. 227-246, out./dez., 2020.

35. A súmula 550 do STJ diz respeito ao escore de crédito e reconhece o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. No entanto, ainda não está claro se essas informações são gerais e prévias ou específicas e fornecidas após a decisão.

36. AFFONSO SOUZA; PERRONE; MAGRANI, op. cit., p. 263.

37. MULHOLLAND; FRAJHOF, op. cit., p. 278.

Já sobre o direito à revisão, é importante compreender que uma revisão efetiva deve permitir a obtenção de conclusões diferentes da decisão original, independentemente de ser realizada por um humano ou por outra máquina[38].[39]

É importante destacar, contudo, que os direitos de revisão e explicação só se aplicam às "decisões tomadas unicamente com base em tratamento automatizado", nos termos do caput do Artigo 20 da LGPD. Como nos processos de recrutamento é comum que a automação represente apenas uma parte do processo decisório, há quem defenda a não incidência do Artigo 20.

No entanto, este artigo não deve ser interpretado literalmente. Deve-se considerar a complexa realidade dos processos decisórios.[40] Se uma parte da decisão foi automatizada, aplica-se o Art. 20 a essa parte. Por exemplo, quando um sistema de IA é usado para filtrar currículos e, em seguida, um humano analisa os currículos do topo do ranking, caso a interferência humana não seja capaz de alterar o resultado da filtragem, os direitos dos candidatos excluídos são diretamente afetados pela automação, e o Art. 20 deve ser aplicado.[41]

Embora represente um avanço importante, a disciplina apresentada pela LGPD para decisões automatizadas é criticada por ser "tímida" e "ineficaz".[42] Essa ineficácia para enfrentar os desafios da automação fica ainda mais evidente diante das ferramentas de Inteligência Artificial, as quais apresentam características particularmente desafiadoras para os direitos dos candidatos. Portanto, além das obrigações impostas pela LGPD e outras normas, as organizações que adotarem IA no recrutamento deverão lidar com desafios especiais causados por esse tipo de sistema.

3. Desafios e perspectivas do uso de IA no recrutamento

3.1 Inferências e violação à proteção de dados pessoais

No âmbito da proteção de dados, o principal desafio decorre do fato de que os sistemas de IA são particularmente bons em fazer inferências e ge-

38. A expressão "pessoa natural" foi suprimida do Art. 20 da LGPD pela Lei nº 13.853/2019. Com isso, parte da doutrina defende a impossibilidade de revisão por pessoa natural, cabendo revisão apenas por outro mecanismo automatizado, enquanto outra parte defende que a revisão por pessoa natural é facultativa, embora seja mais adequada para corrigir eventuais discriminações (LIMA; SÁ, op. cit., p. 232).

39. AFFONSO SOUZA; PERRONE; MAGRANI, op. cit., p. 267.

40. LIMA; SÁ, op. cit., p. 235.

41. MULHOLLAND; FRAJHOF, op. cit., p. 273.

42. Cf. LIMA; SÁ, op. cit., p. 235, e MARTINS, Guilherme Magalhães; MUCELIN, Guilherme. Inteligência artificial, perfis e controle de fluxos informacionais: a falta de participação dos titulares, a opacidade dos sistemas decisórios automatizados e o regime de responsabilização. Revista de Direito do Consumidor. vol. 146. ano 32. p. 93-127. São Paulo: Ed. RT, mar./abr. 2023. p. 104.

rar dados "novos" sobre os candidatos, podendo formar perfis[43] profissionais completos. Por exemplo, algoritmos de reconhecimento facial e previsão podem prever quais candidatas têm maior probabilidade de engravidar ou revelar a sua orientação sexual.[44] Além disso, as empresas tendem a coletar dados excessivos sobre o candidato, os quais, quando misturados, podem gerar inferências invasivas à privacidade.

Essa capacidade de inferência entra em conflito com a privacidade e deve ser contida para evitar tratamentos ilícitos. Caso contrário, as IAs podem expandir a quantidade de informações associadas aos candidatos, invadindo sua vida social e até sua psicologia. Por isso, as IAs não devem ser usadas para revelar dados que o candidato não queria revelar ou não esperava que pudessem ser extraídos dele, salvo se forem dados estritamente relacionados a informações lícitas e relevantes ao trabalho, embora às vezes seja difícil fazer essa distinção.[45]

Nesse esforço, preocupa-se especialmente com a análise, por IAs, de dados disponibilizados publicamente a respeito do candidato, o chamado *background check*.[46] Deve-se atentar para a possível inexatidão ou inadequação dos dados públicos coletados, principalmente na internet.[47] Alimentar IAs com dados públicos potencialmente inexatos e excessivos eleva o risco de erros e violações da privacidade.

Na mesma linha, deve-se evitar o uso de dados pessoais sensíveis. O potencial discriminatório e abusivo dessas informações é historicamente mais elevado, devendo seu uso servir apenas para beneficiar os candidatos, como no caso de cotas raciais.[48] Devido à dificuldade de controlar as inferências e correlações realizadas pelos sistemas de IA, o mais seguro é aplicar cotas e outras distinções sensíveis "manualmente", por meio de humanos ou *softwa-*

43. Em termos gerais, a formação de um perfil consiste: "em dois processos complementares: a inferência de um conjunto de características de um indivíduo ou um grupo de indivíduos, ou seja, o processo de criação do perfil; e trata esse indivíduo ou grupo de indivíduos à luz dessas características encontradas, ou seja, o processo de aplicação do perfil. Colocado de outra forma, significa a coleta e o tratamento de dados sobre um indivíduo ou grupo de indivíduos, cujo objetivo é a avaliação de características ou de aspectos comportamentais, a fim de analisar ou prever determinados atributos, como capacidades cognitivas, interesses ou comportamentos presumíveis". (MARTINS; MUCELIN, op. cit., p. 102).

44. HUNKENSCHROER, A.L., KRIEBITZ, A, op. cit., p. 208.

45. Ibidem, p. 208.

46. Quanto a essa prática, o Tribunal Superior do Trabalho já reconheceu seu potencial abusivo (TST-RR-243000-58.2013.5.13.0023). O background check pode ser realizado somente para funções específicas que o justifiquem, como para cargos que exigem especial confiança.

47. PRACOWNIK, Sofia Mandelert; SALDANHA, Vitor Maimone. Ferramentas de *background check* dentro do universo dos dados pessoais e da inteligência artificial: preocupações necessárias. Revista de Direito e as Novas Tecnologias, vol. 16, jul./set., 2022.

48. SANKIEVICZ; PINHEIRO, op. cit., p. 511

res tradicionais, evitando que a IA use erroneamente esses dados para discriminar candidatos.

Caso a IA utilize dados sensíveis, o ônus de demonstrar a legalidade do tratamento recai sobre o controlador. Em caso de dúvida, será presumida a abusividade da prática. Ou seja, "quando dados sensíveis são utilizados como *inputs* de algoritmos, há uma presunção *iuris tantum* de abusividade, que, no entanto, pode ser afastada caso fique demonstrada a razoabilidade do tratamento"[49].

Entretanto, mesmo as IAs treinadas de maneira adequada podem acabar inferindo dados excessivos ou sensíveis, e pode ser muito difícil ou impossível identificar isso devido à sua opacidade. Portanto, embora se deva sempre buscar utilizar bases de dados adequadas e representativas, bem como adotar medidas para reduzir o risco de a máquina realizar inferências inesperadas, isso pode não ser suficiente diante da forma como esses sistemas funcionam.

3.2 Discriminação algorítmica

Os processos tradicionais de recrutamento não estão livres de preconceitos e discriminações.[50] Embora a Inteligência Artificial tenha o potencial de reduzir esses vieses, nos estágios atuais esses sistemas representam riscos talvez até mais intensos.

O caso envolvendo a IA de recrutamento da Amazon em 2014 é emblemático no contexto da "discriminação algorítmica"[51]. Apesar de não ter recebido informações sobre o gênero dos candidatos e jamais ter sido instruído a priorizar currículos de homens, o algoritmo passou a identificar e prejudicar candidaturas femininas a partir de certos elementos presentes no currículo, como o tipo de linguagem adotada. Treinado com currículos aprovados no passado, majoritariamente de homens brancos, o algoritmo ficou tendencioso contra mulheres e contra formas de discurso comumente associadas ao gênero feminino.[52]

49. MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy, op. cit, p. 439.

50. Especialistas em psicologia, como o Prêmio Nobel de Ciências Econômicas de 2002, Daniel Kahneman, identificaram há anos que os humanos padecem de diversos vieses inconscientes que afetam sua capacidade de tomar decisões racionais em determinados contextos, principalmente diante de decisões complexas.

51. É possível listar pelo menos quatro tipos de discriminação algorítmica: (i) discriminação por erro estatístico; (ii) discriminação pelo uso de dados sensíveis; (iii) discriminação por generalização injusta; e (iv) discriminação limitadora de direitos (Cf. MENDES; MATTIUZZO; FUJIMOTO, op. cit., p. 430). Os detalhes sobre cada tipo fogem do escopo deste artigo.

52. CRAWFORD, op. cit. p. 130.

Este sistema foi descontinuado, mas o problema de viés inerente ao funcionamento das IAs persiste. Isso ocorre porque o problema não advém apenas de sistemas de IA treinados ou programados erroneamente, mas da própria natureza desses sistemas. Toda IA tem como base classificações a respeito do mundo, feitas por alguém ou por um grupo, com base em determinada visão de mundo.[53] Portanto, a própria natureza da programação e do funcionamento das IAs é a causa da existência de vieses e discriminações.

Além disso, garantir a qualidade da base de dados de treinamento é algo cada vez mais desafiador, principalmente diante dos algoritmos de *Big Data*, treinados com milhões de dados, muitas vezes sem supervisão humana direta. Se a base de dados estiver impregnada por algum viés arbitrário, ainda que inconsciente, todas as decisões resultantes potencialmente trarão o mesmo viés.[54] Ainda, mesmo que os dados estejam livre de vieses *a priori* e contenham filtros que evitem inferências sensíveis, as milhões de correlações automáticas feitas pelo sistema ainda podem vir a ser discriminatórias diante da sua elevada capacidade de abstração e criação de correlações inesperadas.

Outra dificuldade decorre do fato de que os dados utilizados no treinamento da IA são sempre históricos, ou seja, representam o passado. Isso pode fazer com que os algoritmos sejam míopes em relação a paradigmas novos ou emergentes, ignorando ou retardando evoluções sociais e, portanto, reforçando visões de mundo anacrônicas. Embora seja possível argumentar que recrutadores humanos também estão sujeitos a esse tipo de viés histórico[55] é inegável que os algoritmos podem causar impactos mais intensos e institucionalizados devido à sua maior capacidade de padronizar decisões. Assim como recrutadores mais velhos são gradualmente substituídos por mais jovens, as IAs devem ser constantemente atualizadas com dados mais recentes para que possam refletir as visões e objetivos da sociedade atual.

Outra face da discriminação algorítmica pode resultar na perpetuação, através da tecnologia, de um certo "padrão de candidato", excluindo do mercado de trabalho, de forma quase definitiva, aqueles que estão "fora do padrão"[56]. Com isso, apenas candidatos alinhados com uma visão corporativa específica e que adotam, por exemplo, uma certa linguagem, terão acesso a determina-

53. Ibidem.
54. ABRUSIO; ARAÚJO, op. cit., p. 327.
55. HUNKENSCHROER; KRIEBITZ, op. cit., p. 204.
56. MENDES; MATTIUZZO; FUJIMOTO, op. cit., p. 426.

dos empregos, excluindo pessoas igualmente capacitadas, mas com diferentes culturas e formas de ser.

Ainda, como é comum que esses sistemas sejam concebidos em outros países e depois aplicados no Brasil, é possível que ocorram vieses oriundos das diferenças entre esses países e o Brasil. Dessa forma, o candidato brasileiro pode ser avaliado de forma inadequada, com base nos parâmetros pensados para o "candidato padrão" americano ou europeu, por exemplo.

Para mitigar os riscos de discriminação, é importante que as organizações conheçam os detalhes sobre o funcionamento do sistema, revisando periodicamente os resultados apresentados. Além disso, os recrutadores devem adotar mecanismos adicionais de controle de qualidade. Por exemplo, embora não exigido por lei, pode-se selecionar aleatoriamente candidatos que foram eliminados pela IA para que um humano os reavalie e, posteriormente, compare com o resultado anterior.[57]

3.3 Opacidade

Os sistemas de IA são notavelmente opacos devido à alta complexidade matemática e abstração dos modelos, tornando-os muitas vezes incompreensíveis até mesmo para observadores técnicos.[58] Sistemas de *Big Data* são ainda mais opacos e difíceis de serem traduzidos para a linguagem natural.[59]

Algoritmos obscuros dificultam a detecção de erros e de discriminações, muitas vezes inviabilizando a adoção de medidas preventivas, mitigadoras ou corretivas. Nesse contexto, os princípios da responsabilidade e da prestação de contas ganham especial destaque, sendo fundamentais para as organizações tomarem medidas para diminuir a opacidade e o potencial discriminatório dos sistemas.[60]

Ainda que um especialista consiga compreender a complexidade por trás de determinado sistema, comunicar essa compreensão é extremamente desa-

57. HUNKENSCHROER; KRIEBITZ, op. cit., p. 206

58. De acordo com Jena Burrell (2016, p. 1), existem pelo menos três tipos de "opacidade": (i) opacidade como política institucional para proteção de segredos, possivelmente com a intenção de esconder informações; (ii) opacidade decorrente da especialidade necessária para compreender a informação; e (iii) opacidade oriunda da incompatibilidade entre a optimização matemática característica do aprendizado de máquina e as demandas da racionalidade humana e os tipos de interpretação semântica.

59. MARANHÃO, Juliano; ABRUSIO, Juliana; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. Revista de Estudos Constitucionais, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021. p. 165.

60. ABRUSIO; ARAUJO, op. cit, p. 327.

fiador, principalmente para quem recebe a informação.[61] Não se pode esquecer que a maioria da população não tem acesso a informações qualificadas sobre Inteligência Artificial, o que deve ser considerado pelos recrutadores ao adotar medidas de transparência e explicação. Deve haver um esforço conjunto, proativo e intenso para contornar o problema da opacidade e oferecer ao público a devida transparência.

No recrutamento de trabalhadores, importantes direitos sociais estão em jogo, o que intensifica o dever de fornecer explicações adequadas aos candidatos. O entendimento do sistema pelo candidato não serve apenas para ajudar a reconhecer discriminações, mas também para viabilizar direitos fundamentais.[62] Ainda, recrutamentos opacos podem ser percebidos pelos candidatos como arbitrários ou sem sentido, especialmente se os recrutadores não conseguem oferecer explicações, o que pode resultar em reclamações, frustração e desinteresse.[63]

Nesse sentido, a exceção conferida aos "segredos comercial e industrial" pelo Art. 20 da LGPD não deve ser utilizada como uma maneira de evitar os deveres de transparência. Mesmo que haja segredos relacionados ao sistema, isso não deve impedir uma explicação, ora mais, ora menos detalhada, mas sempre adequada à transparência devida ao candidato.

Não é necessário divulgar o código-fonte nem entrar em detalhes técnicos, pois isso pouco auxilia o público a entender como o sistema funciona.[64] Também não se espera que cada decisão automatizada seja explicada minuciosamente – o que não é exigido das decisões humanas[65].[66]

Assim, não é necessária uma explicação científica sobre o sistema, mas uma explicação "cotidiana" sobre como ele funciona de forma geral.[67] Basta que a organização articule, da melhor maneira possível, as informações relevantes para o candidato, como: qual foi a lógica decisória programada, como isso afeta os seus interesses, quais características suas podem ser usadas, e quando e como o sistema pode falhar. Se a complexidade do sistema for tão alta que não seja possível explicar, nem de forma geral, os critérios adotados,

61. MULHOLLAND; FRAJHOF, op. cit., p. 280.

62. Ibidem, p. 270.

63. HUNKENSCHROER; KRIEBITZ, op. cit., p. 208.

64. FERRARI; BECKER; WOLKART, op. cit., p. 640.

65. Por exemplo, não é exigido que os entrevistadores humanos expliquem cada detalhe que justifique por que um determinado candidato os agradou ou não.

66. HUNKENSCHROER; KRIEBITZ, op. cit., p. 208 e 209.

67. MULHOLLAND; FRAJHOF, op. cit., p. 271.

um comportamento responsável pode exigir que se reduza a complexidade ou até que se deixe de usar o sistema.[68]

Uma boa prática seria indicar como cada dado inserido no sistema sobre o candidato (*inputs*) pode influenciar o resultado (*outputs*).[69] Além disso, a automação torna possível fornecer *feedbacks* valiosos para milhares de candidatos, com relatórios apresentando pontos "fortes" identificados pela IA, ou pontos que podem ser melhorados.

Outra abordagem envolve o reconhecimento do "princípio da inteligência artificial explicável", pelo qual deve-se buscar soluções técnicas para tornar os sistemas de IA explicáveis "*by design*"[70], garantindo transparência e o direito à autodeterminação informativa.[71] Além disso, é essencial criar mecanismos de auditoria[72] interna e externa dos sistemas para aprimorá-los constantemente.[73] Com essas medidas, os recrutamentos com IA podem proporcionar ainda mais transparência do que se vê atualmente nos recrutamentos tradicionais.

3.4 Questões éticas

A Ética é um campo do saber que caminha ao lado do Direito, posto que o Direito, em última análise, é baseado em princípios éticos fundamentais. Por isso, é necessário considerar as questões éticas que podem impactar o recrutamento feito com Inteligência Artificial.

Recrutamentos com IA, ao darem à máquina o poder de tomar decisões importantes sobre a vida de pessoas, conflitam diretamente com a autonomia humana, podendo levar à desumanização do recrutamento e à desvalorização da vida humana. Além disso, o contato apenas entre candidato-máquina e máquina-recrutador pode reificar as relações interpessoais.[74] Para evitar isso, o recrutamento deve ser humanizado e centrado no candidato, e um recrutador humano deve sempre manter o controle e ser capaz de tomar as decisões finais.

68. Ibidem, p. 210.

69. DATTA, Anupam et al. Algorithmic transparency via quantitative input influence. Proceedings of 37th IEEE Symposium on Security and Privacy, San Jose, USA.

70. Isto é, sistemas de Inteligência Artificial projetados, desde o princípio, visando possibilitar a explicação.

71. ABRUSIO, Juliana. Proteção de dados na cultura do algoritmo. 2019. 320 f. Tese (Doutorado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. p. 292.

72. Nos Estados Unidos, existem projetos de lei para garantir a auditabilidade algorítmica, como o S.1108 - *Algorithmic Accountability Act of 2019* e o H.R.2231 *Algorithmic Accountability Act of 2019*. Na Europa, há uma proposta de regulamentação sobre Inteligência Artificial que trata da auditabilidade dos algoritmos de alto risco (art. 17 da proposta 20).

73. ABRUSIO; ARAUJO, op. cit., p. 328.

74. HUNKENSCHROER; KRIEBITZ, op. cit., p. 205.

Além disso, os atuais sistemas podem ser inadequados para tomar decisões desse tipo. Isso ocorre porque, para configurar esses sistemas matemáticos, é necessário, de alguma forma, traduzir a complexa realidade do mundo para números computáveis. Essa tradução sempre deixará algo de fora, refletindo uma determinada escolha política, cultural e social, consciente ou inconsciente. A suposta neutralidade ou tecnicidade pura dos atuais sistemas de IA se mostram falaciosos, existindo uma "pseudoneutralidade"[75].

Durante o recrutamento, diversos fatores subjetivos são analisados. A definição de um "bom candidato", de uma "boa entrevista", de um "tom de voz confiante" e de outros parâmetros avaliados pela IA não é objetiva. Sempre haverá algum recorte mais ou menos discricionário da realidade. O "bom candidato" será reduzido a uma lista arbitrária de características consideradas como sendo "mais desejáveis" do que outras características.

Diante disso, muitas vezes não basta criar sistemas tecnicamente corretos e treinados com dados sem vieses. A classificação estatística do mundo em si, que é um pressuposto dos sistemas de IA, pode por si só já ser inadequada ou acobertar determinada escolha arbitrária. Assim, focar-se exclusivamente em questões técnicas para enfrentar os vieses discriminatórios pode ocultar questões mais centrais envolvendo as práticas sociais de classificação – de pessoas, discursos, currículos, formas de expressão etc.[76]

Embora muitas vezes seja vendida como sendo inerentemente "objetiva" e "científica", não se deve ignorar os fatores sociais por trás dos algoritmos. Caso contrário, corre-se o risco de naturalizar uma visão de mundo arbitrária apresentada como puramente técnica. As classificações feitas pela IA têm o poder de moldar a realidade, uma vez que a forma como uma pessoa é classificada pelo sistema gradualmente influenciará seu comportamento e posição na sociedade, consolidando "categorias políticas contestadas"[77].

Portanto, é importante reconhecer o aspecto político, social e cultural por trás das práticas classificatórias inerentes a esses sistemas. A partir disso, será possível considerar a complexidade do mundo real e as diferentes visões existentes, tanto no desenvolvimento quanto no uso desses sistemas. Por essa razão, projetos envolvendo IA devem contar com equipes multiculturais e multidisciplinares, além de outras medidas representativas.

75. ABRUSIO, op. cit., p.222.
76. CRAWFORD, op. cit., p. 127 e 128.
77. Ibidem, p. 139.

Considerações finais

As ferramentas de Inteligência Artificial, quando utilizadas no recrutamento de trabalhadores de forma apressada e sem análise crítica, podem representar desafios significativos para a garantia dos direitos fundamentais dos candidatos. Atualmente, essas ferramentas são particularmente propensas a inferências que violam a proteção de dados pessoais, vieses, discriminações e falta de transparência. A sociedade, empresas e legisladores devem abordar esses desafios para evitar que a adoção dessa tecnologia prejudique valores essenciais dos processos seletivos, em vez de ajudar a torná-los mais eficientes e justos.

Nesse esforço, a LGPD e outras normas já apresentam um caminho a ser seguido pelos recrutadores. No artigo, foram destacados deveres já prescritos pelas normas atuais. Entre eles, constatou-se que o uso de IA deve ser transparente e informado de forma fácil e clara ao candidato, e deve utilizar apenas dados adequados e necessários, evitando inferências abusivas e o uso de dados pessoais sensíveis. As organizações devem compreender como o sistema funciona, mantendo recrutadores humanos no controle e criando rotinas de auditoria, revisão e controle de qualidade. Os candidatos devem receber, no mínimo, explicações gerais sobre o sistema, suficientes para exercerem seus direitos. Os desenvolvedores devem buscar programar sistemas explicáveis, entre outras medidas de controle e transparência.

No entanto, a eficácia prática das normas atuais é limitada, principalmente devido à insuficiência do Artigo 20 da LGPD e às lacunas para fiscalizar ou exigir o seu cumprimento.

Além disso, foi destacada a importância de se criar processos humanizados e centrados no candidato, que respeitem a autonomia humana. Ademais, o artigo elucidou a falácia da neutralidade da IA, mostrando que as classificações feitas pelo sistema representam escolhas eminentemente subjetivas, sociais e políticas. Para controlar o poder classificatório da IA, seu desenvolvimento e uso deve passar pelo crivo de equipes multiculturais e multidisciplinares.

Assim, as organizações, principalmente as empresas, devem evitar o frenesi pela rápida adoção de IA em processos como o de recrutamento. Antes disso, é necessário considerar seus impactos jurídicos, éticos, sociais e culturais. Sistemas excessivamente complexos, opacos ou treinados com base em dados de origem duvidosa não devem ser adotados. Em vez disso, as organizações devem utilizar apenas sistemas que possibilitem o respeito aos direitos

dos candidatos, com transparência e responsabilidade, e que tenham sido desenvolvidos adequadamente à realidade social em que estão inseridos.

Embora este artigo tenha identificado normas vigentes capazes de orientar a implementação da IA no recrutamento, entende-se que há lacunas e que é necessário engendrar mecanismos regulatórios especiais, atentos às particularidades desse setor. É necessário discutir e implementar uma regulamentação robusta capaz de garantir maior responsabilidade, explicabilidade e controle da IA, permitindo que essa tecnologia alcance efetivamente o seu potencial para tornar processos, como o de recrutamento, mais eficientes, transparentes e confiáveis.

Referências

ABRUSIO, Juliana. *Proteção de dados na cultura do algoritmo*. 2019. 320 f. Tese (Doutorado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019.

ABRUSIO, Juliana; ARAUJO, André Eduardo Dorster. Inteligência artificial: decisões automatizadas e discriminação nas relações de trabalho. *Revista de Direito do Trabalho e Seguridade Social*. vol. 223. ano 48. p. 321-343. São Paulo: Ed. RT, mai./jun. 2022. Disponível em: <http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-9190>. Acesso em 22 jul. 2023.

AFFONSO SOUZA, Carlos; PERRONE, Christian; MAGRANI, Eduardo. *O Direito à Explicação entre a Experiência Europeia e a sua Positivação na LGPD*. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 243-270.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. (1948). *Declaração Universal dos Direitos Humanos*. [Resolução 217 A III]. Disponível em: <https://www.un.org/en/universal-declaration-human-rights/>. Acesso em 22 jul. 2023.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em 22 jul. 2023.

BRASIL. *Decreto Legislativo nº 186, de 9 de julho de 2008*. Aprova o texto da Convenção sobre os Direitos das Pessoas com Deficiência e de seu Protocolo Facultativo, assinados em Nova Iorque, em 30 de março de 2007. Disponível em: <http://www.planalto.gov.br/ccivil_03/congresso/dlg/dlg-186-2008.htm>. Acesso em 22 jul. 2023.

BRASIL. *Decreto-Lei nº 5.452, de 1º de maio de 1943*. Aprova a Consolidação das Leis do Trabalho. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm>. Acesso em 22 jul. 2023.

BRASIL. *Lei Federal n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 22 jul. 2023.

BRASIL. *Lei Federal n.º 9.029, de 13 de abril de 1995*. Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9029.htm>. Acesso em 22 jul. 2023.

BRASIL. Senado Federal. *Projeto de Lei nº 2338, de 2023*. Dispõe sobre a regulamentação da inteligência artificial e dá outras providências. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em 22 jul. 2023.

BRASIL. Tribunal Superior do Trabalho. *Recurso de Revista nº TST-RR-243000-58.2013.5.13.0023*. Relatora: Dora Maria da Costa. Brasília, 28 de outubro de 2021. Disponível em: <http://aplicacao4.tst.jus.br/consultaProcessual/resumoForm.do?consulta=1&numeroInt=241821&anoInt=2014>. Acesso em 22 jul. 2023.

BURRELL, Jenna. How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data & Society*, jan-jun. 2016. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/2053951715622512>. Acesso em 22 jul. 2023.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.BR). Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas Empresas Brasileiras - TIC Empresas 2021. São Paulo: Cetic.Br, 2021. Disponível em: <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2021/>. Acesso em 22 jul. 2023.

CRAWFORD, Kate. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.* New Haven and London: Yale University Press, 2021.

DATTA, Anupam et al. *Algorithmic transparency via quantitative input influence*. Proceedings of 37th IEEE Symposium on Security and Privacy, San Jose, USA. Disponível em: <http://www.ieee-security.org/TC/SP2016/papers/0824a598.pdf>. Acesso em 22 jul. 2023.

DONEDA, Danilo, et al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. *Revista dos Tribunais*, vol. 995, p. 635-655, set., 2018.

HUNKENSCHROER, A.L., KRIEBITZ, A. Is AI recruiting (un)ethical? A human rights perspective on the use of AI for hiring. *AI Ethics 3*, p. 199–213 (2023). Disponível em: <https://doi.or g/10.1007/s43681-022-00166-4>. Acesso em 22 jul. 2023.

LAURANO, Madeline. *Automation with Humanity:* putting the candidate first. Aptitude Research, patrocinado por Predictive Hire. 2022. Disponível em: <https://content.predictivehire.com/hubfs/Automation%20with%20Humanity%20%7C%20Aptitude%20Research.pdf>. Acesso em 22 jul. 2023.

LEITE, Renato. *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?*. Artigo Estratégico 39. Rio de Janeiro: Instituto Igarapé, dez., 2018.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fática Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: O Direito à Explicação nas Decisões Automatizadas. *Revista Brasileira de Direito Civil - RBDCivil*, Belo Horizonte, v. 26, p. 227-246, out./dez., 2020.

MARANHÃO, Juliano; ABRUSIO, Juliana; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. *Revista de Estudos Constitucionais*, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021.

MARTINS, Guilherme Magalhães; MUCELIN, Guilherme. Inteligência artificial, perfis e controle de fluxos informacionais: a falta de participação dos titulares, a opacidade dos sistemas decisórios automatizados e o regime de responsabilização. *Revista de Direito do Consumidor*. vol. 146. ano 32. p. 93-127. São Paulo: Ed. RT, mar./abr. 2023. Disponível em: <http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2023-3305>. Acesso em 22 jul. 2023.

MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. *Discriminação Algorítmica à Luz da Lei Geral de Proteção de Dados*. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 421-446.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. *Inteligência artificial e a lei de proteção de dados pessoais*: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, Ana. MOULHOLLAND, Caitlin (Coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters (Revista dos Tribunais), 2019. p. 265-290.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. (1965). *Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial*. [Resolução 2106 (XX)]. Disponível em: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CERD.aspx>. Acesso em 22 jul. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. (1966). *Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais*. [Resolução 2200 A (XXI)]. Disponível em: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>. Acesso em 22 jul. 2023.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. (1951). *Convenção sobre Igualdade de Remuneração entre Trabalhadores Homens e Mulheres por Trabalho de Igual Valor* (Convenção n.º 100). Genebra: OIT. Disponível

em: <https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C100>. Acesso em 22 jul. 2023.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. (1958). *Convenção sobre Discriminação em Matéria de Emprego e Ocupação (Convenção n.º 111)*. Genebra: OIT. Disponível em: <https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312256:NO>. Acesso em 22 jul. 2023.

PASQUALE, Frank. Data-Informed Duties in AI Development. 119 Columbia Law Review 1917, *University of Maryland Legal Studies Research Paper*, No. 14, 2019. Disponível em: <https://ssrn.com/abstract=3503121>. Acesso em 22 jul. 2023.

PRACOWNIK, Sofia Mandelert; SALDANHA, Vitor Maimone. Ferramentas de background check dentro do universo dos dados pessoais e da inteligência artificial: preocupações necessárias. *Revista de Direito e as Novas Tecnologias*, vol. 16, jul./set., 2022.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. *Aspectos da Proteção de Dados nas Relações de Trabalho*. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 507-522.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO 3

Moderação de conteúdos e de plataformas digitais

AUTORES

Matheus Mantuani Nunes

Breno Dias Ferreira Maia

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

16

Desafios à Moderação de Conteúdo no Facebook: o discurso do general brasileiro e a decisão do Oversight Board

MATHEUS MANTUANI NUNES

MATHEUS MANTUANI[1]

Sumário: Introdução. 1. Ascensão das Big Techs e Desafios à Moderação de Conteúdo. 2. Constitucionalismo Digital e Oversight Board. 3. O Caso Discurso de General Brasileiro. Considerações Finais. Referências.

Introdução

"A festa da Selma hoje vai está [*sic*] bombando. Não param de chegar convidados! Ela pediu para vocês viralizar [*sic*] esse convite! A entrada é liberada para todos os patriotas do Brasil, tirando crianças e idosos. Vai ser o maior Show de todos os tempos [...]".[2] Estas palavras foram publicadas por um usuário do Twitter, às 02 horas da madrugada do dia 08 de janeiro de 2023. Horas mais tarde, o Palácio do Planalto, o Congresso Nacional e o Supremo Tribunal Federal brasileiros foram invadidos, em uma situação-limite para o Estado de Direito e para a democracia liberal.

A organização dos ataques pela internet, aliás, não se restringiu ao Twitter, de modo que outras plataformas e Big Techs foram utilizadas pelos extremistas para coordenar a invasão a Brasília, como o Facebook da empresa Meta. Este artigo busca analisar justamente a forma como uma publicação de um general brasileiro contribuiu para os ataques, ao permanecer disponível por dezessete dias no Facebook. Por que a plataforma não derrubou o post? Esta moderação de conteúdo[3] ineficiente pôde contribuir para a invasão?

Responder a estas perguntas não é uma tarefa simples, uma vez que as decisões sobre moderação de conteúdo são tomadas a portas fechadas, mas isso não impede uma pesquisa criativa na busca de informações úteis à so-

1. Pós-Graduando em Direito Digital pela UERJ. Graduando em Direito pela UERJ. Atua na área de tecnologia e propriedade intelectual em Rennó Penteado Sampaio Advogados, desde 2021. Foi Editor Técnico e Coordenador da Revista da Faculdade de Direito da UERJ. Estagiou no Tribunal de Justiça do Estado do Rio de Janeiro e na Defensoria Pública do Estado do Rio de Janeiro. Ex-Diretor do Centro Acadêmico Luiz Carpenter e Ex-Representante Discente no Conselho Departamental, Departamento de Direito do Estado e Departamento de Teorias e Fundamentos do Direito da Faculdade de Direito da UERJ. Foi pesquisador e monitor bolsista na UERJ. Autor de artigos publicados em periódicos científicos e em capítulos de livros.

2. FONSECA, Bruno; SCOFIELD, Laura. *Bolsonaristas usam Código "Festa da Selma" para Coordenar Invasão em Brasília*. Pública, São Paulo, 08 de jan. 2023.

3. O termo moderação de conteúdo designa o conjunto de aplicação de regras de empresas privadas, como a Meta e o Twitter, que imponha limites ao exercício da liberdade de expressão na internet. Estes limites podem ser estabelecidos de diversas formas: restrições à visualização do conteúdo ou da conta que o publicou por outros usuários; exclusão, suspensão, edição ou restrição do conteúdo ou da conta; desmonetização; utilização de avisos; apresentação de outros pontos de vista; contextualização; dentre outros. Confiram-se: ARCHEGAS, João Victor; ESTARQUE, Marina. *Redes Sociais e Moderação de Conteúdo: criando regras para o debate público a partir da esfera privada*. Rio de Janeiro: ITS Rio, 2021; e GOLDMAN, Eric. Content Moderation Remedies. *Michigan Technology Law Review*. Estados Unidos da América, Michigan, v. 28, n. 1, mar. 2021.

ciedade civil.[4] Justamente por este motivo, o presente artigo visa a identificar como a decisão de um órgão de autorregulação da Meta, o Oversight Board ou Comitê de Supervisão, no caso "Discurso de General Brasileiro",[5] publicizou questões internas da empresa em matéria de moderação de conteúdo, de forma a garantir à crítica uma maior transparência quanto aos processos internos e quanto aos desafios de uma Big Tech na avaliação de publicações de seus usuários.

Para tanto, o artigo apresentará inicialmente um breve resumo sobre a moderação de conteúdo e sobre a ascensão das grandes plataformas da internet, em um modelo de negócios conhecido como capitalismo de vigilância. Em seguida, busca-se apresentar como a Meta organizou-se a fim de enfrentar os questionamentos a respeito da ineficácia de sua moderação de conteúdo, a partir da criação do Oversight Board e à luz da teoria do constitucionalismo digital. Por fim, a decisão do Comitê de Supervisão no caso Discurso de General Brasileiro[6] será analisada criticamente, com o intuito de identificar os desafios internos da Meta em combater conteúdos nocivos em suas plataformas.

Enquanto supostos novos governadores do discurso *online*, como sustenta Kate Klonick,[7] as complexidades que se apresentam às Big Techs exigem controles internos mais robustos, a fim de se garantir maior legitimidade e coerência decisional para a moderação de conteúdo,[8] motivo pelo qual se conclui que o Oversight Board pode auxiliar a Meta na busca por uma maior eficiência na regulação de discursos, embora existam diversos desafios a serem superados para que haja um equilíbrio entre o Comitê de Supervisão e a sua criadora.

4. KELLER, Daphne; LEERSSEN, Paddy. *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation*. IN: PERSILY, N.; TUCKER, J. A. (Eds.) Social Media and Democracy: the state of the field, prospects for reform. Reino Unido, Cambridge: Cambridge University Press, 2020, pp. 220-251.

5. OVERSIGHT BOARD. 2023-001-FB-UA. *Discurso de General Brasileiro*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

6. Ibidem.

7. KLONICK, Kate. *The New Governors: the people, rules and processes governing online speech*. Harvard Law Review. Estados Unidos da América, Massachusetts, v. 131, n. 6, pp. 1.598-1670, abr. 2018.

8. DOUEK, Evelyn. *Verified Accountability: self-regulation of content moderation as an answer to the special problems of speech regulation*. Hoover Working Group on National Security, Technology & Law. Estados Unidos da América, Califórnia, Aegis Series Paper n. 1.903, set., 2019.

1. Ascensão das Big Techs e Desafios à Moderação de Conteúdo

A fim de que seja possível investigar analiticamente a decisão do Oversight Board no caso Discurso de General Brasileiro,[9] é importante que exista uma compreensão quanto ao significado histórico da moderação de conteúdo na internet. Os professores John Bowers e Jonathan Zittrain, neste sentido, argumentam que a governança de plataformas *online* atravessou três momentos distintos: a era de Direitos (de 1990 a aproximadamente 2010), a era da Saúde Pública (de 2010 até aproximadamente 2020) e a era do Processo (a qual teria seu nascimento tímido na atualidade).[10]

A era de Direitos, conforme os autores, focou excessivamente na proteção à liberdade de expressão *online*, situação que motivou a evolução histórica para a era da Saúde Pública, cuja atenção se voltava ao estabelecimento de responsabilidades aos provedores de aplicações de internet em face do conteúdo publicado por seus usuários, como uma espécie de contrapeso à proliferação de discursos ilegais que não eram combatidos. Este segundo momento, todavia, não foi capaz de contornar os principais desafios existentes à moderação de conteúdo contemporânea, motivo pelo qual a era do Processo buscaria resolver este impasse, através da aposta na cooperação entre o regulador estatal e as plataformas. Isto seria possível por meio da criação de processos de governança que fossem capazes de construir um consenso mínimo sobre como decisões de moderação de conteúdo devem ser implementadas.[11]

Um dos passos iniciais para esta última fase histórica, de acordo com os professores, seria a delegação da governança a entidades externas e independentes das plataformas, como o Oversight Board da Meta, para garantir maior transparência e apresentar esforços efetivos da plataforma na implementação das recomendações da entidade externa.[12] Importa destacar, aliás, que os novos contornos de responsabilidade civil para o assim chamado Direito Digital reforçam deveres de prevenção de danos, de prestação de contas e de proatividade.[13]

9. OVERSIGHT BOARD. *2023-001-FB-UA*. Discurso de General Brasileiro. Estados Unidos da América, Califórnia: Oversight Board, 2023.

10. BOWERS, John; ZITTRAIN, Jonathan. *Answering Impossible Questions: content governance in an age of disinformation*. Harvard Kennedy School Misinformation Review. Estados Unidos da América, Massachusetts, v. 1, n. 1, pp. 1-8, jan., 2020.

11. *Ibidem*.

12. *Ibidem*. Conforme Bowers e Zittrain, os esforços por maior transparência no setor privado em relação à desinformação seriam prejudicados, contudo, por desafios quanto à divulgação de dados a pesquisadores e ao público.

13. MORAES, Maria Celina Bodin de. *LGPD: um novo regime de responsabilização civil dito proativo*. Civilistica. Rio de Janeiro, v. 8, n. 3, pp. 1-6, dez., 2019.

Busca-se, com isso, a mitigação do regime de informação, "forma de dominação na qual informações e seu processamento por algoritmos e inteligência artificial determinam decisivamente processos sociais, econômicos e políticos".[14] O capitalismo de vigilância, ao orientar a experiência humana como matéria-prima gratuita para as práticas econômicas das plataformas,[15] despertou desse modo e por crítica o *techlash*,[16] uma hostilidade perante as plataformas e seus modelos de negócio pautados na exploração de dados pessoais de seus usuários.[17]

A Meta, a fim de se contrapor a estes pontos, busca adotar políticas de moderação de conteúdo. Especificamente no caso do Facebook, objeto de estudo deste artigo, seus Termos de Serviço reconhecem que os usuários apenas criariam uma "comunidade", uma rede social, onde se sentissem protegidos e amparados – logo, haveria um esforço da plataforma em manter a segurança de seus produtos e serviços, o que incluiria a proibição de utilização indevida da plataforma, a publicação de conteúdos prejudiciais para terceiros e demais situações em que o Facebook pudesse prestar assistência ou proteger a comunidade. Assim, a plataforma afirma que ao se deparar com conteúdos ou condutas impróprias poderá adotar as devidas medidas. Para tanto, o Facebook prevê a possibilidade de notificar usuários, oferecer-lhes ajuda, excluir conteúdos, remover ou restringir o acesso de usuários a determinadas funcionalidades, desativar contas ou entrar em contato com as autoridades públicas necessárias.[18]

Em sentido semelhante, os Padrões da Comunidade do Facebook indicam que a Meta reconhece a importância de o Facebook ser um espaço onde as pessoas possam se comunicar e que a empresa leva a sério o papel de eliminar dos seus serviços todo tipo de excessos. A plataforma reforça no documento o seu compromisso com a liberdade de expressão, mas admite que a internet criou "novas e maiores oportunidades de abuso". Desta forma, para guiar

14. HAN, Byung-Chul. *Infocracia: digitalização e a crise da democracia*. Tradução: Gabriel Philipson. Petrópolis: Vozes, 2022, p. 8.

15. ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução: George Schlesinger. São Paulo: Intrínseca, 2019.

16. WOOLDRIDGE, Adrian. *The Coming Tech-Lash*. The Economist. Reino Unido, Londres, 18 de nov. de 2013.

17. Confira-se, por exemplo, os Termos de Serviço do Facebook: "em vez de pagar para utilizar o Facebook e os outros produtos e serviços que oferecemos, ao utilizar os Produtos da Meta abrangidos pelos presentes Termos, você concorda que podemos te apresentar anúncios personalizados e outros conteúdos patrocinados e comerciais [...]. Utilizamos os seus dados pessoais, como informações sobre a tua atividade e interesses, para te apresentar anúncios personalizados e conteúdos patrocinados que possam ser mais relevantes para você." META. *Termos de Serviço*. Estados Unidos da América, Califórnia, 2022. Disponível em: <https://www.facebook.com/terms.php>. Acesso em: 02.12.2023.

18. *Ibidem*.

consequentemente suas práticas de moderação de conteúdo, o Facebook indica como fundamento quatro valores: autenticidade, segurança, privacidade e dignidade.[19]

Entretanto, ocorre que materialmente a atuação da plataforma em matéria de moderação de conteúdo tem gerado debates e discussões acalorados[20] – o que se restará demonstrado também no caso do Discurso de General Brasileiro. Por este motivo, a aposta do Facebook para solucionar o dilema teria sido a criação do Oversight Board, com amparo no disputado conceito de constitucionalismo digital, como passa-se a expor.

2. Constitucionalismo Digital e Oversight Board

A ideia de criação de uma espécie de "Suprema Corte" do Facebook originou-se de uma entrevista de Mark Zuckerberg ao jornalista Ezra Klein.[21] Na ocasião, o CEO da Meta defendeu uma estrutura mais robusta de responsabilidade, prestação de contas e resolução de disputas, acompanhada de mecanismos de "separação de poderes" que garantissem de forma plena os direitos dos dois bilhões de usuários mensais da plataforma. Esta "Suprema Corte" corresponderia, assim, a um "tribunal independente" que julgaria os limites dos discursos aceitáveis na comunidade do Facebook.[22]

Alguns meses depois, Zuckerberg publicou um artigo sobre seu projeto, em que sustentou a impossibilidade de o Facebook tomar sozinho tantas decisões sobre liberdade de expressão e segurança. O empresário defendeu, na ocasião, uma nova maneira de as pessoas recorrerem de decisões em matéria de moderação de conteúdo: por meio de um órgão independente, cujas decisões seriam transparentes e "vinculativas". A partir de uma consulta pública, o

19. "Nós queremos garantir que o conteúdo visto pelas pessoas no Facebook é autêntico. [...] Temos o compromisso de fazer do Facebook um lugar seguro. [...] Temos o compromisso de proteger a privacidade e as informações pessoais. [...] Acreditamos que todas as pessoas são iguais no que diz respeito à dignidade e aos direitos." META. *Padrões da Comunidade do Facebook*. Estados Unidos da América, Califórnia, 2023. Disponível em: <https://transparency.fb.com/pt-pt/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards>. Acesso em: 02.12.2023.

20. Confira-se, por exemplo, o caso do genocídio rohingya em Mianmar: DOUEK, Evelyn. *Facebook's Role in the Genocide in Myanmar: new reporting complicates the narrative*. Estados Unidos da América, Califórnia: Lawfare, 2018. Recomenda-se, ademais, o caso do programa XCheck, o qual conferia certa imunidade à moderação de conteúdo para usuários que correspondessem a importantes influenciadores digitais ou a figuras públicas notórias: HORWITZ, Jeff. *Facebook Says Its Rules Apply to All: company documents reveal a secret elite that's exempt*. The Wall Street Journal, Estados Unidos da América, Nova Iorque, 13 de set. de 2021.

21. KLEIN, Ezra. *Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next*. Estados Unidos da América, Washington, DC: Vox, 2018.

22. DOUEK, Evelyn. *The Supreme Court of Facebook: Mark Zuckerberg floats a governance structure for online speech*. Estados Unidos da América, Califórnia: Lawfare, 2018.

Facebook começou a testar esta nova proposta, no primeiro semestre de 2019, com o objetivo de estabelecer o órgão independente até o final daquele ano.[23]

Por conseguinte, uma versão final do Estatuto foi publicada em setembro de 2019, a fim de formalizar as responsabilidades e a estrutura de governança do órgão, batizado como Oversight Board, ou Comitê de Supervisão, em português. A versão atualizada do documento estabelece que o comitê será composto por um conjunto diversificado de membros, os quais exercerão um "julgamento neutro e independente", e tomarão decisões de forma imparcial. Definiram-se, ademais, as competências do órgão: solicitar que a Meta forneça informações para as deliberações do Comitê; interpretar os Padrões da Comunidade do Facebook e outras políticas relevantes; instruir a Meta quanto à permissão ou à remoção de conteúdo; instruir a Meta a manter ou a reverter uma decisão; emitir explicações sobre suas decisões; e fornecer opiniões consultivas sobre as políticas de conteúdo da Meta.[24]

Ainda, o Estatuto do Oversight Board delimitou que seus membros colaborarão na tomada de decisões a fim de promover um "ambiente de colegialidade", através da emissão de decisões, recomendações e opiniões consultivas, as quais serão baseadas em princípios, a partir de um raciocínio logicamente articulado que promova a liberdade de expressão e os direitos humanos. Para isso, qualquer usuário da Meta, e até mesmo a própria empresa, poderá apresentar casos para análise. Os membros revisarão e decidirão sobre o conteúdo, de acordo com as políticas e os valores da plataforma. Contudo, verifica-se certa dose de discricionariedade ao Comitê, a quem compete definir quais casos serão de fato analisados e decididos. Ademais, decisões anteriores terão valor de "precedentes" e deverão ser consideradas para casos futuros similares.[25]

Em relação aos demais procedimentos a serem adotados pelo Oversight Board, cabe mencionar que a decisão final do órgão incluirá sua determinação quanto ao conteúdo, além da explicação dos critérios que levaram à deliberação, com base nas seguintes soluções: permitir o conteúdo ou removê-lo; manter ou reverter uma decisão. Será possível, inclusive, apresentar recomen-

23. ZUCKERBERG, Mark. *A Blueprint for Content Governance and Enforcement*. Estados Unidos da América, Califórnia: Facebook, 2018.

24. OVERSIGHT BOARD. *Charter*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

25. *Ibidem*.

ração. Por fim, a decisão final terá "efeito vinculante" e a Meta deverá implementá-la prontamente.[26]

A partir desta breve descrição do Oversight Board, notam-se diversos símbolos e conceitos provenientes do Direito Constitucional, utilizados precipuamente no Poder Judiciário, mas aqui invocados para subsidiar a implementação de um órgão privado. De certa forma, a apropriação de racionais de Direito Público traz consigo críticas sobre a utilização do constitucionalismo como mera metáfora, visto que para parte da doutrina a desvinculação das implicações estruturais do fenômeno constitucional geraria possibilidades de deslocamentos ilimitados, arbitrários ou aleatórios.[27]

A tentativa de amenização da concentração de poder privado, através de símbolos constitucionais, poderia operar, na verdade, como um "verniz de legitimação a dinâmicas de poder assimétricas".[28] De acordo com Natali Helberger, a infusão de padrões de valores públicos em empresas privadas voltadas ao lucro poderia apenas reforçar seu papel enquanto governantes do discurso na internet, o que fortaleceria seu poder de opinião e seu poder político.[29]

Em sentido oposto, parte da doutrina reconhece que as plataformas se originam de um equilíbrio complexo entre a garantia de monetização e publicidade, em face da necessidade de moderação de conteúdo –ou seja, entre atender às cobranças da sociedade civil por um ambiente seguro e protetivo, ao mesmo tempo em que se busca manter o máximo de conteúdo possível *online*, uma vez que a fonte de lucro do provedor provém da circulação de informações na rede social, na era da infocracia e do capitalismo de vigilância. Manter usuários ativos gera fluxo de dados e, consequentemente, rendimentos, ao passo em que existem pressões consideráveis para que abusos sejam coibidos. O Oversight Board, então, corresponderia justamente à tentativa de pulverizar o poder concentrado na Meta, a partir do reconhecimento da eficácia horizontal e transcendental dos valores democráticos e dos direitos fundamentais. Isso

26. *Ibidem*. Para uma visão mais específica sobre as responsabilidades e a estrutura de governança do Oversight Board, confiram-se os seus Critérios Fundamentais, Livro de Regras e Regulamentos Internos e Código de Conduta: OVERSIGHT BOARD. *Overarching Criteria for Case Selection*. Estados Unidos da América, Califórnia: Oversight Board, 2023; OVERSIGHT BOARD. *Rulebook for Case Review and Policy Guidance*. Estados Unidos da América, Califórnia: Oversight Board, 2022; e OVERSIGHT BOARD. *Bylaws*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

27. NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: WMF, 2009.

28. KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. *Constitucionalismo Digital: contradições de um conceito impreciso*. Direito e Práxis. Rio de Janeiro, v. 13, n. 4, pp. 2.648-2.689, dez., 2022, p. 2.679.

29. HELBERGER, Natali. *The Political Power of Platforms: how current attempts to regulate misinformation amplify opinion power*. Digital Journalism. Reino Unido, Londres, v. 8, n. 6, pp. 842-854, jul., 2020.

limitaria os poderes da rede social e a sua discricionariedade: é o que se convencionou chamar de constitucionalismo digital.[30]

Esta teoria é disputada atualmente e não possui uma definição precisa e pacificada, mas aqui importa notar que ela pode ser utilizada como um marco para a mitigação da concentração de poder de plataformas digitais, inclusive por meio da autorregulação – como é o caso do Oversight Board –, em uma ideia de "boa governança" ancorada nos princípios do Estado de Direito.[31] Não há uma defesa de empresas pelos defensores do constitucionalismo digital, mas um apontamento direto quanto à necessidade de mais proatividade, ainda que isso vá de encontro aos interesses de mercado.[32]

Ao mesmo tempo, ocorre que em matéria de Direito Digital a regulação deve ser dinâmica e envolver a Lei estatal, as perspectivas econômicas, as normas sociais e a arquitetura tecnológica.[33] Por isto, soluções regulatórias unilaterais estariam em descompasso com tecnologias ágeis e dispostas a contornar obstáculos à inovação. Mecanismos de autorregulação corresponderiam, assim, a desenhos de cooperação entre o agente privado e o regulador, o qual geralmente não possuiria a expertise adequada para intervir em novas tecnologias.[34]

Portanto, ainda que sejam possíveis diversas críticas à construção e à atuação do Oversight Board,[35] fato é que o *techlash* representou pressões intensas por mais transparência, democracia e prestação de contas, como apontado anteriormente, hipótese esta que culminou em uma proposta autorregulatória de novos paradigmas para a participação de usuários na governança das plataformas digitais, aliado à garantia de procedimentos e a uma espécie de

30. ARCHEGAS, João Victor; SALGADO, Eneida Desiree. *Constitucionalismo Digital*. Plural, Curitiba, 31 de out. de 2020.

31. SUZOR, Nicolas. *Digital Constitutionalism: using the Rule of Law to evaluate the legitimacy of governance by platforms*. Social Media + Society, Estados Unidos da América, Califórnia, v. 4, n. 2, jul./set., 2018.

32. A este respeito e por sua vez, a crítica defende que a descrição do Oversight Board como uma espécie de Suprema Corte compreenderia mudanças mais profundas no equilíbrio de poder entre o Estado e grandes empresas de tecnologia, com consequências normativas não intencionais e indesejáveis, uma ameaça à busca de uma governança responsável. COWLS, Josh. *et al. Constitutional Metaphors: Facebook's "Supreme Court" and the legitimation of platform governance*. New Media & Society. Estados Unidos da América, Califórnia, v. 0, n. 0, abr., 2022.

33. LESSIG, Lawrence. *Code: and other laws of cyberspace, version 2.0*. Estados Unidos da América, Nova Iorque: Basic Books, 2006.

34. KELLER, Clara Iglesias; BAPTISTA, Patrícia. *Por Que, Quando e Como Regular as Novas Tecnologias? Os desafios trazidos pelas inovações disruptivas*. Revista de Direito Administrativo. Rio de Janeiro, v. 273, pp. 123-163, set./dez., 2016.

35. A título de exemplo, Angelo Golia defende que a constitucionalização do Facebook deveria passar por uma forte intervenção estatal a fim de combater o capitalismo de vigilância da Meta: GOLIA, Angelo. *Beyond Oversight: advancing societal constitutionalism in the age of surveillance capitalism*. Social Science Research Network Electronic Journal. Países Baixos, Amsterdã, fev., 2021.

devido processo para a moderação de conteúdo: o Comitê de Supervisão da Meta.[36]

Este modelo não foi concebido para ouvir todos os casos apresentados pelos usuários da Meta, nem para abarcar a criação de uma fonte normativa de discursos globalmente aceitos. Todavia, ele pode auxiliar na identificação de pontos fracos nos processos internos da plataforma e nos Padrões da Comunidade,[37] como se observou no caso 2023-001-FB-UA.

3. O Caso Discurso de General Brasileiro

"Venha para Brasília! Vamos invadir! Vamos sitiar os três poderes." As frases compunham uma imagem de Brasília em chamas, após o discurso de um general brasileiro que apoiava a reeleição de Jair Messias Bolsonaro, tudo presente em um vídeo publicado no Facebook. No mesmo dia da publicação do conteúdo, um usuário o denunciou à Meta, por violação aos Padrões da Comunidade. O vídeo totalizou sete denúncias de quatro usuários do Facebook. A partir da primeira denúncia, um analista humano concluiu que a publicação estava de acordo com as políticas da Meta, análise mantida por um segundo analista. Em seguida, cinco moderadores concordaram que o vídeo não violava os Padrões da Comunidade. O conteúdo não foi encaminhado a nenhum especialista, para fins de análises adicionais.[38]

Cinco dias após a publicação do vídeo mantido, terroristas de extrema-direita efetivamente invadiram Brasília. A Meta declarou os eventos como "violadores", de acordo com sua política de organizações e indivíduos perigosos, e afirmou que removeria conteúdos de apoio ou de elogio aos ataques. O Brasil foi, então, indicado como um local temporário de alto risco pela Meta. Após a apelação de um dos usuários ao Comitê de Supervisão, com fundamento de que o vídeo auxiliou na incitação à violência em Brasília, a Meta determinou que as decisões de manter o conteúdo no Facebook teriam sido equivocadas. O vídeo foi removido dezessete dias após a sua publicação. A conta do gene-

36. KLONICK, Kate. *The Facebook Oversight Board: creating an independent institution to adjudicate online free expression*. The Yale Law Journal. Estados Unidos da América, Connecticut, v. 129, n. 2.418, pp. 2.418-2.499, jun., 2020.

37. DOUEK, Evelyn. F*acebook's "Oversight Board": move fast with stable infrastructure and humility*. North Carolina Journal of Law & Technology. Estados Unidos da América, Carolina do Norte, v. 21, n. 1, out., 2019.

38. OVERSIGHT BOARD. *2023-001-FB-UA*. Discurso de General Brasileiro. Estados Unidos da América, Califórnia: Oversight Board, 2023.

ral brasileiro recebeu um *strike* e ficou limitada para realizar novos *posts* por apenas 24 horas.[39]

Ainda assim, o Oversight Board selecionou o caso para identificar como a Meta modera conteúdos relacionados às eleições, bem como para observar os efeitos concretos da seleção de locais temporários de alto risco. Dezenove comentários públicos foram endereçados ao caso.[40]

O InternetLab sustentou que políticas excepcionais da Meta não devem restringir-se tão somente ao período eleitoral, uma vez que os ataques antidemocráticos ocorreram antes, durante e após as eleições de 2022 no Brasil. Ainda, o InternetLab argumentou que regras e definições explícitas sobre discursos antidemocráticos devem ser elaboradas pela Meta, inclusive com a previsão de sanções específicas e gradativas, a partir do auxílio de observadores locais e do treinamento de moderadores de conteúdo.[41]

O ModeraLab, do Instituto de Tecnologia e Sociedade do Rio ("ITS"), por sua vez, defendeu uma aplicação mais transparente das políticas de crise da Meta, uma vez que a indicação do Brasil como um local de alto risco ocorreu antes das eleições de 2022, mas a informação a respeito foi publicizada apenas em 09 de janeiro de 2023. Em paralelo com as teorias de constitucionalismo digital, o ITS comparou as políticas de crise ao estado de emergência, o qual deve ser de imediato tornado público, ser justificado e estar sujeito ao crivo dos órgãos competentes e da população. Como a decisão da Meta foi mantida em segredo, teria faltado transparência e prestação de contas para com sua comunidade de usuários, na opinião do ModeraLab.[42]

Ademais, o ITS defendeu a instituição de um mecanismo de controle de decisões de emergência da Meta, por uma instituição independente, o que poderia ser feito até mesmo pelo Oversight Board, à luz da teoria constitucional de freios e contrapesos. Outro ponto mencionado diz respeito à necessidade de fundamentação das decisões dos moderadores, em casos excepcionais, visto que eles não teriam registrado seu racional para manter a publicação do general brasileiro, motivo pelo qual nem mesmo a Meta teria informações sobre a análise do vídeo – situação que dificultaria a avaliação de equívocos e a implementação de mudanças concretas. O ITS também apontou a importância

39. *Ibidem*.

40. *Ibidem*.

41. CRUZ, Francisco Carvalho de Brito; BORGES, Ester; JOST, Iná. *Comentário do InternetLab sobre o caso 2023-001-FB-UA do Comitê de Supervisão do Facebook*. São Paulo: InternetLab, 2023.

42. MODERALAB. *Comentário Público – Discurso de General Brasileiro (Caso 2023-001-FB-UA)*. Rio de Janeiro: ITS Rio, 2023.

de a Meta contratar moderadores com conhecimento local e específico sobre o contexto político, social e cultural em que o conteúdo se insere, de modo que seria indispensável apresentar com mais transparência quem são, como ocorre a escolha e o que qualifica os especialistas contratados pela empresa.[43]

Além disto, o Oversight Board questionou e a Meta respondeu que os sete moderadores de conteúdo eram europeus fluentes em português, com conhecimento linguístico e cultural suficientes para analisar publicações brasileiras. Em relação aos Padrões da Comunidade, o Oversight Board observou que a Meta não permite declarações que incitem a entrada à força em locais onde haja sinais de risco temporário.[44] Ainda, a fim de fundamentar sua decisão, o Comitê de Supervisão levou em consideração o Pacto Internacional sobre Direitos Civis e Políticos, o Comentário Geral n.º 34 do Comitê de Direitos Humanos da Organização das Nações Unidas ("ONU"), o Artigo de Pesquisa n.º 1/2019 da ONU, Relatórios da ONU sobre liberdade de expressão e opinião e o Plano de Ação de Rabat – o que evidencia o foco no Direito Internacional para a fundamentação das decisões do Oversight Board.[45]

A Meta indicou, ainda, fatores que podem ter contribuído para o erro na moderação de conteúdo. De acordo com a empresa, a referência a "sitiar" os três poderes não configuraria uma entrada forçada, embora o contexto permitisse identificar a intenção golpista da publicação. Indicou-se também a existência de um Centro de Operação Eleitoral, composto por especialistas para fins de responder possíveis problemas em tempo real, que não estaria operando em janeiro de 2023. Outro ponto de atenção apresentado diz respeito à impossibilidade de a Meta obter dados de prevalência sobre alegações específicas, uma vez que seus sistemas seriam configurados apenas com base em violações de políticas. Neste sentido, a empresa informou ao Comitê de Supervisão que não teria dados gerais sobre moderação de conteúdo no contexto das eleições brasileiras e que não avaliaria seu desempenho com base em métricas de sucesso e referências.[46]

A partir destas circunstâncias, o Oversight Board considerou que os esforços de integridade eleitoral da Meta devem se voltar também para o pe-

43. *Ibidem*.

44. META. *Padrões da Comunidade do Facebook*. Estados Unidos da América, Califórnia, 2023. Disponível em: <https://transparency.fb.com/pt-pt/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards>. Acesso em: 02.12.2023.

45. OVERSIGHT BOARD. *2023-001-FB-UA*. Discurso de General Brasileiro. Estados Unidos da América, Califórnia: Oversight Board, 2023.

46. *Ibidem*.

ríodo pós-eleitoral, igualmente vulnerável à desinformação, à manipulação e à violência. O Comitê de Supervisão também indicou que o vídeo do general brasileiro violava os Padrões da Comunidade, porque o post incitava a entrada forçada em locais de alto risco – vale destacar que a Meta designou todo o território brasileiro como um local temporário de alto risco, em virtude do contexto eleitoral polarizado.[47] Como precedentes invocados, o Comitê de Supervisão apontou os casos Suspensão do Ex-Presidente Trump,[48] Bot de Mianmar,[49] Gabinete de Comunicações da Região de Tigré[50] e Animação Knin.[51-52]

Assim, à luz da tese tripartite para restrição da expressão,[53] e dos compromissos voluntários de direitos humanos da Meta, o Oversight Board compreendeu que as regras da empresa quanto à proibição de incitação à violência estavam declaradas explicitamente para os usuários e para os moderadores, em observância ao princípio da legalidade. O requisito do objetivo legítimo igualmente estaria presente, visto que a restrição à liberdade de expressão visava a proteger direitos de terceiros, como à vida, à ordem pública, à segurança nacional, à votação e à participação em assuntos públicos. Por fim, os princípios da necessidade e da proporcionalidade seriam atendidos com a remoção do vídeo, dada a intenção do general, o conteúdo e alcance do discurso e a probabilidade de danos iminentes.[54]

Em relação à ação de monitoramento, a Meta indicou três fatores que poderiam ter contribuído para o erro na moderação pelos analistas: incompreensão da intenção da publicação, por causa de uma falta de pontuação que teria resultado em uma má interpretação; atualizações constantes sobre o trata-

47. *Ibidem*.

48. Em contextos eleitorais, a Meta deve permitir a expressão política, mas coibir riscos graves a outros direitos humanos. OVERSIGHT BOARD. *2021-001-FB-FBR. Suspensão do Ex-Presidente Trump*. Estados Unidos da América, Califórnia: Oversight Board, 2021.

49. A proteção de discursos políticos em períodos de crise política é fundamental. OVERSIGHT BOARD. *2021-007-FB-UA. Bot de Mianmar*. Estados Unidos da América, Califórnia: Oversight Board, 2021.

50. A Meta deve estabelecer um sistema transparente e baseado em princípios para moderar conteúdos em zonas de conflito, a fim de mitigar riscos de utilização da plataforma para a incitação à violência. OVERSIGHT BOARD. 2022-006-FB-MR. Gabinete de Comunicações da Região de Tigré. Estados Unidos da América, Califórnia: Oversight Board, 2022.

51. A Meta deve explicar com mais transparência como um conteúdo é encaminhado para análise de especialistas. OVERSIGHT BOARD. *2022-001-FB-UA. Animação Knin*. Estados Unidos da América, Califórnia: Oversight Board, 2022.

52. OVERSIGHT BOARD. *2023-001-FB-UA. Discurso de General Brasileiro*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

53. Artigo 19. 3. "O exercício do direito previsto no parágrafo 2 do presente artigo [direito à liberdade de expressão] implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para: a) assegurar o respeito dos direitos e da reputação das demais pessoas; b) proteger a segurança nacional, a ordem, a saúde ou a moral públicas." ONU. *Pacto Internacional sobre Direitos Civis e Políticos*. Estados Unidos da América, Nova Iorque: Assembleia-Geral da Organização das Nações Unidas, 1966.

54. OVERSIGHT BOARD. *2023-001-FB-UA. Discurso de General Brasileiro*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

mento de conteúdo, as quais dificultariam o entendimento dos moderadores de que o Brasil estava sujeito na época a um regime diferenciado e de controles mais rígidos; e ausência de percepção sobre violações no *post*. Conforme o Oversight Board, caso esses fatores se confirmassem, isso iria sugerir que os moderadores não analisaram a publicação com o mínimo cuidado necessário ou não assistiram ao vídeo por completo.[55]

Além disso, o Comitê de Supervisão destacou que a Meta não forneceu explicações sobre os motivos pelos quais a publicação do general brasileiro não foi encaminhada para a análise de especialistas. Outro equívoco, para o Oversight Board, diria respeito à dificuldade de articulação da Meta quanto às diversas medidas de avaliação e de mitigação em vigor na época, causada pela falta de uma cadeia de comando mais clara.[56]

Apesar das medidas de transparência implementadas para as eleições brasileiras de 2022, o Comitê de Supervisão criticou a ausência de métricas específicas para mensurar os esforços de integridade da Meta. Para o Oversight Board, seria fundamental que a empresa esclarecesse como as medidas e os protocolos de avaliação de risco seriam executados: a ausência de informações específicas prejudicaria uma avaliação adequada quanto a problemas sistêmicos nas políticas e nas práticas de monitoramento da Meta. Em razão disto, o Comitê de Supervisão encorajou a empresa a fazer divulgações públicas sobre dados relevantes.[57]

Por fim, o Oversight Board declarou-se seriamente preocupado com a falha persistente na identificação da violação às políticas da Meta na publicação do general brasileiro, motivo pelo qual o Comitê de Supervisão decidiu revogar a decisão original da empresa em manter o conteúdo e apresentou duas recomendações à Big Tech. A primeira delas, relativa ao monitoramento, aconselhou o desenvolvimento de uma estrutura para avaliar os esforços de integridade eleitoral da Meta, o que incluiria a criação e o compartilhamento de métricas. A segunda, relacionada à transparência, indicou que a Meta deveria esclarecer publicamente, bem como nomear, descrever e contextualizar o conjunto de seus diversos protocolos de crise.[58]

55. *Ibidem*.
56. *Ibidem*.
57. *Ibidem*.
58. *Ibidem*.

De acordo com Carlos Affonso Souza, a decisão do Oversight Board apontou questões de processo que podem refletir as práticas de outras plataformas e aprimorar os desafios a uma moderação de conteúdo eficaz.[59] A partir das informações disponibilizadas pela própria Meta, aliás, é relevante questionar-se até que ponto existe uma falta de investimento em inteligência artificial e em monitoramento humano de publicações. A dificuldade de aplicação de políticas, a falta de transparência, a monetização e a recomendação algorítmica de desinformação e de discurso de ódio igualmente chamam a atenção para discussões quanto à contribuição direta das Big Techs às crises democráticas contemporâneas. Este ambiente de techlash, vale destacar, vem acompanhado de propostas de maior intervenção do Estado nos espaços digitais.[60] Ao mesmo tempo, diversas iniciativas internacionais procuram endereçar alternativas para garantir maior transparência e responsabilidade na moderação de conteúdo.[61]

Contudo, sistemas de responsabilidade e de prestação de contas são complexos e não emergem plenamente formados tal qual a deusa Atena da cabeça de Zeus.[62] O entrechoque que advém dos conflitos envolvendo a comunicação *online* perpassa pelo que Jack Balkin chama de triângulo da liberdade de expressão, cujos vértices seriam o Estado-nação, as infraestruturas privadas e os usuários. Os problemas que a tríplice relação geram diriam respeito a: novos governadores de discursos, capazes de produzirem censuras e restrições prévias; abusos por parte de burocracias privatizadas que governariam os usuários de forma arbitrária, sem o devido processo ou garantias de trans-

59. SOUZA, Carlos Affonso. *Comitê da Meta aponta os erros na moderação de vídeo golpista no Facebook*. Universo Online, São Paulo, 24 de jun. de 2023.

60. Confiram-se, a título de exemplo: ALEMANHA. *NetzDG. Netzwerkdurchsetzungsgesetz*. Alemanha, Berlim: Deutscher Bundestag, 2017; BRASIL. *PL 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Congresso Nacional, 2020; EUA. *Platform Accountability and Transparency Act: S.5339*. Estados Unidos da América, Washington, DC.: Congresso dos Estados Unidos, 2021; FRANÇA. *Projet de Loi Visant à Sécuriser et Réguler l'Espace Numérique*. França, Versalhes: Parlamento da França, 2023; ÍNDIA. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*. Índia, Nova Deli: Congresso Nacional Indiano, 2021; REINO UNIDO. *Online Safety Bill. A Bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes*. Reindo Unido, Londres: Parlamento do Reino Unido da Grã-Bretanha e Irlanda do Norte, 2021; e UE. *Regulamento dos Serviços Digitais. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE*. União Europeia: Jornal Oficial, 2022.

61. Confiram-se, a título de exemplo: CHANGE THE TERMS. *Change the Terms: reducing hate and disinformation online*. Estados Unidos da América, 2018; CHRISTCHURCH CALL. *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online*. França, Paris, 2019; MANILA PRINCIPLES. *Manila Principles on Intermediary Liability: best practices guidelines for limiting intermediary liability for content to promote freedom of expression and innovation*. Filipinas, Manila, 2015; PARIS CALL. *Paris Call for Trust and Security in Cyberspace*. França, Paris, 2018; THE SANTA CLARA PRINCIPLES. *The Santa Clara Principles on Transparency and Accountability in Content Moderation*. Estados Unidos da América, Califórnia, 2018; e UNESCO. *Safeguarding Freedom of Expression and Access to Information: guidelines for a multistakeholder approach in the context of regulating digital platforms*. Draft. 3.0. França, Paris: Internet for Trust, 2023.

62. DOUEK, Evelyn. *Content Moderation as Systems Thinking*. Harvard Law Review. Estados Unidos da América, Massachusetts, v. 136, n. 2, pp. 526-607, dez., 2022.

parência; e manipulações que seriam facilitadas pela vigilância digital. Para Balkin, algumas reformas poderiam ajudar a solucionar estas situações: uma regulamentação estrutural que promova a concorrência e evite discriminações; maiores garantias de um processo equitativo de moderação; e o reconhecimento de que as plataformas são agentes fiduciários que devem se guiar pela boa-fé nas tratativas com os seus usuários.[63]

O Oversight Board tem a possibilidade de decidir e de endereçar recomendações à Meta para buscar contornar equívocos na moderação de conteúdo e para fortalecer a confiança entre a plataforma e os seus usuários. Contudo, observa-se que o Comitê de Supervisão não pode ser visto como uma solução final para as adversidades da Meta. Ao não responder mais do que 1% das apelações apresentadas, ao ser composto por um pequeno grupo que não reflete por completo a diversidade de usuários do Facebook e do Instagram, e ao não ser completamente independente da Meta – afinal, a empresa financia e escolhe os membros do Comitê –, o Board acaba por enfrentar um certo *déficit* de legitimidade. Por isto, Kevin Frazier defende uma expansão do Comitê, através de um sistema composto por maiores "instâncias", pela criação de comissões de moderação, por um número maior de membros que sejam mais diversos e por maior independência. O Board poderia, desta forma, enfrentar as críticas de ser uma mera campanha de *marketing*, ao passo em que continuaria a exercer um interessante papel de autorregulação.[64]

A Meta afirma que procura um caminho, a partir do auxílio de toda a sociedade, para a governança da internet em suas plataformas. Existem, de fato, diversos desafios para o desenvolvimento de uma regulação eficiente. Variedade de normas nacionais sobre liberdade de expressão, dinamicidade de tecnologias disruptivas, dificuldade na aplicação de regras e o papel de mera intermediação evidenciam a complexidade da matéria. Para a Meta, deve-se assegurar uma responsabilização que crie incentivos para um equilíbrio responsável de valores como segurança, privacidade e liberdade de expressão. Ademais, segundo a Meta, qualquer abordagem reguladora para lidar com conteúdos deve atentar-se à escala global da internet e ao valor das comunicações internacionais, ao mesmo tempo em que deve estudar os impactos de decisões sobre liberdade de expressão e desenvolver uma compreensão

63. BALKIN, Jack. *Free Speech is a Triangle*. Columbia Law Review. Estados Unidos da América, Carolina do Sul, v. 118, n. 7, pp. 2.011-2.056, mai., 2018.

64. FRAZIER, Kevin. *Learning From Mistakes: a guide to expanding the Oversight Board*. Catholic University of Law and Technology. Estados Unidos da América, Washington, DC., v. 31, n. 2, pp. 51-94, mai., 2023.

das capacidades e das limitações da tecnologia na moderação de conteúdo. Assim, busca-se garantir que as empresas tenham flexibilidade para inovar e que elas tenham em conta a severidade que a permanência de um conteúdo nocivo online pode representar para um Estado Democrático.[65]

Apesar de a Meta defender todos estes pontos, é ela própria quem detém o poder imediato para permitir uma transparência mais significativa, para responsabilizar-se pelas suas regras de moderação de conteúdo e para aplicá-las. Por que esperar pela regulamentação estatal? Maior transparência efetivamente permite um maior escrutínio da sociedade civil nas atividades intrínsecas das corporações, o que ao fim garante críticas mais embasadas contra as Big Techs, situação que certamente é considerada pela empresa em suas análises quanto à publicização de decisões internas.[66] Contudo, a era do Processo parece fortalecer-se e a Meta tem a oportunidade de equilibrar seus procedimentos com maiores garantias aos seus usuários. O Oversight Board faz parte desta nova etapa: resta saber se continuará a orientar-se de forma proporcional, ainda que em desacordo com os anjos tronchos do Vale do Silício.[67]

Considerações Finais

Este artigo apresentou um modelo de autorregulação para a busca de uma moderação de conteúdo mais responsiva por parte das assim chamadas Big Techs. A partir da análise do modelo de negócios de plataformas como o Facebook, identificou-se um momento social de techlash e de aversão aos grandes provedores de aplicações de internet, o que foi respondido pela Meta com a criação de um Comitê de Supervisão independente e pautado na teoria do constitucionalismo digital.

O criativo Oversight Board poderá ser uma espécie de modelo a outras Big Techs que buscam endereçar os desafios de combate a discursos nocivos na internet, mas ainda há muito a ser feito caso esta suprema corte privada queira tornar inafastável sua jurisdição sobre a Meta. O caso Discurso de General Brasileiro teve como consequência apenas duas recomendações do Comitê de Supervisão à sua criadora, o que parece insuficiente em vista das inúmeras problemáticas identificadas. Ainda assim, o consenso sobre o equilíbrio corre-

65. META. *Charting a Way Forward on Online Content Regulation*. Estados Unidos da América, Califórnia, 2020.

66. DOUEK, Evelyn. *Facebook's White Paper on the Future of Online Content Regulation: hard questions for lawmakers*. Estados Unidos da América, Califórnia: Lawfare, 2020.

67. VELOSO, Caetano. *Anjos Tronchos*. Rio de Janeiro: Sony Music Entertainment, Inc., 2021. 1 CD (3 min).

to parece construir-se aos poucos perante os precedentes do Oversight Board. Não há acordo sobre o que significa uma moderação de conteúdo eficaz, mas a busca de maior transparência e responsabilidade na tomada de decisão das plataformas comprova-se um primeiro passo fundamental a ser seguido pela Meta.

Em face da quantidade bilionária de usuários do Facebook e do Instagram, faz-se necessário um equilíbrio entre o cabo de guerra regulatório que permeia as grandes plataformas, a fim de respeitar-se e buscar-se uma internet que seja livre, aberta e democrática. Com isso, a autorregulação da Meta demonstra-se uma iniciativa promissora que parece preservar os fundamentos da internet. Ao mesmo tempo, diversos aprimoramentos são necessários, à luz da era do Processo, para que se prossiga na luta por uma rede que respeite a liberdade de expressão, simultaneamente preservando os demais direitos fundamentais, com proporcionalidade, orientação democrática e combate a conteúdos nocivos.

Referências

ALEMANHA. NetzDG. *Netzwerkdurchsetzungsgesetz*. Alemanha, Berlim: Deutscher Bundestag, 2017.

ARCHEGAS, João Victor; ESTARQUE, Marina. *Redes Sociais e Moderação de Conteúdo: criando regras para o debate público a partir da esfera privada*. Rio de Janeiro: ITS Rio, 2021.

ARCHEGAS, João Victor; SALGADO, Eneida Desiree. *Constitucionalismo Digital*. Plural, Curitiba, 31 de out. de 2020.

BALKIN, Jack. *Free Speech is a Triangle*. Columbia Law Review. Estados Unidos da América, Carolina do Sul, v. 118, n. 7, pp. 2.011-2.056, mai., 2018.

BOWERS, John; ZITTRAIN, Jonathan. *Answering Impossible Questions: content governance in an age of disinformation*. Harvard Kennedy School Misinformation Review. Estados Unidos da América, Massachusetts, v. 1, n. 1, pp. 1-8, jan., 2020.

BRASIL. *PL 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília: Congresso Nacional, 2020.

CHANGE THE TERMS. *Change the Terms: reducing hate and disinformation online*. Estados Unidos da América, 2018.

CHRISTCHURCH CALL. *Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online*. França, Paris, 2019.

COWLS, Josh. *et al. Constitutional Metaphors: Facebook's "Supreme Court" and the legitimation of platform governance*. New Media & Society. Estados Unidos da América, Califórnia, v. 0, n. 0, abr., 2022.

CRUZ, Francisco Carvalho de Brito; BORGES, Ester; JOST, Iná. *Comentário do InternetLab sobre o caso 2023-001-FB-UA do Comitê de Supervisão do Facebook*. São Paulo: InternetLab, 2023.

DOUEK, Evelyn. *Content Moderation as Systems Thinking. Harvard Law Review*. Estados Unidos da América, Massachusetts, v. 136, n. 2, pp. 526-607, dez., 2022.

_____. *Facebook's "Oversight Board": move fast with stable infrastructure and humility*. North Carolina Journal of Law & Technology. Estados Unidos da América, Carolina do Norte, v. 21, n. 1, out., 2019.

_____. *Facebook's Role in the Genocide in Myanmar: new reporting complicates the narrative*. Estados Unidos da América, Califórnia: Lawfare, 2018.

_____. *Facebook's White Paper on the Future of Online Content Regulation: hard questions for lawmakers*. Estados Unidos da América, Califórnia: Lawfare, 2020.

_____. *The Supreme Court of Facebook: Mark Zuckerberg floats a governance structure for online speech*. Estados Unidos da América, Califórnia: Lawfare, 2018.

_____. *Verified Accountability: self-regulation of content moderation as an answer to the special problems of speech regulation*. Hoover Working Group on National Security, Technology & Law. Estados Unidos da América, Califórnia, Aegis Series Paper n. 1.903, set., 2019.

EUA. *Platform Accountability and Transparency Act: S.5339*. Estados Unidos da América, Washington, DC.: Congresso dos Estados Unidos, 2021.

FONSECA, Bruno; SCOFIELD, Laura. *Bolsonaristas Usam Código "Festa da Selma" para Coordenar Invasão em Brasília*. Pública, São Paulo, 08 de jan. 2023.

FRANÇA. P*rojet de Loi Visant à Sécuriser et Réguler l'Espace Numérique*. França, Versalhes: Parlamento da França, 2023.

FRAZIER, Kevin. *Learning From Mistakes: a guide to expanding the Oversight Board*. Catholic University of Law and Technology. Estados Unidos da América, Washington, DC., v. 31, n. 2, pp. 51-94, mai., 2023.

GOLDMAN, Eric. *Content Moderation Remedies*. Michigan Technology Law Review. Estados Unidos da América, Michigan, v. 28, n. 1, mar. 2021.

GOLIA, Angelo. *Beyond Oversight: advancing societal constitutionalism in the age of surveillance capitalism*. Social Science Research Network Electronic Journal. Países Baixos, Amesterdã, fev., 2021.

HAN, Byung-Chul. *Infocracia: digitalização e a crise da democracia*. Tradução: Gabriel Philipson. Petrópolis: Vozes, 2022.

HELBERGER, Natali. *The Political Power of Platforms: how current attempts to regulate misinformation amplify opinion power*. Digital Journalism. Reino Unido, Londres, v. 8, n. 6, pp. 842-854, jul., 2020.

HORWITZ, Jeff. *Facebook Says Its Rules Apply to All: company documents reveal a secret elite that's exempt*. The Wall Street Journal, Estados Unidos da América, Nova Iorque, 13 de set. de 2021.

ÍNDIA. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)* Rules. Índia, Nova Deli: Congresso Nacional Indiano, 2021.

KELLER, Clara Iglesias; BAPTISTA, Patrícia. *Por Que, Quando e Como Regular as Novas Tecnologias? Os desafios trazidos pelas inovações disruptivas*. Revista de Direito Administrativo. Rio de Janeiro, v. 273, pp. 123-163, set./dez., 2016.

KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. C*onstitucionalismo Digital: contradições de um conceito impreciso*. Direito e Práxis. Rio de Janeiro, v. 13, n. 4, pp. 2.648-2.689, dez., 2022.

KELLER, Daphne; LEERSSEN, Paddy. *Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation*. IN: PERSILY, N.; TUCKER, J. A. (Eds.) Social Media and Democracy: the state of the field, prospects for reform. Reino Unido, Cambridge: Cambridge University Press, 2020, pp. 220-251.

KLEIN, Ezra. Mark Zuckerberg on Facebook's *Hardest Year, and What Comes Next*. Estados Unidos da América, Washington, DC: Vox, 2018.

KLONICK, Kate. *The Facebook Oversight Board: creating an independent institution to adjudicate online free expression*. The Yale Law Journal. Estados Unidos da América, Connecticut, v. 129, n. 2.418, pp. 2.418-2.499, jun., 2020.

_____. *The New Governors: the people, rules and processes governing online speech. Harvard Law Review*. Estados Unidos da América, Massachusetts, v. 131, n. 6, pp. 1.598-1670, abr. 2018.

LESSIG, Lawrence. *Code: and other laws of cyberspace, version 2.0*. Estados Unidos da América, Nova Iorque: Basic Books, 2006.

MANILA PRINCIPLES. *Manila Principles on Intermediary Liability: best practices guidelines for limiting intermediary liability for content to promote freedom of expression and innovation*. Filipinas, Manila, 2015.

META. *Charting a Way Forward on Online Content Regulation*. Estados Unidos da América, Califórnia, 2020.

_____. *Padrões da Comunidade do Facebook*. Estados Unidos da América, Califórnia, 2023. Disponível em: <https://transparency.fb.com/pt-pt/policies/community-standards/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards>. Acesso em: 02.12.2023.

_____. *Termos de Serviço*. Estados Unidos da América, Califórnia, 2022. Disponível em: <https://www.facebook.com/terms.php>. Acesso em 02.12.2023.

MODERALAB. *Comentário Público – Discurso de General Brasileiro (Caso 2023-001-FB-UA)*. Rio de Janeiro: ITS Rio, 2023.

MORAES, Maria Celina Bodin de. *LGPD: um novo regime de responsabilização civil dito proativo*. Civilistica. Rio de Janeiro, v. 8, n. 3, pp. 1-6, dez., 2019.

NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: WMF, 2009.

ONU. *Pacto Internacional sobre Direitos Civis e Políticos*. Estados Unidos da América, Nova Iorque: Assembleia-Geral da Organização das Nações Unidas, 1966.

OVERSIGHT BOARD. *2021-001-FB-FBR. Suspensão do Ex-Presidente Trump*. Estados Unidos da América, Califórnia: Oversight Board, 2021.

_____. *2021-007-FB-UA. Bot de Mianmar*. Estados Unidos da América, Califórnia: Oversight Board, 2021.

_____. *2022-001-FB-UA. Animação Knin*. Estados Unidos da América, Califórnia: Oversight Board, 2022.

_____. *2022-006-FB-MR. Gabinete de Comunicações da Região de Tigré*. Estados Unidos da América, Califórnia: Oversight Board, 2022.

_____. *2023-001-FB-UA. Discurso de General Brasileiro*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

_____. *Bylaws*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

_____. *Charter*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

_____. *Overarching Criteria for Case Selection*. Estados Unidos da América, Califórnia: Oversight Board, 2023.

_____. *Rulebook for Case Review and Policy Guidance*. Estados Unidos da América, Califórnia: Oversight Board, 2022.

PARIS CALL. *Paris Call for Trust and Security in Cyberspace*. França, Paris, 2018.

REINO UNIDO. *Online Safety Bill. A Bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes*. Reindo Unido, Londres: Parlamento do Reino Unido da Grã-Bretanha e Irlanda do Norte, 2021.

SOUZA, Carlos Affonso. *Comitê da Meta aponta os erros na moderação de vídeo golpista no Facebook*. Universo Online, São Paulo, 24 de jun. de 2023.

SUZOR, Nicolas. *Digital Constitutionalism: using the Rule of Law to evaluate the legitimacy of governance by platforms*. Social Media + Society, Estados Unidos da América, Califórnia, v. 4, n. 2, jul./set., 2018.

THE SANTA CLARA PRINCIPLES. *The Santa Clara Principles on Transparency and Accountability in Content Moderation*. Estados Unidos da América, Califórnia, 2018.

UE. *Regulamento dos Serviços Digitais. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE*. União Europeia: Jornal Oficial, 2022.

UNESCO. *Safeguarding Freedom of Expression and Access to Information: guidelines for a multistakeholder approach in the context of regulating digital platforms*. Draft. 3.0. França, Paris: Internet for Trust, 2023.

VELOSO, Caetano. *Anjos Tronchos*. Rio de Janeiro: Sony Music Entertainment, Inc., 2021. 1 CD (3 min).

WOOLDRIDGE, Adrian. *The Coming Tech-Lash*. The Economist. Reino Unido, Londres, 18 de nov. de 2013.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução: George Schlesinger. São Paulo: Intrínseca, 2019.

ZUCKERBERG, Mark. *A Blueprint for Content Governance and Enforcement*. Estados Unidos da América, Califórnia: Facebook, 2018.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

17

Regulação da liberdade de expressão na Internet: a responsabilização de plataformas digitais por desinformação em legislações nacionais e estrangeiras

BRENO DIAS FERREIRA MAIA

BRENO DIAS FERREIRA MAIA[1]

Introdução

Desde o escândalo da Facebook-Cambridge Analytica, o tema das f*ake news* vem causando enorme impacto no cenário mundial, não apenas em 2016, quando ocorreram as eleições presidenciais dos Estados Unidos e a votação do Brexit, o qual culminou na saída do Reino Unido da União Europeia, mas também nas eleições presidenciais do Brasil tanto em 2018, como mais claramente observado em 2022.

A disseminação da desinformação, fortalecida, entre outros motivos, pelas bolhas digitais, pela transformação das redes sociais como fonte primária de informação e pela era da pós-verdade, aliada ao impacto negativo a direitos fundamentais, como a democracia, trouxe fortes discussões no contexto político internacional sobre maneiras de regular sua disseminação e a possibilidade de responsabilizar provedores de aplicações de internet pelo conteúdo de usuários. No Brasil, por exemplo, tem-se observado discussões sobre a inconstitucionalidade do art. 19 do Marco Civil da Internet (Lei n. 12.965/14) e o conteúdo do Projeto de Lei n. 2.630/2020 (ou "PL das *Fake News*").

Para compreender melhor o atual cenário, o presente trabalho estudará, em um primeiro momento, os conceitos, distinções e abrangências da liberdade de expressão e do direito à informação. Isso permitirá, em sua segunda seção, uma melhor compreensão dos fenômenos das *fake news* e da desinformação, bem como diferenciá-los.

Por fim, serão analisadas as possíveis formas de regulação às plataformas digitais e quais regimes de responsabilidade são adotados sob uma perspectiva de legislações nacionais e estrangeiras, envolvendo os Estados Unidos, a União Europeia, a Alemanha e o Brasil.

1. Advogado, pós-graduado em Direito Administrativo pela Pontifícia Universidade Católica de São Paulo e pós-graduando em Direito Digital pela UERJ em parceria com o Instituto de Tecnologia e Sociedade (ITS Rio) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED).

1. Liberdades de Expressão e à Informação

A liberdade de expressão é a manifestação de pensamento, de ideias e de opiniões do indivíduo e, por consequência, da sociedade[2] [3]. Trata-se do exercício de exteriorização da opinião, ou seja, da "maneira de pensar, ver, julgar"[4] de cada um.

Ela se apresenta sob duas concepções: a formal e a material. Sua formalização é verificada com o exercício do pensamento e da construção de opiniões e ideias, enquanto sua materialização através de sua conformidade com a Constituição, qualificando-a. Ou seja, "[...] não basta pensar e falar, é preciso fazê-los em obediência aos valores constitucionais"[5]. E, para melhor compreensão de sua extensão (e das concepções acima), a liberdade de expressão se divide em quatro dimensões: direito, dever, fundamento e limite.

A dimensão de **direito** advém do exercício de direitos fundamentais como a dignidade da pessoa humana e a cidadania, previstos como fundamentos do Estado Democrático de Direito em nossa Carta Magna. À medida em que a livre manifestação do pensamento em um debate entre indivíduos permite a troca de ideias e experiências, ela também legitima tais direitos fundamentais, qualificando o debate público e fortalecendo o sistema democrático.

Tal debate permite a evolução da sociedade, trazendo-lhe mais direitos, deveres e inclusão, tornando a participação social um **dever** para a liberdade de expressão. Cumpre destacar que não se trata de um dever como obrigação imposta, mas (que precisa ser) assumido em prol da garantia da própria cidadania pluralista e da democracia[6].

Esse dever de participação social serve de **fundamento**, alicerce, à própria democracia, fortalecendo-a, seja de maneira horizontal, no debate entre os cidadãos, seja vertical, com seus representantes, ao trazer aos líderes a per-

2. BARROSO, L. R. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. *Revista de Direito Administrativo*, [S. l.], v. 235, p. 1–36. jan. 2004. Disponível em: https://periodicos.fgv.br/rda/article/view/45123. Acesso em: 20 nov. 2023. p. 18

3. MENEZES, P. B. *Fake News*: Modernidade, Metodologia, Regulação e Responsabilização. 4 ed., rev., ampl. e atual. São Paulo, SP: Editora JusPodivm, 2023. p. 228.

4. OPINIÃO. HOUAISS, A. Grande dicionário Houaiss da língua portuguesa. UOL. Disponível em: https://houaiss.uol.com.br/. Acesso em: 09 jul. 2023.

5. MENEZES, op.cit., p. 231.

6. "[...] uma sociedade democrática dá oportunidade para a expressão de interesses e valores conflitantes. A democracia pluralista demanda um certo consenso, mas tal consenso diz respeito apenas aos seus princípios ético-políticos constitutivos. [...] uma democracia pluralista necessita oportunizar o dissenso e instituições através das quais ele possa se manifestar. Sua sobrevivência depende das identidades coletivas formadas em torno de posições claramente diferenciadas, assim como da possibilidade de escolha entre alternativas reais". MOUFFE, Chantal. Democracia, cidadania e a questão do pluralismo. *Política & Sociedade*, Florianópolis, v. 2, n. 3, p. 11-26, out. 2003. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/3343. Acesso em: 28 nov. 2023. p. 17.

cepção social de seus liderados[7].

Por sua vez, a dimensão como **limite** é verificada através da compressão constitucional de direitos, que irá impedir que um direito exista e/ou seja exercido de maneira absoluta. Isso porque tal compressão opera tal como uma mola que, em determinado momento de conflito, limita um direito (ao comprimir) e posteriormente o impulsiona (ao expandir) frente a outro.

Contudo, o direito em si não é diretamente restringido, mas sim o modo através do qual a manifestação de pensamento é exercida. Assim, a limitação realizada pela liberdade de expressão se apresenta tanto como um dever de supervisão entre os indivíduos, evitando que seus pares abusem de tal liberdade, quanto um direito de ver tais garantias preservadas e consolidadas. É, portanto, "uma baliza constitucional para que todos percebam a importância da manifestação livre em prol do Estado democrático de direito, e não de imposições e vontades pessoais"[8].

O direito à liberdade de expressão em sentido amplo se encontra positivado no artigo 5º da Constituição de 1988, através das liberdades de pensamento (IV), religiosa (VI), e intelectual, artística e científica (IX), bem como na Lei do Marco Civil da Internet, ao figurar como fundamento da disciplina do uso da Internet no Brasil e um de seus princípios basilares (artigos 2º, *caput*, e 3º, I)[9].

Como se pode observar, a liberdade de expressão se trata de um direito fundamental, previsto como cláusula pétrea em nossa Carta Magna, que se apresenta em dimensões distintas mas interligadas, pressupondo o **direito** à manifestação de opinião, como exteriorização e legitimação da dignidade humana e da cidadania, assumindo um **dever**-necessidade de participação social, que permitirá uma **compressão** de direitos pela sociedade através da cobrança democrática e, consequentemente, servindo de **fundamento** para o exercício, preservação e fomento da dignidade humana, cidadania e do Estado Democrático de Direito.

Por sua vez, a liberdade de informação é uma consequência qualificadora da liberdade de expressão, que busca **difundir** as ideias e opiniões construí-

7. "Ao mesmo tempo que pode estabilizar o relacionamento entre líderes e liderados, pode complementar e aumentar a legitimidade entre os atores sociais. Esse duplo viés posiciona a liberdade de expressão com um fundamento do fazer democrático". MENEZES, op. cit., p. 236.

8. "A Atividade de se expressar e o método de se manifestar é que sofrem e recebem limitações e compressões. O direito teoricamente considerado, o núcleo jurídico garantidor de sua efetividade, não comporta, via de regra, restrições excessivas [...]". Ibid., p. 238.

9. "Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão [...]
Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; [...]".

das pela liberdade anterior[10 11]. Essa difusão ocorre em duas etapas: se procedimentaliza pela **propagação** de notícias geradas pela liberdade de expressão e se materializa quando **atinge** seu público específico[12]. Dessa maneira, a liberdade de informação também se divide em dimensões[13], constituindo o trajeto percorrido pela notícia, composto pelo ponto de partida (informar) e o de chegada (informar-se ou ser informado).

A liberdade de **informar** constitui uma ação em que ativamente o emissor da notícia a propaga. Trata-se do ato de comunicar, diante do que se defende que a liberdade de informar não deve comportar restrições no momento de exercício desta dimensão, sob pena de enfraquecer ou desvirtuar o próprio direito, muito embora, assim, ela possa servir de fundamento para, inadequadamente, propagar notícias falsas ou desinformação[14].

Como a divulgação da notícia busca atingir um destino, as liberdades de **informar-se** (ativa) e de **ser informado** (passiva) pressupõem a materialização da liberdade de informação, que atinge o receptor e o coloca em posição de destaque no controle da notícia propagada, quanto ao seu alcance e ao seu grau de influência na sociedade. O receptor, que pode ser a sociedade ou grupos de indivíduos, determina a força de uma democracia (como frágil, oculta ou forte[15]) ao controlar a circulação da informação: podendo ampliá-la (de maneira desmedida, sem controle), controlar seu ritmo (checando a veracidade da informação) ou bloquear seu fluxo (agindo indiferente, desconsiderando-a)[16].

Assim, enquanto a difusão da informação como manifestação de pensamento, que não deve ser suprimida por estar diretamente ligada ao exercício da liberdade de expressão, ela possibilita a disseminação de notícias verdadeiras, imprecisas ou falsas, mas é o seu destino (quem a recebe) que deverá contê-la em benefício dos valores constitucionais democráticos.

10. "[...] A sua caracterização exige algo a mais, instiga uma atividade de propagar tais manifestações anteriormente edificadas pela liberdade de expressão [...]". MENEZES, op. cit, p. 239.

11. "[...] denota a ação de tornar comum, associar, [...] significando algo que se participa, troca de informações, tornar ideias comuns, [...] como ação de comunicar, de dividir". SARLET, I. W.; MOLINARO, C. A. Direito à Informação e Direito de Acesso à Informação como Direitos Fundamentais na Constituição Brasileira. *Revista da AGU*, Brasília, n. 42, p. 9-38, 2014. Disponível em: https://hdl.handle.net/10923/11403. Acesso em: 20 nov. 2023. p. 21.

12. MENEZES, op. cit., p. 241.

13. "[...] o direito à informação [...] cuida-se de desdobramento da própria liberdade de manifestação do pensamento, ou seja, da liberdade de expressão e comunicação [...]". SARLET; MOLINARO, op. cit., p. 14-15.

14. MENEZES, op. cit., p. 243.

15. MENEZES, op. cit., p. 245-246.

16. Parte da doutrina também destaca a categoria do direito à não informação: "[...] o direito de não receber informação [...] o direito à não informação traz um limite ao direito de informar, no qual o valor protegido é a privacidade do indivíduo". PINHEIRO, P. P. Direito digital. 7 ed., rev., ampl. e atual. São Paulo: Saraiva Educação, 2021. p. 83.

O direito à informação também se encontra previsto em nossa Carta Magna, sobretudo no artigo 5º, ao prever o direito de acesso à informação (XIV) , o direito da pessoa de receber informações de seu interesse particular a partir de órgãos públicos (XXXIII) e no artigo 220, *caput*[17], ao vedar sua restrição. O Marco Civil da Internet também estipula a promoção do acesso à informação e ao conhecimento como objetivos do uso da Internet no Brasil[18]. A previsão constitucional de tal liberdade permite que ela figure como o direito à informação, tanto como um direito dos cidadãos serem informados, como um dever estatal de garantí-lo[19].

Diante do exposto, foi possível perceber que as duas primeiras dimensões da liberdade de informação absorvem poderes um tanto distintos para uma mesma liberdade. Isso é mais bem compreendido quando se percebe que a liberdade de informar atua como uma continuação do gênero que é a liberdade de expressão, possibilitando a concretização da própria ação que a envolve (manifestação do pensamento), através de sua propagação.

Por isso, tal dimensão, não deve comportar restrições no momento de seu exercício, visto que sua limitação implicaria efeitos diretos na própria liberdade de expressão, a qual possui uma posição preferencial[20] [21] [22] sobre os demais direitos fundamentais, justamente por servir de base para a dignidade humana, a cidadania e a democracia. Tal posição, porém, não é absoluta, conforme a compressão constitucional de direitos e como se verá a seguir.

Por outro lado, as liberdades de ser informado e de informar-se (ocorridas no destino da notícia) possibilitam a contenção da disseminação de notícias

17. "Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição".

18. "Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção: I - do direito de acesso à internet a todos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;".

19. "[...] a informação subjacente ao direito é uma "função pública", tal fato denota que a informação não mais é somente um "elemento" do direito subjetivo para transformar-se em um autêntico "direito-dever" (dos emissores) com o objetivo de satisfazer o(s) direito(s) dos indivíduos de receber informação (o veraz possível, não importa) completa e objetiva [...]". SARLET; MOLINARO. op. cit., p. 16.

20. Tal ideia é observada por vasta doutrina internacional, conforme bem esclarecido por ALVES, A. F.. *Liberdade de Expressão e Remoção de Conteúdo da Internet*: anonimato, URL, árbitro e interação em portal de notícias. 2018, 245f. Dissertação (Mestrado). Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: http://www.bdtd.uerj.br/handle/1/9832. Acesso em: 28 nov. 2023. p. 43-50.

21. "[...] la libertad de expresión ocupa una posición preferente dentro de los regímenes como el que establece la Carta Política colombiana al ser 'un elemento decisivo para crear condiciones democráticas en la sociedad y la realización misma de la democracia', y 'un elemento estructural básico para la existencia de una verdadera democracia participativa' ". COLÔMBIA. Corte Constitucional. Sentença T-391/07. Segunda sala de revisão. Relator: Magistrado Manuel Jose Cepeda Espinosa. Julgado em 22 maio 2007. Disponível em: https://www.corteconstitucional.gov.co/relatoria/2007/T-391-07.htm. Acesso em: 25 jul. 2023.

22. "As liberdades de expressão e de informação e, especialmente a liberdade de imprensa, somente podem ser restringidos pela lei em hipóteses excepcionais, sempre em razão da proteção de outros valores e interesses constitucionais igualmente relevantes, como os direitos à honra, à imagem, à privacidade e à personalidade em geral". BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 511.961/SP. Relator: Min. Gilmar Mendes, 17 jun. 2019, DJe 13 nov. 2019, p. 3.

em busca de valores democráticos, visto que o objetivo real da liberdade de informação não é apenas servir de complemento àquela, mas de propagar "o livre tráfego de conhecimento dos fatos" tanto públicos como privados[23], distinguindo-se da opinião ou reflexão, que são inerentes à liberdade de expressão[24]. Esta separação é importante pois muitas vezes as liberdades de expressão e de informação são exercidas conjuntamente.

Assim, a liberdade de informação, em sua forma individualizada, pressupõe a presença de quatro requisitos: a veracidade, a imparcialidade, a objetividade e exatidão. A informação precisa ter sua veracidade demonstrável, detalhando todo o processo pelo qual foi obtida, e deve promover a democracia[25]. Ela também deve ser imparcial, seja sem subjetivismos, através da transmissão pura do fato, seja com todas as subjetividades a ela inerentes, com todos os ângulos que compõem o fato, possibilitando um acesso igualitário e amplo para que os cidadãos formulem suas próprias conclusões. A objetividade precisa ser buscada à medida do possível[26], evitando-se misturar juízos de valor e opiniões pessoais, ou camuflá-los ao momento da difusão da informação, para que não leve o ouvinte à confusão acerca do conteúdo divulgado, motivo pelo qual também deve ser exata, ou seja, sem ardil ou erro.

Por tais razões, a materialização do direito à informação (ser informado) demanda um olhar constitucional, pois precisa limitar as notícias que sejam imprecisas ou falsas, visto que a democracia implica um direito fundamental de receber notícias verdadeiras e lícitas[27]. O controle do direito às liberdades de expressão e de informação deve ocorrer apenas quando a notícia atinge o seu receptor, de modo a não permitir que as liberdades de expressão e de informar (procedimentalização) sejam violadas mediante censuras ou opiniões pessoais.

23. Sobre os riscos de limitar a liberdade de informação apenas a fatos públicos: "[...] segmentar a liberdade de informação com tal modelação, significa permitir o câmbio de qualificação do fato com público ou privado, ao sabor da vontade em se intrometer mais ou menos na circulação da notícia. É dizer, passa a ser interessante dizer que certo tipo de fato é de interesse público ou privado e, portanto, fora da proteção dessa liberdade, para que o Estado possa, às claras ou não, fazer a intervenção que bem desejar". ALVES, op. cit., p. 53-54.

24. "Mas não há como confundir fatos com opiniões. Fatos são acontecimentos que podem ser comprovados, corroborados, verificados e demonstrados por evidência ou, por outro ângulo, que são passíveis de refutação pela experiência. Opiniões constituem crenças ou julgamentos subjetivos e variáveis, que dependem do seu emissor e intérprete". ANDRADE, A. G. C. de. Desinformação na era digital. *Revista da AJURIS - QUALIS A2*, [S. l.], v. 49, n. 153, p. 37-66, 2023. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/1333. Acesso em: 20 nov. 2023, p. 43.

25. ALVES, op. cit, p. 56.

26. "[...] comunicação de fatos nunca é uma atividade completamente neutra: até mesmo na seleção dos fatos a serem divulgados há uma interferência do componente pessoal". BARROSO, op. cit., p. 18.

27. Do contrário, a dissimulação informativa bloqueia avanços democráticos, a ordem constitucional e o direito de ser informado. MENEZES, op. cit., 251.

Portanto, em razão das dimensões de ser informado e de informar-se, a liberdade de informação acaba por naturalmente ser mais limitada, seja por necessitar de requisitos como a veracidade e imparcialidade, seja por depender da atitude de seu receptor ao recebê-la, seja por esbarrar na proteção de outros direitos como os autorais, a intimidade, a vida privada etc. (art. 5º, XXVII, XXVIII e XXIX, da CF/88). É por isso que se afirma que a liberdade de expressão, apesar de necessitar de amplitude e deter uma posição preferencial, não pode ser absoluta, tampouco deve ser exercida com violência, sendo passível, porém, de controle a ser realizado, preferencialmente, em momento posterior, ao conflitar com demais direitos fundamentais, mediante ponderação – ou seja, quando difundida através da liberdade de informação –, e não previamente mediante censura[28].

Com isso em mente, surgiu a célebre frase: "Todo mundo tem o direito de ter suas próprias opiniões, mas não seus próprios fatos"[29].

2. *Fake News* e Desinformação

O termo *fake news*, em tradução livre, significa "notícias falsas" e é compreendido como um termo bastante genérico, principalmente por não especificar a compreensão do orador acerca de tal falsidade, nem sua intenção de causar dano a outrem. Exemplo disso é a definição construída por Menezes, excluindo-se notícias com *animus jocandi*[30].

Através do exposto no capítulo anterior, a liberdade de expressão comporta opiniões e pensamentos que, notadamente, não se diferenciam entre "certo" ou "errado". De maneira diversa, as informações se apresentam como fatos, que possuem a veracidade e a exatidão dentre seus pressupostos, sendo, portanto, desvirtuados quando tais características não são atendidas. Daí, exsurge o termo "desinformação", indicando tratar de conteúdos avessos a fatos, ou seja, a informações, podendo se apresentar como falsos, imprecisos ou equivocados.

28. A proibição prévia do exercício de tais liberdades, não prevista na Constituição de 1988, tem a força de eliminar as próprias liberdades em si, sendo possíveis "[...] nas situações-limites, excepcionalíssimas, de quase ruptura do sistema". BARROSO, op. cit., p. 25.

29. Tradução livre de: "Everyone is entitled to his own opinion, but not to his own facts". AN American Original. *Vanity Fair*, [S. l.], 6 out. 2010. Disponível em: https://www.vanityfair.com/news/2010/11/moynihan-letters-201011. Acesso em: 22 jul. 2023..

30. "*Logo, os termos que melhor representam as fake news ao redor do mundo são 'notícias fraudulentas', 'notícias dissimuladas', 'contraconhecimentos"*, 'desinformações' ou 'fatos alternativos'. Percebe-se, com isso, que não se trata de notícias necessariamente falsas, mas também apresentáveis ao público mediante a exposição de fatos reais, que, em razão de eventuais manipulações, desnorteiam o natural acontecimento dos próprios fatos". MENEZES, op. cit., p. 153.

A vagueza que acompanha o termo *fake news*, aliada à dificuldade de identificação de repercussão jurídica[31] e à sua utilização de maneira manipulativa porpolíticos[32] [33], resultou no estudo da "desordem informativa", em diferentes áreas do campo do conhecimento, sugerindo-se que o referido termo seja substituído por "desinformação", que é dividido em três perspectivas: *misinformation*, *disinformation* e *mal-information*.

A primeira trata da desinformação realizada pela propagação de notícias falsas por equívoco ou mesmo ignorância do agente disseminador, sem o propósito de causar danos a outrem. *Disinformation*[34] se refere à propagação dolosa de notícias falsas, sendo as informações "disseminadas com a consciência de sua falsidade ou inexatidão [...] com propósito lesivo"[35] "de proporcionar prejuízos e lesões na sociedade de rede"[36]. E, diferentemente das demais, a *mal-information* se apresenta como um conteúdo verídico, baseado em fatos (e, por isso, reais), mas usado de maneira maliciosa, para causar confusão informacional através da maldade informativa[37]. Nesta, o indivíduo propaga a verdade com intenção de causar prejuízos, sobretudo no sistema democrático[38].

Compreende-se, assim, que o termo correto para a propagação de notícias imprecisas, falsas e/ou maliciosas é a desinformação como gênero, e não simplesmente "notícias falsas", sobretudo por estarem ligadas à violação de preceitos da liberdade de informação. Porém, como a responsabilização civil pressupõe a ocorrência de dano, a discussão deste artigo considera a desin-

31. "Há uma gama enorme de mentiras ou inverdades contadas em sociedade que são inofensivas e não demandam uma resposta jurídica. [...] São irrelevantes, do ponto de vista jurídico, as afirmações comprovadamente falsas ou contrárias às evidências científicas que não trazem nenhum risco de dano". ANDRADE, op. cit., p. 40-41.

32. MELLO, P. C.; BALAGO, R.. Bolsonaro acusa mídia tradicional de fake news em documento para cúpula da democracia de Biden. *Folha de S. Paulo*, [S. l.], 3 dez. 2021. Disponível em: https://www1.folha.uol.com.br/mundo/2021/12/bolsonaro-acusa-midia-tradicional-de-fake-news-em-documento-para-cupula-da-democracia-de-biden.shtml. Acesso em: 23 jul. 2023.

33. TRUMP rebate campanha de jornais e acusa imprensa de publicar mentiras: 'Honestidade vencerá!'. G1, [S. l.], 16 ago. 2018. Mundo. Disponível em: https://g1.globo.com/mundo/noticia/2018/08/16/trump-rebate-campanha-de-jornais-e-acusa-imprensa-de-publicar-mentiras-honestidade-vencera.ghtml. Acesso em: 20 nov. 2023.

34. Em consulta ao significado de "*misinformation*", obtém-se como resultado a "informação incorreta" ou podendo significar que as pessoas estão mal-informadas, bem como a "desinformação", quando a informação tem o objetivo de enganar ("*deceive*"). Isto é interessante, pois ao longo do ciclo da informação, uma notícia pode nascer como *misinformation*, mas ser propagada como *disinformation*. MISINFORMATION. In.: CAMBRIDGE. English-Portuguese Dictionary. Disponível em: https://dictionary.cambridge.org/dictionary/english-portuguese/. Acesso em 18 jul. 2023.

35. ANDRADE, op. cit., p. 40.

36. MENEZES, op. cit., p. 158.

37. O prefixo "mal-" advém de "malice" que, em tradução livre, significa "malícia".

38. "O conteúdo malicioso e perspicaz significa que tais classes de notícias veiculam fatos que possuem aptidão para instaurar discursos ardis, com índole separatista, promovendo uma maldade informativa, ou inclinando a sociedade a receber uma habilidade astuta, em prol de inconformismo social, que gera os refluxos sagazes em desfavor principalmente do sistema democrático". MENEZES, op. cit., p. 159.

formação através das duas últimas espécies abordadas, também largamente utilizadas no cenário mundial e pela definição da Comissão Europeia[39].

3. Veiculação de desinformação na Internet

Toda essa propagação de fatos e opiniões, intrínseca à natureza humana de viver em sociedade, permite o exercício das liberdades de expressão e de informação, e pode ser feita das mais variadas formas, seja verbal, escrita, por gestos e até por expressão artística[40], bem como de maneira impessoal, por veículos da imprensa, como televisão e rádio, e por meio da Internet, através de plataformas digitais (provedores de aplicação de internet).

Cada vez mais conectado, o ser humano aprendeu a depender anatomicamente das tecnologias e da Internet (como parte de seu próprio corpo), expandindo as formas de obter conhecimento e de se expressar. A Internet escala de maneira exponencial a cascata de informações, a infodemia[41], transbordando a mente das pessoas[42].

Não obstante, as plataformas digitais, cada vez mais inteligentes, aprenderam a analisar os comportamentos humanos na esperança de trazer conteúdos mais personalizados ao gosto de cada um, buscando oferecer serviços sob medida. O efeito colateral, contudo, tem sido percebido à medida que se (re)descobre que o ser humano está longe de ser perfeito e possui diversas falhas, como condutas antiéticas, preconceitos e desigualdades (muitas vezes também escondidos deles mesmos)[43] que refletem o modo de pensar e agir da humanidade, sendo ainda mais gritantes sob o choque entre diferentes culturas.

39. "A desinformação é entendida como informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens econômicas ou para enganar deliberadamente o público". COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Combater a desinformação em linha: uma estratégia europeia. COM (2018), 236 final*, Bruxelas, 26 abr. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0236. Acesso em: 22 jul. 2023.

40. "Se é possível expressar-se politicamente pela arte, usualmente a arte tem utilidade além da questão política". ALVES, op. cit., p. 41.

41. "[...] excesso de informações, algumas precisas e outras não, que tornam difícil encontrar fontes idôneas e orientações confiáveis quando se precisa". ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE (OPAS). *Entenda a infodemia e a desinformação na luta contra a COVID-19*. Kit de Ferramentas de Transformação Digital. Ferramentas de Conhecimento. 2020. Disponível em: https://iris.paho.org/handle/10665.2/52054. Acesso em: 28 nov. 2023.

42. A música "Welcome To The Internet" retrata muito mesmo esse cenário, resumindo-o na frase: "Anything and everything, all of the time". Em tradução livre: "Qualquer coisa e tudo, o tempo todo". BURNHAM, B. Welcome To The Internet. Inside. [S. l.]: Kobalt Music Publishing Ltd., 2021. Disponível em: https://www.youtube.com/watch?v=k1BneeJTDcU. Acesso em 22 jul. 2023.

43. "[...] as máquinas herdam o conteúdo a que possuem contato, seja por carregamento inicial de programadores, seja por aprendizado na interação humana, inclusive o preconceito". MARRAFON, M. A.; MEDON, F. Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados. Revista Consultor Jurídico, [S. l.], 9 set. 2019. Disponível em: https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd/. Acesso em: 25 jul. 2023.

Por meio de fenômenos como as câmaras de eco (ou filtros bolha) e a homofilia[44] tal efeito colateral acabou por trazer um campo ainda mais fértil à desinformação, resultando em uma era atualmente chamada de pós-verdade[45]: menos preocupada com a veracidade da informação, o que importa agora é a crença individual, por mais absurda que seja, como ideologias que desafiam fatos científicos (os benefícios das vacinas e a Terra ser redonda).

Este cenário atual, aliado ao *zero rating*[46] que transformou as redes sociais no principal meio de obtenção de informação, motivou diversos estudos da desinformação nas plataformas digitais buscando maneiras de contê-la, de modo a evitar que maiores danos sejam causados às democracias e aos direitos fundamentais dos cidadãos, ambiente foco do presente estudo.

4. Responsabilização por conteúdo desinformativo: regulação das plataformas digitais?

A dinamicidade do meio digital traz diversas repercussões à sociedade, promovendo-lhe constantes mudanças tanto na forma de se organizar e agir, como na vida de pessoas e de empresas, exigindo normas com flexibilidade apta a proteger os direitos envolvidos e as bases fundantes da sociedade, de modo que traga segurança jurídica sem que esta esteja acompanhada de obsoletismo.

O rápido crescimento do mundo virtual reviveu essa preocupação (assim como a inteligência artificial), visto que apesar de inovações visarem melhorias à vida humana e ao meio ambiente, também podem ser desvirtuadas pelos usuários e, sem regras apropriadas, tornarem-se terreno fértil para a prática de crimes sob a crença de ser uma "terra sem lei".

Esta nova realidade, assim, trouxe à tona a discussão sobre a regulação das plataformas digitais, sobretudo quanto à sua responsabilização por conteúdos gerados por terceiros, abrindo o debate sobre a moderação de con-

44. "Entre as principais forças que impulsionam as cascatas informacionais está a 'homofilia' (*homophily*), fenômeno [...] observado nas redes sociais, caracterizado pela maior tendência de os indivíduos se associarem e se relacionarem com outros que compartilhem semelhanças, em termos de gostos, interesses, inclinações políticas, religião, educação, gênero e outras características sociais". ANDRADE, op. cit., p. 52.

45. "[conceito] segundo o qual a verdade é uma noção relativa, que tem menos relevância do que convicções ou crenças pessoais. [...] O que se vê nas redes sociais e em outros meios digitais é tão somente o apego radical a certas crenças, sejam elas ideológicas, políticas, religiosas, ou sentimentos e emoções, com desprezo e repúdio a argumentos, evidências ou provas factuais". ANDRADE, op. cit., p. 42.

46. "[...] o uso contínuo de um plano de dados que limita o acesso da Internet às redes sociais e a sítios específicos impede a realização de checagem de fatos e cria um ambiente de informação unicamente realizada no interior das redes sociais". ALVES, M. A. S.; MACIEL, E. R. H. O fenômeno das fake news: definição, combate e contexto. *Internet & Sociedade*, São Paulo, v.1. n.1, p. 144-171, fev. 2020. Disponível em: http://hdl.handle.net/1843/44432. Acesso em: 20 nov. 2023. p. 157.

teúdo desinformativo, possibilitada sob a aspecto da liberdade à informação (informar-se e ser informado), mas acautelada sob o risco de violar a liberdade de expressão e instaurar a censura, como visto.

4.1. Formas de regulação das plataformas digitais

Atualmente, existem três formas de regulação aplicáveis às plataformas digitais[47] na Internet: a heterorregulação, a autorregulação e a autorregulação regulada.

A heterorregulação (*straight regulation*), também chamada de "regulação pública", consiste em uma regulação realizada através da intervenção estatal, sendo observada mediante a edição de leis específicas pelo Poder Legislativo e sua aplicação pelo Poder Judiciário.

Oposta à primeira, a autorregulação é uma forma de regulação realizada pelos próprios interessados, as plataformas digitais e os usuários, que desenvolvem regras de conduta, com aplicações de sanções[48]. É muito observada nas resoluções de disputas online (*online dispute resolutions*), em que as plataformas criam procedimentos internos para lidar com questões relacionadas ao serviço prestado, extrajudicialmente (como nos casos eBay[49] e Facebook[50]).

A terceira forma de regulação é a autorregulação regulada (*enforced self-regulation*), ou "corregulação", que consiste em uma união das duas anteriores, cenário em que o Estado estabelece as premissas de um mercado ou de determinadas práticas, permitindo às empresas promoverem suas próprias regulações, em complementação à governamental e de maneira mais específica, conferindo maior adaptação e atualização.

O grande desafio quanto à escolha do melhor modelo circunda os possíveis impactos negativos aos envolvidos, valendo-se de pontos de vista liberais,

47. Entendidas como empresas de tecnologias como redes sociais, mensageria instantânea e ferramentas de busca na internet. No Marco Civil da Internet, se apresentam como provedores de aplicações, definidas como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

48. "A autorregulamentação parte do pressuposto de que ninguém é melhor que o próprio interessado para saber quais são as lacunas que o Direito deve proteger, quais são as situações práticas do dia a dia que estão sem proteção jurídica e que caminhos de solução viável podem ser tomados". PINHEIRO, op. cit., p. 121.

49. O sistema de resolução de disputas desenvolvido pelo eBay é uma referência mundial, atingindo 60 milhões de disputas por ano, como uma taxa de acordos de 90%, com mínima intervenção humana. SILVEIRO, J. P. S. Sistemas online de resolução de disputas. *Jota*, [S. l.], 22 set. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/sistemas-online-de-resolucao-de-disputas-22092019. Acesso em: 20 nov. 2023.

50. O formato desenvolvido pelo Facebook envolve um Comitê de Supervisão independente (Oversight Board), que funciona como uma Corte para revisão de decisões sobre remoção de conteúdo. LAVADO, T. Facebook nomeia primeiros 20 membros de comitê que vai julgar remoção de conteúdo; um deles é brasileiro. *G1*, 6 mai. 2020. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/05/06/facebook-nomeia-primeiros-20-membros-de-comite-que-vai-julgar-remocao-de-conteudo-um-deles-e-brasileiro.ghtml. Acesso em: 20 nov. 2023.

ligados à essência da Internet, e conservadores, fincados na necessidade do controle estatal para garantir seu funcionamento. Enquanto a heterorregulação permite um maior controle, este se concentra nas mãos do Estado que, no contexto da desinformação, poderá limitar direitos fundamentais como a própria liberdade de expressão[51] que, apesar da posição preferencial, possibilitaria a ocorrência de censura através de um efeito resfriador nos cidadãos (*chilling effect*), além de envolver processos lentos que dificultem a atualização frequente diante da alta dinamicidade.

Assim, muito se defende a autorregulação porque ela parte do princípio de "[...] legislar sem muita burocracia, observando a Constituição e as leis vigentes. Isso permite maior adequação do direto à realidade social, assim como maior dinâmica e flexibilidade para

que ele possa perdurar no tempo e manter-se eficaz"[52], podendo-se "reconhecer que plataformas como Facebook e Twitter podem fazer muito para impedir a difusão de *fake news* ou de discursos de ódio sem chegar até o ponto da censura total"[53], como de fato o fazem[54].

Contudo, críticos da autorregulamentação defendem que a Internet transformou o livre mercado de ideias em um meio dominado pelo interesse de poucos que detém muito poder[55] e que ela deveria ter evitado a proliferação da desinformação, sem, contudo, consegui-lo[56].

51. "[...] a regulação governamental, que pode acabar por limitar a liberdade de expressão e recair em censura". MOUNK, Y. *O povo contra a democracia*: Por que nossa liberdade corre perigo e como salvá-la. São Paulo: Companhia das Letras, 2019. apud. RODRIGUES, T. M.; BONONE, L. M.; MIELLI, R. V.. Desinformação e Crise da Democracia no Brasil: é possível regular fake news?. *Confluências*, Niterói, v. 22, n. 3, p. 30-52, dez. 2020/mar. 2021. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/8039. Acesso em: 28 nov. 2023. p. 35.

52. PINHEIRO, op. cit., p. 121.

53. MOUNK, op. cit., p. 283. apud RODRIGUES; BONONE; MIELLI, op. cit., p. 35.

54. AUDIÊNCIA pública - Marco Civil da Internet (manhã). Brasília, 28 mar. 2023. 1 vídeo (2:54:35). Publicado pelo STF. Disponível em: https://www.youtube.com/watch?v=AwTODpWW-3E. Acesso em: 20 nov. 2023.

55. "[...] a internet, distante da perspectiva inicial que possibilitava a visualização das potencialidades libertárias dessa tecnologia, tornou-se uma grande 'praça de mercado' oligopolizada por 'um punhado de corporações transnacionais', demandando assim um debate sobre 'as implicações políticas e culturais, inclusive geopolíticas, dessa realidade". DANTAS, M. Internet: praças de mercado sob controle do capital financeiro. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 40., 2017, Curitiba. *Anais* [...]. Curitiba: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2017. p. 1-22, Trabalho 2710-1. p. 2 apud. RODRIGUES; BONONE; MIELLI, op. cit., p. 35-36.

56. "A autorregulação não se tem mostrado suficiente para dar conta dos diversos abusos ocorridos na Internet, entre eles o da proliferação das *fake news*. [...] 'autorregulação regulada' dos grandes provedores de serviços na Internet, através do qual seja possível associar as vantagens da autorregulação – em especial a expertise tecnológica das redes sociais e a sua agilidade na correção de fraturas no ecossistema informacional – com as vantagens da regulação estatal – em especial o poder de coerção e a atuação voltada primordialmente para o atendimento do interesse público". ANDRADE, op. cit., p. 61.

4.2. Análise de legislações nacionais e estrangeiras

A ideia de uma regulação híbrida tem sido adotada por muitos países, em diferentes níveis quanto à responsabilização (*liability*) das plataformas digitais, buscando implementar a moderação de conteúdo sobre a base de princípios como a transparência (normalmente ligada também à prestação de contas – *accountability*), a publicidade, o contraditório e o devido processo legal. O que se tem buscado, na realidade, é que as plataformas digitais, por deterem o conhecimento técnico necessário, sejam controladas e responsabilizadas caso não atuem diligentemente diante de conteúdos ilícitos, dentre eles a desinformação.

Ocorre que a desinformação nem sempre é clara, justamente por seu propósito de causar dano através da confusão informacional, necessitando da participação da sociedade civil, de agências de checagem de fatos e do Poder Judiciário (ou seja, a liberdade de expressão enquanto **dever**). A própria discussão sobre a constitucionalidade do artigo 19 do Marco Civil da Internet no STF[57] adveio de casos em que as plataformas não lograram identificar o conteúdo como ofensivo ou o perfil como falso[58]. Em um deles, o pedido liminar foi negado pelo juiz de direito, ao entender que o conteúdo estaria dentro dos limites da liberdade de expressão.

Nos Estados Unidos foi incluída a Seção 230[59] no *Communications Decency Act* (CDA), reconhecendo a isenção de responsabilidade dos provedores por conteúdos gerados por terceiros (*safe harbors*) [(c), (1) e (2)] ao proteger a moderação do "bom samaritano", definida como a realizada espontaneamente e de boa-fé contra conteúdo entendido pela plataforma digital como censurável, independentemente de ser protegido constitucionalmente [(c), (2)], salvo violações a direitos autorais, crimes relativos a obscenidades ou à exploração sexual de crianças, e à privacidade de comunicações eletrônicas (d).

No Brasil, por meio do art. 19 do Marco Civil da Internet[60], os provedores de aplicações de internet também não são responsáveis por conteúdo de tercei-

57. Supremo Tribunal Federal. Temas 533 e 987 de repercussão geral.

58. "[...] quando a professora de português Aliandra Vieira, de Belo Horizonte, foi alvo de uma comunidade no Orkut com comentários de desafetos seus no ensino médio". PINHO, A. Ações de professora e dona de casa podem mudar regras da internet no Brasil. Folha de S. Paulo, [S. l.], 8 abr. 2023. Disponível em: https://www1.folha.uol.com.br/poder/2023/04/acoes-de-professora-e-dona-de-casa-podem-mudar-regras-da-internet-no-brasil.shtml. Acesso em 23 jul. 2023.

59. Disponível em: https://www.law.cornell.edu/uscode/text/47/230. Acesso em: 26 nov. 2023.

60. "Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário".

ros, sendo apenas responsabilizados caso descumpram ordem judicial para remoção de conteúdo julgado ilegal, ressalvadas apenas (i) nudez não consensual, em que basta uma notificação do interessado, e (ii) violações de direitos autorais e/ou conexos, ainda pendente de lei específica. Diferente do CDA, a lei brasileira restringe mais a liberdade de moderação das plataformas digitais, vindo a responsabilizá-las por moderações operadas sem ordem judicial e fora das exceções citadas.

A União Europeia, por sua vez, implementou o Regulamento de Serviços Digitais (*Digital Services Act* – DSA) – já em vigor, mas sua implementação completa ocorrerá em 2024 –, que parte do princípio da derrubada após notificação (*notice and takedown*), ou seja, sem necessidade de monitoramento geral e contínuo (vedado por seu artigo 8º)[61].

Apesar de se fundar em uma atuação repressiva após tomar ciência do conteúdo ilegal [art. 16 (3)], assim como os modelos estadunidense e brasileiro, o DSA diverge ao abrangir o dever de moderação de conteúdo diante de simples notificação recebida pelos meios oficiais das plataformas. Ainda, este Regulamento traz em seu bojo o princípio da transparência ao obrigar as plataformas digitais a motivarem decisões de remoção de conteúdo ilícito (mas não quando for mantido por ser considerado lícito), assim como o devido processo legal e o contraditório, ao instaurar procedimento a ser seguido, com a revisão de decisões (pelo "sistema interno de gestão de reclamações"). Percebe-se, assim, que ele segue uma tendência de maior transparência às plataformas digitais, possibilitando, inclusive, uma prestação de contas (*accountability*) de suas decisões internas.

Contudo, o DSA não define prazos para o devido processo legal interno e para notificações diante de suspeitas de crime, valendo-se de conceitos jurídicos indefinidos como "diligente", "sem demora justificada" [artigo 20 (4)] e "imediatamente" [artigo 18 (1)], trazendo um ônus desmedido. Outro risco presente é a criação dos organismos com poderes de resolução extrajudicial de conflitos, visto que serão certificados pelo "coordenador dos serviços digitais do Estado-Membro", o que pode implicar em uma parcialidade, mascarada pelo Estado-Membro certificador, e evidenciar os problemas da heterorregulação.

61. "Artigo 8.º **Inexistência de obrigações gerais de vigilância ou de apuramento ativo dos factos**. Não será imposta a esses prestadores qualquer obrigação geral de controlar as informações que os prestadores de serviços intermediários transmitem ou armazenam, nem de procurar ativamente factos ou circunstâncias que indiquem ilicitudes".

Visando a conter preventivamente a desinformação, a Alemanha promulgou o *Network Enforcement Act* (*NetzDG*, ou *Netzwerkdurchsetzungsgesetz*), em outubro de 2017, que trouxe às plataformas obrigações de transparência e accountability, e definiu procedimentos diante de conteúdos ilícitos. Obriga-se a informação imediata aos usuários do motivo da moderação de conteúdo ilícito, bem como o compartilhamento de boas práticas na criação de formas de sua detecção automática. Porém, muitas vezes, justificar a moderação pode inviabilizar investigações policiais, resultados em processos judiciais e até expor a vítima denunciante.

Mas a real crítica à lei alemã é, além de não definir o que é a desinformação, impor uma responsabilização direta às plataformas digitais pelo conteúdo gerado por terceiros em seu ambiente virtual, em prazos curtos e sob pena de multas altíssimas[62], gerando um evidente risco de remoção de conteúdos legítimos e até possibilitando um controle de conteúdo por entes privados com análises precipitadas, violando a liberdade de expressão[63] – assim como o fazem os prazos genéricos contidos no DSA.

No Brasil, há também o Projeto de Lei n. 2.630/2020[64], que iniciou com a proibição de conteúdos de desinformação e não a mais define. Atualmente, concentra esforços em "comportamentos ilegítimos e no uso abusivo e ilegal de recurso econômico"[65], ou seja, "deixou de abordar o que pode ou não ser dito nas redes sociais"[66]. Trata-se de projeto discutido há três anos que recebeu às pressas da votação de maio de 2023 uma "versão substitutiva", com cerca de 40% de conteúdo novo[67], na qual, apesar de ter sido retirada a figura da entidade autônoma de supervisão (autarquia especial com poderes de fiscalização e aplicação de sanções), ela surpreendeu ao prever o protocolo de segurança (artigo 12), que permite o controle pelo governo sobre a forma de propagação dos conteúdos nas plataformas digitais, possibilitando uma censura estatal de viés político às vésperas de eleições.

62. Obriga-as a excluir conteúdos que violem o Código Penal alemão em prazos de um dia a uma semana para casos complexos, sob pena de multa de até cinquenta milhões de euros em caso de descumprimento.

63. ALVES; MACIEL, op. cit., p. 162-163.

64. Última versão, apresentada em 27/04/2023, pelo Dep. Orlando Silva (PCdoB/SP). Consulta em: 02 dez. 2023.

65. RODRIGUES; BONONE; MIELLI, op. cit., p. 44.

66. MACHADO, C. V.; DURIGAN, V. C.; PEREIRA, L.. PL das Fake News: entenda o que é, seu impacto e as principais críticas. *Jota*, [S. l.], 18 abr. 2022. WIKIJOTA. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/pl-das-fake-news-entenda-o-que-e-seu-impacto-e-as-principais-criticas-18042022. Acesso em: 20 nov. 2023.

67. PL DAS FAKE NEWS: o que muda na internet do Brasil?. [Locução de]: Emanuel Bonfim. Entrevistada: Carlos Affonso de Souza. *Estadão Notícias*, [S. l.], 2 mai. 2023. Podcast. Disponível em: https://open.spotify.com/episode/21XVTMuFc1G9tpmO-4qZ1bR?si=c346fc36fc5448b6&nd=1&dlsi=6f559793b2ff4f1b. Acesso em: 20 nov. 2023.

O projeto também não engloba todas as plataformas digitais, limitando sua aplicação a categorias específicas com mais de dez milhões de usuários (art. 2º), restringindo o conceito de provedores de aplicação de internet presente na Lei n. 12.965/14. Neste ponto, compartilha-se o alerta dado pelo Professor Carlos Affonso de Souza quanto a pequenas plataformas também serem capazes de causar grandes impactos na sociedade[68].

Não fosse o bastante, o PL também procura expandir a imunidade parlamentar (art. 33, §6º), criando super usuários, com maior proteção contra moderação de conteúdo, apesar de se reconhecer que a desinformação parte muitas vezes da própria política[69] [70].

Assim como as demais regulações, o projeto brasileiro prevê transparência às decisões de moderação, contraditório e sua revisão, bem como *accountability* através de relatórios sobre os controles de conteúdo e o protocolo de segurança, caso acionado (arts. 11 e 15). Interessante notar que também impõe *liability* às plataformas digitais por conteúdos gerados por terceiros, mas de maneira solidária, se não removidos "diligentemente" (arts. 6º e 7º).

Vale mencionar que a previsão de remuneração de conteúdos jornalísticos em redes sociais também não é clara, havendo uma brecha para que grupos ilegítimos se façam passar pela imprensa e tenham caminho aberto para propagação de desinformação, possibilitando cenários de contradição com a própria previsão de responsabilização civil de seu artigo 6º.

Pela presente análise, restou claro que as principais legislações do mundo, apesar de bem-intencionadas ao visarem maior transparência e prestação de contas, acabaram por adotar medidas extremas na responsabilização de plataformas digitais pelos conteúdos gerados por terceiros em seus ambientes virtuais, trazendo o risco de um controle imparcial pelo Estado ou acentuado por entes privados, obrigando estes a moderar conteúdos de forma "diligente", sem tempo suficiente para uma análise adequada de seu teor e contexto, criando um campo aberto para a violação da liberdade de expressão – imagine-se a complexidade em identificar, de imediato, se determinado conteúdo seria uma *disinformation* (ilícito) ou uma sátira (lícito).

68. Ibid.

69. SCHIOCHET, A. *et al*. Lula e Bolsonaro usam dados falsos em debate marcado por confrontos sobre pandemia e corrupção. *Agência Lupa*, Rio de Janeiro, 16 out. 2022. Disponível em: https://lupa.uol.com.br/jornalismo/2022/10/16/debate-band--lula-bolsonaro. Acesso em: 25 jul. 2023.

70. ANDRADE, op. cit., p. 56-60.

Considerações finais

Com o presente trabalho, foi possível compreender que enquanto a liberdade de expressão possui uma posição preferencial sobre demais direitos fundamentais, apresentando-se pela manifestação de pensamento que alicerça a própria democracia e dignidade humana, e constituindo um direito que não comporta restrição em sua origem, a liberdade de informação esbarra no direito fundamental a notícias lícitas e verídicas.

Compreender que a desinformação é um termo mais preciso e adequado do que *fake news* possibilitou observar que o direito à informação comporta moderação quando verificada a prática dolosa de confusão informacional em meio às plataformas digitais.

A partir desta base conceitual, foram apresentados distintos cenários regulatórios das plataformas digitais em âmbito internacional, observando-se que diferentes tentativas de sua responsabilização trazem maiores riscos à liberdade de expressão, ao pressionarem as plataformas a moderar conteúdos lícitos que, de início, sugiram um ar de ilicitude, ou ao darem poderes exagerados de controle ao Estado. Contudo, a corregulação, já presente no Brasil pela Lei nº 12.965/14 e pelas medidas das plataformas em moderar conteúdos adequadamente, parece se apresentar como um melhor caminho, considerando os princípios constitucionais e infraconstitucionais previstos em nosso ordenamento jurídico, que garantem uma base legal sólida e permitem uma ampla construção de melhores práticas para o setor – o que é muito favorável à imagem dos provedores de aplicação de internet ante seus usuários.

Pensar o contrário pode incorrer em extremismos, como visto na lei alemã, na atribuição de poderes de controle ao interesse estatal (também de forma direta no PL n. 2.630/20 e indireta no DSA) e na obrigação das plataformas de identificarem conteúdos ilícitos através de conceitos jurídicos indeterminados, em prazos curtos que o próprio Judiciário muitas vezes não é capaz de fazer.

Por fim, apesar das tentativas de regulação analisadas, pouco se tem visto quanto à promoção de educação digital como política pública, tema de alta relevância em um cenário como o brasileiro, em que ocorre o fenômeno do *zero rating*, que concentra a obtenção de informação em plataformas digitais, e que traz dificuldades à sociedade na checagem de sua veracidade, no controle de sua circulação, e no fortalecimento da democracia.

Referências

ALVES, A. F.. *Liberdade de Expressão e Remoção de Conteúdo da Internet*: anonimato, URL, árbitro e interação em portal de notícias. 2018, 245f. Dissertação (Mestrado). Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: http://www.bdtd.uerj.br/handle/1/9832. Acesso em: 28 nov. 2023.

ALVES, M. A. S.; MACIEL, E. R. H. O fenômeno das fake news: definição, combate e contexto. *Internet & Sociedade*, São Paulo, v.1. n.1, p. 144-171, fev. 2020. Disponível em: http://hdl.handle.net/1843/44432. Acesso em: 20 nov. 2023.

AN American Original. *Vanity Fair*, [S. l.], 6 out. 2010. Disponível em: https://www.vanityfair.com/news/2010/11/moynihan-letters-201011. Acesso em: 22 jul. 2023.

ANDRADE, A. G. C. de. Desinformação na era digital. *Revista da AJURIS - QUALIS A2*, [S. l.], v. 49, n. 153, p. 37-66, 2023. Disponível em: https://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/1333. Acesso em: 20 nov. 2023.

AUDIÊNCIA pública - Marco Civil da Internet (manhã). Brasília, 28 mar. 2023. 1 vídeo (2:54:35). Publicado pelo STF. Disponível em: https://www.youtube.com/watch?v=AwTODpWW-3E. Acesso em: 20 nov. 2023.

BARROSO, L. R. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. *Revista de Direito Administrativo*, [S. l.], v. 235, p. 1–36. jan. 2004. Disponível em: https://periodicos.fgv.br/rda/article/view/45123. Acesso em: 20 nov. 2023.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Câmara dos Deputados: 2002.

BRASIL. Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados: 2014.

BRASIL. Projeto de Lei n. 2.630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília, Senado Federal, 2020.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 511.961/SP*. Relator: Min. Gilmar Mendes, 17 jun. 2019, DJe 13 nov. 2019.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 1.037.396/SP*. Relator: Min. Dias Toffoli.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 1.057.258/MG*. Relator: Min. Luiz Fux.

BURNHAM, B. *Welcome To The Internet*. Inside. [S. l.]: Kobalt Music Publishing Ltd., 2021. Disponível em: https://www.youtube.com/watch?v=k1BneeJTDcU. Acesso em 22 jul. 2023.

CAMBRIDGE. English-Portuguese Dictionary. Disponível em: https://dictionary.cambridge.org/dictionary/english-portuguese/. Acesso em 18 jul. 2023.

COLÔMBIA. Corte Constitucional (Segunda Sala de Revisão). *Sentença T-391/07*. Relator: Magistrado Manuel Jose Cepeda Espinosa, 22 maio 2007. Disponível em: https://www.corteconstitucional.gov.co/relatoria/2007/T-391-07.htm. Acesso em: 25 jul. 2023.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Combater a desinformação em linha: uma estratégia europeia. *COM (2018), 236 final*, Bruxelas, 26 abr. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0236. Acesso em: 22 jul. 2023.

DANTAS, M. Internet: praças de mercado sob controle do capital financeiro. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 40., 2017, Curitiba. *Anais* [...]. Curitiba: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2017. p. 1-22, Trabalho 2710-1.

HOUAISS, A. *Grande dicionário Houaiss da língua portuguesa*. UOL. Disponível em: https://houaiss.uol.com.br/. Acesso em: 09 jul. 2023.

LAVADO, T. Facebook nomeia primeiros 20 membros de comitê que vai julgar remoção de conteúdo; um deles é brasileiro. *G1*, 6 mai. 2020. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/05/06/facebook-nomeia-primeiros-20-membros-de-comite-que-vai-julgar-remocao-de-conteudo-um-deles-e-brasileiro.ghtml. Acesso em: 20 nov. 2023.

MACHADO, C. V.; DURIGAN, V. C.; PEREIRA, L.. PL das Fake News: entenda o que é, seu impacto e as principais críticas. *Jota*, [S. l.], 18 abr. 2022. WIKIJOTA. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/pl-das-fake-news-entenda-o-que-e-seu-impacto-e-as-principais-criticas-18042022. Acesso em: 20 nov. 2023.

MARRAFON, M. A.; MEDON, F. Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados. *Revista Consultor Jurídico*, [S. l.], 9 set. 2019. Disponível em:https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd/. Acesso em: 25 jul. 2023.

MELLO, P. C.; BALAGO, R.. Bolsonaro acusa mídia tradicional de fake news em documento para cúpula da democracia de Biden. *Folha de S. Paulo*, [S. l.], 3 dez. 2021. Disponível em: https://www1.folha.uol.com.br/mundo/2021/12/bolsonaro-acusa-midia-tradicional-de-fake-news-em-documento-para-cupula-da-democracia-de-biden.shtml. Acesso em: 23 jul. 2023.

MENEZES, P. B. *Fake News*: Modernidade, Metodologia, Regulação e Responsabilização. 4 ed., rev., ampl. e atual. São Paulo, SP: Editora JusPodivm, 2023.

MOUFFE, Chantal. Democracia, cidadania e a questão do pluralismo. *Política & Sociedade*, Florianópolis, v. 2, n. 3, p. 11-26, out. 2003. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/3343. Acesso em: 28 nov. 2023.

MOUNK, Y. *O povo contra a democracia*: Por que nossa liberdade corre perigo e como salvá-la. São Paulo: Companhia das Letras, 2019.

ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE (OPAS). *Entenda a infodemia e a desinformação na luta contra a COVID-19*. Kit de Ferramentas de Transformação Digital. Ferramentas de Conhecimento. 2020. Disponível em: https://iris.paho.org/handle/10665.2/52054. Acesso em: 28 nov. 2023.

PINHEIRO, P. P. *Direito digital*. 7 ed., rev., ampl. e atual. São Paulo: Saraiva Educação, 2021.

PINHO, A. Ações de professora e dona de casa podem mudar regras da internet no Brasil. *Folha de S. Paulo*, [S. l.], 8 abr. 2023. Disponível em: https://www1.folha.uol.com.br/poder/2023/04/acoes-de-professora-e-dona-de-casa-podem-mudar-regras-da-internet-no-brasil.shtml. Acesso em 23 jul. 2023.

PL DAS FAKE NEWS: o que muda na internet do Brasil?. [Locução de]: Emanuel Bonfim. Entrevistada: Carlos Affonso de Souza. *Estadão Notícias*, [S. l.], 2 mai. 2023. Podcast. Disponível em: https://open.spotify.com/episode/21X-VTMuFc1G9tpmO4qZ1bR?si=c346fc36fc-5448b6&nd=1&dlsi=6f559793b2ff4f1b. Acesso em: 20 nov. 2023.

RIBEIRO, A. *et al*. Checamos Lula e Bolsonaro no debate da Globo. *Aos Fatos*, [S. l.], 28 out. 2022. Disponível em: https://www.aosfatos.org/noticias/debate-globo-lula-bolsonaro-checamos/. Acesso em: 25 jul. 2023.

RODRIGUES, T. M.; BONONE, L. M.; MIELLI, R. V.. Desinformação e Crise da Democracia no Brasil: é possível regular fake news?. *Confluências*, Niterói, v. 22, n. 3, p. 30-52, dez. 2020/mar. 2021.

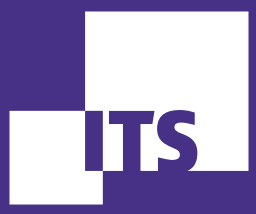
Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/8039. Acesso em: 28 nov. 2023.

SARLET, I. W.; MOLINARO, C. A. Direito à Informação e Direito de Acesso à Informação como Direitos Fundamentais na Constituição Brasileira. *Revista da AGU*, Brasília, n. 42, p. 9-38, 2014. Disponível em: https://hdl.handle.net/10923/11403. Acesso em: 20 nov. 2023.

SCHIOCHET, A. *et al*. Lula e Bolsonaro usam dados falsos em debate marcado por confrontos sobre pandemia e corrupção. *Agência Lupa*, Rio de Janeiro, 16 out. 2022. Disponível em: https://lupa.uol.com.br/jornalismo/2022/10/16/debate-band-lula-bolsonaro. Acesso em: 25 jul. 2023.

SILVEIRO, J. P. S. Sistemas online de resolução de disputas. *Jota*, [S. l.], 22 set. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/sistemas-online-de-resolucao-de-disputas-22092019. Acesso em: 20 nov. 2023.

TRUMP rebate campanha de jornais e acusa imprensa de publicar mentiras: 'Honestidade vencerá!'. *G1*, [S. l.], 16 ago. 2018. Mundo. Disponível em: https://g1.globo.com/mundo/noticia/2018/08/16/trump-rebate-campanha-de-jornais-e-acusa-imprensa-de-publicar-mentiras-honestidade-vencera.ghtml. Acesso em: 20 nov. 2023.



Acesse nossas redes

itsrio.org

Este livro foi composto nas fontes Termina, FreightSans Pro e Public Sans e lançado pelo Instituto de Tecnologia e Sociedade, em janeiro de 2024.