DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Plataformas digitais e proteção de dados pessoais

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
setembro/2023

ITS
UERJ UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
DIREITO UERJ
CEPED

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

Plataformas digitais e proteção de dados pessoais

COORDENAÇÃO
Sérgio Branco
Chiara de Teffé

PUBLICAÇÃO
setembro/2023

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)

Plataformas digitais e proteção de dados pessoais
[livro eletrônico] / coordenação Sérgio Branco,
Chiara de Teffé. -- Rio de Janeiro :
ITS - Instituto de Tecnologia e Sociedade,
2023. -- (Diálogos da pós-graduação em direito
digital)
PDF

Vários autores.
Bibliografia.
ISBN 978-85-5596-005-5

1. Artigos - Coletâneas 2. Direito digital
3. Proteção de dados - Leis e legislação 4. Proteção
de dados pessoais 5. Plataforma digital I. Branco,
Sérgio. II. Teffé, Chiara de. III. Série.

23-172415 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.). *Plataformas digitais e proteção de dados pessoais*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2023. 370p.

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

LISTA DE AUTORES

Ana Clara Gonçalves Flauzino

Ana Paula de Oliveira Quintana Ferreira

Bernardo Diniz Accioli de Vasconcellos

Bianca Alves Batista

Carolina Fiorini Ramos Giovanini

Celina Carvalho

Ellen Nice Lyra de Souza

Giovana Carneiro

Gabriel Lacerda Ferreira

Janaina Costa

Jeannine de Souza Hagnauer

Lucas Cabral de Souza Ramos

Lucas Lavogade

Nice Siqueira do Amaral

Rayanne Conceição de Almeida Santos

Ricardo Godoy Vidal da Silva Paiva

Tatiana Chagas dos Santos Coutinho

Vanessa Vargas dos Santos

APRESENTAÇÃO

O avanço da tecnologia criou a demanda por profissionais capacitados nos diversos ramos do Direito Digital, que dominem de forma crítica e dinâmica temas como proteção de dados pessoais, inteligência artificial e liberdade de expressão na internet.

Diante disso, o ITS Rio juntamente com o CEPED e a UERJ desenvolveram uma pós-graduação ***lato sensu*** em Direito Digital que busca trazer os principais debates relativos ao campo, alinhando teoria e prática, academia e mercado. O curso foi cuidadosamente elaborado para atender às demandas da sociedade que está em constante transformação. Até o momento, nossa rede Alumni já conta com mais de 600 estudantes conectados.

O ITS está há anos contribuindo com a produção de pesquisas e estudos de ponta sobre o Direito Digital. Nessa perspectiva, 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 18 artigos de integrantes do programa de pós-graduação *lato sensu* em Direito Digital, incluindo estudantes e assistentes acadêmicos de disciplinas do curso, para compor a obra coletiva. Temas como proteção de dados pessoais, telessaúde, jurimetria, tributação na economia digital, *decentralized autonomous organizations* (DAOS), plataformização e cooperativismo, regulação de plataformas digitais, metaverso, inteligência artificial e *smart contracts* 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 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, 12 de agosto de 2023.

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/CEPED 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 OABRJ. 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). Atua como advogada em áreas do Direito Civil e do Direito Digital e como consultora em proteção de dados pessoais.

Sérgio Branco

Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (Uerj). Autor dos livros “Memória e Esquecimento na Internet”, “Direitos Autorais na Internet e o Uso de Obras Alheias”, “O Domínio Público no Direito Autoral Brasileiro – Uma Obra em Domínio Público” e “O que é Creative Commons – Novos Modelos de Direito Autoral em um Mundo Mais Criativo”. 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). Advogado. Cofundador e diretor do ITS Rio.

SUMÁRIO

EIXO I — Plataformas digitais e inovação

SUMÁRIO

EIXO II

Proteção de dados pessoais e novas tecnologias

SUMÁRIO

EIXO III

Inteligência Artificial e suas aplicações

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO I

Plataformas digitais e Inovação

AUTORES

Ellen Nice Lyra de Souza

Celina Carvalho e Giovana Carneiro

Bernardo Diniz Accioli de Vasconcellos

Victor Gomes Barcellos

Ana Paula de Oliveira Quintana Ferreira

Lucas Lavogade

Ricardo Godoy Vidal da Silva Paiva

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

1

O mundo virtual e seus desafios reais: a moderação de conteúdo no metaverso

ELLEN NICE LYRA DE SOUZA

ELLEN NICE LYRA DE SOUZA[1]

Sumário: Introdução. 1. O metaverso de mundos virtuais. 1.1. O metaverso e sua definição através dos seus objetivos. 2. O mundo digital como espelho do mundo real. 2.1. O mundo virtual e o dano no metaverso. 2.2. O assédio no metaverso: Casos Nina Jane e Chanelle Siggens. 2.3. Aliciamento de menores no metaverso: a Investigação da BBC no VRChat. 3. Moderação no metaverso: os obstáculos do provedor de aplicação. 3.1. Marco Civil da Internet: Aplicação e Provedor de Aplicação. 3.2. Políticas de Conteúdo: uma alternativa ao controle de conteúdo previsto em lei. 3.3. Lei Geral de Proteção de Dados Pessoais: consentimento do titular e os dados pessoais no metaverso. Considerações Finais. Referências.

Introdução

Este artigo propõe-se a discutir os desafios encontrados na moderação de conteúdo gerado por terceiros no metaverso. Para tanto, é feita uma análise da importância do metaverso na sociedade no contexto atual, sobretudo diante da pandemia do COVID-19, bem como é traçada uma busca a respeito da definição de metaverso.

Em seguida, discute-se a necessidade de moderação de conteúdo nos mundos digitais, sob a ótica do Marco Civil da Internet, da Lei Geral de Proteção de Dados e da criação de políticas de conteúdo, mediante a apresentação de casos de violação de direitos no mundo digital, com o intuito de identificar obstáculos encontrados à moderação efetiva de conteúdo no metaverso.

Por fim, este trabalho tem por objetivo desenvolver uma análise geral da necessidade de regulamentação adequada no ambiente digital do metaverso, levando em consideração as dificuldades encontradas para o êxito no controle de conteúdo em tempo real, com o intuito de não inviabilizar o próprio desenvolvimento da tecnologia.

1. O metaverso dos mundos virtuais

Com a pandemia do COVID-19, o metaverso se tornou o centro de muitas discussões no ambiente da tecnologia. Em um momento em que o contato hu-

1. Advogada de Propriedade Intelectual. Graduada pelo Centro Universitário Ibmec. Pós-graduada pelo programa de pós-graduação da Universidade de Lisboa, em parceria com a Associação Portuguesa de Direito Intelectual. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro). Atualmente, é parte do corpo jurídico de empresa de tecnologia como foco no comércio eletrônico, prestando consultoria interna em áreas do Direito Civil.

mano não poderia ocorrer, o metaverso, ainda visto com desconfiança, passou a ser uma possível alternativa.

Fato é que o conceito de metaverso não é algo propriamente novo. A ideia de vivenciar experiências da vida real em ambiente virtual já foi explorada em plataformas como o Second Life[2] e até em jogos, como a franquia The Sims[3]. O Second Life, por exemplo, anteriormente era apenas visto como um jogo e hoje já se tornou uma plataforma capaz de hospedar reuniões de trabalho no ambiente virtual[4], de modo similar a vida real.

Ainda, não necessariamente o metaverso se propõe a criar experiências efetivamente fidedignas às da vida real, mas também experiências sensoriais ainda mais intensas que a da realidade. Em abril de 2020, o rapper Travis Scott realizou um show no ambiente virtual do jogo Fortnite, um jogo de ação em um ambiente de fantasia que permite a interação entre diversos jogadores de forma realista. O show, feito através de um avatar do artista em tamanho gigante, foi assistido por 14 milhões de usuários, público inimaginável em um show presencial[5]. De acordo com a revista Forbes, a apresentação no ambiente do Fortnite arrecadou 20 milhões de dólares, montante muito superior ao arrecadado em apenas um show presencial de sua turnê[6].

Nesse sentido, vale destacar que em 2020 muitos países se encontravam com restrições de eventos em razão da crise da pandemia do COVID-19, o que impossibilitou a realização de diversos eventos e impactou profundamente a indústria do entretenimento. Assim, o ambiente virtual se mostrou como uma alternativa para esse mercado. O artista Travis Scott foi pioneiro no uso do mundo digital como plataforma para shows.

2. Second Life é um ambiente virtual em 3D que proporciona a interação social simulando uma vida real ao usuário. Ver mais em: https://secondlife.com/

3. The Sims é um jogo de simulação produzido pela Maxis, que visa oferecer ao jogador a experiência de jogo com situações da vida real, vividas por um avatar/ personagem criado pelo próprio jogador (o “Sim”). Ver mais em: https://www.ea.com/pt-br/games/the-sims

4. SECOND LIFE. Remote Work and Event Solutions: https://www.connect.secondlife.com/about. Acesso em 12 de janeiro de 2023.

5. HAHNE, Stephanie. Travis Scott faz história com show épico e virtual no jogo “Fortnite”. Publicado em 24 de abril de 2020. Disponível em: https://www.tenhomaisdiscosqueamigos.com/2020/04/24/travis-scott-fortnite/. Acesso em 05 de janeiro de 2023.

6. VALENTINA, Rebekah. Travis Scott reportedly grossed roughly $20m for Fortnite concert appearance. Publicado em 01 de dezembro de 2020. Disponível em: https://www.gamesindustry.biz/travis-scott-reportedly-grossed-roughly-usd20m-for--fortnite-concert-appearance. Acesso em 05 de janeiro de 2023.

Em outubro desse mesmo ano, a Meta lançou o dispositivo de realidade virtual Oculus Quest 2[7], um *headset* que ganhou grande popularidade e visa aumentar o contato do usuário com o ambiente virtual através da tecnologia de realidade aumentada, tornando-o ainda mais interativo. Atualmente, o dispositivo já está na terceira geração e, desde o lançamento da primeira versão em 2019 gerou a arrecadação de US$ 1,5 bilhões à Meta, que segue em contínuo crescimento[8] e evidencia também o aumento de interesse na tecnologia.

Com o aumento do interesse em dispositivos de realidade virtual, estima-se que o segmento de venda de destes gerará receitas globais de até US$ 50 bilhões até 2030[9]. Portanto, já podemos imaginar uma sociedade onde o uso da realidade virtual, sobretudo a realidade virtual aumentada, poderá ser comum, o que nos abre uma gama de possibilidades não apenas de interações sociais comuns, mas também comerciais, que é o caso do VR Commerce, já existente nos dias atuais e pouco popularizado[10].

Além disso, cumpre destacar a importância social da realidade virtual no que se refere à acessibilidade de experiências a pessoas com deficiência. Nesse sentido, a tecnologia da realidade virtual funciona como um meio de acesso a cenários virtuais sem que haja deslocamento ou muitos esforços, viabilizando a participação de uma pessoa com deficiência que tem dificuldade de locomoção, por exemplo, em atividades às quais esta não teria acesso, ou teria acesso com mais dificuldade, no mundo exterior[11].

Ainda, os impactos da realidade virtual e do metaverso não se restringem apenas ao ambiente virtual. Se por um lado, há a preocupação do aumento do índice de sedentarismo em razão do uso de tecnologias, por outro, a realidade

7. META. *Introducing Oculus Quest 2, the Next Generation of All-in-One VR*. Publicado em 16 de setembro de 2020. Disponível em: https://about.fb.com/news/2020/09/introducing-oculus-quest-2-the-next-generation-of-all-in-one-vr/. Acesso em 11 de janeiro de 2023.

8. ROAD TO VR. *Quest Store surpasses $1.5 Billion in Content Revenue, Showing Continue Growth*. Publicado em 18 de outubro de 2022. Disponível em: https://www.roadtovr.com/oculus-quest-store-revenue-1-billion-milestone-growth-meta/. Acesso em 11 de janeiro de 2023.

9. FERNANDES, Victor. Realidade virtual será segmento de US$ 50 bilhões até 2030. Publicado em 03 de agosto de 2022. Disponível em: https://www.panrotas.com.br/mercado/tecnologia/2022/08/realidade-virtual-sera-segmento-de-us-50-bilhoes-ate-2030_191032.html. Acesso em 11 de janeiro de 2023.

10. O VR Commerce consiste na interação social da compra e venda de produtos ocorrida no ambiente de realidade virtual com realidade aumentada, proporcionando às partes uma experiência imersiva e fidedigna ao ambiente real. Ver mais em: https://news.ifood.com.br/futuro-do-consumo-o-que-e-vr-commerce/

11. SERRA, Maysa Venturoso Gongora Buckeridge Serra, *et al*. Realidade Virtual para Pessoas com Deficiência: O Uso do Vídeo Game como Prática de Lazer. LICERE - Revista do Programa de Pós-graduação Interdisciplinar em Estudos do Lazer, [S. l.], v. 21, n. 4, p. 529–548, 2018. DOI: 10.35699/1981-3171.2018.1952. Disponível em: https://periodicos.ufmg.br/index.php/licere/article/view/1952. Acesso em 11 de janeiro de 2023.

virtual também se mostra como uma alternativa para produzir cenários onde há o exercício de atividade física sem o efetivo deslocamento a um espaço físico apropriado[12]. É o caso do uso da realidade virtual em treinos de futebol, onde o usuário consegue ter a experiência de estar em um campo de futebol simplesmente através do uso de um *headset* de realidade virtual e acessórios que são capazes de detectar seus movimentos. Assim, o usuário poderá interagir com o cenário através de movimentos comuns ao esporte correspondente[13], resultando na prática de atividade física por meio da interação no ambiente virtual.

Sendo assim, a realidade virtual e o metaverso nos abrem inúmeras possibilidades em diversos ramos, impactando em infinitas áreas da vida de cada pessoa. No entanto, ao transferirmos situações da vida real ao mundo virtual, também transferimos os problemas que as seguem, que muitas vezes são inerentes à própria vida humana e nos traz a seguinte pergunta: como os solucionar no ambiente virtual?

1.1. O metaverso e sua definição através dos seus objetivos

O metaverso encontra-se em construção, razão pela qual não há ainda uma definição estabelecida. No momento atual, temos apenas uma definição do que ele poderá ser baseado no que foi construído até agora, o que pode nos dar algumas respostas[14].

Nesse sentido, a pesquisadora Terry Winters destaca que o metaverso tem como objetivo a disponibilização de um universo digital paralelo, conectado ao mundo físico através de múltiplas tecnologias[15], que acabam por resultar em um mundo digital totalmente funcional. Na visão de Winters, a finalidade do metaverso é simular, não só de forma visual como também sensorial, o próprio

12. SERRA, Maysa Venturoso Gongora Buckeridge Serra, *et al*. Realidade Virtual para Pessoas com Deficiência: O Uso do Vídeo Game como Prática de Lazer. LICERE - Revista do Programa de Pós-graduação Interdisciplinar em Estudos do Lazer, [S. l.], v. 21, n. 4, p. 529–548, 2018. DOI: 10.35699/1981-3171.2018.1952. Disponível em: https://periodicos.ufmg.br/index.php/licere/article/view/1952. Acesso em 11 de janeiro de 2023

13. ONIRIA. Como usar realidade virtual (VR) para treinamentos? Disponível em: https://oniria.com.br/como-usar-realidade-virtual-vr-para-treinamentos/. Acesso em 11 de janeiro de 2023.

14. ANDRADE, Renato. Metaverso: A próxima fronteira da inovação. 1ª Edição. E-Book Kindle, 2022. Pg. 10.

15. WINTERS, Terry. *The Metaverse: Buying Virtual Land*, NFTS, WEB3 *& Preparing for the Next Big Thing*. P.

mundo físico[16], permitindo que os integrantes desse mundo virtual possam ter experiências do mundo físico no ambiente digital.

Ainda no que se refere à definição de metaverso a partir do seu objetivo, o "Metaverse Roadmap Project" define que o metaverso é a convergência da realidade física virtualmente aprimorada (através do uso de gadgets de realidade virtual aumentada, por exemplo) e a realidade do mundo físico propriamente dito. Com essa convergência, os usuários são capazes de usufruir das funcionalidades do metaverso[17].

De todo modo, ambos conceitos possuem um ponto em comum: o metaverso tem por objetivo conectar a realidade do mundo físico ao ambiente digital, com o intuito de proporcionar a vivência de experiências típicas do mundo físico no mundo digital.

2. O mundo digital como espelho do mundo real

Levando em consideração o próprio objetivo do metaverso, é necessário o analisar do ponto de vista estrutural. Para que o metaverso cumpra sua funcionalidade, é essencial que um sistema forneça o ambiente necessário. Para isso, temos os mundos digitais, que funcionam como plataformas para viabilizar as interações inerentes ao metaverso.

Como exemplo, temos o Meta Horizon Worlds[18], o mundo digital criado pela Meta e que pode ser acessado pelo *Oculus Quest*. Nele, a partir da criação de um avatar, o usuário é capaz de interagir com outros e até participar de atividades sociais na própria plataforma. Nessa mesma linha, há o Second Life, mencionado anteriormente, que expandiu sua funcionalidade até para fins comerciais, permitindo que a plataforma seja o meio para encontros profissionais no mundo digital.

Além dos mundos digitais, existem as "MetaGalaxies", que correspondem a múltiplos mundos virtuais coexistentes e vinculados através de uma mesma comunidade e mesmo controlador[19]. Um exemplo é o ActiveWorlds, onde o

16. Ibidem.

17. Smart, J.M., Cascio, J. and Paffendorf, J., Metaverse Roadmap Overview, 2007. Disponível em: https://www.metaverseroadmap.org/overview/. Acesso em 11 de janeiro de 2023.

18. Ibidem.

19. MARTINS, Patrícia Helena Marta. FONSECA, Victor Cabral. SEREC, Fernando Eduardo. Metaverso: Aspectos Jurídicos. São Paulo: Editora Almedina, 2022. Pg, 50.

usuário pode se mover de um mundo virtual ao outro sem sair da plataforma geral do ActiveWorlds.

Nesse contexto podemos dizer que o metaverso é composto por inúmeros mundos digitais isolados e inúmeras "galáxias virtuais", formadas por diversos mundos digitais. De acordo com Patrícia Helena Martins Marta Martins *et al*:

> O que se entende por metaverso, portanto, seria a progressão final. Um ecossistema onde a MetaWorlds e MetaGalaxies interagem através de um protocolo de transporte virtual padronizado, que independe da autoridade controladora dos ambientes envolvidos. Isso porque (...) o metaverso está inserido em um contexto de internet descentralizada, a Web 3.0, impulsionada por conteúdo gerado e controlado pelo próprio usuário, em uma lógica não monopolista[20].

Assim, neste momento, podemos concluir que o metaverso é composto por inúmeras plataformas digitais (mundos virtuais) onde ocorrem interações típicas do mundo real entre os seus usuários. Portanto, o mundo virtual é uma aplicação, acessada através da internet, que conecta o usuário a inúmeras funcionalidades que visam cumprir os objetivos do metaverso.

Tratando-se de aplicação que tem por objetivo simular o mundo real, é previsível que os problemas do mundo real também sejam transferidos ao mundo virtual - sobretudo os problemas jurídicos, o que torna necessária a discussão da responsabilização de atos ocorridos no plano virtual sob o ponto de vista legal.

2.1 O assédio no metaverso: Casos Nina Jane e Chanelle Siggens

Em 2021, a inglesa Nina Jane Patel acessou a plataforma Horizon Worlds, da Meta, para testá-la. Ao criar sua conta na plataforma, a usuária criou um avatar com as suas características reais e correspondente ao gênero feminino. Em 60 segundos de uso da plataforma, Nina afirmou ter sido vítima de assédio sexual por 3 a 4 avatares masculinos, ocasião na qual agredida verbalmente e fisicamente[21].

20. Ibidem.

21. PATEL, Nina Jane. *Fiction vs. Non-Fiction*. Publicado em 21 de dezembro de 2021. Disponível em: https://ninajanepatel.medium.com/fiction-vs-non-fiction-d824c6edfbe2. Acesso em 11 de janeiro de 2023.

No mesmo ano, a canadense Chanelle Siggens usou um dispositivo Oculus Quest para jogar o Population One, um jogo *multiplayer* de realidade virtual. Ao acessar a plataforma do jogo, enquanto aguardava o início de uma partida, um outro jogador simulou estar a apalpando e ejaculando em seu avatar. Ao pedir para que o avatar parasse de a assediar, o mesmo reagiu como se pudesse fazer o que quisesse, já que estava no metaverso[22].

É importante ressaltar que os atos ocorridos no ambiente virtual geram impactos no mundo real, uma vez que um dos objetivos do metaverso é proporcionar experiências do mundo real inclusive sob a ótica sensorial. A realidade virtual foi desenvolvida para que o corpo e a mente não façam distinção entre as experiências vividas no mundo virtual e no mundo real[23]. Sendo assim, ao passar por essa experiência no ambiente virtual, Nina e Chanelle sofreram como se estivessem passando pelas mesmas situações no mundo real.

2.2. Aliciamento de menores no metaverso: a investigação da BBC no VRChat

Em 2022, uma pesquisadora da BBC News acessou o metaverso do VRChat, um aplicativo direcionado a maiores de 13 anos. Ao criar a sua conta, utilizou dados falsos com o intuito de se passar por uma criança e ver como é a experiência proporcionada pela plataforma a uma pessoa dessa faixa etária.

Ao acessar o metaverso, a pesquisadora identificou que havia ambientes comuns e de livre acesso, mas também havia ambientes direcionados a adultos. Para sua surpresa, crianças circulavam livremente em ambientes de adultos e eram encorajadas por outros usuários a participar de atividades sexuais, sem qualquer tipo de moderação ou filtro.

Em suas palavras, apesar da plataforma ter também um direcionamento a jovens menores de idade, parecia muito mais um "*playground* para adultos do que para crianças", com muitos ambientes com atmosfera erótica e que poderiam ser acessados por qualquer usuário[24].

22. FRENKEL, Sheera. BROWNING, Kellen. *The Metaverse's Dark Side: Here Come Harassment and Assaults*. Publicado em 30 de dezembro de 2021. Disponível em: https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html. Acesso em 11 de janeiro de 2023.

23. MOURA, Tathiany Rezende de, *et al*. Influência da realidade virtual sobre a percepção corporal: relato de caso. Publicado em 2015. Disponível em: https://www.metodista.br/revistas/revistas-unimep/index.php/sr/article/view/2256/1462. Acesso em 11 de janeiro de 2023.

24. CRAWFORD, Angus. SMITH, Tony. Crianças entram em clubes de strip virtuais com app do Metaverso, revela investigação da BBC. Publicado em 2 de março de 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60500772. Acesso em 11 de janeiro de 2023.

3. Moderação no metaverso e os obstáculos do provedor de aplicação

Diante do exposto, vemos que o mundo digital reflete os problemas reais do mundo físico. Portanto, apesar do ambiente ser novo, as interações - inclusive violações - não são tão novas. Ao fornecer uma plataforma para interação entre terceiros, é crível esperar que vá ocorrer violações de toda e qualquer natureza.

Nesse contexto, surge a necessidade da moderação do conteúdo imputado por terceiros no ambiente digital. Assim, a plataforma digital se depara com duas possibilidades: se autorregular ou esperar uma regulamentação do poder público?

Se por um lado, há o perigo de permitir que o poder público tome a iniciativa de regulamentação da moderação de conteúdo em plataformas digitais, podendo adotar medidas extremamente conservadoras em prol da ordem pública[25], a ausência de qualquer tipo de moderação nesses ambientes as torna inseguras e pouco interessantes para os possíveis usuários, prejudicando o objetivo econômico da plataforma digital.[26]

Fato é que a moderação de conteúdo é de total interesse da plataforma, razão pela qual muitas optam por se autorregular, sem desconsiderar também a regulação em razão da legislação vigente. Assim, o controle de conteúdo no ambiente digital pode ocorrer por determinação legal ou em razão da violação de políticas de conteúdo[27].

A moderação por força de lei está intrinsecamente conectada ao conceito de responsabilidade civil. Ao determinar que um agente deve moderar um determinado conteúdo, diretamente ou em condições específicas, a legislação entende que este é também responsável pela veiculação daquele conteúdo, uma vez que, caso não o remova, estará descumprindo a própria lei. Apesar disso, ao condicionar a responsabilização do provedor de aplicação, o legisla-

25. KLONICK, Kate. The New Governors: The People, Rules, and Processes Governing Online Speech. Publicado em abril de 2018. Disponível em: https://harvardlawreview.org/print/vol-131/the-new-governors-the-people-rules-and-processes-governing-online-speech/. Acesso em 30 de abril de 2023.

26. ESTARQUE, Marina. ARCHEGAS, João Victor. Redes sociais e moderação de conteúdo: criando regras para o debate público a partir da esfera privada. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/Relatorio_RedesSociais-ModeracaoDeConteudo.pdf. Acesso em 30 de abril de 2023.

27. MONTEIRO, Artur Péricles Lima, et al. Armadilhas e Caminhos na Regulação de Conteúdo. Disponível em: https://internetlab.org.br/wp-content/uploads/2021/09/internetlab_armadilhas-caminho-moderacao.pdf. Acesso em 30 de abril de 2023.

dor também reconhece a incapacidade técnica deste em realizar a moderação prévia e massiva do conteúdo.

Já a moderação por políticas de conteúdo tem como base as diretrizes criadas pela própria empresa responsável pelo mundo virtual, que podem englobar não só restrições impostas pela própria lei, como também atos que são considerados tipicamente lícitos, mas que - por opção da empresa - devem ser restringidos. Assim, as políticas de conteúdo são os principais instrumentos da autorregulação no ambiente digital, uma vez que tem por objetivo não somente criar diretrizes para remoção de conteúdo, mas também conscientizar e educar o próprio usuário quanto a noção de "conteúdo irregular" e a necessidade de sua remoção, lhe oferecendo, inclusive, canais para denúncia de conteúdo irregular[28].

3.1. Marco Civil da Internet: a responsabilidade do provedor de aplicações de internet por conteúdo de terceiro

Para a análise da moderação por força de lei, é importante destacar a definição de "aplicação da internet" contida no Marco Civil da Internet, qual seja: "Art. 5º Para os efeitos desta Lei, considera-se: (...) VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet."

Da exegese do conceito de "aplicação da internet" previsto em lei, entende-se que provedor de aplicação é aquele que fornece um "conjunto de funcionalidades que podem ser acessadas através de um terminal conectado à internet". Considerando o entendimento de que o mundo virtual é uma plataforma, é possível classificar o provedor do mundo virtual como o provedor de aplicação.

Partindo desse conceito, destaca-se o *caput* do art. 19 do Marco Civil da Internet:

> 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

28. SILVA, Thays Bertoncini da. Critérios para moderação e remoção de conteúdo da internet. Publicado em 06 de fevereiro de 2023. Disponível em: https://www.migalhas.com.br/depeso/381066/criterios-para-moderacao-e-remocao-de-conteudo--da-internet. Acesso em 30 de abril de 2023.

> 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.

Portanto, a classificação de provedor do ambiente virtual como um provedor de aplicações de internet dá a este uma responsabilidade subjetiva[29] no que se refere ao controle do conteúdo e das informações criadas por terceiros e veiculadas na plataforma, ou seja, o provedor de aplicação necessariamente precisará ter agido de maneira negligente, imprudente ou imperita[30]. Para que a culpa seja existente, o provedor de aplicação precisa descumprir uma ordem judicial.

Em um cenário de ocorrência de dano no ambiente virtual, o indivíduo que sofreu o dano necessariamente precisa recorrer ao judiciário para ter acesso a uma decisão judicial e só assim, poderá cessar o ato ilícito. Entre a identificação do ato ilícito e a publicação da decisão judicial necessária, há um período contínuo de ocorrência do dano. Assim como nas interações no mundo real, há questões que precisam ser moderadas de forma imediata.

Nesse sentido, o art. 21 do Marco Civil da Internet prevê o *notice and take-down* com o objetivo de promover a retirada imediata de conteúdo pornográfico de usuários divulgado de forma não autorizada mediante simples envio de notificação extrajudicial[31]. Tal medida visa impedir a circulação de conteúdo de pornografia de vingança. No entanto, restringe-se a conteúdo de teor erótico.

Sendo assim, a legislação atual não engloba a determinação de retirada de qualquer conteúdo que esteja violando algum direito líquido e certo, ficando a cargo do provedor de aplicação criar sistemas ou não para remover conteúdo

29. A responsabilidade subjetiva baseia-se na culpa. Assim, além do nexo causal e do dano, é necessário que o agente tenha tido culpa para a ocorrência do resultado, a qual deve ser apurada a partir da identificação de condutas negligentes, imprudentes ou imperitas.

30. TEPEDINO, Gustavo. VALVERDE, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. Fundamentos do direito civil: responsabilidade civil. Rio de Janeiro, 2ª edição. Forense. 2021, p. 31.

31. Marco Civil da Internet. Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

ofensivo sem a necessidade de ordem judicial. Desse modo, o texto legal atual permite que o provedor de aplicação ocupe um estado de omissão opcional de controle de conteúdo, que pode ser altamente lesiva para os usuários do metaverso.

Não obstante o exposto, deve-se destacar que o modelo de responsabilidade civil atribuído ao provedor de aplicação pelo Marco Civil da Internet é de suma importância para evitar excessos da autorregulação, uma vez que a ausência deste significaria a atribuição total de uma responsabilidade civil objetiva. Tal atribuição não só poderia incentivar o monitoramento e a moderação massiva de conteúdo à exclusivo critério do próprio provedor, como também criaria um cenário de arbitrariedade em favor do provedor, que passaria a ter a opção de moderar conteúdo que, apesar de controverso, não fosse necessariamente lesivo ou ilícito[32].

3.2. Políticas de Conteúdo: uma alternativa ao controle de conteúdo previsto em lei

Além do controle de conteúdo previsto em lei, que exige uma ordem judicial específica na maioria das vezes[33], é possível que a moderação de conteúdo se dê de forma autônoma, com base na política de conteúdo estabelecida pelo próprio provedor de aplicação. Uma política de conteúdo traz mais segurança para a plataforma, já que esclarece aos usuários os parâmetros para que este possa a usar de modo regular.

Assim, a política de conteúdo versa sobre a regularidade de um conteúdo publicado por terceiro na plataforma de aplicação, que pode contemplar também a legalidade. Ao incluir em sua política a restrição a atos que também sejam ilegais, o provedor de aplicação torna este ato também irregular. A classificação conjunta de um ato como irregular facilita a sua moderação, já que a ilegalidade não necessariamente é evidente e eventualmente, poderá necessitar de apreciação na esfera judicial. Já o conteúdo efetivamente irregular poderá ser retirado com base somente na violação da política de conteúdo, sem a necessidade de ter uma decisão judicial.

32. TEFFÉ, Chiara Spadaccini de. Responsabilidade Civil de Provedores na Rede: Análise da Aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. Disponível em: https://www.migalhas.com.br/depeso/381066/criterios-para-moderacao-e-remocao-de-conteudo-da-internet. Acesso em 30 de abril de 2023.

33. Destaque-se a exceção para casos de remoção de conteúdo pornográfico não autorizado, o qual não depende de ordem judicial e sim, de mera notificação.

O uso da política é extremamente eficaz para a proteção de direitos líquidos e certos, mas o seu sucesso depende essencialmente da capacidade de moderação de conteúdo pela plataforma. Isto é, a capacidade do provedor de receber e analisar inúmeras denúncias em tempo razoável para agir de modo a coibir a prática de atos irregulares no mundo virtual, que acaba se mostrando o grande desafio no campo da moderação de conteúdo.

Com isso, a moderação por políticas internas pode ser feita proativamente, por sistemas automatizados ou manualmente. A moderação manual exige mão-de-obra, razão pela qual não é uma primeira opção. Assim, esbarramos no desafio da moderação automatizada, que nos mostra que a evolução do metaverso vem com a evolução geral da tecnologia. Se por um lado hoje somos capazes de construir mundos digitais, há também novas formas de burlar o controle no ambiente digital.

Dentre esses, destaca-se a *hash poisoning*, que consiste na manipulação do *hash* que identifica o conteúdo violador, com o intuito de confundir o sistema e assim, resultar em inúmeros falsos positivos, podendo inviabilizar o próprio sistema de moderação[34]. Além disso, há também a dificuldade no mapeamento das violações e atuação em tempo real

Portanto, a moderação proativa em um mundo (ainda que digital) é um desafio sem precedentes, razão pela qual não pode ser exigida de forma prévia, sob o risco de inviabilizar a própria evolução do metaverso. No entanto, a ausência de qualquer moderação ou a morosidade no controle de conteúdo irregular acaba transformando o ambiente digital em um terreno fértil para a ocorrência de atos ilícitos.

3.3. Lei Geral de Proteção de Dados Pessoais: consentimento do titular e os dados pessoais no metaverso

Para que o indivíduo tenha toda a experiência sensorial do metaverso, de forma completa e funcional, uma série de dados pessoais é captada e processada de forma massiva, o que gera uma preocupação quanto a forma de obtenção e tratamento destes dados[35]. De acordo com a advogada Marcela Joel-

34. MONTEIRO, Artur Péricles Lima. Desafios e oportunidades da moderação de conteúdo no metaverso. Disponível em: https://itsrio.org/wp-content/uploads/2022/12/relatorio-diVerso_Desafiosoportunidades-modera%C3%A7%C3%A3o-conteudo-V4.pdf. Acesso em 12 de janeiro de 2023.

35. ROMAN, Juliana. FERREIRA, Rafaela. VIEIRA, Victor. Proteção de dados pessoais da realidade virtual à aumentada:

sons, o uso de um óculos de realidade aumentada pelo período de 20 minutos pode fazer com que sejam captados mais de 20 milhões de dados pessoais, que incluem as reações do indivíduo, sua biometria e seu comportamento[36].

Ao usar um *gadget* de realidade virtual, a cada reação, seu usuário fornece uma nova fonte de dados que poderá ser registrada e tratada pelo seu controlador e/ ou operador[37]. Assim, ao fazer qualquer coleta de dado pessoal, a plataforma de metaverso já está sujeita à Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais ("LGPD" e por essa razão, já cabe a ela adotar as medidas necessárias para se adequar às determinações da LGPD[38]. Nesse contexto, surge a necessidade da autorregulação através de políticas institucionais que versem sobre a privacidade e o tratamento dos dados pessoais desses titulares no ambiente do metaverso. Quando falamos de dados pessoais, é essencial falarmos também da importância das Políticas de Privacidade e Tratamento de Dados e da necessidade de avaliarmos a validade do consentimento dado por esses titulares quanto a coleta e tratamento dos seus dados pessoais.

De acordo com uma pesquisa feita pela instituição britânica ThinkMoney em 2020, 90% das pessoas aceitavam os termos e condições de uso de plataformas digitais sem os ler[39]. Na mesma linha, a empresa de auditoria Deloitte[40] efetuou uma pesquisa onde constatou que 91% dos norte-americanos não leem as políticas institucionais, incluindo a política de privacidade[41]. Portanto,

---

boas práticas internacionais. Disponível em: https://irisbh.com.br/wp-content/uploads/2023/01/Protecao-de-dados-da-realidade-virtual-a-aumentada-IRIS.pdf. Acesso em 30 de abril de 2023.

36. PRÓXIMO NÍVEL. Metaverso exigirá mais cuidados com proteção de dados. Publicado em 01 de julho de 2022. Disponível em: https://proximonivel.embratel.com.br/lgpd-metaverso-exigira-mais-cuidado-com-protecao-de-dados/. Acesso em 30 de abril de 2023.

37. Deve-se ressaltar que a atribuição da posição de controlador e/ ou operador de dados pessoais depende da função desempenhada por este, podendo o operador também ser o controlador e vice-versa, a depender de cada caso.

38. SILVA, Mariana Maria. Metaverso: como seus dados serão protegidos na abordagem da Lei Geral de Proteção de Dados. Publicado em 10 de agosto de 2022. Disponível em: https://exame.com/future-of-money/metaverso-como-seus-dados-serao-protegidos-na-abordagem-da-lei-geral-de-protecao-de-dados/. Acesso em 30 de abril de 2023.

39. L8. LGPD: por que ler os termos de uso é tão importante? Disponível em: https://www.l8group.net/lgpd-por-que-ler-os-termos-de-uso-e-tao-importante/. Acesso em 30 de abril de 2023.

40. Associação de Empresas e Profissionais da Informação – ABEINFO. É fundamental ler contratos, termos de uso e políticas de privacidade. Publicado em 30 de outubro de 2020. Disponível em: https://abeinfobrasil.com.br/e-fundamental-ler-contratos-termos-de-uso-e-politicas-de-privacidade/. Acesso em 30 de abril de 2023.

41. TELLES, Fernando. 90% das pessoas não leem termos e condições de apps, revela estudo. Publicado em 23 de dezembro de 2020. Disponível em: https://www.showmetech.com.br/pessoas-nao-leem-termos-e-condicoes-de-apps/. Acesso em 30 de abril de 2023.

se a grande maioria dos usuários não lêem as políticas institucionais dessas empresas – seja em razão da complexidade delas ou por falta de interesse – há que se questionar o grau de validade do consentimento dado por estes usuários.

O consentimento dado sem o devido conhecimento de com o que está se consentindo abre a possibilidade de um excesso de coleta e tratamento de dados pessoais[42], prejudicando a própria privacidade do usuário, na medida em que o responsável pela coleta e tratamento destes dados se sente confortável para incluir o que for de seu interesse nestas políticas, ainda que a coleta de um dado ou outro não seja especificamente necessária. Essa situação de conforto se dá devido a certeza de que a grande maioria dos usuários não lerão estas políticas e que o consentimento, ainda que sem qualquer mínimo indício de leitura do teor da política, será considerado válido.

Considerações finais

O metaverso é uma extensão do mundo real e ao mesmo tempo, um espelho da nossa realidade. Ao transferirmos situações da vida real ao metaverso, nos deparamos com os mesmos problemas já existentes na nossa realidade, mas em um ambiente digital. Apesar do ambiente não ser físico, os efeitos das interações - sejam bons ou ruins - acabam refletindo na na realidade.

Como dito, apesar de não termos um metaverso efetivamente amplo e sim, metaversos restritos a determinados mundos digitais, já é possível identificar graves violações de direitos e a ocorrência de crimes nestes ambientes. A mera possibilidade - para além da ocorrência destes atos ilícitos - já é suficiente para justificar a necessidade de moderação sistêmica do metaverso, dentro da capacidade do seu provedor. No entanto, a exigência efetiva de uma moderação prévia é incompatível com o próprio objetivo do metaverso, bem como poderia causar um ambiente digital sujeito a censura.

No mundo real, não há moderação ou controle prévio, há apenas medidas que visam atenuar os efeitos de um dano sofrido ou punir pelo cometimento de um crime. Por ser um espelho da realidade, a moderação prévia no metaverso

42. Algo similar ocorre no CadÚnico, o principal instrumento de consolidação de dados pessoais e gestão do Bolsa Família, uma vez que os dados contidos no CadÚnico são usados para definir os beneficiários do programa em questão. A necessidade de submissão de dados pessoais para fazer parte de um programa tão fundamental já coloca o titular desses dados em uma posição de vulnerabilidade, já que este não vai se opor ao uso, tratamento e divulgação exacerbada de seus dados pessoais, já que necessita ter acesso ao programa social. Ver mais em: https://internetlab.org.br/pt/artigos/bolsa-familia--pensando-a-privacidade-das-titulares/

torna-se impossível. Todavia, não significa que seja impossível ter qualquer tipo de moderação no mundo digital - muito pelo contrário, a moderação no mundo digital é necessária. O grande desafio é: como moderar de forma eficaz?

Se, por um lado, temos o Marco Civil da Internet, que prevê em seu art. 19 a responsabilidade de moderação de conteúdo de uma plataforma ao provedor de aplicação, também prevê a exigência de decisão judicial para que o provedor atue, o que torna a medida ineficaz no metaverso. Se um indivíduo sofre uma difamação no ambiente digital, será necessário que este recorra ao judiciário no mundo físico para obter uma ordem judicial e só assim, o provedor de aplicação deverá tomar as devidas atitudes contra o indivíduo que o difamou e eventualmente, apagar o conteúdo difamatório, se ainda houver. Entre o período da identificação do ato ilícito e a moderação efetiva, há um longo caminho a ser percorrido e a morosidade pode simplesmente deixar o usuário infrator impune ou não ser mais efetiva, em razão do decurso do tempo.

Já a moderação por políticas de conteúdo se mostra mais eficaz na medida em que não depende de uma decisão judicial prévia. No entanto, esbarra nas limitações técnicas do próprio provedor em oferecer uma reação rápida e imediata a atos ilícitos ocorridos em tempo real. Além disso, a moderação geral, com uma resposta rápida, depende essencialmente de um monitoramento contínuo de todas as interações que ocorrem na plataforma, que se mostra um grande desafio quando falamos de mundos digitais gigantescos e populosos.

Fato é que a moderação total e perfeita é impossível. Por ser uma extensão da realidade física, é impossível ter um controle absoluto do mundo digital. Isso não significa que não há a necessidade de exigir medidas mínimas a fim de mitigar a ocorrência de atos ilícitos no metaverso. Um exemplo é a Safe Zone[43] criada no Meta Horizon Worlds, que funciona como um "espaço de fuga" ao usuário, no qual ele poderá inclusive reportar imediatamente qualquer violação que tenha sofrido ou identificado. No caso do VRChat, o provedor identificou o uso de modificadores de sistema que facilitavam o cometimento de violações na plataforma, razão pela qual passou a proibir o uso destes e banir todos os usuários que foram identificados com modificadores. Tais medidas,

43. Ver mais em: https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/safe-zone-in--horizon/

apesar de não serem efetivamente direcionadas, já nos dão um caminho por onde seguir.

Se a moderação caso a caso é complexa, a saída é criar alternativas genéricas e restrições contundentes para evitar a ocorrência de práticas ilícitas no ambiente digital. No campo legislativo, há a necessidade de adequação ao metaverso, que não pode ter uma moderação condicionada ou meramente opcional. É necessário estabelecer a exigência de padrões mínimos, como canais eficazes de denúncias, criação de espaços seguros, dentre outros. Assim, com a evolução do metaverso, o campo jurídico deverá o acompanhar a fim de tornar o mundo digital uma extensão segura do mundo real.

Referências

ANDRADE, Renato. **Metaverso: A próxima fronteira da inovação**. 1ª Edição. E-Book Kindle, 2022.

Associação de Empresas e Profissionais da Informação – ABEINFO. É fundamental ler contratos, termos de uso e políticas de privacidade. Publicado em 30 de outubro de 2020. Disponível em: https://abeinfobrasil.com.br/e-fundamental-ler-contratos-termos-de-uso-e-politicas-de-privacidade/. Acesso em 30 de abril de 2023.

BRASIL. **Lei nº 12.965/2014 – Marco Civil da Internet**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso 12 de janeiro de 2022.

CRAWFORD, Angus. SMITH, Tony. **Crianças entram em clubes de strip virtuais com app do Metaverso, revela investigação da BBC**. Publicado em 2 de março de 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60500772. Acesso em 11 de janeiro de 2023.

Drummond, Julia. Valente, Mariana. Neris, Natália. Fragoso, Nathalie. **Bolsa família: pensando a privacidade das titulares**. Publicado em 12 de maio de 2020. Disponível em: https://internetlab.org.br/pt/artigos/bolsa-familia-pensando-a-privacidade-das-titulares/. Acesso em 30 de abril de 2023.

ESTARQUE, Marina. ARCHEGAS, João Victor. R**edes sociais e moderação de conteúdo: criando regras para o debate público a partir da esfera privada**. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/Relatorio_RedesSociaisModeracaoDeConteudo.pdf. Acesso em 30 de abril de 2023.

FERNANDES, Victor. **Realidade virtual será segmento de US$ 50 bilhões até 2030.** Publicado em 03 de agosto de 2022. Disponível em: https://www.panrotas.com.br/mercado/tecnologia/2022/08/realidade-virtual-sera-segmento-de-us-50-bilhoes-ate-2030_191032.html. Acesso em 11 de janeiro de 2023.

FRENKEL, Sheera. BROWNING, Kellen. **The Metaverse's Dark Side: Here Come Harassment and Assaults**. Publicado em 30 de dezembro de 2021. Disponível em: https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html. Acesso em 11 de janeiro de 2023.

HAHNE, Stephanie. **Travis Scott faz história com show épico e virtual no jogo "Fortnite"**. Publicado em 24 de abril de 2020. Disponível em: https://www.tenhomaisdiscosqueamigos.com/2020/04/24/travis-scott-fortnite/. Acesso em 05 de janeiro de 2023.

L8. **LGPD: por que ler os termos de uso é tão importante?** Disponível em: https://www.l8group.net/lgpd-por-que-ler-os-termos-de-uso-e-tao-importante/. Acesso em 30 de abril de 2023.

MARTINS, Patricia Helena Marta. FONSECA, Victor Cabral. SEREC, Fernando Eduardo. **Metaverso: Aspectos Jurídicos**. São Paulo. Editora Almedina, 2022.

META. ***Introducing Oculus Quest 2, the Next Generation of All-in-One VR***. Publicado em 16 de setembro de 2020. Disponível em: https://about.fb.com/news/2020/09/introducing-oculus-quest-2-the-next-generation-of-all-in-one-vr/. Acesso em 11 de janeiro de 2023.

MONTEIRO, Artur Péricles Lima, *et al*. **Armadilhas e Caminhos na Regulação de Conteúdo**. Disponível em: https://internetlab.org.br/wp-content/uploads/2021/09/internetlab_armadilhas-caminho-moderacao.pdf. Acesso em 30 de abril de 2023.

MONTEIRO, Artur Pericles Lima. **Desafios e oportunidades da moderação de conteúdo no metaverso**. Disponível em: https://itsrio.org/wp-content/uploads/2022/12/relatorio-diVerso_Desafiosoportunidades-modera%C3%A7%C3%A3o-conteudo-V4.pdf. Acesso em 12 de janeiro de 2023.

MOURA, Tathiany Rezende de, *et al*. **Influência da realidade virtual sobre a percepção corporal: relato de caso**. Publicado em 2015. Disponível em: https://www.metodista.br/revistas/revistas-unimep/index.php/sr/article/

view/2256/1462. Acesso em 11 de janeiro de 2023.

IFOOD. **Futuro do consumo: o que é VR Commerce?**. Publicado em 02 de março de 2022. Disponível em: https://news.ifood.com.br/futuro-do-consumo-o-que-e-vr-commerce/. Acesso em 30 de abril de 2022.

ONIRIA. **Como usar realidade virtual (VR) para treinamentos?** Disponível em: https://oniria.com.br/como-usar-realidade-virtual-vr-para-treinamentos/. Acesso em 11 de janeiro de 2023.

PATEL, Nina Jane. ***Fiction vs. Non-Fiction***. Publicado em 21 de dezembro de 2021. Disponível em: https://ninajanepatel.medium.com/fiction-vs-non-fiction-d824c6edfbe2. Acesso em 11 de janeiro de 2023.

PRÓXIMO NÍVEL. **Metaverso exigirá mais cuidados com proteção de dados**. Publicado em 01 de julho de 2022. Disponível em: https://proximonivel.embratel.com.br/lgpd-metaverso-exigira-mais-cuidado-com-protecao-de-dados/. Acesso em 30 de abril de 2023.

ROAD TO VR. **Quest Store surpasses $1.5 Billion in Content Revenue, Showing Continue Growth**. Publicado em 18 de outubro de 2022. Disponível em: https://www.roadtovr.com/oculus-quest-store-revenue-1-billion-milestone-growth-meta/. Acesso em 11 de janeiro de 2023.

ROMAN, Juliana. FERREIRA, Rafaela. VIEIRA, Victor. **Proteção de dados pessoais da realidade virtual à aumentada: boas práticas internacionais**. Disponível em: https://irisbh.com.br/wp-content/uploads/2023/01/Protecao-de-dados-da-realidade-virtual-a-aumentada-IRIS.pdf. Acesso em 30 de abril de 2023.

SECOND LIFE. ***Remote Work and Event Solutions:*** https://www.connect.secondlife.com/about. Acesso em 12 de janeiro de 2023.

SERRA, Maysa Venturoso Gongora Buckeridge Serra, *et al*. **Realidade Virtual para Pessoas com Deficiência: O Uso do Vídeo Game como Prática de Lazer**. LICERE - Revista do Programa de Pós-graduação Interdisciplinar em Estudos do Lazer, [S. l.], v. 21, n. 4, p. 529–548, 2018. DOI: 10.35699/1981-3171.2018.1952. Disponível em: https://periodicos.ufmg.br/index.php/licere/article/view/1952. Acesso em 11 de janeiro de 2023

SILVA, Mariana Maria. **Metaverso: como seus dados serão protegidos na abordagem da Lei Geral de Proteção de Dados**. Publicado em 10 de agosto de 2022. Disponível em: https://exame.com/future-of-money/metaverso-como-seus-dados-serao-protegidos-na-abordagem-da-lei-geral-de-protecao-de-dados/. Acesso em 30 de abril de 2023.

SILVA, Thays Bertoncini da. **Critérios para moderação e remoção de conteúdo da internet**. Publicado em 06 de fevereiro de 2023. Disponível em: https://www.migalhas.com.br/depeso/381066/criterios-para-moderacao-e-remocao-de-conteudo-da-internet. Acesso em 30 de abril de 2023.

Smart, J.M., Cascio, J. and Paffendorf, J., ***Metaverse Roadmap Overview***, 2007. Disponível em: https://www.metaverseroadmap.org/overview/. Acesso em 11 de janeiro de 2023.

TEFFÉ, Chiara Spadaccini de. **Responsabilidade Civil de Provedores na Rede: Análise da Aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça**. Disponível em: https://www.migalhas.com.br/depeso/381066/criterios-para-moderacao-e-remocao-de-conteudo-da-internet. Acesso em 30 de abril de 2023.

TELLES, Fernando. **90% das pessoas não leem termos e condições de apps, revela estudo**. Publicado em 23 de dezembro de 2020. Disponível em: https://www.showmetech.com.br/pessoas-nao-leem-termos-e-condicoes-de-apps/. Acesso em 30 de abril de 2023.

TEPEDINO, Gustavo. VALVERDE, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil: responsabilidade civil**. Rio de Janeiro, 2ª edição. Forense. 2021.

VALENTINA, Rebekah. ***Travis Scott reportedly***

grossed roughly $20m for Fortnite concert appearance. Publicado em 01 de dezembro de 2020. Disponível em: https://www.gamesindustry.biz/travis-scott-reportedly-grossed-roughly-usd20m-for-fortnite-concert-appearance. Acesso em 05 de janeiro de 2023.

WINTERS, Terry. ***The Metaverse: Buying Virtual Land, NFTS, WEB3 & Preparing for the Next Big Thing***. 2021. E-Book Kindle.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

2

A investida do órgão regulador para as plataformas digitais: vozes a favor e contra no debate sobre o PL 2630/2020

CELINA CARVALHO E GIOVANA CARNEIRO

Introdução

Na década passada, o otimismo marcou a visão popular a respeito da internet, sendo uma grande promessa para o debate livre, plural e democrático de ideias. À época, eventos como a Primavera Árabe sobressaíram no imaginário coletivo com demonstrativo da capacidade das redes sociais para oferecer uma ferramenta de mobilização social. O recorte contrasta com o panorama atual. Acontecimentos como o escândalo da Cambridge Analytica,[3] a invasão no capitólio em 2021 nos Estados Unidos[4] e, a nível nacional, os episódios antidemocráticos de 8 de janeiro de 2023 e as subsequentes ameaças de ataques às escolas[5] alimentaram uma generalizada revolta contra as *Big Techs* e, por consequência, a pressão para a intervenção estatal.

Com isso, diversas respostas e soluções foram desenhadas com um sentimento em comum: as atividades das empresas de tecnologia precisavam ser controladas – o chamado *techlash*.[6] A atuação puramente autorregulatória demonstrou-se insuficiente para promover uma adequada proteção de direitos

1. Advogada. Pós-Graduada em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade do Estado do Rio de Janeiro. Assistente acadêmico das disciplinas de Lei Geral de Proteção de Dados, Responsabilidade Civil dos Provedores de Internet e Direito do Consumidor da Internet da Pós-Graduação do Instituto de Sociedade do Rio de Janeiro (ITS Rio). Pesquisadora do Laboratório de Regulação Econômica da UERJ (UERJ Reg.).

2. Advogada. Mestre em Direito Público pela Universidade do Estado do Rio de Janeiro (UERJ). Graduada em Direito pela Universidade do Estado do Rio de Janeiro. Assistente acadêmico das disciplinas de Direito Internacional e Jurisdição da Internet e Contratos Eletrônicos da Pós-Graduação do Instituto de Sociedade do Rio de Janeiro (ITS Rio). Pesquisadora do Laboratório de Regulação Econômica da UERJ (UERJ Reg.).

3. CONFESSORE, Nicholas. *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. The New York Times, 04 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 28 abr. 2023.

4. SANCHES, Mariana. Invasão do Congresso nos EUA | 'Banho de sangue é inevitável às vezes': por dentro do ato que levou à invasão histórica e estado de emergência em Washington. BBC News Brasil, 07 jan. 2021. Disponível em: https://www.bbc.com/portuguese/internacional-55572422. Acesso em: 28 maio 2023.

5. Dino cobra de plataformas monitoramento sobre incitação à violência nas escolas. G1 Globo News, 07 abr. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/04/07/dino-cobra-de-plataformas-monitoramento-sobre-incitacao-a-violencia-nas-escolas.ghtml. Acesso em: 29 maio 2023.

6. Cunhado ao final de 2018, indica o movimento em prol da regulação das atividades de empresas de tecnologia. Ver: FOROOHAR, Rana. Year in a World: Techlash. Financial Times, [s.l.], [20--]. Disponível em: https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e. Acesso em: 23 maio 2023.

fundamentais na rede. Em seu lugar, cresce a importância de abordagens corregulatórias para o desenvolvimento seguro da "internet livre".[7] É nesse contexto, inclusive, que este artigo parte da premissa de que o espaço digital demanda algum grau de intervenção ordenadora do Estado.

No Brasil, a Lei Federal nº 12.965/2014 (Marco Civil da Internet - MCI) passou a garantir que a internet não seria uma "terra sem lei". Elaborado a partir de robusto processo de debate multissetorial, estabelece o regime de responsabilidade de intermediários dos provedores de aplicação no Brasil. Segundo seu artigo 19, os provedores de aplicação de internet não são responsáveis pelos atos de terceiros até que uma ordem judicial declare o conteúdo ilegal. Esse regime de responsabilidade aprovado em 2014 não ficou, contudo, imune às críticas. O criticismo atingiu seu ápice na discussão sobre a constitucionalidade do dispositivo a partir de recurso extraordinário protocolado em 2017, que aguarda julgamento no Supremo Tribunal Federal (STF).[8]

Nos anos seguintes, foram propostos diversos projetos de lei com o propósito de regulamentar a oferta de serviços e/ou produtos na internet no Brasil, dentre os quais se destacou o Projeto de Lei nº 2630/2020 (PL 2630).[9] Face ao processo eleitoral de 2020, foi apelidado de "PL das Fake News" e tinha sua justificativa voltada ao combate da desinformação e à proteção do processo eleitoral de agentes maliciosos.

O techlash não se restringiu ao Brasil. No âmbito da União Europeia, destacam-se os esforços realizados a partir de 2019 para a construção do pacote legislativo *Digital Services Package*, composto pelo *Digital Services Act* (DSA) e pelo *Digital Markets Act* (DMA).[10] Antes disso, a Lei Alemã (*Netzwerkdurch-*

7. KELLER, Clara Iglesias. Regulação nacional de serviços na Internet. Rio de Janeiro: Lumen Juris, 2019, pp. 174-175.

8. Para mais informações, ver RE 1037396, Rel. Min. Dias Toffoli. Disponível em <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em 8 de maio de 2023.

9. De autoria do Senador Alessandro Vieira, foi aprovado pelo Plenário do Senado Federal em 30 de junho de 2020. Na Câmara dos Deputados, o Dep. Orlando Silva foi designado como relator. Até o momento da elaboração do artigo, a versão do texto apresentada em 27 de abril de 2023 era a mais recente e, por isso, será a que nos basearemos ao citarmos seus dispositivos, salvo menção em contrário. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334>. Acesso em 26 de maio de 2023.

10. Abordados em mais detalhes na seção 2 do artigo, são os dois marcos europeus centrais à regulação do ambiente digital que inspiraram as atuais proposições discutidas no legislativo brasileiro.

setzungsgesetz - NetzDG)[11] estabeleceu, a partir de 2017, obrigações de transparência e de remoção expedita para as plataformas.

Exposto esse breve panorama, este artigo busca organizar parte da discussão em torno do "como" regular, mais especificamente expor os argumentos a favor e contra a figura de uma autoridade supervisora, que se tornou um dos elementos-chave do PL 2630. Para tanto, o trabalho está dividido como se segue. Na seção 1, tecemos breves apontamentos sobre a tramitação legislativa e os principais pontos do PL 2630, abordando o *status* da regulação das plataformas digitais no Brasil, com ênfase em seu arranjo institucional. Tendo em vista a inspiração das últimas versões do PL 2630 no DSA, apresentamos, na seção 2, o arranjo institucional nele previsto. Na sequência, na seção 3, mapeamos as propostas para autoridade supervisora que receberam mais atenção. Em sede de conclusão, indicamos a necessidade de um debate mais robusto sobre esse arranjo regulatório.

1. O contexto regulatório da internet no Brasil

Como mencionado, o PL 2630 marcou os últimos três anos como o expoente na regulação da internet. Este capítulo apresenta brevemente seu histórico de tramitação legislativo e questões que merecem mais cuidado, a fim de contextualizar a introdução da figura da autoridade. Importante mencionar, desde já, que por "autoridade" designamos um corpo institucional com atribuições de supervisão (não necessariamente de fiscalização e sanção), que *não* estão acopladas direta ou indiretamente nos provedores de aplicações sujeitos às disposições da lei. Assim, "autoridade" designa conselhos multissetoriais dos quais participam agentes estatais, entidades parte da Administração Pública direta ou indireta, e afins. Não designa, para fins deste trabalho, instituições ou conselhos formados na estrutura de agentes privados.

Em junho de 2020, o projeto foi aprovado no Senado Federal e encaminhado à Câmara dos Deputados. A versão do texto aprovada no Senado previa um

11. Para a lei alemã na íntegra, ver: ALEMANHA. [*Netzwerkdurchsetzungsgesetz* (2017)]. *Netzwerkdurchsetzungsgesetz* [2021]. Disponível em: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Acesso em: 28 maio 2023. Para um comparativo entre ela e as soluções regulatórias dispostas no MCI, ver: BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. Revista Direito FGV, v.19, 2023. Disponível em: https://www.scielo.br/j/rdgv/a/qwwzmCyw5FmFQmTpRw3HCQh/?format=pdf&lang=pt. Acesso em: 28 maio 2023.

Conselho de Transparência e Responsabilidade na Internet, com 21 conselheiros que se reuniriam na sede do Congresso Nacional e teriam suas despesas cobertas pelo Senado Federal.[12]

Em março de 2022, foi apresentado o primeiro substitutivo do PL na Câmara dos Deputados[13] com mira voltada às eleições presidenciais de outubro daquele ano. No entanto, o pedido de urgência foi rejeitado[14] e, assim, sua tramitação desacelerou - tendo um intervalo de mais de seis meses até nova movimentação. Naquela versão, o Comitê Gestor da Internet no Brasil (CGI.br), órgão de composição multissetorial existente desde 1995,[15] detinha a função de contribuir com estudos e diretrizes para autorregulação das plataformas, além de poder requerer informações a respeito das metodologias utilizadas para a detecção de desconformidades que motivaram a intervenção em contas e conteúdos por terceiros.

Recentemente, a pauta voltou a ganhar força, estimulada pelo Governo Federal,[16] em conjunto à pressão por respostas aos eventos antidemocráticos de 8 de janeiro de 2023 e às ameaças de ataques às escolas[17]. Nesse contexto, em 30 de março de 2023, o Governo Federal encaminhou ao Poder Legislativo

12. Cf. Artigos 26-29 do texto do PL 2630 aprovado pelo Senado Federal em 30 de junho de 2020. Senado Federal. PL 2630. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em 26 maio de 2023.

13. De autoria do Dep. Orlando Silva, Substitutivo apresentado em março de 2022. Disponível em: <https://www.camara.leg.br/midias/file/2022/03/fake.pdf>. Acesso em 26 maio de 2023.

14. A Câmara rejeita urgência para projeto que criminaliza fake news. G1 Globo, em 06.04.2022. Disponível em: <https://g1.globo.com/politica/noticia/2022/04/06/camara-rejeita-urgencia-para-projeto-que-criminaliza-fake-news.ghtml>. Acesso em: 29 de maio de 2023.

15. O CGI.br foi criado pela Portaria Interministerial nº 147/1995, à época publicada em conjunto pelo Ministério das Comunicações e Ministério da Ciência e Tecnologia. Ele foi pensado como um comitê multissetorial desde a sua concepção, cuja composição inclui representantes do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica. O Decreto Federal nº 4.829/2003 refina sua estrutura de governança, mantendo os assentos de diferentes setores e estabelecendo a eleição democrática dos representantes do terceiro setor e da comunidade científica e tecnológica. Conforme o artigo 1º do mesmo Decreto, algumas de suas atribuições são a proposição de estudos, de programas de pesquisa e diretrizes estratégicas, além da articulação de ações sobre a proposição de normas e procedimentos relativos à regulamentação de atividades realizadas na internet.

16. Dino diz que governo está desenvolvendo projeto para regulamentação de redes sociais. CNN Brasil, 13 de março de 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/dino-diz-que-governo-esta-desenvolvendo-projeto-para-regulamentacao-de-redes-sociais/>. Acesso em 26 maio de 2023.

17. Em reunião no Palácio do Planalto, o ministro Flávio Dino ressaltou a importância da regulação da internet para combater à violência nas escolas, tendo em vista que a organização dos ataque se dá por meio das redes sociais. Disponível em: <https://www.camara.leg.br/noticias/953831-regulacao-da-internet-e-essencial-para-combater-ataques-a-escolas-aponta-flavio-dino/>. Posteriormente, foi publicada do Ministério da Justiça e Segurança Pública que designa a Secretaria Nacional do Consumidor (SENACON) o poder de instaurar processo administrativo para apuração e responsabilização das plataformas de rede sociais, pelo eventual descumprimento do dever geral de segurança e cuidado em relação à propagação de conteúdos ilícitos, danos e nocivos que incentivem ataques contra ambiente escolar ou façam apologia e incitação a esses crimes ou a seus perpetradores, ver: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-edita-portaria-com-novas-diretrizes-para-redes-sociais-apos-ataques-nas-escolas/portaria-do-ministro_plataformas.pdf.

sua sugestão de redação ao projeto[18]. Divulgada de maneira não oficial, o texto incluía conceitos que não haviam sido objeto de debate até então, como a previsão de "entidade autônoma de supervisão" e questões envolvendo "riscos sistêmicos" e "dever de cuidado". A versão continha mais de 20 artigos inéditos em relação à anterior.

Em sequência, nos dias 18 e 25 de abril, novas versões extraoficiais do texto vieram a público, incorporando parte da proposta sugerida pelo governo. Ainda no dia 25 de abril, aprovou-se o requerimento de urgência para a votação do projeto cujo texto integral sequer fora formalmente discutido. Ambas continham dispositivos sobre a figura da entidade reguladora, trazida pelo Poder Executivo.

Logo após, em 27 de abril, o texto final do relator Deputado Orlando Silva retirou a previsão de criação de uma "entidade autônoma de supervisão", em seu parecer oficialmente apresentado ao Plenário da Câmara dos Deputados.[19] A justificativa seria a recepção negativa do dispositivo. O CGI.br permaneceu no texto com atribuições de pesquisa e elaboração de diretrizes para guiar a criação dos novos mecanismos de transparência previstos para regular a atuação das plataformas.

Na tentativa de fornecer respostas imediatas aos últimos episódios, o PL acabou por capturar as mais diversas discussões sobre a regulação da internet e ampliar seu escopo. A contar de sua concepção, o projeto acumulou diferentes facetas: regras para vincular a verificação de contas ao fornecimento de documento de identidade, previsões para a rastreabilidade de mensagens, ampliação da imunidade parlamentar para as redes sociais, remuneração aos veículos de imprensa pela utilização de conteúdo jornalístico, entre outras.[20]

O imaginário público reflete a confusão sobre o objeto do projeto. Relembra até a controvérsia viral que dividiu a internet em 2015, em que um grupo enxergava um vestido azul e preto, enquanto outros viam apenas dourado e

18. De autoria do Poder Executivo, apresentada em 30 de março de 2023, a proposta foi divulgada por vias não oficiais. Disponível em: <https://www.telesintese.com.br/wp-content/uploads/2023/03/Contribuicoes_PL2630.pdf>. Acesso em 26 maio de 2023.

19. De autoria do Dep. Orlando Silva, apresentado em 27 de abril de 2023. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334>.

20. Ver: PL das fake news: aprovado no Senado, entenda o que pode mudar. UOL Tilt, 30 de jun. de 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/06/30/com-44-votos-senado-aprova-pl-das-fake-news.ht>. ITS Rio. 9 pontos de atenção sobre o PL das Fake News (PL 2630/20), 31 de março de 2022. Disponível em: <https://itsrio.org/wp-content/uploads/2022/04/9-pontos-de-aten%C3%A7%C3%A3o-sobre-o-PL-das-Fake-News-PL-2630_20.pdf>. Acesso em 29 de maio de 2023.

branco - a proposta legislativa é alvo de interpretações conflitantes[21]. Para alguns, é o "PL da Censura",[22] que cria restrições excessivas às plataformas e viola o direito à liberdade de expressão por sua mera existência. Para outros, reflete uma intervenção bem-vinda e necessária para manter a ordem no ambiente digital e reduzir o poder das "*Big Techs*".[23]

Feitos comentários gerais sobre a tramitação do projeto, cabe explicar brevemente seu escopo de aplicação e as obrigações impostas aos provedores. Ao delimitar o escopo de aplicação da lei, o artigo 2º do PL 2630 limita sua abrangência àqueles que, "constituídos na forma de pessoa jurídica, ofertem serviços ao público brasileiro e exerçam atividade de forma organizada, e cujo número médio de usuários mensais no país seja superior a 10.000.000 (dez milhões)". Nesse sentido, incluiu-se (i) redes sociais; (ii) ferramentas de busca; (iii) mensageria instantânea e, (iv) para fins de remuneração pelos conteúdos protegidos por direitos autorais, os provedores de aplicações de conteúdo por demanda, todos definidos no artigo 5º.[24]

No que tange às obrigações impostas, o Capítulo II, "Da Responsabilização dos Provedores", por meio dos artigos 6º e ss., estabelece que os provedores podem ser responsabilizados por danos decorrentes de conteúdos gerados por terceiros, quando houver descumprimento das obrigações de dever de cuidado. Isto é, devem agir diligentemente para previr e mitigar práticas ilícitas no âmbito de seus serviços, na forma do artigo 11 do projeto. De forma complementar, impõem-se o dever de identificar diligentemente os riscos sistêmicos decorrentes da concepção ou do funcionamento de seus serviços (artigo 7 do projeto), a necessidade de identificar o anunciante (artigo 26 do projeto) e, ainda, de remuneração por conteúdos jornalísticos (artigo 32 do projeto).

No final, a difusão de diferentes versões extraoficiais e introdução de tópicos sem amplo debate parece ter contribuído para a oposição à previsão. Nas

21. Debate sobre a cor de um vestido domina redes sociais. Veja, 27 de fev. 2015. Disponível em: <https://veja.abril.com.br/cultura/debate-sobre-a-cor-de-um-vestido-domina-redes-sociais>. Acesso em 29 de maio de 2023.

22. NOVO. 5 armadilhas do Projeto de Lei 2630, o "PL da Censura", 27 abr. 2023. Disponível em: <https://novo.org.br/5-armadilhas-do-projeto-de-lei-2630-ou-pl-da-censura/>. Acesso em 29 maio de 2023.

23. Estela Aranha: Marco Civil falhou com as redes sociais. Convergência Digital, 27 jan. 2023.Disponível em: <https://www.convergenciadigital.com.br/Internet/Estela-Aranha%3A-Marco-Civil-falhou-com-as-redes-sociais-62382.html>. Acesso em 1º jun. 2023.

24. Excluem-se os provedores cuja atividade primordial seja de comércio eletrônico, para a realização de reuniões fechadas por vídeo ou voz, enciclopédias online sem fins lucrativos, repositórios científicos e educativos, plataformas de desenvolvimento e compartilhamento de software de código aberto, busca e disponibilização de dados obtidos do poder público, e plataformas de jogos e apostas online.

palavras de João Brant, secretário de Políticas Digitais da Secretaria de Comunicação da Presidência da República, o modelo de autoridade regulatória ainda "estava amadurecendo" entre os integrantes do governo.[25] Abaixo, confeccionamos um quadro para ilustrar as versões - oficiais e extraoficiais - apresentadas desde a chegada do projeto à Câmara dos Deputados para auxiliar na compreensão da sua tramitação no que tange à previsão da autoridade.

Tabela 1 - Autoridade estatal nas versões do PL 2630

Data do PL (versões oficiais segundo o portal da Câmara dos Deputados; versões extraoficiais estimadas)	03/07/2020 (versão oficial disponível no portal da Câmara dos Deputados)	31/03/2022 (versão oficial disponível no portal de notícias da Câmara dos Deputados)	30/03/2023 (versão proposta **pelo Governo**, disponibilizada extraoficialmente)	18/04/2023 (versão extraoficial compartilhada em fóruns especializados)	25/04/2023 (versão extraoficial compartilhada em fóruns especializados)	27/04/2023 (versão oficial disponível no portal da Câmara dos Deputados)
Tipo de documento	Apresentação pelo Senado Federal.	Apresentação de Substitutivo pelo Deputado Orlando Silva.	Minuta de substitutivo (proposta pelo Governo)	Novo documento	Novo documento	Parecer Preliminar de Plenário n. 1 PLEN, pelo Deputado Orlando Silva. (após aprovação do regime de urgência, em 25/04/2023)
Autoridade estatal	Conselho de Transparência e Responsabilidade na Internet (Art. 25-29), instituído pelo Congresso Nacional	Atribuições ao Comitê Gestor da Internet no Brasil (CGI.br), já existente (Art. 33-34)	Entidade autônoma de supervisão a ser estabelecida pelo Poder Executivo (Art. 39-43 e 49)	Atribuições ao Comitê Gestor da Internet no Brasil (CGI.br), seguidas pela criação de uma entidade autônoma de supervisão a ser estabelecida pelo Poder Executivo (Art. 55-58)	Atribuições ao Comitê Gestor da Internet no Brasil (CGI.br), seguidas pela criação de uma entidade autônoma de supervisão a ser estabelecida pelo Poder Executivo (Art. 55-58)	Atribuições ao Comitê Gestor da Internet no Brasil (CGI.br), já existente (Art. 51)

Fonte: as autoras, a partir das versões e minutas apresentadas do PL 2630[26]

Apesar da exclusão da previsão de entidade autônoma de supervisão na versão de 27 de abril de 2023, a preocupação com a regulação das plataformas digitais vem acompanhada da necessidade de saber quem, em um arranjo institucional multifacetado e complexo, será a referência de governança para tal sistema. Nesse sentido, a discussão acerca do sistema de governança para o PL 2630 deve continuar. É justamente nessa linha que se formulou um dos questionamentos na consulta pública, de iniciativa do CGI.br, sobre a regulação das plataformas digitais, em que se busca saber quais agentes devem estar envolvidos na arquitetura regulatória[27].

Para fomentar o debate sobre a eventual criação de nova autoridade ou

25. SOUZA, Nivaldo. Relatório do PL das Fake News não cria autoridade autônoma de fiscalização. JOTA, 28 abr. 2023. Disponível <https://www.jota.info/legislativo/relatorio-do-pl-das-fake-news-nao-cria-autoridade-autonoma-de-fiscalizacao-28042023>. Acesso em 1º jun. 2023.

26. Para mais informações sobre os documentos apresentados, confere-se tabela comparativa realizada pelo ITS Rio. Disponível em: <https://www.vozesdaregulacao.org.br/analise-pl2630>. Acesso em 1º jun. 2023.

27. Diálogos CGI.br. Consulta sobre Regulação das Plataformas Digitais. Disponível em: https://dialogos.cgi.br/documentos/debate/consulta-plataformas/. Acesso em 1º jun. 2023.

atribuição de competência para entes já pré-estabelecidos, recorremos à experiência internacional da União Europeia, que serve de inspiração à boa parte das disposições do projeto brasileiro[28]. Dessa forma, pudemos utilizá-la de insumo na reflexão das propostas ventiladas durante a discussão da arquitetura institucional brasileira.

2. O arranjo institucional do *Digital Services Act* (DSA)

Em 15 de dezembro de 2020, a Comissão Europeia apresentou a primeira versão do texto do *Digital Services Act* (DSA), como parte do pacote legislativo conhecido como *Digital Services Package*. O pacote foi composto pelo DSA e pelo *Digital Markets Act* (DMA), sendo o primeiro focado na "criação de um ambiente on-line mais seguro para usuários e empresas digitais e na proteção dos direitos fundamentais no espaço digital" e o segundo na garantia de um setor "competitivo e justo", com "igualdade de condições para todas as empresas digitais, independentemente de seu tamanho".[29]

As versões dos regulamentos sofreram diversas alterações e foram alvo de discussões legislativas ao longo de 2021 e 2022. Em 14 de setembro de 2022, o texto final do Regulamento UE 2022/1925 – o DMA – foi aprovado, com vigência total a partir de 25 de junho de 2023.[30] O texto final do DSA – Regulamento UE 2022/2065 –, por sua vez, foi aprovado em 19 de outubro de 2022, com totalidade em vigor a partir de 17 de fevereiro de 2024.[31] [32]

Em atenção ao objeto principal deste artigo – os arranjos institucionais vislumbrados e debatidos no âmbito do PL 2630 –, investigar com atenção o DSA é útil para fins comparativos. Ressalte-se que tais fins não implicam necessa-

28. Lei europeia que inspira PL das Fake News foca na transparência, não no conteúdo; entenda. CNN Brasil, 14 maio 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/lei-europeia-que-inspira-pl-das-fake-news-foca-na-transparencia-nao-no-conteudo-entenda/>. Confira também o comparativo elaborado pelo escritório de advocacia Baptista Luz, em: <https://baptistaluz.com.br/pl-2630-20-e-digital-services-act/>.

29. Trechos em tradução livre. Disponível em: <https://www.consilium.europa.eu/en/policies/digital-services-package/>. Acesso em 05 junho de 2023.

30. Como dispõe o artigo 54 do DMA, alguns dispositivos possuem datas de vigência distintas.

31. De maneira similar ao DMA, alguns dispositivos do DSA possuem datas de vigência distintas. Conforme seu artigo 93, algumas previsões vigoram a partir de 16 de novembro de 2022.

32. Para uma linha do tempo sobre as discussões, bem como as aprovações finais mencionadas, ver: European Council of the European Union. Timeline – Digital Services Package. Disponível em: https://www.consilium.europa.eu/en/policies/digital-services-package/timeline-digital-services-package/. Acesso em 05 jun. 2023.

riamente em uma incorporação das soluções ali descritas, mas principalmente na busca por uma compreensão da solução sugerida para avaliar se valem ou não os paralelos muitas vezes mencionados na discussão no Brasil. Durante o debate legislativo, não foram poucos os que identificaram o DSA como fonte de inspiração para o projeto brasileiro,[33] tendo sido mencionado mais de 20 vezes no parecer sobre o PL publicado em abril de 2023.[34]

Nesse contexto, vale entender, antes de adentrar em seu arranjo institucional, quais são as obrigações previstas pelo DSA aos provedores de aplicação. Para defini-las, o DSA divide os provedores de aplicação em categorias, sendo todos eles denominados "serviços intermediários" (*intermediary services*). Os serviços intermediários, conforme o artigo 3, *alínea g*, do DSA, abrangem três tipos de serviço: (i) serviço de "simples transporte" (*mere conduit*), que consista na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço ou na concessão de acesso a uma rede de comunicações, (ii) um serviço de "armazenagem temporária" (*caching service*), que consista na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço, que envolva a armazenagem automática, intermédia e temporária dessas informações, apenas com o objetivo de tornar mais eficaz a transmissão posterior das informações a outros destinatários, a pedido destes; (iii) um serviço de "armazenagem" (*hosting service*), que consista na armazenagem de informações prestadas por um destinatário do serviço a pedido do mesmo. Esses serviços intermediários são a categoria mais abrangente do DSA.

Além dessa categoria mais abrangente, existem duas outras: (a) plataformas *online*, descritas pelo serviço de armazenagem mencionado acima, sendo que além de armazenarem informações a pedido, também as distribuem ao público, conforme o artigo 3, alínea i, do DSA; e (b) plataformas de busca (*online search engine*), definidas no artigo 3, alínea j, como serviços intermediários que permitem que os usuários realizem buscas em todos os sites em um determinado idioma e retorna resultados em qualquer formato em que as

33. *E.g.*: https://www.cnnbrasil.com.br/politica/lei-europeia-que-inspira-pl-das-fake-news-foca-na-transparencia-nao-no--conteudo-entenda/ , entrevista de Victor Duringan e Rafael Zanatta, para quem "o PL das *Fake News* tem forte influência do DSA em relação à prevenção de riscos sistêmicos", destacando "o compromisso com a transparência como um ponto em comum dos projetos"; "Em contrapartida, o projeto de lei brasileiro tem um foco menor sobre a questão econômica e de competitividade entre as empresas de tecnologia.". Veja também o comparativo elaborado pelo escritório de advocacia Baptista Luz, em: https://baptistaluz.com.br/pl-2630-20-e-digital-services-act/

34. Câmara dos Deputados. Projeto de Lei 2630/2020, versão apresentada em 27 abril 2023. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334>. Acesso em 26 maio de 2023.

informações relacionadas ao conteúdo solicitado possam ser encontradas. As plataformas de busca parecem se encaixar como uma quarta categoria de serviços intermediários, apesar de não serem diretamente indicados como tal na estrutura do DSA.

Essa aparente confusão nas categorias não é por acaso. Em verdade, é um dos pontos mais confusos do texto aprovado e reflete as movimentações legislativas entre o primeiro texto publicado em 2020 e a versão final. O texto publicado inicialmente não mencionava as plataformas de busca como o fez ao final, deixando-as como parte das demais classificações. Para Gregor Schmid e Philipp Koehler, essa inserção gerou ambiguidades desnecessárias e "teria sido preferível atribuir claramente os mecanismos de busca *online* a um tipo específico de serviços intermediários, semelhante à classificação das plataformas online como um subconjunto de serviços de armazenagem".[35]

Ainda no que tange a classificação desses serviços, essencial para o sistema de obrigação em camadas criado, tanto as plataformas online como as plataformas de busca podem ser *qualificadas* como "de muito grande dimensão". Essa qualificação depende de uma análise e posterior decisão da Comissão Europeia, nos termos do artigo 33 do DSA.

O requisito objetivo para ser considerada de grande dimensão é possuir um número médio mensal de destinatários ativos do serviço na União Europeia igual ou superior a 45 milhões, equivalente a 10% da população da União.[36] Em decisão publicada em abril de 2023, a Comissão Europeia indicou 17 plataformas *online* de muito grande dimensão (Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube e Zalando) e 2 plataformas de busca de muito grande dimensão (Bing e Google Search).[37]

De qualquer maneira, classificar determinado serviço é o primeiro pas-

35. SCHIMID, Gregor. KOEHLER, Philipp. Digital Services Act – an overview. TaylorWessing. Disponível em: https://www.taylorwessing.com/en/insights-and-events/insights/2022/11/digital-services-act-ein-ueberblick. Acesso em 25 maio de 2023.

36. Como dispõe o artigo 33 do DSA e o Considerando 76, esse número deverá ser atualizado pela Comissão Europeia a pode ser modificado em decorrência de mudanças fáticas. A Comissão Europeia deve contar, ainda, com a atuação do Coordenador de Serviços Digitais para analisar o número mensal de destinatários do serviço.

37. Comissão Europeia. Press release. *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413. Acesso em 25 maio 2023.

so para delimitar a quais obrigações ele estará sujeito. A primeira camada, mais profunda e central ao sistema como um todo, define um padrão geral de obrigações, dispostas nos artigos 11 a 15 do DSA. Essa camada é aplicável a todas as categorias e é formada pelas obrigações de possuir mecanismos de transparência, termos e condições de serviço com requisitos específicos, cooperação com as autoridades competentes e pontos de contato, conforme necessário. A segunda camada aplica-se ao serviço de armazenagem, incluindo as plataformas *online*, criando obrigações adicionais listadas nos artigos 16 a 18 do DSA, como mecanismos de notificação e ação frente a conteúdos considerados ilegais, o fornecimento de justificativa em casos de moderação de conteúdo e, ainda, a notificação às autoridades frente à suspeita de atividades ilícitas.

A terceira camada, definida entre os artigos 19 e 32 do DSA, cria obrigações específicas para plataformas *online*. Enquanto a segunda camada é aplicável a todos os serviços de armazenagem, a terceira aplica-se apenas para a parcela desses serviços que se categoriza como plataformas *online*. Não se aplica, dessa maneira, considerando a classificação do artigo 3, alínea i, do DSA, aos serviços de armazenagem em que a posterior disseminação é um "recurso menor e puramente auxiliar ou uma funcionalidade menor do serviço principal". Nessa terceira camada, da qual estão isentas pequenas e médias empresas, com base na definição da Recomendação da Comissão de 06/05/2003 relativa à definição de micro, pequenas e médias empresas (Recomendação 2003/361/EC), incluem-se a obrigação de garantir a possibilidade de optar por métodos extrajudiciais de resolução de conflitos e a de suspender, por período razoável e após as devidas notificações, usuários que promovam sistematicamente conteúdos ilegais manifestos.

A quarta camada, por fim, se destina às plataformas *online* e de busca "qualificadas", ou seja, aquelas de muito grande dimensão conforme os dados reportados e posterior decisão da Comissão Europeia. Como mencionado no Considerando 76, "as plataformas *online* de muito grande dimensão e as plataformas de busca de muito grande dimensão podem implicar riscos sociais com âmbito e impacto diferentes dos causados por plataformas de menor dimensão", devendo seus fornecedores "suportar os mais elevados níveis de exigência em matéria de obrigações de devida diligência, proporcionais ao seu impacto social". Essa camada, descrita entre os artigos 33 e 43 do DSA, busca, portanto, endereçar os chamados "riscos sistêmicos" e apresenta obrigações adicionais voltadas a sistemas de recomendação e de gerenciamento de cri-

ses, por exemplo.[38]

É possível perceber que apesar da dimensão qualificada produzir efeitos aparentemente iguais nas plataformas *online* e de busca de muito grande dimensão, essas últimas não estão abarcadas, a princípio, pelas segunda e terceira camadas de obrigação. Isso porque não são, ao menos pela definição do artigo 3, alínea j, um serviço de armazenagem. A figura abaixo busca consolidar essas camadas de acordo com as respectivas categorias de serviços.

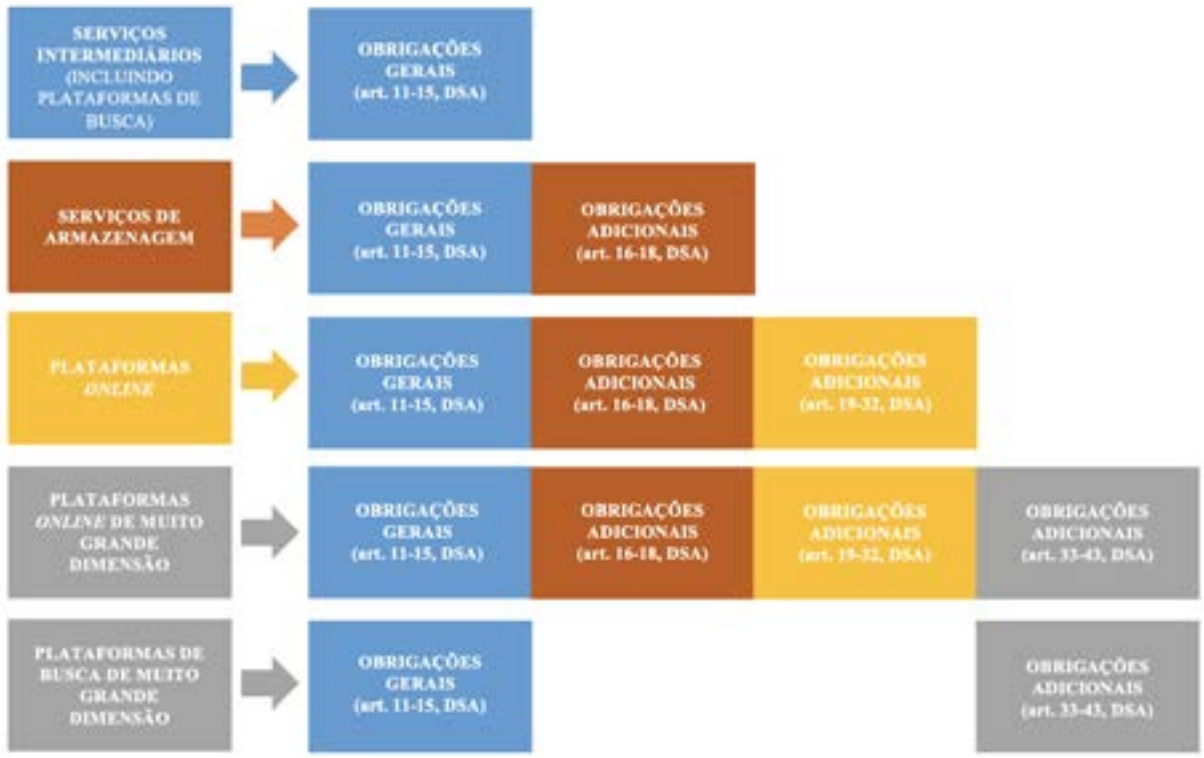

Figura 1 – Sistema em camadas do DSA

Fonte: Traduzido e adaptado e traduzido pelas autoras a partir de SCHIMID, Gregor. KOEHLER, Philipp. Digital Services Act – an overview. TaylorWessing. Disponível em: https://www.taylorwessing.com/en/insights-and-events/insights/2022/11/digital-services-act-ein-ueberblick. Acesso em 25 maio de 2023.

Apresentadas as obrigações delimitadas pelo DSA, passamos a retomar o ponto central deste artigo – qual seja, o papel das instituições estatais na aplicação e supervisão do DSA. Compreender o sistema de *enforcement* criado pelo DSA implica reconhecer o aspecto harmonizador de uma legislação como o DSA a nível europeu. O *Digital Services Package*, como um todo, parte de dois movimentos importantes para uma análise comparativa.

38. É como descreve o próprio título da Seção 5 do DSA: "Obrigações adicionais para provedores de plataformas online de muito grande dimensão e de plataformas de buscas de muito grande dimensão para gerenciar riscos sistêmicos." Em tradução livre de: "*Additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks*".

O primeiro é o reconhecimento, por parte da União Europeia, da necessidade de harmonização entre os países europeus a fim de garantir um desenvolvimento tecnológico alinhado e coerente entre si. Turillazzi, Tadeo, Floridi e Casolari examinam quatro macro áreas de interesse a partir do DSA (harmonização, conteúdo ilegal, responsabilidade de intermediários e confiança consumerista),[39] sendo a sobre harmonização a mais relevante ao presente estudo.

O segundo movimento é relacionado a uma narrativa crescente na União Europeia de incremento do poder regulatório e normativo da União sobre aspectos da economia digital. Essa narrativa não é nova – é exemplificada, inclusive, pelo Regulamento 2016/679 da UE, o Regulamento Geral sobre a Proteção de Dados (RGPD ou GDPR, *General Data Protection Regulation*, em inglês). É dele que surge o *Brussels Effect* apontado por Anu Bradford em relação a diversos setores da economia e, no que tange o digital, ao GDPR e a algumas ações sobre discurso de ódio.[40] O DSA pode acabar tendo o mesmo efeito ao implementar uma nova sistemática de regulação de provedores a nível europeu.[41]

Na sistemática criada pelo DSA, três entidades desempenham papéis importantes na implementação e aplicação do regulamento: o Coordenador de Serviços Digitais, o Comitê e a Comissão Europeia. Nos termos do artigo 49 do DSA, cada Estado-Membro deve designar um Coordenador de Serviços Digitais (*Digital Services Coordinator*) até 17 de fevereiro de 2024. Esses coordenadores devem ser designados pelos Estados-Membros que, segundo o artigo 50, devem garantir que o coordenador tenha "todos os recursos necessários para realizar suas tarefas, incluindo recursos técnicos, financeiros e humanos suficientes para supervisionar adequadamente todos os prestadores de serviços intermediários de sua competência",[42] bem como possuir autonomia

39. TURILLAZZI, Aina; CASOLARI, Federico; TADDEO, Mariarosaria; FLORIDI, Luciano. *The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications*. Janeiro de 2022. Disponível em: https://ssrn.com/abstract=4007389. Acesso em: 23 maio 2023, p.9.

40. BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: 2020, p.131. No mesmo sentido: VERMEULEN, Mathias. Online Content: To Regulate or not to Regulate - Is that the Question? APC Issue Paper, ago. 2019. Disponível em: https://ssrn.com/abstract=3557914, p. 3. Acesso em 23 maio 2023.

41. Cf. TURILLAZZI, Aina; CASOLARI, Federico; TADDEO, Mariarosaria; FLORIDI, Luciano. The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications. Janeiro de 2022. Disponível em: https://ssrn.com/abstract=4007389. Acesso em: 23 maio 2023, p.23.

42. Em tradução livre de: "(...) *all necessary resources to carry out their tasks, including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence*."

financeira.

O DSA prevê, ademais, a criação do Comitê Europeu para Serviços Digitais (*European Board for Digital Services*), conforme o artigo 61. Segundo o artigo 62, o Comitê será composto por representantes dos Estados-Membros e presidido pela Comissão Europeia. O Comitê terá a função de apoiar a Comissão na implementação do DSA, emitindo opiniões e recomendações sobre as medidas propostas pela Comissão, por exemplo. Além disso, como dispõe seu artigo 63 (1), alíneas a e b, o Comitê pode apoiar a coordenação de investigações conjuntas e apoiar as autoridades competentes na análise de relatórios e resultados de auditorias de plataformas de muito grande dimensão.

A Comissão Europeia, por fim, possui um papel central na implementação e aplicação do DSA. Ela é o órgão de coordenação do sistema como um todo, em especial dos *Digital Services Coordinators*. Embora não trate de uma seara hierarquicamente superior ao Estado-membro, suas decisões afetarão, de modo mais sistemático, todo o território europeu. É por isso, inclusive, que cabe à Comissão, em cooperação com os Coordenadores de Serviços Digitais e o Comitê, "coordenar a avaliação de questões sistêmicas e emergentes em toda a União em relação a plataformas *online* e de busca de muito grande dimensão", conforme o artigo 64(2) do DSA.

Essas três entidades, portanto, desempenham papéis complementares para garantir a implementação e aplicação efetiva do DSA na União Europeia. O Coordenador de Serviços Digitais age no âmbito nacional, supervisionando a aplicação do DSA em seu país e estabelecendo pontos de contato com os provedores de serviços e as demais autoridades. O Comitê fornece apoio e orientação à Comissão Europeia, enquanto esta última desempenha um papel central na elaboração de propostas, aplicação e fiscalização do cumprimento do DSA. Em linhas gerais, o texto final do DSA foi considerado um importante avanço para a proteção dos direitos fundamentais no ambiente digital.[43]

43. Veja, por exemplo, a opinião da organização Access Now: "O resultado final tem marcas de compromissos políticos, mas a UE estabeleceu um precedente para um manual de regras de moderação de conteúdo que coloca os direitos fundamentais em seu centro." Em tradução livre de: "T*he final outcome has marks of political compromises but the EU set a precedent for a content moderation rulebook that puts fundamental rights at its center.*" PIRKOVA, Eliska. *The Digital Services Act: your guide to the EU's new content moderation rules*. Access Now, março de 2023. Disponível em: https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

3. Mapeando as propostas de arranjos institucionais no Brasil

Como visto na Tabela 1 da primeira seção, quanto ao arranjo institucional, as propostas do PL 2630 apresentadas oficial e extraoficialmente parecem girar entre (i) criar uma nova autoridade e (ii) designar um órgão existente, nos dois casos com atribuições consultivas e/ou de supervisão.[44] Quanto aos dois primeiros casos, as redações analisadas indicam a atribuição a um órgão não especificado do Poder Executivo ("entidade autônoma de supervisão") e ao CGI.br. Com a finalidade de elucidar as diferentes vozes do debate, esta seção apresenta as propostas para a autoridade e sua repercussão entre especialistas.

Em sua versão de março de 2022, o PL conferia ao CGI.br uma série de prerrogativas para auxiliar e, em alguma medida supervisionar, a autorregulação das plataformas digitais. A título de exemplo, cita-se o poder de realizar de estudos, pareceres e recomendações sobre liberdade, responsabilidade e transparência na internet; apresentar diretrizes para elaboração de Código de Conduta, realizar estudos sobre os procedimentos de moderação adotados pelas mídias sociais e fornecer diretrizes para as políticas de uso dos provedores.

A conferência de tais prerrogativas relembra argumento desenvolvido por Luna Barroso ao vislumbrar mecanismos regulatórios para as plataformas digitais. Para ela, a fiscalização de um eventual sistema de autorregulação regulada "deve ser atribuída a um órgão especializado, com representação majoritária da sociedade civil".[45] O CGI.br, por sua vez, poderia vir a desempenhar essa função no Brasil.[46] Ele não seria capaz de sancionar plataformas digitais por violações pontuais e específicas, mas poderia conduzir função de análise

44. Nada impede, ainda, uma terceira hipótese, em que inexiste um único órgão para implementar e/ou supervisionar a lei - cabendo sua aplicação, como diversas outras no ordenamento jurídico brasileiro, ser garantida pelo Poder Judiciário e outros órgãos descentralizados. Essa possibilidade não é endereçada por este artigo, vez que ele se debruça justamente pelo debate que se formou a partir da atribuição, pelo PL 2630, de funções a uma autoridade em sua arquitetura. Para mais reflexões a respeito de tal abordagem, incluindo possível inspiração em um sistema como o Sistema Nacional de Defesa do Consumidor, ver: RAMOS, Pedro Henrique. Afinal, precisamos de um órgão regulador da internet no país? Negócios Globo, 17 maio 2023. Disponível em: <https://epocanegocios.globo.com/colunas/coluna/2023/05/afinal-precisamos-de-um-orgao-regulador-da--internet-no-pais.ghtml>. Acesso em 1º jun. 2023.

45. BARROSO, Luna van Brussel. Liberdade de expressão e democracia na era digital: o impacto das mídias socais no mundo contemporâneo. Belo Horizonte: Fórum, 2022, p.283.

46. BARROSO, Luna van Brussel. Liberdade de expressão e democracia na era digital: o impacto das mídias socais no mundo contemporâneo. Belo Horizonte: Fórum, 2022, p.283.

sistêmica, inclusive examinando relatórios de transparência.[47]

Em sentido similar, comentando sobre a proposta formalizada, Bia Barbosa, representante do terceiro setor no CGI.br, ressaltou que o comitê não deve ser a autoridade responsável por fiscalizar o cumprimento da lei, tampouco aplicar sanções. Sua atuação deve fazer parte da arquitetura regulatória, por meio do fornecimento de diretrizes e critérios para a implementação do projeto.[48] É necessário, portanto, ter cautela na previsão de determinados mecanismos fiscalizatórios ao CGI.br.

Mais recentemente, a sugestão de minuta do Poder Executivo,[49] em seu artigo 39, contém a previsão de "entidade autônoma de supervisão". De acordo com a minuta, a entidade definirá, por meio de regulamentação própria, o procedimento de apuração e critérios de aplicação das sanções administrativas e infrações. Nas duas versões posteriores (apresentadas nos dias 18 e 25 de abril), são apresentadas disposições semelhantes que permitem ao Poder Executivo estabelecer entidade autônoma de supervisão para detalhar em regulamentação os dispositivos do que trata o projeto, fiscalizar a observância pelos provedores, instaurar processos administrativos e, comprovado o descumprimento aplicar sanções cabíveis. A entidade deveria contar com garantias de autonomia técnica, administrativa e independência do processo de tomada de decisões, com espaços formais de participação multissetorial.

A Comissão de Privacidade, Proteção de Dados e Inteligência Artificial da OAB/SP manifestou suas preocupações quanto à falta de autonomia ao órgão proposto.[50] Ainda que estivesse estabelecido a autonomia técnica, administrativa e independência no processo de tomada de decisões, somente autarquias têm garantia de autonomia administrativa e estas devem ser criadas por

47. BARROSO, Luna van Brussel. Liberdade de expressão e democracia na era digital: o impacto das mídias socais no mundo contemporâneo. Belo Horizonte: Fórum, 2022, p.283.

48. Criação de órgão fiscalizador é retirada de nova versão do PL das Fake News. Mobiletime, 28 abr. 2023. Disponível em: <https://www.mobiletime.com.br/noticias/28/04/2023/criacao-de-orgao-fiscalizador-e-retirada-de-nova-versao-do-pl-das-fake-news/>. Da mesma forma, em nota publicada em 28 de abril de 2023, o CGI.br se posiciona nessa linha. Disponível em: https://cgi.br/esclarecimento/nota-publica-sobre-debate-em-torno-do-pl-2630-2020/. Acesso em 26 de maio de 2023.

49. De autoria do Poder Executivo, apresentada em 30 de março de 2023, a proposta foi divulgada por vias não oficiais. Disponível em: <https://www.telesintese.com.br/wp-content/uploads/2023/03/Contribuicoes_PL2630.pdf>. Acesso em 26 maio de 2023.

50. OAB. Comissão de Privacidade, Proteção de Dados e Inteligência Artificial da OAB SP manifesta preocupação quanto ao PL 2630/2020. Jornal da Advocacia, OAB/SP, 27 abr. 2023. Disponível em: <https://jornaldaadvocacia.oabsp.org.br/noticias/comissao-de-privacidade-protecao-de-dados-e-inteligencia-artificial-da-oab-sp-manifesta-preocupacao-quanto-ao-pl-2630-2020/>. Acesso em 1º jun. 2023.

lei específica, o que não ocorre no caso. Com isso, da forma como foi desenhada pelo projeto, o órgão seria vinculado ao Poder Executivo, sem real garantia de poderes autônomos.[51]

Como solução para enfrentar o referido problema, Renato Toledo sugere uma possível releitura das competências privativas do chefe do Poder Executivo para iniciativa de processos legislativos. Por considerar que "a Administração Pública evoluiu de um modelo piramidal para outro policêntrico", com número expressivo de instituições e arranjos complexos, responsáveis pela tutela efetiva de direitos, vislumbra a revisão da medida que foi pensada à época de outro contexto da Administração Pública.[52]

Discorre, assim, sobre duas possibilidades: (i) conceder interpretação restritiva à competência privativa prevista no artigo 61, §1, inciso II da Constituição Federal, assim "apenas nos casos em que um projeto de lei versar de forma central e imediata sobre a organização administrativa, a criação de cargos ou de funções, a deflagração do processo legislativo deverá ser necessariamente do chefe do Poder Executivo"; alternativamente (ii) cogita a revisão da jurisprudência do STF de que a sanção de projeto de lei não convalida vício de inconstitucionalidade - em nova interpretação, a sanção poderia sanar eventual vício de dispositivos específicos, quando o tema central do projeto não versar exclusivamente sobre a organização administrativa.[53]

No campo dos que apoiam a assimilação das novas funções a um órgão pré-existente para além do CGI.br, ressaltamos a possibilidade mencionada pela Agência Nacional de Telecomunicações (Anatel) para que se aproveite a sua estrutura operacional. Sustenta-se que a sua atual conjuntura poderia ser utilizada no controle das plataformas, semelhante ao trabalho realizado

51. Vale lembrar, inclusive, discussão semelhante ocorreu no processo de criação da Autoridade Nacional de Proteção de Dados (ANPD). Sua estrutura administrativa fora objeto de controvérsia na tramitação da Lei Geral de Proteção de Dados, inicialmente recepcionada como órgão da Administração Pública direta, mas posteriormente, foi transformada em autarquia de natureza especial, pela Medida Provisória nº 1.124/2022.

52. TOLEDO, Renato. Governança regulatória e organização administrativa. JOTA, 07 jun. 2023. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/reg/governanca-regulatoria-e-organizacao-administrativa-07062023>. Acesso em 7 jun. 2023.

53. *Ibidem*.

durante as eleições a pedido do Tribunal Superior Eleitoral (TSE)[54], ao notificar os provedores a respeito das decisões com pedidos de bloqueio proferidas pelas Cortes Superiores[55]. Carlos Baigorri, presidente da Anatel, se pronunciou a favor da agência assumir o papel fiscalizatório, sob o argumento de já possuírem a configuração necessária para a função e "já exercerem poder de polícia no que diz respeito a conteúdo", ainda que não seja a atividade mais tradicional.[56]

Por sua vez, tal proposta foi alvo de críticas. Em nota emitida pela Coalização de Direitos da Rede (CDR),[57] que reúne mais de 50 entidades do direito digital, foram listadas uma série de motivos contrários à indicação da Anatel como autoridade supervisora. Argumentam que a Anatel não teria a expertise necessária nos temas de regulação de plataformas, tendo em vista que sua atuação não é próxima à pauta do conteúdo, nem a matérias de direitos fundamentais centrais ao debate. Além da falta de competência, apontam falha da agência no cumprimento de suas atribuições no setor de telecomunicações, com base em auditoria do Tribunal de Contas da União que indicaria ineficiências e a necessidade de mais transparência em sua atuação. Assim, defendem que o cenário seria agravado, caso reivindicassem mais competência, o que prejudicaria o avanço da conectividade no Brasil.

Em sentido semelhante, as entidades de Tecnologia da Informação e Comunicação, incluindo ABES, Abinee e Brasscom, também se opuseram à nomeação da Anatel e se posicionaram favoráveis a manter a centralidade da Autoridade Nacional de Proteção de Dados (ANPD) no tema.[58] De acordo com a nota, haveria conflito de competência entre eventual entidade supervisora prevista no PL 2630 e a ANPD.

54. SOUZA, Nivaldo. Anatel segue cotada como órgão regulador das plataformas no PL das Fake News. JOTA, 02 maio de 2023. Disponível em: <https://www.jota.info/legislativo/anatel-segue-cotada-como-orgao-regulador-das-plataformas-no-pl-das-fake-news-02052023>. Acesso em 1º jun. 2023.

55. Anatel recebeu nove decisões do Judiciário para bloqueio de sites em 2022. Teletime, 13 out. 2022. Disponível em: <https://teletime.com.br/13/10/2022/anatel-recebeu-nove-decisoes-do-judiciario-para-remocao-de-sites-em-2022/>.

56. Anatel mistura redes com conteúdo e diz estar pronta para fiscalizar plataformas online. Convergência Digital, 25 abr. 2023. Disponível em: https://www.convergenciadigital.com.br/Internet/Anatel-mistura-redes-com-conteudo-e-diz-estar-pronta-para-fiscalizar-plataformas-online-63068.html?UserActiveTemplate=mobile>. Acesso em 1º jun. 2023.

57. Coalização Direitos na Rede. Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel. CDR. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2023/04/CDR-Nota-sobre-Anatel-como-orgao-regulador.pdf. Acesso em 1º jun. 2023.

58. Fake News: Brasscom, Abinee e ABES saem em defesa da ANPD como autoridade autônoma da Internet. Convergência Digital, 30 abr. 2023. Disponível em: <https://www.convergenciadigital.com.br/Internet/Fake-News%3A-Brasscom%2C-Abinee-e-ABES-saem-em-defesa-da-ANPD-como-autoridade-autonoma-da-Internet-63098.html>. Acesso em 1º jun. 2023.

Por último, cabe destacar a sugestão apresentada pela Ordem dos Advogados do Brasil (OAB), em ofício encaminhado ao Dep. Orlando Silva, em que sugere a criação de um sistema tripartite regulatório para supervisionar a aplicação da lei,[59] por entender que não seria possível um único órgão, setor ou agente desempenhar tal função. No texto, propõe-se a seguinte divisão: (i) criação de um Conselho de Políticas Digitais, responsável por fiscalizar e aplicar a regulação, como, por exemplo, ao analisar os relatórios de riscos sistêmicos e de transparência publicados pelas plataformas. Seria composto por representantes dos três poderes, mas também da ANPD, OAB, CADE e Anatel; (ii) o CGI.br seria responsável por promover debates, estudos e diretrizes sobre o tema; (iii) entidade privada de autorregulação para deliberar sobre casos concretos de moderação de conteúdo das plataformas digitais.

Por um lado, especialistas consideram a proposta positiva por sua multissetorialidade.[60] Para Christian Perrone, a proposta pode servir como alternativa viável e seria positiva a estrutura do conselho com uma visão ampla e abertura para os diferentes setores.[61] Há também pontos que foram alvo de críticas por considerarem a concepção difícil de ser operacionalizada.[62]

Nesse contexto, a ANPD apresentou sua contribuição ao debate,[63] em especial, endereçando suas preocupações em relação a potenciais conflitos entre as competências legais da ANPD, previstas na LGPD, e os dispositivos da proposta. Em termos práticos, entende que o PL 2630 concederia margem para que sejam atribuídas a outra entidade pública parte das competências legais da ANPD de regulamentação, fiscalização e aplicação de sanções a plataformas digitais no que concerne à proteção de dados pessoais. A título de exemplo, cita as orientações e regulamentações de temas atribuídos pelo PL à entidade supervisora autônoma, que já estão nos planos regulatórios da autoridade, como a proteção de crianças e adolescentes no ambiente digital,

59. Proposta da OAB de sistema tripartite para regular plataformas divide especialistas. Mobiletime, 15 maio 2023. Disponível em: <https://www.mobiletime.com.br/noticias/15/05/2023/proposta-da-oab-de-sistema-tripartite-para-regular-plataformas-divide-especialistas/. Acesso em 1º jun. 2023.

60. *Ibidem*.

61. *Ibidem*.

62. *Ibidem*.

63. ANPD. Contribuição preliminar para o debate público sobre a Lei de Liberdade, Responsabilidade e Transparência na Internet, 27 abr. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/contribuicao-preliminar-para-o-debate-publico-sobre-a-lei-de-liberdade-responsabilidade-e-transparencia-na-internet>. Acesso em 1º jun. 2023.

inteligência artificial e decisões automatizadas.[64]

O posicionamento da ANPD evidencia que instituições reguladoras – assim como leis – não são criadas num vácuo. Há um contexto legal e técnico pré-existente que deve ser considerado na operacionalização de atribuições legais. Nesse contexto, as plataformas digitais já estão sujeitas a um robusto arcabouço de regras setoriais e suas respectivas autoridades competentes. Esse, inclusive, é o desenho dos artigos 17 a 21 do Decreto nº 8771/2016, que regulamentou o Marco Civil da Internet e reafirmou as respectivas competências da Anatel, da Secretaria Nacional do Consumidor, do Conselho Administrativo de Defesa Econômica e do CGI.br. Qualquer proposta de regulação passará por esses diversos setores - portanto, avaliar formas de coordenação e cooperação entre essas diferentes autoridades será essencial para a construção de um sistema de governança eficaz na regulação das plataformas.

Diante do exposto, apesar da remoção da previsão sobre a autoridade autônoma de supervisão, o debate continuará permeando o tema. Caso não se tenha órgão para figurar a arquitetura institucional da regulação das plataformas, a legislação pode ficar sem devido *enforcement* e mera "letra de lei"[65] e, com isso, o Poder Judiciário absorverá a demanda de fiscalizar a implementação da legislação. Por outro lado, ainda que se tenha supervisão, sua efetivação por órgãos não independentes pode colocar em risco os valores de liberdade de expressão, entre outros direitos fundamentais ao espaço democrático.

Conclusão

Como visto, as idas e vindas do PL 2630 trouxeram uma camada de complexidade à discussão sobre autoridade reguladora. Ante a um processo legislativo marcado por picos de movimentações frenéticos, períodos estagnados e minutas circuladas extraoficialmente, incluir nova autoridade supervisora, sem a realização de audiências públicas a respeito, ou mesmo sem que a pro-

64. ANPD. Contribuição preliminar para o debate público sobre a Lei de Liberdade, Responsabilidade e Transparência na Internet, 27 abr. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/contribuicao-preliminar-para-o-debate-publico-sobre-a-lei-de-liberdade-responsabilidade-e-transparencia-na-internet>. Acesso em 1º jun. 2023.

65. Cf. COUTINHO, Diogo R.; KIRA, Beatriz. PL das Fake News sem órgão regulador é lei desdentada. Folha de S. Paulo, maio de 2023. Disponível em: https://www1.folha.uol.com.br/opiniao/2023/05/pl-das-fake-news-sem-orgao-regulador-e-lei-desdentada.shtml#:~:text=Aus%C3%AAncia%20de%20autoridade%20p%C3%BAblica%20independente%20cria%20incertezas%20e%20enfraquece%20prop%C3%B3sito&text=O%20projeto%20de%20lei%202.630,n%C3%A3o%20entregar%20o%20que%20promete. Acesso em 1º jun. 2023.

posta fosse remetida às comissões especializadas, gerou pouca segurança quanto ao preparo estatal para operacionalizar proposta.

Ao investigar os arranjos institucionais do DSA, para fins comparativos, observou-se que o diploma delimitou com profundidade categorias para os diferentes atores afetados pela regulação. Tal distinção, para além de conceitual, denuncia a variedade e complexidade de agentes envolvidos no ecossistema regulado. Em razão disso, reconhece-se o aspecto harmonizador da legislação no âmbito do sistema *enforcement* criado. O modelo de governança institucional conta com três entidades protagonistas.

O processo brasileiro de construção desse sistema de governança demarca influência da norma estrangeira - por mais que seja essa influência em si passível de críticas -, é possível identificar semelhanças, como, por exemplo, a sugestão de criação de um sistema tripartite regulatório para supervisionar a aplicação da lei. Nesse contexto, vale recorrer aos ensinamentos da experiência europeia para compreender que a operacionalização desse sistema se deu com intuito de harmonização entre os diferentes Estados-membros.

É passível de reflexão se mecanismos similares funcionariam dentro do complexo e multifacetado ecossistema brasileiro. Como demonstrado, as plataformas digitais já estão sujeitas a um robusto arcabouço de regras setoriais e suas respectivas autoridades competentes. Qualquer proposta de regulação passará por esses diversos setores - portanto, avaliar formas de coordenação entre essas diferentes autoridades será importante para a construção de um sistema de governança eficaz na regulação das plataformas. Para tanto, faz-se necessário considerar a mais transparência e formalização das propostas apresentadas, para viabilizar a promoção do debate com os entes envolvidos, seja por meio de comissões especializadas, audiências e outros meios de participação social.

Referências

ALEMANHA. [*Netzwerkdurchsetzungsgesetz* (2017)]. *Netzwerkdurchsetzungsgesetz* [2021]. Disponível em: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>.

Anatel recebeu nove decisões do Judiciário para bloqueio de sites em 2022. *Teletime*, 13 out. 2022.

Disponível em: <https://teletime.com.br/13/10/2022/anatel-recebeu-nove-decisoes-do-judiciario-para-remocao-de-sites-em-2022/>.

ANPD. **Contribuição preliminar para o debate público sobre a Lei de Liberdade, Responsabilidade e Transparência na Internet**, 27 abr. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/contribuicao-preliminar-para-o-debate-publico-sobre-a-lei-de-liberdade-responsabilidade-e-transparencia-na-internet>.

BARROSO, Luna van Brussel. **Liberdade de expressão e democracia na era digital: o impacto das mídias sociais no mundo contemporâneo**. Belo Horizonte: Fórum, 2022.

BRADFORD, Anu. ***The Brussels Effect: How the European Union Rules the World***. Oxford: 2020.

BREGA, Gabriel Ribeiro. **A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira**. Revista Direito FGV, v.19, 2023. Disponível em: https://www.scielo.br/j/rdgv/a/qwwzmCyw5FmFQmTpRw3HCQh/?format=pdf&lang=pt.

Câmara dos Deputados. **Projeto de Lei 2630/2020**, versão apresentada em 27 abril 2023. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334>.

_____. **Projeto de Lei 2630/2020**, substitutivo apresentado em março de 2022. Disponível em: <https://www.camara.leg.br/midias/file/2022/03/fake.pdf>. Acesso em 26 maio de 2023.

Coalização Direitos na Rede. **Órgão independente de supervisão das plataformas é essencial, mas não pode ser Anatel**. *CDR*. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2023/04/CDR-Nota-sobre-Anatel-como-orgao-regulador.pdf.

Comissão Europeia. Press release. ***Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines***. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

CONFESSORE, Nicholas. ***Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.*** The New York Times, 04 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Diálogos CGI.br. **Consulta sobre Regulação das Plataformas Digitais**. Disponível em: https://dialogos.cgi.br/documentos/debate/consulta-plataformas/. Acesso em 1º jun. 2023.

Dino cobra de plataformas monitoramento sobre incitação à violência nas escolas. *G1 Globo News*, 07 abr. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/04/07/dino-cobra-de-plataformas-monitoramento-sobre-incitacao-a-violencia-nas-escolas.ghtml.

Dino diz que governo está desenvolvendo projeto para regulamentação de redes sociais. *CNN Brasil,* 13 de março de 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/dino-diz-que-governo-esta-desenvolvendo-projeto-para-regulamentacao-de-redes-sociais/>.

Estela Aranha: Marco Civil falhou com as redes sociais. *Convergência Digital*, 27 jan. 2023. Disponível em: <https://www.convergenciadigital.com.br/Internet/Estela-Aranha%3A-Marco-Civil-falhou-com-as-redes-sociais-62382.html>.

European Council of the European Union. *Timeline – Digital Services Package*. Disponível em:

https://www.consilium.europa.eu/en/policies/digital-services-package/timeline-digital-services-package/.

Fake News: Brasscom, Abinee e ABES saem em defesa da ANPD como autoridade autônoma da Internet. *Convergência Digital*, 30 abr. 2023. Disponível em: <https://www.convergenciadigital.com.br/Internet/Fake-News%3A-Brasscom%2C-Abinee-e-ABES-saem-em-defesa-da-ANPD-como-autoridade-autonoma-da-Internet-63098.html>.

KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet**. Rio de Janeiro: Lumen Juris, 2019, pp. 174-175.

Lei europeia que inspira PL das *Fake News* foca na transparência, não no conteúdo; entenda. *CNN Brasil*, 14 maio 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/lei-europeia-que-inspira-pl-das-fake-news-foca-na-transparencia-nao-no-conteudo-entenda/>.

NOVO. **5 armadilhas do Projeto de Lei 2630, o "PL da Censura"**, 27 abr. 2023. Disponível em: <https://novo.org.br/5-armadilhas-do-projeto-de-lei-2630-ou-pl-da-censura/>.

OAB. **Comissão de Privacidade, Proteção de Dados e Inteligência Artificial da OAB SP manifesta preocupação quanto ao PL 2630/2020**. *Jornal da Advocacia, OAB/SP*, 27 abr. 2023. Disponível em: <https://jornaldaadvocacia.oabsp.org.br/noticias/comissao-de-privacidade-protecao-de-dados-e-inteligencia-artificial-da-oab-sp-manifesta-preocupacao-quanto-ao-pl-2630-2020/>.

PL das fake news: aprovado no Senado, entenda o que pode mudar. *UOL Tilt*, 30 de jun. de 2020. Disponível em:<https://www.uol.com.br/tilt/noticias/redacao/2020/06/30/com-44-votos-senado-aprova-pl-das-fake-news.ht>.

ITS Rio. **9 pontos de atenção sobre o PL das Fake News (PL 2630/20)**, 31 de março de 2022. Disponível em: <https://itsrio.org/wp-content/uploads/2022/04/9-pontos-de-aten%C3%A7%C3%A3o-sobre-o-PL-das-Fake-News-PL-2630_20.pdf>.

Proposta da OAB de sistema tripartite para regular plataformas divide especialistas. *Mobiletime*, 15 maio 2023. Disponível em: <https://www.mobiletime.com.br/noticias/15/05/2023/proposta-da-oab-de-sistema-tripartite-para-regular-plataformas-divide-especialistas/>.

SCHIMID, Gregor. KOEHLER, Philipp. ***Digital Services Act – an overview***. TaylorWessing. Disponível em: https://www.taylorwessing.com/en/insights-and-events/insights/2022/11/digital-services-act-ein-ueberblick.

SOUZA, Nivaldo. Anatel segue cotada como órgão regulador das plataformas no PL das Fake News. *JOTA*, 02 maio de 2023. Disponível em: <https://www.jota.info/legislativo/anatel-segue-cotada-como-orgao-regulador-das-plataformas-no-pl-das-fake-news-02052023>.

_____. Relatório do PL das Fake News não cria autoridade autônoma de fiscalização. *JOTA*, 28 abr. 2023. Disponível <https://www.jota.info/legislativo/relatorio-do-pl-das-fake-news-nao-cria-autoridade-autonoma-de-fiscalizacao-28042023>.

The Digital Services Act: your guide to the EU's new content moderation rules. Access Now, março de 2023. Disponível em: https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/.

TURILLAZZI, Aina; CASOLARI, Federico; TADDEO, Mariarosaria; FLORIDI, Luciano. ***The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications***. Janeiro de 2022. Disponível em: https://ssrn.com/abstract=4007389. Acesso em: 23 maio 2023.

TOLEDO, Renato. **Governança regulatória e organização administrativa**. JOTA, 07 jun. 2023. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/reg/governanca-regulatoria-e-organizacao-administrativa-07062023>.

VERMEULEN, Mathias. ***Online Content: To Regulate or not to Regulate - Is that the Question?*** APC Issue Paper, ago. 2019. Disponível em: <https://ssrn.com/abstract=3557914>.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

3

Responsabilidade civil da e nas redes: ocaso de parâmetros de ponderação e eclosão de dilemas causais

BERNARDO DINIZ ACCIOLI DE VASCONCELLOS

BERNARDO DINIZ ACCIOLI DE VASCONCELLOS[1]

Dans une avalanche, aucun flocon ne se sent jamais responsable.[2]

Sumário: Introdução: responsabilidade, um termo polissêmico; 1. Ocaso de pelo menos três parâmetros do Superior Tribunal de Justiça; 2. Necessidade de o operador se debruçar sobre questões até então ignoradas: o nexo causal; Considerações finais; Referências

Introdução: responsabilidade, um termo polissêmico

O ano de 2023 será provavelmente lembrado como aquele em que a comunidade jurídica brasileira mais se voltou para o termo "responsabilidade", em suas diversas acepções: civil, penal, administrativa, moral... De fato, "serão responsabilizados", na voz passiva, foi conjugado, por ocasião dos ataques de 8 de janeiro, pelo presidente do Senado Federal, Rodrigo Pacheco,[3] pelo presidente da Câmara dos Deputados, Arthur Lira,[4] pela presidente do Supremo Tribunal Federal, Min.ª Rosa Weber,[5] pelo presidente do TSE, Min. Alexandre de Moraes,[6] e pelo ministro da Justiça e da Segurança Pública, Flávio Dino.[7]

1. Mestrando em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Bacharel em Direito, com ênfase em Contencioso, pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Assistente acadêmico da disciplina "Direitos da Personalidade e Novas Tecnologias", da pós-graduação em Direito Digital do ITS Rio em parceria com a UERJ-CEPED. Advogado. E-mail: baccioli@outlook.com.br.

2. Citação atribuída por vezes a Voltaire, por vezes a Stanislaw Jerzy Lec.

3. MINGOTE, Bianca. Invasores serão responsabilizados e pagarão pelos danos, diz Pacheco. **Senado Notícias**, 11/01/2023. Disponível em: https://www12.senado.leg.br/noticias/audios/2023/01/invasores-serao-responsabilizados-e-pagarao-pelos-danos-diz-pacheco. Acesso em 24/05/2023.

4. XAVIER, Luiz Gustavo. Lira diz que todos serão chamados à responsabilidade, inclusive parlamentares: presidente inclui "parlamentares que postaram vídeos publicando inverdades sobre as agressões ao prédio da Câmara. **Agência Câmara de Notícias, 16/01/2023**. Disponível em: https://www.camara.leg.br/noticias/934281-lira-diz-que-todos-serao-chamados-a-responsabilidade-inclusive-parlamentares/. Acesso em 24/05/2023.

5. "Os que a conceberam, os que a praticaram, os que a insuflaram e os que a financiaram serão responsabilizados com o rigor da lei nas diferentes esferas. Só assim, se estará a reafirmar a ordem constitucional, sempre com observância ao devido processo legal, resguardadas, a todos os envolvidos, as garantias do contraditório e da ampla". ATAQUES golpistas não abalaram crença na democracia, diz Rosa Weber: ministra discursou na abertura do Ano Judiciário no plenário do STF. **Agência Brasil,** 01/02/2023. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2023-02/ataques-golpistas-nao-abalaram-crenca-na-democracia-diz-rosa-weber. Acesso em 24/05/2023.

6. VELOSO, Natália. Extremistas serão responsabilizados, diz Alexandre de Moraes: ministro afirma que bolsonaristas radicais que participaram de atos violentos nas sedes dos Três Poderes serão punidos. **Poder 360**, 08/01/2023. Disponível em: https://www.poder360.com.br/justica/extremistas-serao-responsabilizados-diz-alexandre-de-moraes/. Acesso em 24/05/2023.

7. ALVES, Chico. Financiadores de atos ilegais serão responsabilizados, diz Flávio Dino. **Uol Notícias**, 08/01/2023. Disponível em: https://noticias.uol.com.br/colunas/chico-alves/2023/01/08/financiadores-de-atos-ilegais-serao-responsabilizados-diz-flavio-dino.htm?utm_source=twitter&utm_medium=social-media&utm_content=geral&utm_campaign=noticias. Acesso em 24/05/2023.

Por mais que, evidentemente, a acepção primeira do termo "responsabilizado", no contexto, remeta à ideia de punição por meio do direito penal, um *ex delicto*, uma decorrência civilista, pôde ser notado na fala de algumas das autoridades (como o "...e pagarão pelos danos", de Pacheco).

De fato, com os atos antidemocráticos, o tema de imputação e ressarcimento de danos ocorridos na rede — ou ocorridos fora dela, mas iniciados ou impulsionados a partir dela — tem voltado à tona, revolvendo com força dois temas que sempre foram afetos: escolhas jurídico-políticas e elementos responsabilidade civil. Dizer se se indeniza, por que se indeniza, o quanto se indeniza e quem indeniza: cada uma dessas perguntas singularmente considerada remete o intérprete a diversas cláusulas gerais.[8] Apesar de a responsabilidade se configurar apenas no caso de convergência das respostas, a escolha da metodologia empregada permite muitas vezes, na prática, que o intérprete escolha a resposta em casos limítrofes. Isso porque, com frequência, mais de uma solução é possível e válida à solução desses questionamentos, o que pode ensejar resultados heterogêneos para uma mesma questão.

De mais a mais, em um contexto de PL das *Fake News* (PL 2.630/2020), tema 987 do STF (constitucionalidade do *caput* do art. 19 do Marco Civil da Internet, Lei nº 12.965/2014), "*duty of care*", "riscos sistêmicos", Google *vs*. González[9] e Twitter *vs*. Taamneh *et al*.,[10] nunca se falou tanto sobre radicalização, desinformação e responsáveis. É necessário, contudo, observar que, conquanto a argumentação em relação aos pressupostos da responsabilidade civil possa, de fato, acarretar mais de uma resposta certa, a resposta precisa ser compatível com a lógica, com a estrutura e com a função do instituto.

A dinâmica das redes, apesar por vezes se assemelhar à mídia tradicional, a ela não se limita. A Internet e as mídias sociais não são um desenvolvimento natural e linear da televisão e do rádio, que possam ser absorvidos por inter-

8. As perguntas remetem aos pressupostos da responsabilidade civil segundo: dano, antijuridicidade, fator de atribuição e nexo causal. GOLDENBERG, Isidoro. **La relación de causalidad en la responsabilidad civil**, 2ª ed., Buenos Aires: La Ley, 2000.

9. Google vs. González 598 U. S. ____ (2023)

10. Twitter vs. Taamneh et al 598 U. S. ____ (2023)

pretação analógica,[11] de modo que podem ser açodadas tanto a extensão à rede da jurisprudência e dos dispositivos relativos aos veículos de comunicação social quanto uma ideia de tratamento uniforme aos diferentes tipos de plataformas, e, dentro delas, aos diferentes tipos de perfil.

Nesse sentido, torna-se relevante e oportuno que se retomem os pressupostos e o estado da arte da responsabilidade civil brasileira, salientando algumas das particularidades e dos desafios do enfrentamento de cada um deles na e pela rede, tendo em vista as formas pelas quais esta funciona. Dessa forma, o presente artigo pretende responder à pergunta: quais são os desafios da responsabilidade civil brasileira da e nas redes? Para tanto, analisa-se como as particularidades fáticas do funcionamento das mídias sociais interferem nas categorias clássicas dos pressupostos da responsabilidade, bem como seu impacto daquelas nos critérios comumente usados pelo Superior Tribunal de Justiça na solução de conflitos.

1. Ocaso de pelo menos três parâmetros do Superior Tribunal de Justiça

O Superior Tribunal de Justiça tem elencado diversos critérios de ponderação para conflitos envolvendo liberdade de expressão e direitos da personalidade.[12] Trata-se de parâmetros que o intérprete deve observar para definir a existência de dano indenizável, ou, de certa forma, que adentram o requisito da culpa ou do dolo, ou, ainda, da boa-fé (por vezes objetiva, por vezes subjetiva) do suposto ofensor.

11. STF, Medida cautelar na tutela provisória antecedente 39/DF, Rel. Min. Nunes Marques, J. 02/06/2022, pp. 19. No interessante trecho, o Min. Nunes Marques registrou que "Outro ponto importante é que a internet está aberta a todos os candidatos. Não existe nesse meio de comunicação um mecanismo pelo qual um candidato possa impedir o outro de se exprimir. Não há uma estação difusora nas mãos de alguém. Ante os baixos custos e a facilidade da publicação de conteúdo na internet, a manifestação de um candidato não impede nem limita a manifestação de seus concorrentes. Logo, a ideia de que o meio de comunicação pode desigualar a disputa precisa ser repensada aqui em termos diferentes daqueles que estavam na base das interpretações sobre a televisão e o rádio, sob pena de a intervenção judicial vir a, ela mesma, desequilibrar o pleito em favor de candidatos que, por qualquer razão, não souberam ou não quiseram ingressar nessa nova forma de expressão comunicativa".

12. São eles: a) a veracidade da notícia; b) a notoriedade do retratado (se pessoa desconhecida ou se pessoa famosa); c) o grau de identificação do retratado; d) a licitude do meio empregado para a obtenção da informação; e) o local do fato (se público ou privado); f) o interesse público e jornalístico na divulgação do fato; g) o grau de atualidade da matéria; h) o grau de necessidade de veiculação da imagem para noticiar o fato; i) o grau de preservação do contexto original; j) a expectativa de privacidade do retratado; k) a continência e a pertinência do fato noticiado; l) a ausência da intenção de ofender; m) a ausência de abuso do direito de informar; e n) em caso de imagem, o grau de exposição do retratado (se isolado, ou se inserido numa multidão, por exemplo). Estes critérios são todos explorados por Maria Celina Bodin de Moraes, Luís Roberto Barroso e Anderson Schreiber. Cf. BODIN DE MORAES, Maria Celina. Honra, liberdade de expressão e ponderação. **Civilistica.com**. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: http://civilistica.com/honraliberdade-de-expressao-e-ponderacao/. Acesso em 10 jul. 2020. BARROSO, Luís Roberto. Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do código civil e da lei da imprensa. In. **Revista de Direito Administrativo** v. 235, jan.-mar. 2004, Rio de Janeiro, pp. 25-27. SCHREIBER, Anderson. **Direitos da personalidade**, 3ª ed. São Paulo: Atlas, 2014, p. 116.

Em relação aos direitos à imagem e à intimidade, o tribunal tem entendido que a expectativa de privacidade da vítima deve ser sopesada pelo magistrado[13], notadamente que "a captação e a divulgação de qualquer manifestação pessoal do sujeito sem o seu consentimento devem ser admitidas apenas em caráter excepcional, quando justificadas por outros interesses merecedores de tutela à luz do ordenamento jurídico". [14]

Nesse sentido, por exemplo, a Terceira Turma do STJ já entendeu que a divulgação de conversa mantida em aplicativo de mensageria privada configura dano moral[15]. No julgado, sopesadas as particularidades do caso concreto, aludiu-se, sobretudo, ao fato de que as partes haviam optado por um aplicativo que criptografasse as comunicações, e que a finalidade da exposição não foi proteger outros direitos, mas apenas causar dano. Dessa forma, na ponderação entre direito à intimidade e direito à liberdade de informação, aquele deveria prevalecer.

Apesar de o argumento, por si só, não ser apto à reforma da conclusão da ponderação, indaga-se: até que ponto a criptografia do aplicativo foi preponderante para sua escolha pelas partes? Ou ainda: a existência de criptografia enseja, por si só, expectativa de privacidade? Isso porque, por mais que se presuma que a conversa não será interceptada por terceiros, não é possível afirmar que a arquitetura do aplicativo em questão se assemelhe a uma cabine blindada: o próprio aplicativo permite o encaminhamento de mensagens, não há qualquer vedação a capturas de tela, e as mensagens permanecem no grupo, a princípio, eternamente.[16] A efemeridade do real se contrapõe ao registro do digital.

Efeito semelhante ocorre em relação ao direito à imagem. A doutrina elenca o critério do "grau de consciência do retratado em relação à captação de

13. "[O] grau de consciência do retratado em relação à possibilidade de captação de sua imagem no contexto de onde foi extraída". (SCHREIBER, Anderson. **Direitos da personalidade**, 3ª ed. São Paulo: Atlas, 2014, p. 116).

14. SCHREIBER, Anderson. **Direitos da personalidade**, 3ª ed. São Paulo: Atlas, 2014, p. 148.

15. STJ, REsp n. 1.903.273/PR, relatora Ministra Nancy Andrighi, Terceira Turma, julgado em 24/8/2021, DJe de 30/8/2021.

16. O WhatsApp, por exemplo, desde o final de 2022, implementou mecanismo que torna impossível a realização de capturas de tela em imagens de visualização única. Apesar de a medida não ser infalível (ainda é possível tirar uma fotografia da tela com uma câmera externa), evidentemente há uma maior expectativa de privacidade no caso em imagens efêmeras. SAIBA como bloquear prints de fotos e vídeos de visualização única no WhatsApp: com a atualização mais recente, aplicativo de mensagens passou a impedir capturas de qualquer mídia temporária de forma nativa. **G1**, 13/12/2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/12/13/saiba-como-bloquear-prints-de-fotos-e-videos-de-visualizacao-unica-no-whatsapp.ghtml. Acesso em 01/06/2023.

sua imagem no contexto de onde foi extraída", como no célebre caso de modelo que manteve relações sexuais, em público, mas em praia reclusa.[17] Seria possível argumentar que alguém que mantém seu perfil aberto, nas mídias sociais, ou que possua milhões de seguidores em sua conta (ainda que fechada), por exemplo, poderia imaginar que sua imagem seria usada para ilustrar uma notícia sobre si? Nesses casos, talvez o parâmetro de expectativa possa operar, no mundo digital, contra a proteção da pessoa humana, de modo que um critério de vinculação da captação ou da divulgação à finalidade inicialmente dada pela vítima parece mais objetivamente aferível e mais protetivo.[18]

Por último, o critério de notoriedade do retratado (por vezes referido como o critério da "pessoa pública" ou de "figura pública") já era bastante criticado pela doutrina.[19] Com efeito, o argumento de figura pública é usado com frequência para afastar o dano moral decorrente de excessos da liberdade de expressão ou da liberdade de imprensa.[20] Entretanto, na complexidade atual das redes, o critério, já controvertido, torna-se excessivamente elástico. Sobre o tema, é interessante remeter aos dois votos vencidos do caso Shkelzen Berisha *vs*. Guy Lawson, *et al.*, da Suprema Corte dos Estados Unidos,[21] justamente por se tratar de um país que apresenta todo o seu sistema de responsabilidade civil envolvendo liberdade de expressão centrada no conceito de figura pública.[22]

De antemão, é necessário ter em mente que o direito estadunidense faz uma clivagem importante entre o merecimento de tutela da pessoa comum e o merecimento de tutela da "figura pública" quando da aferição da existência de dano à honra indenizável. Naquele direito, "figuras privadas" necessitam apenas comprovar negligência comum, isto é, que o homem médio teria per-

17. SCHREIBER, Anderson. **Direitos da personalidade**, 3ª ed. São Paulo: Atlas, 2014, p. 116.

18. O princípio da finalidade já se encontra, por exemplo, na LGPD, art. 6º, I.

19. Anderson Schreiber critica, por exemplo, a nomenclatura "pessoa pública", porque "pessoas são privadas por definição" e os critérios baseados em "pessoa pública" e em "local público" na realidade mais autorizam violações da personalidade do que a protegem. (SCHREIBER, Anderson. **Direitos da personalidade**, 3ª ed. São Paulo: Atlas, 2014, p. 113).

20. Ver, por exemplo, STJ, AgInt no AREsp n. 2.166.995/SP, relator Ministro Antonio Carlos Ferreira, Quarta Turma, julgado em 12/12/2022, DJe de 15/12/2022; STJ, REsp n. 1.867.286/SP, relator Ministro Marco Buzzi, Quarta Turma, julgado em 24/8/2021, DJe de 18/10/2021.

21. Shkelzen Berisha vs. Guy Lawson et al., 594 US (2021).

22. Para uma análise mais extensa sobre a responsabilidade civil por escritos nos Estados Unidos, permita-se remeter a VASCONCELLOS, Bernardo Diniz Accioli de. Actual malice, Sistema Interamericano de Direitos Humanos e responsabilidade civil por dano à honra da figura pública: possíveis desafios sob o prisma civil-constitucional. **Civilistica.com**. Rio de Janeiro, a. 12, n. 1, 2023. Disponível em: <http://civilistica.com/actual-malice-sistema/>. Acesso em 31/05/2023.

cebido a falsidade, e isso admite algumas presunções. Entretanto, para que se conceba a violação da honra de "figuras públicas" é necessário comprovar, grosso modo, que (i) o fato desabonador à honra era falso; e (ii) que quem divulgou sabia da falsidade à época, ou que não claramente não se importava com a verdade.[23] Foi o que se estabeleceu em New York Times *vs.* Sullivan.[24] A diminuição da proteção das figuras públicas, desde o seu precedente fundante, sofreu uma série de esgarçamentos. Inicialmente concebida apenas para agentes públicos,[25] ela foi paulatinamente sendo estendida para figuras públicas,[26] e depois a toda e qualquer pessoa que se exponha ao debate público,[27] ainda que involuntariamente.[28]

No caso Berisha *vs.* Lawson, julgado em 2021, a Suprema Corte dos Estados Unidos reiterou sua jurisprudência e negou-se a admissão[29] de recurso contra decisão de corte inferior, que afastara indenização a Shkelzen Berisha. Berisha havia pleiteado compensação em decorrência da publicação de livro, por Guy Lawson e outros, associando-o à máfia albanesa e ao tráfico de armas, a partir de "fontes frágeis". Berisha era, de fato, filho de importante político da Albânia, mas seria ele uma figura pública para o público estadunidense? Dois votos vencidos, contudo, teceram interessantes observações sobre o critério de "figura pública", para o direito dos Estados Unidos, na atualidade.

23. Sobre o tema, permita-se remeter a MELLO, Rodrigo Gaspar. **Liberdade de expressão, honra e censura judicial**: uma defesa da incorporação da doutrina da malícia real ao direito brasileiro. 2ª Ed. Rio de Janeiro: Lumen Juris, 2021.

24. O regime jurídico anterior ao precedente permitia, com base em Crown vs. John Peter Zenger (1735), o exercício da exceção da verdade para qualquer que fosse a acusação, isto é, o ônus era do réu (MELLO, Rodrigo Gaspar. **Liberdade de expressão, honra e censura judicial**: uma defesa da incorporação da doutrina da malícia real ao direito brasileiro. 2ª Ed. Rio de Janeiro: Lumen Juris, 2021, pp. 18-21.). Antes de 1735, o entendimento majoritário da Star Chamber desde 1606 era no sentido de que "as imputações verdadeiras eram ainda mais graves do que as falsas porque teriam maior potencial de provocar a ruptura da paz". (Ibid., p. 17.).

25. New York Times Co. v. Sullivan, 376 U. S. 254, 280 (1964).

26. Curtis Publishing Co. *vs.* Butts e Associated Press v. Walker, 388 U.S. 130 (1967)

27. Gertz vs. Robert Welch, Inc., 418 U.S. 323, 334-335, 342 (1974)

28. 378 F. Supp. 3d 1145, 1158 (SD Fla. 2018); ver também Rosanova *vs.* Playboy Enterprises, Inc., 580 F. 2d 859, 861 (CA51978) ("Não basta, para rebater a afirmação de que uma pessoa é uma figura pública, afirmar, com sinceridade, que não se escolhe sê-lo").

29. No direito estadunidense, o writ of certiorari é uma das duas formas de se ter acesso à instância superior. Em linhas gerais, certiorari é o ato discricionário por meio do qual uma corte superior decide se vai ou não revisar o julgamento de um caso decidido por uma corte inferior. Em linhas gerais, pode ser traduzido como "avocação de causas para revisão". Cf. GOYOS JR, Durval de Noronha. Noronha's legal dictionary: English-Portuguese, Portuguese-English. 4th ed. São Paulo, Brasil: Editora Observador Legal, 2000, p. 66. Nesse caso, o Sr. Shkëlzen Berisha pediu à Suprema Corte que revisse o precedente constitucional aplicado pela corte inferior ao caso.

O Juiz Clarence Thomas registrou, por exemplo, que, antes do caso Sullivan, historicamente prevalecia a regra de que escritos contra pessoas públicas eram, na verdade, mais sérios e perigosos do que contra pessoas privadas, e que não estava claro como escolher se expor ao público justificaria menor grau de proteção do ordenamento jurídico, sobretudo quando a vítima não parecia ter buscado os holofotes voluntariamente. Ele aludiu, por exemplo, ao caso de Katherine McKee, que, lançada aos holofotes da mídia por denunciar um estupro, perdera o grau de proteção de honra que tinha enquanto não havia feito a denúncia[30] e viera a ser vítima de difamações.

O Juiz Neil Gorsuch, por sua vez, argumentou que, no mundo atual, a depender do recorte que se faça, qualquer pessoa pode se enquadrar no conceito de figura pública. Nesse sentido, o magistrado salientou que a dinâmica das redes sociais e o fato de que a mídia como um todo encontra-se altamente segmentada permitem que pessoas sejam ao mesmo tempo amplamente conhecidas para um público e absolutamente anônimas para outro. Apesar de a Corte já haver desenvolvido o conceito de pessoa pública de assunto específico (que remete ao contexto do discurso), o magistrado afirma que, na prática, o conceito é excessivamente maleável:

> Mas o mundo de hoje também lança uma nova luz sobre essas concepções. Hoje, cidadãos comuns podem se tornar "figuras públicas" nas mídias sociais da noite para o dia. Indivíduos podem ser considerados "famosos" devido a sua notoriedade em certos canais da nossa mídia, hoje altamente segmentada, ao passo que permanecem desconhecidos na maioria dos demais canais. Instâncias inferiores têm até mesmo entendido que um indivíduo pode tornar-se uma figura pública de assunto específico simplesmente se defendendo de uma declaração difamatória. Outras pessoas, como vítimas de violência sexual que procuram confrontar seus agressores, podem ter relutantemente escolhido adentrar a esfera pública e ainda assim acabar por também ser tratadas como figuras públicas de assunto específico. Em muitos aspectos, parece que chegamos a um mundo que foi aventado pelos votos vencidos dos julgados desta Corte que se originaram do caso Sullivan, mas rejeitado pelos votos condutores – um mundo onde "querendo ou não, todos nós somos figuras públicas em algum grau".
> Mais uma vez, não está claro até que ponto esses desdobramen-

30. 586 U. S. ____ (2019)

> tos recentes servem os propósitos originais do caso Sullivan. Não só essa doutrina evoluiu para um subsídio à publicação de falsidades em uma escala que ninguém poderia ter previsto, mas também veio a deixar sem reparação bem mais pessoas do que se poderia prever. E essas mesmas categorias e testes que esta Corte inventou e instruiu instâncias inferiores a usar – "famosos de forma generalizada", "figura públicas de assunto específico" – parecem cada vez mais maleáveis e até mesmo arcaicas quando qualquer um pode atrair algum grau de notoriedade do público em algum segmento de mídia. Regras que visavam à garantia de um debate robusto sobre as ações tomadas por agentes públicos de alto escalão que se encontravam à frente de assuntos públicos parecem, cada vez mais, deixar o americano comum sem recursos frente a terríveis difamações. Pelo menos tal como são aplicadas hoje, está longe do óbvio se as regras do caso Sullivan contribuem mais para encorajar pessoas de boa vontade a se engajar em um autogoverno democrático ou as desencorajar de arriscar a dar, por menor que seja, qualquer passo em direção à vida pública.[31]

No Brasil, interessante e recente caso, pautado pelo conceito de pessoa pública, foi analisado pelo Tribunal de Justiça do Estado de São Paulo, envolvendo uma caixa de supermercado e um deputado e apresentador de programa de televisão defensor dos direitos do consumidor. Em 2005, em célebre vídeo, o apresentador tentava levar apenas a unidade de produtos que normalmente seriam vendidos em engradados, pelo que a caixa recusou-se a vender separadamente. O apresentador reagiu efusivamente, alertando que chamaria a polícia. Tudo foi gravado por câmeras de televisão e ganhou grande repercussão.[32]

Quinze anos mais tarde, em 2020, o apresentador, candidato à Prefeitura de São Paulo, novamente veiculou o mesmo vídeo de 2005 em que discutia com a trabalhadora, mas dessa vez com finalidade eleitoral, e para criticar a funcionária. Em seguida, ele comentou em uma difusão ao vivo, no YouTube, que seu opositor teria contratado a referida funcionária para desaboná-lo na campanha à Prefeitura. Ajuizada a ação de indenização pelo uso indevido da imagem da funcionária, e pelo dano à honra decorrente dos comentários de

31. Berisha vs. Lawson, 586 U. S. ____ (2019), pp. 6-8, tradução livre do julgado.

32. O inusitado episódio repercute, até hoje, em páginas de memes. Contudo, não está no escopo do presente artigo o caráter humorístico do uso da imagem. No caso concreto, a reprodução se deu tão somente com fins comerciais e, em seguida, eleitorais.

que ela teria sido comprada pela oposição, o apresentador, então, sustentou que (i) a própria funcionária o havia criticado em público anteriormente; (ii) que ela realmente chegara a receber uma visita do candidato opositor; e (iii) que ele, apresentador, apenas teria se defendido das críticas, ainda que de forma áspera.

O Tribunal de Justiça do Estado de São Paulo, então, entendeu que não havia ofensa, fosse no uso desautorizado da imagem da funcionária, fosse à honra. Para tanto, sopesou o fato de que ela teria decidido "se manifestar politicamente via internet" desde 2016, e que "por ter-se colocado, ainda que limitadamente às circunstâncias do caso, como pessoa pública, deve tolerar maior flexibilidade em relação aos parâmetros aplicados na configuração do dano":

> Obrigação de fazer. Responsabilidade civil. Utilização, supostamente indevida, da imagem da autora pelo requerido, seguida de críticas pessoais, no bojo de campanha eleitoral por ele empreendida no ano de 2020. Ausência, todavia, de qualquer vulneração relevante a direitos de personalidade da autora. **Demandante que, por sua própria iniciativa, desde o ano de 2016 passara a se manifestar politicamente via internet, sendo inclusive procurada por jornalistas, partidos políticos e portais de conteúdo para replicação do conteúdo que produzira. Requerente que, ademais, e ainda que de maneira gratuita e bastante limitada, cedeu à campanha eleitoral de diametral oponente do requerido o direito de utilização de sua imagem, passando ainda a criticá-lo, enquanto candidato a cargo político**. Material produzido pelo demandado, pois, que o foi apenas em resposta à atuação voluntária da autora, e sem qualquer excesso em seu teor, ressalvadas eventuais pungência e eloquência de linguagem. Manifestações que se acham insertas no escopo da liberdade de expressão e de livre manifestação do pensamento. **Demandante que, por ter-se colocado, ainda que limitadamente às circunstâncias do caso, como pessoa pública, deve tolerar maior flexibilidade em relação aos parâmetros aplicados na configuração do dano, justamente pela posição que ocupa**. Ausência, em resumo, de lesão extrapatrimonial relevante. Sentença de improcedência mantida. Recurso improvido.[33]

Percebe-se, no caso em comento, como o parâmetro de "pessoa pública", empregado uma vez que a vítima se manifestou na Internet sobre o assunto,

33. TJSP; Apelação Cível 1004831-21.2021.8.26.0008; Relator Vito Guglielmi; Órgão Julgador: 6ª Câmara de Direito Privado; Foro Regional III - Jabaquara - 5ª Vara Cível; Data do Julgamento: 10/05/2023; Data de Registro: 10/05/2023, grifou-se.

foi utilizado, conquanto "limitadamente às circunstâncias do caso", para afastar a ampla proteção do direito à imagem que a pessoa humana recebeu, seja da Constituição da República, seja do Código Civil.[34]

Dessa forma, percebe-se como a Internet pode afetar, no mundo atual, os consolidados parâmetros de parâmetros de (i) expectativa de privacidade; (ii) grau de consciência do retratado em relação à captação de sua imagem no contexto de onde foi extraída; e (iii) pessoa pública.

Necessidade de o operador se debruçar sobre questões até então ignoradas: o nexo causal

O modelo tradicional de responsabilidade civil brasileira baseia-se na concomitância de três pressupostos: (i) dano injusto; (ii) conduta culpável (ou arriscada); e (iii) nexo causal entre a conduta e o dano.[35] Os dois últimos requisitos, prova da culpa (ou risco) e prova do nexo de causalidade, foram chamados pela academia ao longo das décadas de "filtros da responsabilidade civil" ou "filtros da reparação" por funcionarem como óbices à plena indenização da vítima.[36]

Com efeito, nos últimos séculos, a responsabilidade civil, inicialmente subjetiva, baseada na diabólica prova de culpa psicológica, caminhou para uma paulatina abordagem normativa. De igual modo, surgiram regimes de responsabilidade por culpa presumida, ou, então, da substituição do filtro da culpa pelo filtro do risco, dando origem à responsabilidade objetiva. O próprio risco, por sua vez, inicialmente criado como critério substituidor da culpa, distancia-se cada vez mais da responsabilidade objetiva, para criar uma formulação negativa de responsabilidade (a dita responsabilidade sem culpa).[37] Com o ocaso da culpa, o nexo causal assume, cada vez mais, o papel central da responsabilidade civil, para além de passar a garantir a segurança do instituto.[38]

34. No caso em comento, veja-se, tampouco havia atualidade da imagem captada em 2005. Tampouco parecia ser necessário expor novamente o rosto da funcionária. Caso se entendesse que a nova divulgação do evento de 2005 era essencial e decorrente de interesse público, ainda assim o rosto da funcionária poderia ter sido borrado.

35. CAVALIERI FILHO, Sergio. **Responsabilidade civil**. São Paulo: Atlas, 2014, p. 33. Como se mencionou em rodapé anteriormente, há autores que incluem o "fator de imputação" como um dos pressupostos.

36. A expressão no direito brasileiro é comentada por SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. 2 ed. São Paulo: Ed. Atlas, 2009.

37. SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Ed. Atlas, 2ª ed, 2011, p. 6.

38. GAMA, Guilherme Calmon Nogueira da; VIOLA, Rafael. Perspectivas sobre o nexo de causalidade: passado, presente futuro. **Revista de Direito Civil Contemporâneo**, v. 29, 2021, p. 240.

No direito brasileiro, consagrou-se o chamado "princípio da reparação integral" no art. 944, do Código Civil,[39] mas o agente só responde pelo dano na medida em que lhe deu causa: "é preciso saber o que indenizar".[40] Nessa toada, a doutrina, em análise à funcionalização do instituto, tem reconhecido ao nexo causal dois importantes papeis:[41] um primeiro, voltado para a imputação ("a quem se deve atribuir um resultado danoso", também chamado de nexo causal interno[42]); e um segundo, voltado para a aferição do dano indenizável (nexo causal externo).[43] Nesse sentido, é importante frisar que não mais à culpa se dá a medida da indenização, mas ao nexo.[44]

As novas mídias, por seu turno, chamam cada vez mais a atenção pela pluralidade de danos que uma mesma conduta pode ter, e pela pluralidade de vítimas. Imagina-se, por exemplo, que Caio divulgue vídeo em aplicativo de mensageria móvel, passando-se pelo médico Tício,[45] confessando uma série de condutas desabonadoras (algumas verdadeiras e outras falsas) e pregando contra a vacinação. Poder-se-ia imaginar lesão aos individuais personalíssimos de Tício, como imagem (nas vertentes imagem-atributo e imagem retrato),

39. Art. 944. A indenização mede-se pela extensão do dano.

40. MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2009, p. 82.

41. CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil**. Rio de Janeiro: Renovar, 2005, pp. 22/27. De igual modo, Cristiano Chaves de Farias, Nelson Rosenvald e Felipe Braga Netto concluem que " delimitação da indenização requer uma percuciente análise da causalidade, para que se no caso concreto saibamos "quem" indeniza e "o que" se indeniza. (ROSENVALD, Nelson et. al.. **Curso de Direito Civil**, vol. 3, 2ª Ed. São Paulo: Atlas, 2015, p. 367).

42. BREBBIA, Roberto H. **La relación de causalidad en derecho civil**. Rosario: Juris, 1975, pp. 47/48, **apud** MULHOLLAND, Caitlin Sampaio, **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2009, p. 98.

43. Idem.

44. CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil**. Rio de Janeiro: Renovar, 2005, p. 21.

45. A hipótese em análise envolve uso de deepfakes, i.e., recriação de faces e de expressões de pessoas por meio de inteligência artificial (SCHREIBER, Anderson et al.. Deepfakes: regulação e responsabilidade civil. In : TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **O direito civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, pp. 609-626). Ressalva-se que a prática por si só não é ilícita, à medida que pode ser usada para fins legítimos, como o humor (RAIS, Diogo. Desinformação e retirada de conteúdo. Webinar Imersão em Direito e Tecnologia. São Paulo: FGV, 06 nov. 2020. Disponível em <https://www.youtube.com/watch?v=sS6UqssLKgQ&feature=youtu.be>. Acesso em 06 nov. 2020). Recentemente, o uso da tecnologia popularizou-se em sites pornográficos, o que levou à criação de algoritmo que banisse a técnica (DEEPFAKE: La pornographie et la politique, les sujets de prédilection des vidéos truquées. **20 Minutes**, Paris, 10 out. 2019. Disponível em : < https://www.20minutes.fr/high-tech/2625039-20191010-deepfake-pornographie-politique-sujets-predilection-videos--truquees>. Acesso em 11 nov. 2020.)

honra (objetiva e subjetiva), nome, voz[46] e identidade pessoal,[47] ou até mesmo danos patrimoniais, se da situação Tício perdesse seus clientes do consultório.

Do outro lado da moeda, na faceta transindividual, viola-se o direito constitucional à informação,[48] daqueles que recebem o conteúdo fraudulento, por se tratar de conteúdo objetivamente falso,[49] além do direito à saúde daqueles que, crendo na mentira, recusam-se a se vacinar,[50] ensejando conforme as especificidades do caso dano moral coletivo,[51] ou ainda os chamados novos danos sociais.[52,53]

Como a responsabilidade passa por crescente objetivação, e como cada vez mais se reconhecem novos danos, o requisito do nexo causal, tradicionalmente deixado de lado, ou aferido de forma intuitiva[54], passa a receber importância fundamental. O nexo causal, como ressalta Agostinho Alvim, tem assu-

46. A voz, antes vista dentro do contexto do direito à imagem, dele ganhou autonomia. Cf. PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**: Vol. 1, 26ª Ed. Rev. e Atual. por Maria Celina Bodin de Moraes. Rio de Janeiro: Forense, 2013, p. 217.

47. Direito autônomo cada vez mais reconhecido pela doutrina, a violação ao direito à identidade pessoal está com frequência presente na divulgação de fake news sobre candidatos a cargos públicos. (KONDER, Carlos Nelson de Paula. O alcance do direito à identidade pessoal no direito civil brasileiro. **Pensar - Revista de Ciências Jurídicas**, v. 23, 2018. p. 4).

48. BARROSO, Porfirio; TALAVERA, María del Mar López. La libertad de expresión y sus limitaciones constitucionales, 1998, p. 49, **apud** BARROSO, Luís Roberto. **Colisão entre liberdade de expressão e direitos da personalidade**. Critérios de ponderação. Interpretação constitucionalmente adequada do código civil e da lei da imprensa. In. Revista de Direito Administrativo v. 235, jan.-mar. 2004, Rio de Janeiro.

49. CARVALHO, Luis Gustavo Grandinetti Castanho de. **Liberdade de informação e o direito difuso à informação verdadeira**. Rio de Janeiro: Ed. Renovar, 1994, p. 56.

50. O exemplo foi parcialmente baseado em caso real. (Não é verdade que vacina contra a Covid-19 cause câncer e danos genéticos ou torne alguém gay. **Folha de São Paulo**, São Paulo, 29 out. 2020. Disponível em: < https://www1.folha.uol.com.br/equilibrioesaude/2020/10/nao-e-verdade-que-vacina-contra-a-covid-19-cause-cancer-danos-geneticos-ou-homossexualismo.shtml >. Acesso em 02 nov. 2020).

51. Para uma distinção terminológica entre dano moral coletivo e dano social, remete-se a TARTUCE, Flávio. **Manual de direito civil**. 3ª ed. São Paulo: Método, 2020, e-book, n.p.

52. "Os danos sociais (...) são lesões à sociedade, no seu nível de vida, tanto por rebaixamento de seu patrimônio moral – principalmente a respeito da segurança – quanto por diminuição na qualidade de vida". (AZEVEDO, Antonio Junqueira de. Por uma nova categoria de dano na responsabilidade civil: o dano social. In: AZEVEDO, Antônio Junqueira de. **Novos estudos e pareceres de direito privado**. São Paulo: Saraiva, 2009, p. 378)

53. Enunciado 455 da V Jornada de Direito Civil do CJF/STJ: A expressão "dano" no art. 944 abrange não só os danos individuais, materiais ou imateriais, mas também os danos sociais, difusos, coletivos e individuais homogêneos a serem reclamados pelos legitimados para propor ações coletivas.

54. O nexo de causalidade é verdadeiramente um dos maiores mistérios da doutrina, sendo objeto de eterno dissenso. Ao se escolher o critério adotado, em ato verdadeiramente político, é possível atingir resultados diametralmente opostos dos que se atingiriam ao escolher critério diverso. As teorias causais dividem-se em generalizadora (teoria da equivalência dos antecedentes causais) e teorias individualizadoras: i) teoria da causa próxima; ii) teoria da causa eficiente e da causa preponderante; iii) teoria da causalidade adequada (e a subteoria da necessariedade da causa); iv) teoria do escopo da norma jurídica violada; v) teoria da ação humana; vi) teoria do dano direto e imediato; e vii) teoria da imputação objetiva. Atualmente, no direito brasileiro, encontram-se em maior uso as teorias do dano direto e imediato e da causalidade adequada, muito embora, na prática, poucas sejam as decisões judiciais que definam corretamente a teoria escolhida, ou mesmo que façam maiores digressões sobre a existência de nexo causal em cada caso concreto, de modo que frequentemente o tema é abordado de forma intuitiva e atécnica.

mido papel cada vez mais central na responsabilidade civil contemporânea.[55]

O ínsito funcionamento das novas mídias, por sua vez, apresenta interessantíssimos desafios, dentre eles a complexidade inerente ao fato de que parte das vítimas da desinformação, por exemplo, que não tem dever de dizer a verdade (culpa normativa), ou sequer culpa psicológica em muitos casos, contribui para a extensão do dano, ao recompartilhar o conteúdo, seja virtualmente, seja presencialmente.

Seria, então, o criador de um conteúdo danoso responsável por todos os seus recompartilhamentos? Seria possível responsabilizá-lo até mesmo pela extensão do dano a que um terceiro, que sequer o conhece, deu causa por meio de recompartilhamento? Há interrupção causal a cada recompartilhamento? Trata-se de um novo dano, ou de mera extensão do dano anterior?[56] Tratar-se-ia de concausa superveniente absolutamente independente, ou ainda de dano indireto? O compartilhamento por terceiros é consequência necessária da criação de *fake news*?[57] Pode-se no caso falar em causalidade mínima, ou ainda em causalidade aditiva no compartilhamento?[58] Há solidariedade entre todos os que contribuíram na cadeia causal?

Explica-se: é que até então o criador e difusor da notícia fraudulenta era com frequência o mesmo agente (imprensa ou editora), ao passo que nas redes sociais há o ingresso de milhões de usuários na cadeia informacional (e causal), em decorrência da possibilidade de compartilhamento do conteúdo lesivo.

55. ALVIM, Agostinho. **Da inexecução das obrigações e suas consequências**. São Paulo: Saraiva, 1955, p. 342.

56. Lívia Teixeira Leal e Mariana Ribeiro de Siqueira opinam que o compartilhamento seria mera continuidade da cadeia causal, ao se aplicar a teoria da condição sine qua non. LEAL, Lívia Teixeira; SIQUEIRA, Mariana Ribeiro. Responsabilidade civil pelo compartilhamento de mensagens pelo Whatsapp. In. SCHREIBER, Anderson et al.. **Direito e mídia**: tecnologia e liberdade de expressão. Indauatuba: Foco, 2020, p. 110.

57. Como explica Schreiber, a teoria do dano direto e imediato, aplicada tout court, excluía a ressarcibilidade do dano direto ou remoto. Dessa forma, desenvolveu-se a chamada subteoria da necessariedade causal, pela qual se podem "identificar danos indiretos, passíveis de ressarcimento, desde que sejam consequência necessária da conduta tomada como causa". (SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. 2 ed. São Paulo: Ed. Atlas, 2009, p. 59/60).

58. Aqui, sustenta-se que o impacto isolado de cada compartilhamento apresentaria contributo mínimo para o resultado danoso. O conceito é narrado por Mafalda Miranda Barbosa. "Do ponto de vista de cada um dos agentes, a causalidade diz-se, então, mínima. Da perspetiva da produção do dano, a causalidade pode afirmar-se como aditiva. Nessa medida, as hipóteses em apreço apresentam alguma similitude com as situações de causalidade cumulativa necessária: nestas, existe mais do que uma causa para o dano, sendo que todas são necessárias para que este se produza. Há, porém, uma diferença que não pode ser escamoteada: enquanto nas hipóteses de causalidade cumulativa necessária o que verdadeiramente se torna dilemática é a comprovação da adequação do comportamento para a produção do dano, cumprindo-se o teste da condicionalidade sem a qual, nos casos de causalidade aditiva, as dificuldades parecem situar-se nos dois polos, o da condicionalidade e o da adequação, já que, sendo o contributo causal de tal modo insignificante, a eliminação do comportamento do sujeito não alteraria o iter conducente ao dano". (BARBOSA, Mafalda Miranda. Causalidade mínima. In. BRAGA NETTO, Felipe Peixoto; SILVA, Michael César (Orgs.). **Direito privado e contemporaneidade**: desafios e perspectivas do direito privado no século XXI, vol. 3. Indaiatuba: Foco, 2020, pp. 3/24).

Disso poderia decorrer a responsabilidade de toda a cadeia causal solidariamente, caso se adotasse a teoria da causalidade adequada.[59] Essa teoria baseia-se no conceito de prognose póstuma. Como explica Viola, "a causalidade adequada prescinde da análise concreta [de causalidade], pautando-se em um juízo de probabilidade baseado na experiência da vida e da natureza do que normalmente se sucede com as coisas".[60] Esse juízo deve atender tanto à *prognose* póstuma feita por pessoa normal, quanto pelo agente causador do dano.[61]

Se, por um lado, essa teoria estende demais a cadeia causal, ela não parece ser, contudo, a teoria adotada pelo ordenamento jurídico brasileiro. O legislador, na redação do Código Civil de 2002, reproduziu a redação do diploma anterior,[62] consagrando a teoria da interrupção do nexo causal, (ou teoria do dano direto e imediato),[63] que envolve a noção de necessariedade da causa, desenvolvida por Dumoulin e Pothier.[64]

No Brasil, Agostinho Alvim destacou-se dentre os defensores dessa teoria, afirmando que "é indenizável todo o dano que se filia a uma causa, ainda que remota, desde que ela lhe seja causa necessária, por não existir outra que explique o mesmo dano".[65] Embora naturalmente se compartilhe algo que já existia, a mera condicionalidade (se A não tivesse criado o conteúdo danoso, B

59. LEAL, Lívia Teixeira; SIQUEIRA, Mariana Ribeiro. Responsabilidade civil pelo compartilhamento de mensagens pelo WhatsApp. In. SCHREIBER, Anderson et al.. **Direito e mídia**: tecnologia e liberdade de expressão. Indaiatuba: Foco, 2020, p. 120.

60. VIOLA, Rafael. **Risco e causalidade**. Indaiatuba: Foco, 2023, p. 141.

61. TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil**, volume 4: responsabilidade civil (Org. Gustavo Tepedino). Rio de Janeiro: Forense, 2020, p. 88.

62. Mais evidente, saliente-se, foi a solução argentina. Ao contrário do Código Brasileiro, o código civil daquele país destinou, dentro do capítulo destinado aos fatos, ao menos nove artigos sobre a investigação do liame causal (arts. 901/909). O legislador daquele país distingue entre as consequências imediatas de um fato (consecuencias inmediatas, que se costumam suceder segundo o curso natural e ordinário das coisas), consequências mediatas (consecuencias mediatas, que resultam da ligação do fato com um acontecimento distinto), e consequências casuais (consecuencias casuales, consequências mediatas imprevisíveis), definindo claramente as hipóteses de incidência de cada uma delas.

63. TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil**, volume 4: responsabilidade civil (Org. Gustavo Tepedino). Rio de Janeiro: Forense, 2020, p. 89.

64. De acordo com o exemplo clássico de Pothier, se A vende uma vaca para B, ocultando uma doença preexistente, A torna-se responsável não apenas pela morte do animal vendido, como também pela totalidade do gado de B acometida pelo contágio. Entretanto, se, em decorrência da morte do gado, B não consegue cultivar suas terras, e, em razão disso, não consegue pagar seus credores, que conseguem o decreto de falência de B, levando os bens de B a leilão a preço vil, não há de se falar em responsabilidade de A pelos mencionados danos, que seriam indiretos e teriam outras causas que não a venda da vaca contaminada, como a omissão de B em mitigar seus prejuízos, seja alugando gado que auxiliasse a cultivar as terras, seja cultivando ele próprio, sem a ajuda animal. (POTHIER, Robert Joseph. **Traité des obligations**, t. 1. Paris: Debure l'ainê, 1761, pp. 182-185)

65. ALVIM, Agostinho. **Da inexecução das obrigações e suas consequências**. São Paulo: Saraiva, 1972, p. 356.

não poderia ter compartilhado), sob a teoria do dano direto e imediato, não se confunde com a necessariedade aludida pela doutrina.[66]

Dessa forma, poder-se-ia questionar se, à luz do Código Civil, A, ao disseminar uma mensagem que contenha desinformação, ou ao compartilhar conteúdo erosivo à democracia, pode ser responsabilizado também pelo recompartilhamento e pela repercussão do material nas mídias sociais. Indaga-se: apesar de inevitavelmente ter havido culpa, até mesmo dolo, houve causalidade jurídica?

Essa discussão não era de grande relevância na era da grande mídia. Na realidade, fazia sentido que se usasse algum parâmetro como a repercussão da ofensa,[67] como a tiragem do jornal ou o índice de audiência da emissão, sobretudo porque criador e divulgador do conteúdo danoso se confundiam. Nas redes, entretanto, diante da possibilidade de compartilhamento orgânico muito superior ao inorgânico, surgem questionamentos. Por mais que um conteúdo publicado tenha sido inicialmente divulgado por robôs, são os usuários humanos os principais responsáveis por espalhá-lo.[68]

A solidariedade dos integrantes da cadeia de compartilhamento quanto ao dano ocasionado também suscita questões doutrinárias. Via de regra, a solidariedade não se presume (art. 265, CC), e, apesar do disposto no art. 942, *caput*, CC,[69] subsiste o questionamento quanto à ausência de solidariedade na causalidade sucessiva. Se se entender que a hipótese de recompartilhamento se amolda a esse conceito, quem posteriormente recompartilhasse conteúdo ilícito não seria tratado como coautor do dano: seria "como se o agente responsável pela 2ª série causal tivesse causado um dano distinto do anterior".[70]

66. O segundo pressuposto refere-se à relação entre o 1º e o 2º fato (e não mais entre o 1° fato e o dano). Se não existir qualquer relação entre esses dois fatos, ou se entre o 1º e o 2º fato existir apenas uma relação de mera condicionalidade, pode ocorrer a interrupção do nexo causal. No entanto, se entre o 1° e o 2° fato existir uma relação de necessariedade, de tal modo que o 2° fato seja conseqüência necessária do 1º, não há que se falar em interrupção do nexo causal. (CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil**. Rio de Janeiro: Renovar, 2005, p. 161.).

67. BODIN DE MORAES, Maria Celina. **Danos à pessoa humana**: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003 p. 295/296; e SCHREIBER, Anderson. Direitos da personalidade, 3ª ed. São Paulo: Atlas, 2014, 274 p.

68. DIZIKES, Peter. Study: On Twitter, false news travels faster than true stories: research project finds humans, not bots, are primarily responsible for spread of misleading information. **MIT News**, 08/03/2018. Disponível em: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308. Acesso em 30mai2023.

69. Art. 942. Os bens do responsável pela ofensa ou violação do direito de outrem ficam sujeitos à reparação do dano causado; e, se a ofensa tiver mais de um autor, todos responderão solidariamente pela reparação.

70. "Contudo, quando as causas são sucessivas, é possível cogitar-se de uma espécie de "causalidade parcial" em que cada uma das causas vai dar origem a uma parcela independente do dano que, justamente por ser formado por partes autônomas, será imputado a diferentes autores sem a regra da solidariedade. É como se o agente responsável pela 2ª série causal tivesse causado um dano distinto do anterior. Neste caso, 'impor a solidariedade é agredir a regra da causalidade jurídica'. Cada agente de-verá responder tão-só pelo dano que causou". (CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil**. Rio de Janeiro: Renovar, 2005, p. 30).

O efeito prático disso opera em desfavor da vítima: ajuizar ações contra todos os integrantes da cadeia de compartilhamento, para além de custoso, seria absolutamente impraticável quando o conteúdo se propaga em redes criptografadas, como os aplicativos de mensageria privada mais populares.

Longe de ser um problema teórico, já houve famosíssimos casos, no Brasil, de danos decorrentes da divulgação de informações falsas ou distorcidas causaram danos reais, ainda que a violência não fosse diretamente incitada pela mensagem, como no caso Escola Base (iniciado pela mídia tradicional), [71] e no linchamento de Fabiane de Jesus, dona de casa executada por supostamente praticar magia negra com crianças em Guarujá (em boato que se iniciou por rede social).[72]

A arquitetura das redes enseja maiores considerações atinentes à causalidade jurídica da responsabilização do que nela se propaga: assim como um vírus voluntariamente disseminado no centro de uma metrópole – em que o dano causado pelo Paciente Zero rapidamente se espalha exponencialmente aos demais pacientes, que não cogitam estarem contaminados – os danos causados pela disseminação de desinformação aproveitam-se de concausas para se espalhar. Nesse sentido, Rais:

> É muito comum que o uso das primeiras vítimas como uma espécie de elo para compor uma corrente difusora de fake news. Assim, aquelas pessoas que de boa-fé acreditam estar em contato com uma verdadeira notícia passam – ainda que sem perceber – a colaborar com a disseminação e difusão de notícias falsas. Portanto, toda essa produção de escoa com o apoio das próprias vítimas.[73]

Dessa forma, esse movimento, a princípio direta e artificialmente induzido pelos agentes propagadores de desinformação, acaba por produzir a maior parte de seus danos por meio de suas próprias vítimas, que passam a integrar

71. SILVA, Gabriela de Barros. Como o caso Escola Base enterrou socialmente os envolvidos. **Canal de Ciências Criminais**, 18 mai. 2018. Disponível em: <https://canalcienciascriminais.com.br/caso-escola-base/>. Acesso em 20 out. 2020.

72. ROSSI, Mariane. Mulher espancada após boatos em rede social morre em Guarujá, SP. **G1**, Rio de Janeiro, 5 abr. 2014. Disponível em: <http://g1.globo.com/sp/santos-regiao/noticia/2014/05/mulher-espancada-apos-boatos-em-rede-social--morre-em-guaruja-sp.html>. Acesso em 20 out. 2020.

73. RAIS, Diogo; SALES, Stela Rocha. Fake news, deepfakes e eleições. In. RAIS, Diogo (Org.). **Fake news**: a conexão entre a desinformação e o direito, 2ª Ed. São Paulo: RT, 2020, p. 31.

a cadeia causal.[74] Nessa toada, até mesmo a analogia com vírus encontra limites, porque o vírus não exige ação ou até mesmo vontade do hospedeiro para se espalhar.[75]

Ainda sobre o tema, a doutrina civilista precisa se voltar para questões como a causalidade intermediada psiquicamente, seja nas condutas omissivas, seja nas omissivas, que nem no direito penal encontram solução consensual.[76] Até que ponto se poderia dizer que a informação ou a mensagem de ódio, veiculadas por A, deram causa a dano produzido por B, no sentido de influenciar decisivamente na sua tomada de decisão? Ou, então, imagine-se que, superada a questão da imputação da plataforma no direito brasileiro,[77] até que ponto se pode dizer que o algoritmo de recomendação, por exemplo, causou um atentado terrorista?[78]

Os inúmeros debates quanto às controvérsias causais na rede ainda são bastante tímidos, mas são necessários para que se garanta segurança jurídica das decisões e respostas congruentes com o sistema de responsabilidade civil adotado pelo direito brasileiro. Afinal, apesar de ainda ser abordado de forma intuitiva, o nexo causal possui requisitos normativos e deve ser provado pelo autor (art. 373, I, CPC), e não apenas negado pelo réu (até porque, ainda que o réu possa provar a interrupção da causalidade, não se pode provar a ausência de causalidade, prova negativa). O ônus da prova impõe ao autor a comprovação do nexo, e, consequentemente, ao juiz de o fundamentar, sob pena de nulidade da decisão (art. 93, X, CF; e art. 489, §1º, CPC).

74. A doutrina tem dividido os agentes propagadores de fake news em cinco categorias: i) robôs (totalmente automatizados); ii) ciborgues (parcialmente automatizados); iii) robôs políticos (pessoas reais que emprestam suas contas para robôs de campanhas eleitorais); iv) fake clássico (pessoas reais); e v) ativistas em série. Além disso, identificou-se que a propagação de fake news é muito mais intensa entre pessoas reais do que por perfis automatizados (RAIS, Diogo; SALES, Stela Rocha. **Op. Cit.**, p. 35).

75. Na verdade, a contaminação massiva de uma população de víveres por vírus é um dos exemplos clássicos de Pothier de dano direto e imediato (Cf. nota de rodapé 64). A analogia com a rede apresenta problemas, porque animais não são imputáveis, seja porque o contágio, no caso, entre os animais, não é um ato voluntário.

76. Sobre o tema, remete-se a ROXIN, Claus. Problemas da causalidade intermediada psiquicamente. **Revista Brasileira de Ciências Criminais**, vol. 100, 2013, pp. 253-285.

77. Atualmente, o art. 19 do Marco Civil da Internet confere imunidade às plataformas pelo conteúdo inserido por terceiros até que haja ordem judicial específica de remoção.

78. Essa discussão foi objeto de discussão, pela Suprema Corte dos Estados Unidos, no recente caso Twitter v. Taamneh, referenciado na introdução deste artigo. No litígio, buscava-se a responsabilização civil da plataforma pelo ataque terrorista promovido pelo Estado Islâmico em uma boate na Turquia. A Corte ressaltou que: "*When there is a direct nexus between the defendant's acts and the tort, courts may more easily infer such culpable assistance. But, the more attenuated the nexus, the more courts should demand that plaintiffs show culpable participation through intentional aid that substantially furthered the tort. And, if a plaintiff 's theory would hold a defendant liable for all the torts of an enterprise, then a showing of pervasive and systemic aid is required to ensure that defendants actually aided and abetted each tort of that enterprise*". (Acórdão, p. 30).

Considerações finais

Este artigo pretendeu abordar os desafios da responsabilidade civil brasileira da e nas redes. Para tanto, discorreu-se sobre as dificuldades que os parâmetros de expectativa de privacidade, de grau de consciência do retratado em relação à captação de sua imagem no contexto de onde foi extraída; e de pessoa pública — comumente aludidos pela jurisprudência do Superior Tribunal de Justiça e pela doutrina civilista — enfrentam quanto aplicados à lógica das novas mídias e do funcionamento da rede.

Em seguida, abordaram-se diversas situações em que a discussão do conteúdo normativo do nexo causal e de sua prova precisam ser chamados ao centro do debate da responsabilidade civil. A dinâmica descentralizada de disseminação de informações na Internet suscita interessantíssimas discussões quanto a questões como causalidade mínima, causalidade intermediada psiquicamente, causalidade na instigação, causalidade omissiva, causalidade sucessiva e imputação e solidariedade de toda a cadeia de compartilhamento. Com a crescente superação dos demais requisitos da responsabilidade, que passa por crescente objetivação, o nexo causal, antes aferido muitas vezes intuitivamente, passa a desempenhar papel central. A dinâmica da Internet, por sua vez, parece complicar cada vez mais um tema já espinhoso.

Por fim, conclui-se que, a despeito de haver um anseio político por maior responsabilidade, há questões importantes atinentes à causalidade a serem enfrentadas tanto pela doutrina, quanto pela jurisprudência, sobretudo se consideradas a distribuição do ônus da prova pelo Código de Processo Civil Brasileiro e a necessidade de fundamentação das decisões judiciais quanto aos pressupostos da responsabilidade.

Referências

ALVIM, Agostinho. **Da inexecução das obrigações e suas consequências**. São Paulo: Saraiva, 1955

ALVIM, Agostinho. **Da inexecução das obrigações e suas consequências**. São Paulo: Saraiva, 1972

AZEVEDO, Antonio Junqueira de. Por uma nova categoria de dano na responsabilidade civil: o dano social. In: AZEVEDO, Antônio Junqueira de. **Novos estudos e pareceres de direito privado**. São Paulo: Saraiva, 2009

BARBOSA, Mafalda Miranda. Causalidade mínima. In. BRAGA NETTO, Felipe Peixoto; SILVA, Michael César (Orgs.). **Direito privado e contemporaneidade: desafios e perspectivas do direito privado no século XXI**, vol. 3. Indaiatuba: Foco, 2020

BARROSO, Luís Roberto. Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do código civil e da lei da imprensa. In. **Revista de Direito Administrativo** v. 235, jan.-mar. 2004, Rio de Janeiro, pp. 1-36.

BODIN DE MORAES, Maria Celina. **Danos à pessoa humana:** uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003

BODIN DE MORAES, Maria Celina. Honra, liberdade de expressão e ponderação. **Civilistica.com**. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: http://civilistica.com/honra-liberdade-de-expressao-e-ponderacao/. Acesso em 10 jul. 2020

CAVALIERI FILHO, Sergio. **Responsabilidade civil**. São Paulo: Atlas, 2014

CARVALHO, Luis Gustavo Grandinetti Castanho de. **Liberdade de informação e o direito difuso à informação verdadeira**. Rio de Janeiro: Ed. Renovar, 1994

CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil**. Rio de Janeiro: Renovar, 2005

GAMA, Guilherme Calmon Nogueira da; VIOLA, Rafael. **Perspectivas sobre o nexo de causalidade: passado, presente futuro**. Revista de Direito Civil Contemporâneo, v. 29, 2021, p. 240.

GOLDENBERG, Isidoro. ***La relación de causalidad en la responsabilidade civil***, 2ª ed., Buenos Aires: La Ley, 2000

GOYOS JR, Durval de Noronha. ***Noronha's legal dictionary: English-Portuguese, Portuguese-English***. 4th ed. São Paulo, Brasil: Editora Observador Legal, 2000, p. 66

KONDER, Carlos Nelson de Paula. O alcance do direito à identidade pessoal no direito civil brasileiro. **Pensar - Revista de Ciências Jurídicas**, v. 23, 2018

LEAL, Lívia Teixeira; SIQUEIRA, Mariana Ribeiro. **Responsabilidade civil pelo compartilhamento de mensagens pelo Whatsapp**. In. SCHREIBER, Anderson et al.. Direito e mídia: tecnologia e liberdade de expressão. Indauatuba: Foco, 2020, p. 110

MELLO, Rodrigo Gaspar. **Liberdade de expressão, honra e censura judicial:** uma defesa da incorporação da doutrina da malícia real ao direito brasileiro. 2ª Ed. Rio de Janeiro: Lumen Juris, 2021

MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2009

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil:** Vol. 1, 26ª Ed. Rev. e Atual. por Maria Celina Bodin de Moraes. Rio de Janeiro: Forense, 2013

POTHIER, Robert Joseph. **Traité des obligations**, t. 1. Paris: Debure l'ainê, 1761.

RAIS, Diogo. Desinformação e retirada de conteúdo. **Webinar Imersão em Direito e Tecnologia**. São Paulo: FGV, 06 nov. 2020. Disponível

em <https://www.youtube.com/watch?v=s-S6UqssLKgQ&feature=youtu.be>. Acesso em 06 nov. 2020

RAIS, Diogo; SALES, Stela Rocha. Fake news, deepfakes e eleições. In. RAIS, Diogo (Org.). **Fake news**: a conexão entre a desinformação e o direito, 2ª Ed. São Paulo: RT, 2020

ROSENVALD, Nelson et. al.. **Curso de Direito Civil**, vol. 3, 2ª Ed. São Paulo: Atlas, 2015

ROXIN, Claus. **Problemas da causalidade intermediada psiquicamente**. Revista Brasileira de Ciências Criminais, vol. 100, 2013, pp. 253-285

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil:** da erosão dos filtros da reparação à diluição dos danos. São Paulo: Ed. Atlas, 2ª ed, 2009

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil:** da erosão dos filtros da reparação à diluição dos danos. São Paulo: Ed. Atlas, 2ª ed, 2011

SCHREIBER, Anderson. **Direitos da personalidade, 3ª ed.** São Paulo: Atlas, 2014

SCHREIBER, Anderson et al.. **Deepfakes:** regulação e responsabilidade civil. In : TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **O direito civil na era da inteligência artificial**. São Paulo: Thomson Reuters Brasil, 2020, pp. 609-626

TARTUCE, Flávio. **Manual de direito civil**. 3ª ed. São Paulo: Método, 2020, e-book, n.p.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil, volume 4**: responsabilidade civil (Org. Gustavo Tepedino). Rio de Janeiro: Forense, 2020

VASCONCELLOS, Bernardo Diniz Accioli de. Actual malice, Sistema Interamericano de Direitos Humanos e responsabilidade civil por dano à honra da figura pública: possíveis desafios sob o prisma civil-constitucional. **Civilistica.com**. Rio de Janeiro, a. 12, n. 1, 2023. Disponível em: <http://civilistica.com/actual-malice-sistema/>.

VIOLA, Rafael. **Risco e causalidade**. Indaiatuba: Foco, 2023

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

4

Plataformização do trabalho artístico e o cooperativismo artesanal da Artisans

VICTOR GOMES BARCELLOS

VICTOR GOMES BARCELLOS[1]

Sumário: Introdução. 1. A plataformização da sociedade. 2. A plataformização do setor artístico. 3. Cooperativismo de plataforma como alternativa. 4. Cooperativas de plataforma no setor artístico. 5. O case da Artisans Cooperative. Considerações finais. Referências.

Introdução

A plataformização tem se consolidado tanto como uma tendência geral para o trabalho no século XXI nos mais diversos setores da economia. A grande maioria das cadeias de produção passa hoje, em alguma medida, por uma plataforma digital - até mesmo nos setores mais tradicionais. Deste modo, um modelo de negócios recente, que nasce num contexto muito específico e em segmentos particulares tem se expandido na tentativa de se consolidar como o novo paradigma para o trabalho mundial.

Apesar de se observar o caráter expansionista da plataformização, a compreensão de seus efeitos exige uma análise localizada, capaz de observar seus efeitos em segmentos específicos. Pela tendência monopolística das plataformas, os artistas se vêem obrigados a se alienar de suas obras para suas empresas detentoras e aceitarem suas regras, de maneira a poder fazê-las acessíveis ao público e conseguirem remuneração por seu trabalho. Observamos que os trabalhadores deste setor se encontram em uma situação contraditória - por um lado, as plataformas deram a eles mais autonomia, reduziram barreiras de entrada e ampliaram seu público potencial. Por outro, tornaram-se extremamente dependentes delas, passaram a ter que adequar sua produção para a performance algorítmica e receberem rendimentos ínfimos e pouco transparentes.

Apesar dessa precária condição, os artistas desempenham papel importantíssimo na sociedade, desempenhando papel central nos processos de formação da nossa subjetividade. Quem somos, o que fazemos e o que queremos passam pelas representações consumidas em forma de arte. Além disso, historicamente, foi um segmento sempre marcado pelas características que cada vez mais têm marcado a realidade do trabalho digital e sendo chamadas de *gig*

1. Doutorando em Comunicação e Cultura na Universidade Federal do Rio de Janeiro (UFRJ). Coordenador de comunicação e marketing no Data Privacy Brasil. Assistente acadêmico da disciplina “Cidades Inteligentes” da Pós-graduação em Direito Digital ITS-UERJ. Contato: victorgbarcellos@gmail.com

economy (economia de bicos) - contratos por projetos, por tempo determinado e com remuneração variável. De certa forma, como afirma a cooperativa Art.coop em seu website, "os artistas são os trabalhadores de bico originais"[2]. Justamente por esses motivos, são um importante laboratório para a imaginação de novos mundos do trabalho possíveis.

O fenômeno da plataformização, apesar de se apresentar hoje como sinônimo de precarização e alienação, contém também potenciais reapropriações capazes de dar mais autonomia e melhores condições aos trabalhadores da arte. Deste modo, cabe aos criadores de todos os tipos criar novas formas de organização do trabalho artístico que combatam sua dupla alienação - dos outros trabalhadores e de suas obras. E em sinergia com os movimentos pela cultura livre[3], que reivindicam o acesso aberto aos bens culturais.

Atualmente, diversas comunidades de artistas se inspiram na proposta do cooperativismo de plataforma para prototipar modelos alternativos de governança do trabalho artístico. Com significativas diferenças entre si - desde organização formal, modelos de financiamento e porte - compartilham de dois princípios fundamentais: a gestão coletiva e a propriedade compartilhada. Assim, nessas experiências, almeja-se que as decisões centrais sejam tomadas coletivamente, e a propriedade da organização (com todos os ativos e passivos que a compõem) seja de todos envolvidos nela. Diante dos problemas suscitados por esse fenômeno, consideramos esses modelos alternativos de governança como possibilidades reais para um trabalho artístico mais democrático, igualitário e inclusivo.

Os debates em torno do tema ganham cada vez mais força ao redor do mundo e o ano de 2022 foi marcado por um grande aumento de sua presença nos ambientes acadêmicos e políticos. No Brasil, podemos destacar o papel da 7ª Conferência de Cooperativismo de Plataforma[4], promovida pelo *Platform Cooperativism Consortium* (PCC) em parceria com Instituto de Tecnologia e Sociedade (ITS) em novembro de 2022 no Rio de Janeiro, Brasil. A conferência reuniu centenas de pessoas de vários países interessadas no tema para discutir suas conexões com múltiplas áreas - políticas públicas, empreendedorismo,

2. Disponível em: <http://art.coop/>. Acesso em: 20/05/2023.

3. FOLETTO, Leonardo. A cultura é livre: uma história da resistência antipropriedade. São Paulo: Autonomia Literária, 2021.

4. Disponível em: <https://platform.coop/events/owning-the-future-sustainably-scaling-cooperatives-in-the-digital-economy/>. Acesso em: 20/05/2023.

mobilidade, artes, blockchain e muito mais. No entanto, ainda são poucas as iniciativas brasileiras que se apresentam como plataformas cooperativas – e a maioria delas não são cooperativas formalmente, mas coletivos, organizações da sociedade civil, startups e outros.

Neste trabalho, dedicamo-nos a analisar os impactos da plataformização no trabalho artístico e a proposta do cooperativismo de plataforma como um modelo alternativo. Na primeira parte, realizamos revisão bibliográfica sobre o conceito de plataformização, buscando na literatura suas principais definições e as colocando em diálogo. Então, realizamos o recorte para o setor artístico, buscando compreender seus efeitos específicos neste segmento. Em seguida, apresentamos o cooperativismo de plataforma como um movimento que vem ganhando aderência em todo o mundo e propõe um modelo mais democrático e igualitário para a organização do trabalho com arte. Por fim, analisamos a Artisans Cooperative[5], uma comunidade criativa de artesãos que está criando um marketplace cooperativo de arte feita à mão.

1. A plataformização da sociedade

As plataformas digitais vêm se consolidando como a infraestrutura básica da sociedade, intermediando as relações humanas e o acesso a bens e serviços públicos e privados. Mais especificamente para nosso interesse neste trabalho, observamos o número crescente de indivíduos que trabalham direta ou indiretamente por meio das plataformas digitais. Assim, para compreender a realidade do trabalho no presente e futuro, é preciso compreender sua lógica e suas influências nas dinâmicas laborais.

Apesar de estar em curso já nos últimos anos, essa tendência foi acelerada nos últimos anos, especialmente após a pandemia do Coronavírus. O distanciamento social e a instabilidade econômica aceleraram a plataformização, que explorou uma alta de demanda em suas duas pontas - a do trabalho e a do consumo. De um lado, aproveitou o aumento da oferta de trabalho de pessoas que perderam seus postos formais, e de outro se beneficiou do aumento da demanda por bens e serviços essenciais no isolamento social. Até mesmo os setores mais tradicionais foram impelidos a se digitalizar, migrando parte ou toda sua dinâmica para plataformas digitais.

5. Disponível em: <https://artisans.coop/>. Acesso em: 20/05/2023.

Um dos primeiros autores a teorizar sobre o regime de produção centrado em plataformas digitais foi Nick Srnicek, no livro *Platform Capitalism* (2017). Na definição do autor[6], as plataformas possuem quatro características principais:

a. seu papel de mediadoras - constituindo uma infraestrutura de mediação entre diferentes grupos.
b. seus efeitos de rede - ou seja, a relação entre o número de usuários de uma plataforma e seu valor.
c. o uso de subsídios cruzados - a oferta de serviços gratuitos com o objetivo de aumentar o número de usuários e monetizar outros serviços pagos.
d. a definição das "regras do jogo" - seu controle sobre as regras de interação, produção e circulação de valor dentro da rede.

Na visão do Srnicek, estamos diante da ascensão de uma nova fase do capitalismo, que tem por principal característica a exploração econômica dos dados. É também destacada a necessidade de uma análise multifocal, pois para o autor as novas tecnologias precisam ser acompanhadas de novos modelos organizacionais para se concretizarem.

Para Van Dijk, Poell e de Wall[7], pode-se dizer que adentramos uma nova ordem sociotécnica, a sociedade de plataforma. Sua obra busca evidenciar as bases das plataformas, chegando à conclusão de três elementos principais:

a) elas são abastecidas por dados;
b) organizadas por algoritmos;
c) geridas por relações de posse guiadas por modelos de negócios;
d) governadas por acordos de usuários.

Ainda segundo os autores, sua operação se processa por meio dos seguintes mecanismos - dataficação, comodificação e seleção. Assim, pode-se resumir a dinâmica das plataformas nos três passos que representam a apropriação dos dados, sua conversão em valor econômico e a seleção de quais produtos e serviços oferecer. Diante do fato de que elas são desenhadas com o propósito único de exploração, questionam-se como defender os valores públicos frente à expansão de sua presença em todas as esferas da vida em sociedade.

6. SRNICEK, Nick. Platform Capitalism. Cambridge: Polity Press, 2016.

7. VAN DIJCK, J.; POELL, T.; DE WAAL, M. The Platform Society. New York: Oxford, 2018.

De acordo com Grohmann[8], o fenômeno da plataformização deve ser entendido como a imbricação entre três fatores:

a) a financeirização;
b) a dataficação;
c) e a racionalidade neoliberal.

Em primeiro lugar, trata-se de uma gradual conversão de todos os valores em cifras financeiras, fazendo com o que o valor monetário se sobreponha a todos os outros. Em segundo, diz respeito à crescente presença dos dados na vida cotidiana e sua valorização enquanto commodity no modo de produção capitalista. Por fim, consolida uma racionalidade ditada pelas transações econômicas com o único objetivo da valorização de capital. Desse modo, evidencia um processo que é ao mesmo tempo tecnológico, financeiro e político; sem os quais a compreensão da plataformização cairia num reducionismo.

Portanto, de acordo com todos os autores citados, a plataformização não pode ser entendida simplesmente como a disseminação de uma nova tecnologia. Ela precisa ser entendida dentro de um contexto social, cultural e econômico. As plataformas conforme conhecemos atualmente não nasceram orientadas ao bem comum, com o objetivo de melhorar a qualidade de vida das pessoas, e sim orientadas à valorização do capital, potencializando a exploração econômica dos dados. Logo, seu propósito, os algoritmos que as regem e seus modelos de governança estão voltados à geração de excedente, seja financeiro ou informacional - e não ao atendimento das necessidades humanas.

Para Trebor Scholz, não apenas os pesquisadores críticos ao Capitalismo de Plataforma se deram conta de sua dimensão exploratória. Os próprios trabalhadores já demonstram consciência de que as promessas da chamada "economia do compartilhamento" (*sharing economy*) não se cumpriram. Se a ideologia que permeava o Vale do Silício na ascensão das primeiras plataformas prometia a libertação humana por meio da tecnologia e da flexibilidade, hoje os trabalhadores se dão conta de que na verdade ingressaram numa dependência cada vez maior das plataformas. E conclui: "o capitalismo de plataforma é incrivelmente não efetivo em cuidar das pessoas."[9]

8. GROHMANN, Rafael. Plataformização do trabalho: entre a dataficação, a financeirização e a racionalidade neoliberal. Disponível em: <https://seer.ufs.br/index.php/eptic/article/view/12188/10214>. Acesso em: 15/03/2021.

9. SCHOLZ, T. Uberworked and Underpaid. London: Polity Press, 2016. p. 61.

2. A plataformização do setor artístico

Se o fenômeno da plataformização se dissemina por todos os setores, deve-se considerar que seus impactos em cada um deles possuem especificidades e gradações distintas. Neste trabalho, elegemos o setor artístico para uma análise mais aprofundada, que se justifica pelo fato de que historicamente o setor sempre foi marcado pela informalidade, por baixa renda e pela ausência de controle dos artistas sobre suas obras.

A particularidade do setor cultural é destacada por Marisol Sandoval: a autora apresenta a contradição presente no trabalho chamada economia criativa, que apesar de ter sua atividade reconhecida socialmente como privilegiada, comumente apresenta condições de trabalho precarizadas e instáveis.

> Se há um achado principal que pode ser concluído das pesquisas sobre o trabalho no setor cultural, certamente é o de que as vidas nos trabalhos chamados criativos são complexas e contraditórias, combinando satisfação e níveis relativamente altos de autonomia com insegurança, baixos salários, ansiedade e desigualdade.[10]

Portanto, o discurso sobre a autonomia desse setor e o prestígio alcançado por alguns poucos artistas ofusca a realidade da massa de trabalhadores precarizados. A autora identifica, então, na carreira desses profissionais o ideal do capitalismo neoliberal, já que a pretensa liberdade de seu ofício faz com que toda a responsabilidade recaia sobre os indivíduos. O que muitas vezes resulta em ansiedade e insegurança, já que possuem poucas regulações e sindicatos com quem contar para a garantia de seus direitos.

A fragilidade dos trabalhadores da cultura fica ainda mais evidente em momentos de crise como o da pandemia de Covid-19. Se em tempos pré-pandêmicos o setor já era caracterizado pela instabilidade, neste momento se demonstrou como um dos setores mais impactados. De acordo com pesquisa do IPEA[11] 48,8% dos agentes culturais perdeu totalmente sua receita entre maio e julho de 2020. Como alternativas para a saída da crise, as necessidades mais apontadas pelos entrevistados foram: acesso a informações direcionadas ao

10. SANDOVAL, Marisol. Enfrentando a Precariedade com Cooperação: cooperativas de trabalhadores no setor cultural. Revista Parágrafo. v. 5, n. 1, p. 111-127, 2017. Disponível em: <http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/567>. Acesso em: 15/03/2021. p. 112.

11. IPEA. Disponível em: <https://www.ipea.gov.br/portal/images/stories/PDFs/conjuntura/201015_cc49_cultura.pdf>. Acesso em:

setor (18,69%), participação em redes/*networking* (17,53%), informações sobre como se portar na reabertura (16,71%), consultoria (13,88%), apoio psicológico (1,73%), treinamento (12,96%) e outros (6,49%). Cabe notar que a maior parte das necessidades expressas pelos trabalhadores culturais está ligada à conexão, à formação de redes solidárias de apoio e troca de informações.

Se o setor é marcado por contradições, o fenômeno da plataformização torna-o ainda mais complexo. Isso porque, por um lado, as plataformas tornaram mais fácil aos artistas levarem suas obras às audiências e monetizá-las. Mas por outro, acabam ficando dependentes das plataformas, que definem o modo como suas obras serão disponibilizadas e o valor a ser pago pelo seu acesso.

> como as mercadorias culturais contingentes são inerentemente dependentes da plataforma, seus produtores são efetivamente cúmplices na aceitação de mecanismos econômicos, estratégias de gestão e estruturas de governança e infraestruturas que igualam a desproporcionalidade, dependência e desigualdade.[12]

Para Nieborg e Poell (2018), o principal efeito da plataformização da economia criativa é a contingência -cada vez mais, as obras culturais são efêmeras e personalizadas de acordo com a audiência. Assim, são os algoritmos quem ditam o que, como e quando sua obra será consumida; tirando esse controle dos próprios artistas ou usuários.

> A plataformização, como este artigo sugere, marca a reorganização da produção e circulação cultural, tornando as mercadorias culturais contingentes. Essa contingência apresenta novos problemas para teóricos e críticos culturais, que são confrontados com objetos culturais que resistem à estabilização. Textos instáveis levantam uma série de desafios metodológicos e culturais. Em vez de bens culturais físicos fixos, a distribuição digital transforma jogos e notícias em serviços personalizados que diferem para cada indivíduo, com base no tempo, localização, perfil do usuário e comportamento. Os desenvolvedores podem alterar o conteúdo em tempo real e combinado com plataformas orientadas por publicidade, isso tem implicações profundas para a acessibilidade, precisão e diversidade do conteúdo.[13]

12. NIEBORG, D.; POELL, T. The platformization of cultural production: Theorizing the contingent cultural commodity. New Media & Society, v. 20, n. 11, p. 4275-4292, 2018. p. 15. Tradução nossa.

13. NIEBORG, D.; POELL, T. The platformization of cultural production: Theorizing the contingent cultural commodity. New Media & Society, v. 20, n. 11, p. 4275-4292, 2018. p. 15. Tradução nossa.

Deste modo, os trabalhadores da arte encontram desafios particulares na plataformização de seu setor. A aparente flexibilidade de sua atividade esconde uma precarização que se aprofunda com a introdução das plataformas em sua prática profissional, distanciando-os de suas obras e o deixando à mercê de definições e cálculos algorítmicos. Sem uma rede de apoio ou uma coalização pela luta por seus direitos, artistas se vêem deixados à própria sorte.

3. Cooperativismo de plataforma como alternativa

Diante desse cenário, o que resta aos trabalhadores é aceitar a inexorável plataformização ou é possível imaginar um outro futuro do trabalho? A perspectiva histórica nos ajuda a perceber que a história é contingente - se atualmente esta virtualidade do trabalho se efetuou, também quer dizer que outras são possíveis. Cabe então aos diversos atores participarem em conjunto da construção de algo novo. Como afirma Scholz,

> Uma internet das pessoas é possível! Uma coalizão de designers, trabalhadores, artistas, cooperativas, desenvolvedores, sindicatos inovadores, advogados públicos pode mudar as estruturas para que todos possam colher os frutos do próprio trabalho.[14]

Um grupo de pesquisadores da The New School desde meados de 2017, especialmente Trebor Scholz e Nathan Schneider, busca propor alternativas para uma apropriação coletiva e democrática dessas infraestruturas digitais. Os autores passaram a propor a reinvenção do tradicional modelo cooperativo de trabalho combinada a uma apropriação coletiva das plataformas digitais.

O movimento do cooperativismo de plataforma está maior do que nunca. Cada vez mais, sua proposta está mudando de um conceito radical discutido nas universidades de Nova Iorque para um modelo que inspira projetos concretos ao redor do mundo. Este começou como um exercício conceitual de conectar a tradição da economia cooperativa com as novas tecnologias, tentando explorar o melhor dos dois mundos. Mas agora, é um ecossistema diversificado de pesquisadores, empreendedores, desenvolvedores, designers e trabalhadores em geral que estão engajados em uma verdadeira transformação da economia digital.

14. SCHOLZ, Trebor. Cooperativismo de plataforma: contestando a economia do compartilhamento corporativa. São Paulo: Fundação Rosa Luxemburgo, 2017. p. 46.

Segundo a Organização Internacional do Trabalho - OIT (2021), o cooperativismo de plataforma pode ser definido como

> Uma tradição empresarial de plataforma que oferece uma alternativa ao atual modelo dominante de capitalismo de plataforma, sustentado pelos princípios de propriedade cooperativa, governança democrática e solidariedade. As empresas-plataforma cooperativistas podem ser de propriedade coletiva e governadas por trabalhadores, consumidores ou ambos, e podem operar com/sem apoio público.[15]

Para tanto, propõem a criação de plataformas que sejam geridas pelos próprios trabalhadores, e não sejam intermediadas por grandes corporações. Dessa forma, eles podem ter controle sobre todo o processo de produção, baseando-se em decisões democráticas e realizando uma distribuição mais igualitária dos lucros. Esse projeto, denominado Cooperativismo de Plataforma, é apontado como uma das formas de unir os trabalhadores na criação de novas infraestruturas para a consolidação de relações de produção fundamentadas no bem comum.

> O cooperativismo de plataforma é um termo que descreve mudanças tecnológicas, culturais, políticas e sociais. O cooperativismo de plataforma é um horizonte da esperança. Não é uma utopia concreta; é uma economia emergente. Alguns modelos que irei descrever agora já existem há dois ou três anos, enquanto outros ainda são aplicativos imaginários. Alguns são protótipos, outros são experimentos; e todos introduzem um conjunto alternativo de valores.[16]

Claramente, o cooperativismo não pode ser tomado como a panaceia para todos os problemas do trabalho em plataformas digitais. Uma das críticas mais comuns ao projeto do cooperativismo é o de que, em dado momento de seu desenvolvimento, elas podem se distanciar de seus princípios originais. Evidentemente este é um dos principais riscos que se corre ao tentar criar um microambiente cooperativo dentro de um macroambiente capitalista. Todavia,

15. INTERNATIONAL LABOUR ORGANIZATION - ILO. Platform labour in search of value: A study of worker organizing practices and business models in the digital economy. Geneva: ILO, 2021. Disponível em: <https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/---coop/documents/publication/wcms_809250.pdf>. Acesso em 15/03/2023. Tradução nossa. p.6.

16. SCHOLZ, Trebor. Cooperativismo de plataforma: contestando a economia do compartilhamento corporativa. São Paulo: Fundação Rosa Luxemburgo, 2017. p. 63.

Scholz responde da seguinte maneira a essa crítica:

> Uma objeção comum às cooperativas é que elas são tão suscetíveis às pressões do mercado quanto qualquer empreendimento capitalista, o que torna a autoexploração inevitável. Eventualmente, cooperativas também podem resultar em artimanhas de estágios não pagos e trabalho voluntário não compensado. Cooperativas estão expostas à competição sem dó do mercado, mas, à luz do lucro de 20% a 30% que empresas como Uber estão ganhando, uma abordagem seria as cooperativas de plataforma oferecerem seus serviços por preços mais baixos. Elas poderiam ter 10% de lucro, o que depois seria parcialmente traduzido como benefícios sociais para os trabalhadores. Cooperativas também poderiam florescer em mercados de nicho, focalizando clientes de baixa renda como público-alvo.[17]

Outros autores também se dedicaram a identificar os limites das cooperativas, como Grohmann (2018) e Sandoval (2019). De acordo com o primeiro, ao observar empiricamente as plataformas nota-se que elas não são homogêneas, baseadas em uma essência de princípios que as definiram. Ao contrário, são marcadas por gradações entre modelos radicais de cooperação e adaptações que se assemelham mais a pequenas empresas. Além disso, identifica que uma parte delas apresenta em seus enunciados um foco maior no aspecto democrático do que em seu viés igualitário, enfatizando mais a participação de diversos atores em suas decisões, mas pouco na distribuição equitativa dos lucros. Em seus termos,

> Podemos observar como os discursos acerca do trabalho em cooperativas são modalizados, inclusive nas áreas de cultura e comunicação, desde um projeto cooperativo-empreendedor, mais próximo ao de uma startup, até outros que tenham por base um projeto político de transformação social.[18]

Numa linha semelhante, Sandoval situa as cooperativas na ambivalência entre a subversão e a cooptação. Para a autora, o principal fator que coloca em

17. SCHOLZ, Trebor. Cooperativismo de plataforma: contestando a economia do compartilhamento corporativa. São Paulo: Fundação Rosa Luxemburgo, 2017. p. 58.

18. GROHMANN, Rafael. Cooperativismo de plataforma e suas contradições: análise de iniciativas da área de comunicação no Platform.Coop. Liinc em Revista, Rio de Janeiro, v.14, n.2, p. 19-32, maio 2018. Disponível em: <http://revista.ibict.br/liinc/article/view/4149>. Acesso em: 15/03/2021. p. 23.

risco sua proposta subversiva é o do poder corrosivo da competição capitalista. Ou seja, é possível que as cooperativas se sintam na necessidade de incorporar a maximização dos lucros para que garantam sua sobrevivência frente às empresas capitalistas. Ou ainda, ao aceitar investimentos externos, sejam iniciais ou ao longo de sua expansão, acabam por ter de se comprometer com os retornos aos investidores, e não propriamente com os princípios cooperativistas.

> Ao contribuir para a construção de estruturas econômicas alternativas baseadas em solidariedade, cooperação e propriedade coletiva, as cooperativas e trabalhadores podem também desempenhar um papel de transformar as condições de trabalho no setor cultural. Contudo, como todo projeto prefigurativo, as cooperativas de trabalhadores não podem escapar totalmente das pressões do sistema existente. Os projetos alternativos no setor cultural necessitam navegar por tensões complexas e potenciais conflitos entre processos criativos, necessidade econômica e aspirações políticas.[19]

Portanto, o cooperativismo de plataforma pode ser considerado uma das alternativas que, somadas a outras - como a regulação das empresas do capitalismo de plataforma e a criação de plataformas públicas, pode melhorar a vida dos trabalhadores. Apesar de seus limites e contradições, o projeto exercita o imaginário para uma reapropriação das plataformas pelos trabalhadores na construção de uma realidade do trabalho mais democrática e justa.

4. Cooperativas de plataforma no setor artístico

O cooperativismo de plataforma, por ser um conceito formulado ainda recentemente e ter seu debate concentrado em determinadas regiões do mundo, ainda carece de análises empíricas que observem suas dinâmicas em mercados específicos. Entretanto, elas têm crescido em número e abrangência, estando presentes em cada vez mais segmentos e agregando uma quantidade crescente de trabalhadores e entusiastas.

Como dito anteriormente, temos diversas organizações que não se intitulam como cooperativas, mas apresentam diversas das suas características. De

19. SANDOVAL, Marisol. Enfrentando a Precariedade com Cooperação: cooperativas de trabalhadores no setor cultural. Revista Parágrafo. v. 5, n. 1, p. 111-127, 2017. Disponível em: <http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/567>. Acesso em: 15/03/2021. p. 120.

outro lado, muitos projetos que se denominam cooperativas, mas apresentam traços de startups ou microempresas. Entretanto, existem diversos esforços de pesquisa com o intuito de mapeá-las, classificá-las e analisá-las. A principal delas é o diretório colaborativo[20] do Platform Cooperativism Consortium (PCC), site que reúne informações sobre as diversas iniciativas ao redor do mundo. No momento da elaboração deste artigo, o diretório contava com 315 cooperativas listadas no total. O documento contém informações descritivas de cada plataforma - como nome, descrição, website, localidade e contato. Além de categorizá-las segundo seu tipo e segmento, o que possibilita uma série de análises quanto à presença, a atividade e o setor de cada uma delas.

Em termos de pesquisas mais qualitativas, podemos citar o relatório "*Sharing like we mean it*"[21], publicado pelo coletivo *Cultural Workers Organisation*. Com base em uma pesquisa com cooperativas de plataforma cultural, eles descobriram que 90,8% de seus trabalhadores estão "extremamente" ou "um pouco" satisfeitos com suas condições gerais de trabalho. Além disso, 40,7% oferecem um nível salarial que "atende à média". Em relação às políticas e benefícios no local de trabalho, 87,2% deles têm políticas de "equidade na contratação", 79,2% declararam pagar "salário mínimo (ou superior)" e 76,5% têm "processos de resolução de conflitos/disputas" . A pesquisa foi realizada em 2019 e 2020 em cooperativas em indústrias criativas no Canadá, Reino Unido e Estados Unidos; e foi respondida por 106 cooperativas e 12 membros de cooperativas de trabalhadores foram entrevistados.

Em pesquisa anterior[22], durante um fellowship no *Institute for Cooperative Digital Economy* (ICDE), analisamos 15 cooperativas de plataforma listadas no diretório e classificadas na categoria Arte (*Art*). A partir desta análise, desenvolvemos *framework* com 6 categorias de cooperativas do setor artístico:

a. Comunidades: coletivos com o objetivo central de conectar artistas a partir de sua prática e experiência profissional.
b. Provedoras de serviços: organizações que conectam prestadores de serviços no segmento com consumidores.

20. PLATFORM COOPERATIVISM CONSORTIUM. Directory. Disponível em: <https://directory.platform.coop/>. Acesso em: 15/03/2023.

21. CULTURAL WORKERS ORGANIZE. Sharing Like We Mean It: Working Co-operatively in the Cultural and Tech Sectors. Disponível em: <https://culturalworkersorganize.org/wp-content/uploads/2021/01/Sharing-Like-We-Mean-It-Web.pdf>. Acesso em: 15/07/2022.

22. Disponível em: <https://archive.org/details/victor-barcellos/>. Acesso em: 06/06/23.

c. Marketplaces: lojas virtuais em que os artistas podem disponibilizar e comercializar suas obras.
d. Crowdfundings: plataformas para a captação de recursos de apoio a artistas.
e. Incubadoras: oferecem consultoria para o desenvolvimento e expansão de cooperativas.
f. Laboratórios: espaços de experimentação artística.

O critério para a categorização foi sua atividade final principal e os textos de apresentação disponíveis em seus *websites*. Pudemos notar que a maioria delas se propõe como uma comunidade para discussão, troca de experiências e apoio entre artistas. Conforme mencionado anteriormente, o estabelecimento de relações entre profissionais da cultura é considerada como uma das principais necessidades para a melhoria de suas condições de trabalho. Ao formar comunidades com o espírito cooperativo ao invés da competição, os artistas podem aliviar as pressões econômicas e desenvolverem seus talentos sem o objetivo único do lucro.

De modo geral, identificamos que essas iniciativas constituem potenciais alternativas à vigente plataformização do trabalho artístico. Apesar de ainda estarem em estágio de emergência, a heterogeneidade desses projetos indica que o modelo cooperativo pode funcionar nas diversas áreas do setor da cultura. Pode ser que essas organizações não cheguem a se constituir como consideráveis concorrentes às plataformas capitalistas. Ainda assim, suas melhores condições de trabalho podem atrair cada vez mais artistas, contribuir para a conscientização das injustiças do atual modo de produção e fomentar a imaginação de novas relações entre tecnologia e trabalho mais democráticas e igualitárias.

Em suma, podemos verificar que apesar de seu número reduzido e concentração geográfica, já existem cooperativas de plataforma no setor artístico que buscam conectar artistas e promover um trabalho mais democrático e igualitário. E considerando a demanda dos trabalhadores culturais por redes de apoio e maior controle sobre suas produções, o cooperativismo encontra grande potencial de crescimento e diversificação dentro do setor criativo.

5. O case da Artisans Cooperative

A Artisans Cooperative é uma cooperativa formalizada no Estado de Oregon, nos Estados Unidos, que funciona como um marketplace cooperativo para artistas que desenvolvem trabalhos artesanais. Definem-se como

> Um mercado artesanal online para uma rede inclusiva de criativos. Somos uma cooperativa de propriedade de membros, administrada por membros e beneficiada por membros. Promovemos a criatividade, apoiamos os meios de subsistência dos artistas, criamos oportunidades para coletivos de arte de impacto social e conectamos pessoas por meio de uma comunidade artística equitativa.[23]

Assim como boa parte das primeiras cooperativas de plataforma, a iniciativa nasce se colocando como uma alternativa direta a uma empresa já dominante em seu respectivo mercado - no caso da Artisans se menciona a *Etsy*[24], um site de comércio eletrônico de produtos artesanais. Portanto, esta se enquadra na categoria de *marketplace* mencionada anteriormente, em que artistas cooperativos podem usar sua plataforma para comercializar suas obras.

Em entrevista realizada por email no dia 29/05/2023 com um de seus representantes, como parte de pesquisa em andamento de Doutorado, definiram seu modelo de governança como uma "Corporação cooperativa multissetorial", afirmando possuírem 3 classes de membros: artesãos (produtores/trabalhadores), apoiadores (consumidores) e funcionários (trabalhadores). O caráter *multistakeholder* está presente em boa parte das experiências cooperativas e costuma ser uma de suas principais marcas.

Quando perguntados sobre seu modelo de financiamento, afirmaram que estão levantando fundos iniciais de uma combinação de investimentos - competições de negócios, doações e *buy-ins* de membros. A iniciativa recebeu apoio da Start.coop[25], aceleradora de cooperativas responsável por financiar e escalar diversos projetos ao redor do mundo. Uma vez operacional, a Artisans pretende que seu sustento passe a vir principalmente por comissões de vendas.

Com relação ao seu alinhamento aos movimentos do cooperativismo de plataforma e da Economia Solidária, constatam que "ambos são movimentos importantes com os quais nossa causa está alinhada, mas conferências e *webinars* estão fora de nosso alcance em termos de dinheiro e tempo". Desse modo, é curioso notar que apesar do papel conceitual desses movimentos na experiência da Artisans, estes se veem desconectados de suas atividades.

23. Disponível em: <https://artisans.coop/about/>. Acesso em 31/05/2023. Tradução nossa.

24. Disponível em: <https://www.etsy.com/>. Acesso em 31/05/2023.

25. Disponível em: <https://www.start.coop//>. Acesso em 31/05/2023.

Por fim, quando questionados a respeito de como viam o papel de tecnologias como a inteligência artificial e *blockchain*, responderam que "Como uma startup que trabalha com voluntários de baixa renda e uma comunidade dispersa de proprietários de microempresas, *blockchain* e *tokens* estão fora de nosso alcance como uma cooperativa". Assim, por mais que essas tecnologias se apresentem hoje como grandes potencializadoras da produção artística, a iniciativa analisada não vê sua adoção no horizonte.

Considerações finais

A plataformização vem se consolidando como uma nova realidade sociotécnica nos diversos setores da sociedade. No setor artístico, o fenômeno aprofunda a precarização e a individualização do trabalho, especialmente após a pandemia do coronavírus. O cooperativismo de plataforma se apresenta como uma alternativa para um trabalho mais horizontal e justo, devolvendo aos artistas o poder sobre suas obras. Para que se possa oferecer melhores condições aos trabalhadores da cultura, é preciso que as cooperativas superem os desafios e complexidades de se consolidarem como alternativas dentro do capitalismo de plataforma. E além disso, é necessário que ganhem a ciência e a aderência dos trabalhadores do sul global, onde a precarização da classe é ainda maior.

Com isso, foi possível identificar que o cooperativismo de plataforma, enquanto modelo de organização do trabalho no contexto da plataformização, vai ao encontro das necessidades apresentadas pelos trabalhadores da arte. Suas carências e contradições, aprofundadas pela pandemia do coronavírus, podem ser amenizadas pelos princípios do cooperativismo. E assim, artistas podem retomar a propriedade sobre as suas obras e criar meios de realizar seu valor.

Referências

BARCELLOS, Victor. **Art for everyone: Platformization of cultural work and cooperativism as an alternative**. Nova Iorque: Platform Cooperativism Consortium, 2023.

CULTURAL WORKERS ORGANIZE. **Sharing Like We Mean It: Working Co-operatively in the Cultural and Tech Sectors**. Disponível em: <https://culturalworkersorganize.org/wp-content/uploads/2021/01/Sharing-Like-We-Mean-It-Web.pdf>. Acesso em: 15/07/2022.

GROHMANN, Rafael. **Cooperativismo de plataforma e suas contradições: análise de iniciativas da área de comunicação no Platform.Coop**. Liinc em Revista, Rio de Janeiro, v.14, n.2, p. 19-32, maio 2018. Disponível em: <http://revista.ibict.br/liinc/article/view/4149>. Acesso em: 15/03/2021.

_____. **Plataformização do trabalho: entre a dataficação, a financeirização e a racionalidade neoliberal**. Disponível em: <https://seer.ufs.br/index.php/eptic/article/view/12188/10214>. Acesso em: 15/03/2021.

INTERNATIONAL LABOUR ORGANIZATION - ILO. ***Platform labour in search of value: A study of worker organizing practices and business models in the digital economy***. Geneva: ILO, 2021. Disponível em: <https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emp_ent/---coop/documents/publication/wcms_809250.pdf>. Acesso em 15/03/2023.

NIEBORG, D.; POELL, T. ***The platformization of cultural production: Theorizing the contingent cultural commodity***. New Media & Society, v. 20, n. 11, p. 4275-4292, 2018.

PLATFORM COOPERATIVISM CONSORTIUM. Directory. Disponível em: <https://directory.platform.coop/>. Acesso em: 15/03/2023.

SANDOVAL, Marisol. **Enfrentando a Precariedade com Cooperação: cooperativas de trabalhadores no setor cultural**. Revista Parágrafo. v. 5, n. 1, p. 111-127, 2017. Disponível em: <http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/567>. Acesso em: 15/03/2021.

_____. ***Entrepreneurial Activism? Platform Cooperativism Between Subversion and Co-optation***. Critical Sociology, 2019. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0896920519870577>. Acesso em: 15/03/2021.

SCHOLZ, Trebor. **Cooperativismo de plataforma: contestando a economia do compartilhamento corporativa**. São Paulo: Fundação Rosa Luxemburgo, 2017.

_____. ***Uberworked and Underpaid***. London: Polity Press, 2016.

SRNICEK, Nick. ***Platform Capitalism***. Cambridge: Polity Press, 2016.

VAN DIJCK, J.; POELL, T.; DE WAAL, M. ***The Platform Society***. New York: Oxford, 2018.

ZANATTA, Rafael. **Cooperativismo de Plataforma no Brasil: Dualidades, Diálogos e Oportunidades**. Rio de Janeiro: Instituto de Tecnologia e Sociedade (ITS Rio), 2022. Disponível em: <http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/567>. Acesso em: 15/03/2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

5

As “Decentralized Autonomous Organizations” (DAOS): do contexto do surgimento à aplicabilidade no mundo atual

ANA PAULA DE OLIVEIRA QUINTANA FERREIRA

Introdução

Desde os tempos mais antigos, os seres humanos sentem a necessidade de se arranjar em grupos, conforme a similaridade dos seus interesses. A partir dessa necessidade de organização, o homem vem, nas últimas décadas, utilizando-se fortemente da tecnologia no seu cotidiano para a consecução das mais diversas atividades de forma agrupada, sejam elas no âmbito do lazer, nas suas atividades laborativas, para fins educacionais e diversas outras áreas de atuação.

O homem já se encontra submerso nesse universo tecnológico permeado de inovações, em que certos conceitos se destacam e ganham enorme visibilidade de tempos em tempos. A título de exemplificação, em 2017, houve o *boom* das ICOS (*Initial Coin offers*) - projetos tecnológicos baseados na tecnologia *blockchain* e financiados via criptomoedas[2]. Em 2021, tivemos em evidência os NFTs - *Non Fungible Tokens*, que, inclusive, trazem muita especulação, pois parte da premissa que o ativo criado a partir da tecnologia *blockchain* confere a identidade digital que o torna autêntico e único. Nas palavras de Lemos, isso significa que "[...] a capacidade de transformar o que por natureza é abundante em escasso"[3] e, mais recentemente, as DAOs, em inglês, *Decentralized Autonomous Organization*, que, em linhas gerais, trata-se de uma espécie de sociedade virtual sem liderança central, a qual será o objeto central do estudo proposto neste trabalho.

1. Advogada Sênior (América Latina) na AVEVA Software Brasil Ltda. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio), em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro). Pós-graduada em Direito Empresarial e dos Negócios pela Universidade Cândido Mendes (AVM/UCAM). Bacharel pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).

2. CAMPINO, José, BROCHADO, Ana, ROSA, Álvaro. Fatores de sucesso das Initial Coin Offerings (ICOS) - A importância do capital Humano. Disponível em: article_83059.pdf (iscte-iul.pt) . Acesso em: 20 dez. 2022.

3. LEMOS, Ronaldo. O Impacto de NFT é maior do que se pensa. Disponível em: https://itsrio.org/pt/artigos/impacto-de-nft-e-maior-do-que-se-pensa/ Acesso em: 20 dez. 2022.

Com efeito, podemos afirmar que as sociedades empresariais são mais um desdobramento dessa característica humana de associação e que as chamadas *Decentralized Autonomous Organization*, ou, como são mais comumente conhecidas, pelo seu acrônimo, as DAO constituem, em linhas gerais, sociedades virtuais, com a particularidade de não possuírem uma liderança central.

As DAO surgem, portanto, em continuidade a essa evolução das sociedades empresariais, desafiando os modelos até então existentes, ao passo que trazem um novo mecanismo de governança empresarial, o qual está baseado na Tecnologia de *Blockchain*. Dita tecnologia emerge, como um novo paradigma, para construir sistemas descentralizados, ou seja, que prescindem de uma autoridade central.

A *blockchain* muito se popularizou com o advento dos chamados cripto ativos. Contudo, logo se notou que tal tecnologia poderia ir além de temas financeiros, podendo alcançar até mesmo temas como governança corporativa.

O presente artigo não pretende esgotar o tema, mas traz algumas considerações e aspectos sobre essa nova modalidade de se organizar uma sociedade, chamada *Decentralized Autonomous Organization*. Este artigo está dividido em três seções, além de introdução e conclusão. A primeira seção, intitulada "conceito e contexto de surgimento da *Decentralized Autonomous Organization*", como o nome já dispõe, abordará um pouco sobre o que são e como nasceram as DAO. A segunda, por sua vez, tratará de alguns aspectos e particularidades das DAO, a função dos *smart contracts* em uma DAO, exemplos de utilização de uma DAO, vantagens e desvantagens das DAO. Por fim, a terceira seção tratará de possíveis caminhos para a aplicabilidade das DAO num contexto nacional.

1. O conceito e o contexto de surgimento das DAO

1.1 Conceito

O Universo Tecnológico tem por característica marcante o fato de estar permeado por frequentes inovações. Nesse viés, vem ganhando visibilidade de forma muito latente as chamadas *blockchains*, sobretudo após a popularização das criptomoedas ou, melhor dizendo, cripto ativos, destacando-se o *bitcoin* como a mola propulsora de tal inovação.

O conceito de *blockchain* pode ser extraído do seu próprio nome, cuidando de uma cadeia de blocos organizados e encadeados, como ressalta Ronaldo Lemos:

> Interligados sequencialmente e de forma ordenada, criando um histórico transparente e imutável de transações e registros nela armazenados. Vale notar, no entanto, que esta tecnologia engloba diferentes conceitos e tecnologias, dentre os quais alguns deles se encontravam no escopo das ciências da computação há mais de duas décadas, como a comunicação ponto-a-ponto (P2P) dos sistemas distribuídos e a criptografia assimétrica[4].

Em 2017, foi a vez das ICOS (*Initial Coin Offers*). Apesar de ter surgido em 2013, foi em 2017 que o conceito esteve em maior evidência. O ICO é o meio não regulamentado pelo qual os fundos são criados para um novo empreendimento em criptomoeda. Nas palavras de Watson:

> A Oferta Inicial de Moedas (ICO) é um meio de c*rowdfunding* para lançar uma nova criptomoeda. Tradicionalmente, a venda de tokens é organizada antes do lançamento da criptomoeda, a fim de arrecadar dinheiro para o desenvolvimento técnico. A oferta inicial de moedas é notável por pouca ou nenhuma regulamentação governamental[5].

Uma oferta inicial de moedas é usualmente realizada por *startups* para evitar o rigoroso e regulamentado processo de captação de capital exigido por investidores de risco ou bancos. São semelhantes aos IPOs (*Initial Public Offerings*). Porém, enquanto os IPOs lidam com investidores, as ICOs lidam com entusiastas que estão interessados em investir em um novo projeto. Ainda segundo Watson[6],

Também difere do IPO (oferta pública inicial), pois a aquisição dos tokens não concede a propriedade da empresa que desenvolve a nova criptomoeda. Enquanto os IPOs são bem definidos e compreendidos pelos governos, os ICOs

4. LEMOS, Ronaldo. Blockchain para aplicações de interesse público. 2019. Disponível em: https://feed.itsrio.org/como-usar-a-blockchain-para-promover-o-interesse-p%C3%BAblico-c7fb1f7e186e Acesso em: 19 dez. 2019.

5. WATSON, Andy. What is Initial Coin Offering (ICO)? Disponível em: https://www.coinspeaker.com/guides/what-is-initial-coin-offering/. Acesso em: 26 dez. 2019.

6. WATSON, Andy. What is Initial Coin Offering (ICO)? Disponível em: https://www.coinspeaker.com/guides/what-is-initial-coin-offering/. Acesso em: 26 dez. 2019.

são mais obscuros. A Comissão de Valores Mobiliários dos EUA e outras agências reguladoras estão atualmente examinando a prática. Os proponentes afirmam que os tokens são algo entre um título e uma moeda.

Em 2021, destacando-se também como um dos diversos domínios possíveis no uso das *blockchains*, tivemos em evidência os Tokens não fungíveis, ou, ainda, os NFTs - *Non Fungible Tokens*, inclusive com muita especulação. Em linhas gerais, um *token* não fungível (NFT) é uma tecnologia que permite registrar de maneira distribuída a posse de um bem não fungível. Portanto, o NFT é um token ou certificado que comprova a propriedade de itens exclusivos. São utilizados para provar a propriedade de bens exclusivos como itens colecionáveis ou de investimento, pois se pode revender um NFT e obter lucros com base no seu valor atual[7].

Por fim, mais recentemente, em 2021, passou-se a abordar, com bastante destaque, as DAOS, em inglês, *Decentralized Autonomous Organization*, objeto central deste estudo. Vale dizer, em linhas gerais, que a DAO é uma sociedade virtual sem uma liderança central. Numa tradução livre do conteúdo extraído do site da Ethereum:

> DAO é uma organização de propriedade coletiva e governada por blockchain que trabalha para uma missão compartilhada.
>
> DAOs nos permitem trabalhar com pessoas afins em todo o mundo sem confiar em um líder benevolente para gerenciar os fundos ou operações. Não há CEO que possa gastar fundos por capricho ou CFO que possa manipular os livros. Em vez disso, as regras baseadas em blockchain inseridas no código definem como a organização funciona e como os fundos são gastos.
>
> Eles têm tesouros embutidos que ninguém tem autoridade para acessar sem a aprovação do grupo. As decisões são regidas por propostas e votações para garantir que todos na organização tenham voz e tudo aconteça de forma transparente na cadeia[8].

Ao desmembrarmos a expressão *Decentralized Autonomous Organization*, em português, Organização Autônoma Descentralizada, a palavra “organiza-

7. VALEONTI, F. *et al*. *Crypto collectibles, museum funding and openglam: Challenges, opportunities and the potential of non-fungible tokens* (NFTS). Disponível em: https://www.mdpi.com/2076-3417/11/21/9931. Acesso em: 03 de Jan 2023.

8. ETHERUM ORG. What are DAOS? Disponível em: https://ethereum.org/en/dao/#:~:text=A%20DAO%20is%20a%20collectively,manage%20the%20funds%20or%20operations. Acesso em: 27 dez. 2022.

ção" não necessariamente pressupõe um sinônimo de "instituição". Uma "organização" não precisa ser institucionalizada para existir. Ela pode ser um coletivo de pessoas com um objetivo comum: um projeto, uma ação, um produto, a etapa de um trabalho, dentre outros aspectos. Quando abordamos a "autonomia", ela existirá com relação ao intermediário (e a relação será regida por um código final, quanto à própria governança, que se dará por esse código e não de um contrato social), no que concerne à própria execução do código (que fará aquilo para o que foi programado) e no que tange à participação individual (pessoas poderão aderir, pelo tempo que quiserem, contribuindo da forma que puderem ou lhes convier). Por fim, o termo "descentralizadas" se refere à tecnologia *blockchain*, à governança (mais horizontalizada, a depender da forma como o código é programado, como os critérios de desempate. A descentralização permite uma maior democratização das decisões tomadas.

As DAOs, assim como os demais institutos previamente mencionados, utilizam a rede *blockchain* e as suas interações são realizadas de forma autônoma por contratos digitais programáveis, os *smart contracts*. A *blockchain*, como acima exposto, é uma tecnologia de registro, os quais são programáveis para automatizar e autoexecutar funções. É justamente nesse *modus operandi* que se logra instituir uma organização automatizada, autoexecutável, a qual dispensa um intermediário pessoa física para controlá-la.

A comunidade Ethereum aduz, em linhas gerais, que as DAOS são organizações/sociedades que não possuem hierarquia, vale dizer, não possuem um poder/órgão centralizador, justamente com fins de evitar poderes injustificados/ilegítimos oriundos de pessoas que agem de forma arbitrária. Em uma tradução livre,

O conceito geral de 'organização autônoma descentralizada' é o de uma entidade virtual que possui um determinado conjunto de membros ou acionistas que, talvez com uma maioria de 67%, têm o direito de gastar os fundos da entidade e modificar seu código. Os membros decidiriam coletivamente sobre como a organização deveria alocar seus fundos. Os métodos para alocar os fundos de um DAO podem variar de recompensas, salários a mecanismos ainda mais exóticos, como uma moeda interna para recompensar o trabalho. Isso basicamente replica os artifícios legais de uma empresa tradicional ou sem fins lucrativos, mas usando apenas a tecnologia *blockchain* criptográfica para aplicação. Até agora muito da conversa sobre DAOs tem sido sobre o modelo 'capitalista' de uma 'corporação autônoma descentralizada' (DAC) com acionistas que recebem dividendos e ações negociáveis; uma alternativa, talvez

descrita como uma 'comunidade autônoma descentralizada', faria com que todos os membros tivessem uma participação igual na tomada de decisões e exigisse que 67% dos membros existentes concordassem em adicionar ou remover um membro. A exigência de que uma pessoa só pode ter uma associação precisaria ser aplicada coletivamente pelo grupo[9].

Portanto, diversamente de uma organização tradicional, uma DAO, em geral, não tem hierarquia e não está sujeita à soberania de um país em específico, pois a sua programação ocorre via internet, podendo os seus participantes estar em qualquer lugar, sendo eles livres para se associarem e se desassociarem da DAO, conforme desejem. Não obstante existirem e agirem predominantemente on-line, as DAO, conforme expõe Tiana Laurence, podem gerenciar ativos que existem tanto on-line como off-line[10].

Qualquer alteração numa DAO requer deliberação, por votação. Nesse contexto, o sistema automatizado dos *smart contracts* permite verificar se a maioria dos votantes está de acordo para que, somente então, seja dado prosseguimento à alteração, de forma automatizada.

1.2 Contexto de surgimento

Existe vasta literatura sobre organizações descentralizadas (SHUBIK, 1962; BECKHARD, 1966; FREELAND; BAKER, 1975). No entanto, as primeiras referências à verdadeira "Organização Autônoma Descentralizada" (DAO) só surgiram na década de 1990, para descrever sistemas multiagentes em um ambiente IoT (DILGER, 1997) ou ação descentralizada não violenta no movimento social de contra-globalização (SCHNEIDER, 2014)[11].

No entanto, o significado moderno de DAOs pode ser rastreado até o conceito anterior de Corporação Autônoma Descentralizada (DAC), cunhado alguns anos após o surgimento do Bitcoin (NAKAMOTO, 2008). O conceito DAC foi usado informalmente em fóruns online e bate-papos pelos primeiros entusiastas de criptomoedas, utilizando corporações autônomas descentralizadas e distribuídas de forma intercambiável. Foi apenas em 2013 que o termo se

9. ETHEREUM ORG. Ethereum Whitepaper. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 26 Dez 2022.

10. LAURENCE, Tiana. I*ntroduction to blockchain technology: the many faces of blockchain technology in the 21st century*. Países Baixos: Van haren Publishing, 2019.

11. DECENTRALISED AUTONOMOUS ORGANISATION. *Internet Policy Review*. Disponível em: https://policyreview.info/open--abstracts/decentralised-autonomous-organisation. Acesso em: 26 dez. 2022.

tornou mais amplamente adotado e discutido publicamente em vários sites, em particular pelo cofundador da Bitcoin Magazine Vitalik Buterin (BUTERIN, 2013).

Em outras palavras, pode-se dizer que o conceito moderno de DAOs foi, de certa forma, difundido e popularizado em 2013 pelo russo Vitalik Buterin, co-criador da rede Ethereum. A sua popularização se deu num contexto mundial de constante desconfiança das pessoas perante as instituições tradicionais. Além disso, com a expansão das DeFi - *Decentralized Finance*s (em português, Finanças Descentralizadas), em 2020, as DAOs se tornaram mais populares e provocaram um aumento na demanda por organizações descentralizadas para diferentes projetos. Numa tradução livre, a DeFi: "é uma tecnologia financeira emergente que desafia o atual sistema bancário centralizado. O DeFi elimina as taxas que os bancos e outras empresas financeiras cobram pelo uso de seus serviços e promove o uso de transações ponto a ponto, ou P2P"[12].

O *Bitcoin*, por exemplo, foi criado para permitir a livre transferência e guarda de ativos digitais. A ideia das DeFi é fazer a mesma coisa, mas com os serviços financeiros. A sua principal rede descentralizada é a Ethereum.

Feitas essas considerações acerca do conceito e surgimento das DAO, abordar-se-ão adiante alguns aspectos particulares e exemplos de utilização da modalidade de DAO.

2. Aspectos das DAO

2.1 A função dos *Smart Contracts* numa DAO

Antes de tratar propriamente das suas funcionalidades, faz-se mister entender o que são os *smart contracts*, também conhecidos como contratos inteligentes. De difícil conceituação, conforme indica Frazão, a ideia "está associada à possibilidade de traduzir comportamentos em códigos, de forma que serão softwares que gerenciarão a performance contratual"[13].

Em continuação à sua definição, Frazão dispõe, ainda, que o fenômeno

12. SHARMA, Rakesh. *What Is Decentralized Finance (DeFi) and How Does It Work?* Disponível em: https://www.investopedia.com/decentralized-finance-defi-5113835#:~:text=Decentralized%20finance%20(DeFi)%20is%20an%20emerging%20financial%20technology%20that%20challenges,peer%2C%20or%20P2P%2C%20transactions. Acesso em: 3 de Jan 2023.

13. FRAZÃO, Ana. O que são contratos inteligentes ou *smart contracts*? Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-04-11-O_que_sao_contratos_inteligentes_ou_smart_contracts_Quais_sao_suas_principais_repercussoes_para_a_regulacao_juridica.pdf. Acesso em: 27 dez. 2022

está ligado à possibilidade de conversão da linguagem natural na linguagem computacional e, para que isso ocorra, faz-se necessário que as obrigações contratuais sejam traduzidas em um código binário. A autora também traz, nos seus estudos, a forte relação que há entre contratos inteligentes e *blockchain*, já que "foram as características e funcionalidades desta última - especialmente a imutabilidade e a distribuição digital de conteúdos entre vários usuários - que possibilitaram o crescimento desse tipo de contrato"[14].

A partir daí, concluiu a autora supramencionada que se desenharam as características dos contratos inteligentes, dentre as quais: "(i) a sua natureza eletrônica, (ii) a sua implementação por meio de softwares, (iii) as suas pretensões de certeza e previsibilidade, (iv) a pretensão de autonomia quanto ao seu cumprimento (autoexecutabilidade) e (v) a autonomia quanto ao seu conteúdo, o que lhes permitiria inclusive desconhecer ou mesmo violar diretamente as regras jurídicas"[15].

Recentemente, os *smart Contracts* têm sido construídos com o uso da tecnologia *blockchain*, o que, segundo Berenger, possui diversas vantagens, já que "a gravação de contratos implementados por algoritmos em códigos armazenados nos blocos da cadeia garante a perpetuidade e transparência do acordo. A natureza irretroativa do blockchain impede que as regras sejam alteradas em benefício de qualquer pessoa"[16].

Dando continuidade às suas explicações de como essa sistemática se dá no universo das DAO, Berenger nos ensina:

> Um smart contract, quando criado, tem seu código gravado na blockchain. A partir do momento que a execução do código é iniciada, o modelo DAO começa a ser constituído com adesões de membros e interação de usuários estabelecendo-se, dessa forma, uma organização autônoma e descentralizada com funcionamento ininterrupto. Por ser um software autônomo, o código do *smart contract* é imutável, não podendo ser modificado por nenhuma pessoa, nem

14. FRAZÃO, Ana. O que são contratos inteligentes ou smart contracts? Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-04-11-O_que_sao_contratos_inteligentes_ou_smart_contracts_Quais_sao_suas_principais_repercussoes_para_a_regulacao_juridica.pdf . Acesso em: 27 dez. 2022.

15. FRAZÃO, Ana. O que são contratos inteligentes ou smart contracts? Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-04-11-O_que_sao_contratos_inteligentes_ou_smart_contracts_Quais_sao_suas_principais_repercussoes_para_a_regulacao_juridica.pdf . Acesso em: 27 dez. 2022.

16. BERENGER, Francis *et al*. A Análise de um Modelo Organizacional Autônomo e do seu Artefato Digital: O modelo DAO sob a lente das dinâmicas das rotinas. Disponível em: http://adcont.net/index.php/adcont/adcont2019/paper/view/3380. Acesso em: 27 dez. 2022

> mesmo por seu criador. As organizações autônomas são implementadas considerando-se mecanismos de consenso que possibilitam aos seus membros tomarem decisões. Esses mecanismos têm como base tokens que são adquiridos pelos associados da DAO por intermédio de criptomoedas. Os tokens são associados ao contrato e obtidos na proporção de criptomoedas que o associado transfere para o *smart contract*. Regras de votação dentro da organização, definidas e implantadas nos contratos, consideram a quantidade de tokens que cada membro possui para se chegar a uma decisão[17].

A Ethereum evidencia, ainda, que os *Smart Contracts* constituem a espinha dorsal de uma DAO[18], pois definem as regras da organização e mantém o aspecto financeiro do grupo. Depois que o contrato estiver ativo no Ethereum, ninguém poderá alterar as regras, exceto por votação. Se alguém tentar fazer algo que não esteja coberto pelas regras e pela lógica do código, ele falhará. Como o financeiro também é definido pelo *smart contract*, isso significa que ninguém pode gastar o dinheiro sem a aprovação do grupo. Isso significa que os DAOs não precisam de uma autoridade central. Ao invés disso, o grupo toma decisões coletivamente e os pagamentos são automaticamente autorizados quando os votos são aprovados.

Isso é possível, porque os contratos inteligentes são à prova de adulteração quando são lançados no Ethereum. Não é possível simplesmente editar o código (as regras DAOs) sem que se perceba, já que tudo é publicizado.

2.1.1 algumas controvérsias oriundas dos *smart contracts* no âmbito das DAOs

Os contratos, precipuamente, visam a mitigar riscos para as partes pactuantes. Entretanto, para que isso se faça de maneira eficaz, é preciso que se defina com muita clareza e cautela. Se bem os contratos são feitos para serem cumpridos (*pacta sunt servanda*), é preciso que haja clareza acerca de como serão tratadas eventuais quebras contratuais, especialmente no que tange às consequências legais oriundas de descumprimento.

17. BERENGER, Francis et al. A Análise de um Modelo Organizacional Autônomo e do seu Artefato Digital: O modelo DAO sob a lente das dinâmicas das rotinas. Disponível em: http://adcont.net/index.php/adcont/adcont2019/paper/view/3380. Acesso em: 27 dez. 2022.

18. ETHERUM ORG. *What are DAOS?* Disponível em: https://ethereum.org/en/dao/#:~:text=A%20DAO%20is%20a%20collectively,manage%20the%20funds%20or%20operations. Acesso em 27 dez. 2022.

E é justamente nesse ponto que se apresenta um enorme desafio. Os *Smart Contracts*, conceitualmente, são instrumentos autoexecutáveis, auditáveis e que não permitem ambiguidades. Por outro lado, existem negócios jurídicos altamente complexos, com uma enorme gama de variáveis. Por mais que se estabeleçam cláusulas amplas e abrangentes, pode, sim, ocorrer, a necessidade de uma intervenção pós-contratual, a ser manejada por um sistema legal.

Neste contexto. Viana questiona a viabilidade dos *smart Contracts* para contratações de alta complexidade, a saber:

> Logo, se por um lado os chamados *smart contracts* podem ser extremamente vantajosos, por outro, em sistemas complexos, como o que serão necessários para viabilizar o funcionamento de algumas DAOs, podem representar desvantagens, tornando-se, por vezes, até inviáveis.[19]

Portanto, paira uma dúvida acerca da capacidade de *smart Contracts*, de fato, serem capazes de substituir instrumentos contratuais. A referida autora cogita que tal impasse possa ser solucionado por inteligências artificiais e redes neurais treinadas para solucionar esses imbróglios. Mas o importante, segundo conclui Viana, é que se tenha cautela, pois demasiada burocratização pode desconfigurar a própria essência, fazendo com que percam o seu propósito, já que se tornariam um mero espelho dos sistemas jurídicos atuais.[20]

2.2 Exemplos de utilização e vantagens e desvantagens das DAO

Existem diferentes tipos de DAO para diferentes propostas. Há, por exemplo, as redes de profissionais autônomos para montar um espaço físico ou compartilhar assinatura de um software e as DAOS para empreendimentos -criação de um fundo de capital de investimento e votação de projetos que devem ser apoiados. Ademais, há o capital resultante, que pode ser reembolsado mais tarde e redistribuído aos envolvidos, bem como a inovação social, sendo essa uma forma de levantar fundos para iniciativas específicas e muitas outras hipóteses.

19. VIANA, Fernanda Vilela. *Smart Contracts* e a problemática frente às relações complexas das DAOs. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=35. Acesso em: 13 mar. 2023.

20. VIANA, Fernanda Vilela. *Smart Contracts* e a problemática frente às relações complexas das DAOs. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=35. Acesso em: 13 mar. 2023.

As DAOs podem ter muitas finalidades, dentre elas: investimentos, arrecadação de fundos, empréstimos e comercialização de NFTs. Temos como exemplos atuais de DAOs[21]: Uniswap (UNI), maior corretora de criptomoedas descentralizada do mundo; Compound (COMP), um protocolo de empréstimos; Radicle (RAD), uma rede descentralizada de colaboração de código; Rarible (RARI), software de compra e venda de ativos personalizados, como NFTs, e MakerDAO (MKR), um projeto que une uma DAO a uma *stablecoin* cripto-colateralizada chamada DAI, com o intuito de criar um ecossistema DeFi (finanças descentralizadas) completo.

Além disso, conforme a equipe do Money Times, o próprio Bitcoin é considerado a primeira DAO totalmente funcional, "uma vez que reúne os três principais aspectos do sistema: possui um conjunto pré-programado de regras, funciona de maneira autônoma e é coordenado por meio de um protocolo de consenso distribuído"[22].

Com efeito, a DAOs, a exemplo de muitos outros institutos nesse universo tecnológico, ainda representam uma novidade e que desperta muita especulação. Além disso, possui vantagens e desvantagens, como qualquer organização societária, as quais devem ser avaliadas antes de que se conclua pela conveniência ou não da sua adoção.

Dentre as vantagens, a que merece enorme destaque é a transparência que permeia o seu funcionamento, desde as regras de governança até as votações e qualquer tomada de decisão seja sobre investimentos, orçamento ou qualquer outro assunto relevante, já que tudo devidamente registrado em *blockchain* e permanece disponível para todos. Assim, é possível decidir como gastar os fundos e acompanhar todo o processo envolvido.

Em adição, a falta de hierarquia se apresenta como uma das vantagens nas DAOs. Ideias inovadoras e sugestões relacionadas à governança do negócio podem ser apresentadas por qualquer membro da organização, sem distinção de cargos. Isso facilita a apresentação de ideias inovadoras por qualquer pessoa e, claro, a sua consideração por todos. Não é necessária uma autoridade central nas DAOs, já que o grupo decide de maneira coletiva. Os pagamentos

21. MONEYTIMES. O que são DAOs e qual papel elas cumprem no universo dos criptoativos? Disponível em: https://www.moneytimes.com.br/conteudo-de-marca/o-que-sao-daos-e-qual-papel-elas-cumprem-no-universo-dos-criptoativos/. Acesso em: 27 dez. 2022.

22. MONEYTIMES. O que são DAOs e qual papel elas cumprem no universo dos criptoativos? Disponível em: https://www.moneytimes.com.br/conteudo-de-marca/o-que-sao-daos-e-qual-papel-elas-cumprem-no-universo-dos-criptoativos/. Acesso em: 27 dez. 2022.

são autorizados de maneira automática mediante a aprovação dos votos dos participantes, que são computados por *tokens*. É necessário destacar que o código da organização deverá manter os seguros arrecadados de forma segura, acompanhar os proprietários que detêm o *token* da DAO, definir as regras de governança e gerenciar os processos de votação. O código da organização deverá definir o modelo de negócio (se houver), os parâmetros operacionais e os termos de pagamento. Isso tudo ocorrerá de forma clara para aqueles que desejem participar, sob pena de comprometer a sua autonomia.

A acessibilidade também merece destaque, já que, para integrar uma DAO, basta ser um usuário ativo do mercado de criptomoedas de qualquer lugar do mundo, sem qualquer tipo de restrição. Por fim, destaca-se a facilidade de angariar recursos. Nesse contexto, surgem dúvidas de como, por exemplo, seria possível uma DAO estar em conformidade com regras de lavagem de dinheiro, com participantes espalhados por todo o mundo.

Ainda no que concerne às desvantagens, destacam-se primordialmente certos riscos, sobretudo os concernentes à não regulamentação da DAO como forma societária, já que carecerá das proteções jurídicas existentes em relação às formas societárias reguladas, o que torna mais desafiador o dimensionamento dos riscos.

Outro desafio que se apresenta é a responsabilização pelos atos praticados por uma DAO. Quem responderia, por exemplo, por uma violação de direito autoral realizada por uma DAO? Aliadas a essas novas tecnologias, surgem situações antes não previstas por legislações e regulamentações em geral, o que traz à tona a discussão sobre o papel do Direito com relação às inovações que surgem nos diferentes âmbitos da humanidade. Para que as DAOs possam se comunicar com o mundo físico, é preciso que haja algum quadro jurídico. Como tudo é muito novo, as possíveis soluções para o problema ainda estão a caminho.

> Uma outra questão é a tendência de pessoas considerarem os seus projetos como DAO, sem efetivamente serem, já que, como qualquer instituto, existem premissas básicas, requisitos que o qualifiquem como tal.

Por fim, sem o propósito de exaurir o tema, destaca-se que outra grande desvantagem, indubitavelmente, gira em torno do aspecto da falta de segurança. Sob a ótica desta análise, vale trazer à baila o caso da “The DAO”. Desenvolvida com base na *blockchain* do Ethereum, tal organização autônoma foi

criada como um fundo de risco para financiar startups usuárias da tecnologia de *blockchain*. Essas poderiam solicitar um aporte financeiro e, uma vez aprovado o seu projeto pelos membros da organização, receberia investimento em criptoativos, a partir da adesão ao *smart contract* da The DAO, ficando todas as informações sobre o financiamento, aprovação e investimento registradas publicamente na *blockchain*. A fase inicial de operação ocorreu de 30 de abril de 2016 até 28 de maio de 2016. Ao final, mais de 10.000 pessoas tinham investido na The DAO o total de 11.994.260,98 ether, criptomoeda do Ethereum, equivalente a cerca de US$ 250 milhões, um valor sem precedentes no universo de *crowdfunding* até então[23].

Pouco tempo depois, em 17 de junho de 2016, uma falha no código do *smart contract* foi explorada e um *hacker* desviou cerca de 3.6 milhões de Ether, algo em torno de 70 milhões de dólares na época do ataque[24]. Essa situação crítica gerou uma intervenção no modelo DAO, com a finalidade de impedir que o montante desviado pudesse ser trocado por qualquer moeda conversível. Nesse caso, houve um inequívoco desrespeito ao princípio da imutabilidade dos blocos do *blockchain*[25].

Posteriormente, uma solução definitiva, conhecida como *hard fork*, foi adotada. Blocos com informações indesejadas da blockchain Ethereum foram desconsiderados com recomeço da gravação sequencial a partir de um determinado ponto. Com isso, um novo contrato foi criado permitindo que os investidores retirassem todos os seus *tokens* associados ao contrato anterior. Essa decisão fez com que as regras originais do smart contract fossem “quebradas” e a The DAO foi definitivamente apagada da *blockchain.*[26]

As intervenções realizadas no caso The DAO na *blockchain* Ethereum foram bastante polêmicas. Nas palavras de Berenger:

> Alguns grupos argumentaram que a realização de um *hard fork* foi

23. BERENGER, Francis et al. A Análise de um Modelo Organizacional Autônomo e do seu Artefato Digital: O modelo DAO sob a lente das dinâmicas das rotinas. Disponível em: http://adcont.net/index.php/adcont/adcont2019/paper/view/3380. Acesso em: 27 dez. 2022.

24. FALKON, Samuel. *The Story of the DAO — Its History and Consequences*. Disponível em: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee. Acesso em: 03 Jan. 2023.

25. SIEGEL, David. Understanding The DAO Attack. Disponível em: https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/. Acesso em: 28 dez. 2022.

26. DUPONT, Q. *Experiments in Algorithmic Governance: A history and ethnography of “The DAO,” a failed Decentralized Autonomous Organization*. In: CAMPBELL-VERDUYN, M. (ed.). Bitcon and Beyond - Cryptocurrencies, Blockchains and Global Governance. Nova York: Routledge, 2018.

> um ato autoritário que feriu o princípio democrático de uma DAO. Se o 'código é lei', o invasor apenas explorou uma falha no código do contrato. Partindo desse princípio, qualquer tipo de bloqueio na ação realizada estaria indo contra o espírito de uma organização autônoma descentralizada. Quanto às possíveis perdas financeiras que poderiam ter ocorrido, pode-se considerar que os membros da DAO aceitaram voluntariamente associar-se à organização concordando com o contrato proposto, o que incluiria possíveis falhas existentes no código do contrato.

O caso The DAO, conforme ressalta Berenger é, de fato, um marco relevante no estudo de modelos organizacionais "diante do ineditismo da proposta e do grande interesse despertado por investidores que aportaram capital significativo em uma comunidade de pessoas anônimas regidas apenas por um software que automatizava todo relacionamento entre as partes".

O insucesso desse grande experimento tem permitido um estudo mais aprofundado sobre a estruturação de uma organização autônoma descentralizada. A partir daí, novos modelos DAO vêm sendo estudados e criados, para as mais diversas finalidades e propósitos.

2.3 As DAO no Brasil

Na prática, operacionalizar umas DAOs traz muitas dificuldades, visto que a maioria das pessoas e empresas ainda não estão preparadas e/ou devidamente inseridas no âmbito da web 3.0 e do universo dos *tokens*. Também não resta claro como se dá a operacionalização de temas corriqueiros como a contratação de colaboradores, abertura de contas em bancos ou, ainda, o recolhimento de tributos.

Destarte, o ordenamento jurídico pátrio, no que concerne aos tipos societários existentes, não foi estruturado com vistas a uma com controle e administração distribuídos, com a ausência de endereço fiscal, com regras automáticas e sem uma figura e/ou um grupo de figuras centrais responsáveis pela gestão e administração da organização. Por essa razão, as DAOs têm experimentado todo tipo de dificuldade no relacionamento com outras organizações, pessoas e autoridades.

Portanto, no Brasil, assim como na maioria dos países, as DAOs não possuem um reconhecimento legal, de forma que a sua implementação não é reconhecida como uma organização legalmente válida, considerando a legislação vigente. Além disso, como bem salienta Borges, "levando em conta o atual ordenamento jurídico brasileiro, seria necessário enfrentar a questão da

responsabilidade quanto aos negócios e atividades desempenhadas por uma DAO, uma vez que inexiste uma figura central de controle"[27].

Ainda segundo Borges, outro desafio para a estruturação de uma DAO no país reside na natureza jurídica dos tokens de governança por ela emitidos:

> A rigor, os tokens emitidos por uma DAO, que conferem ao seu detentor poder de voto nas deliberações e direito de participação nos eventuais resultados dos negócios desenvolvidos, independente da forma em que tais resultados são distribuídos - seja na forma de tokens ou de moeda fiduciária -, podem ser caracterizados como valores mobiliários, na forma do artigo 2º da Lei nº 6.385/76[28].

Assim, ainda que ocorra o reconhecimento da validade jurídica das DAOs, faz-se necessária uma definição quanto à possibilidade de oferta/distribuição de seus *tokens*, uma vez que a atual legislação de mercado de capitais traz algumas obrigações incompatíveis com o processo de tokenização pela tecnologia *blockchain*, o que conforme explicitado pelo autor retromencionado, irá requerer experimentação e análise da CVM pelo Sandbox Regulatório.

Apesar do seu enorme potencial, a princípio, nem todo tipo de negócios comportaria a descentralização e distribuição do processo decisório sem divisões hierárquicas propostas pelo modelo DAO. Entretanto, para modelos de negócio que não dependam de decisões operacionais diárias, a DAO poderia se mostrar um excelente mecanismo, na medida em que poderia facilitar o processo de captação de recursos, além de permitir maior engajamento dos investidores pela participação direta nas tomadas de decisão.

Há grandes benefícios na instituição de DAOs, como os já mencionados: possibilidade de conglomeração de indivíduos em vários cantos do mundo, a ideia de comunidade, a ausência de hierarquias verticais rígidas e outras discorridas ao longo do trabalho. Conforme aduz Palhares, é cedo para afirmar que serão o futuro das organizações, mas seguramente servirão de inspiração para o futuro:

> Embora seja cedo para afirmar categoricamente que DAOs serão o futuro das organizações, não restam dúvidas de que essas novas

27. BORGES, Rodrigo. DAO: um novo modelo de organização. Disponível em: https://mittechreview.com.br/dao-um-novo-modelo-de-organizacao/. Acesso em: 28 dez. 2022.

28. BORGES, Rodrigo. DAO: um novo modelo de organização. Disponível em: https://mittechreview.com.br/dao-um-novo-modelo-de-organizacao/. Acesso em: 28 dez. 2022.

> estruturas, pautadas e, tecnologia de registros públicos, terão papel relevante na forma em que pessoas se organizam para atingir objetivos comuns ao longo dos próximos anos e dificilmente não farão parte do cotidiano das novas gerações.[29]

Ainda, assim, Palhares entende se posiciona no sentido de que "não há como ignorar os diversos desafios jurídicos que precisarão ser enfrentados até que as organizações autônomas centralizadas ganhem esse status e se tornem ubíquas"[30].

Considerações finais

As organizações estão cada vez mais permeadas por tecnologias digitais. Produtos, serviços, processos e modelos de negócio vêm sendo construídos a partir de artefatos inteligentes e se espera que esse seja o futuro, ou melhor, já é o presente. Tecnologias emergentes têm proporcionado o surgimento de modelos processuais a partir de novas formas de organização. Observa-se nas organizações a multiplicação de *smart devices* que ampliam a capacidade de captura de dados com análise e tomada de decisão, muitas vezes de forma autônoma. Como consequência, modelos organizacionais como as DAO, até então inéditos, vêm surgindo e se aprimorando. Nesse contexto, novas rotinas emergem, influenciadas por artefatos digitais e novos desenhos organizacionais. É inegável que as DAOs constituem mais um passo na evolução dos tipos de organização, possibilitando, pelo emprego da tecnologia *Blockchain*, a participação direta em processos decisórios e a estruturação de organizações efetivamente globais e distribuídas.

Esse trabalho objetivou realizar uma análise das DAO como novo modelo organizacional, construído a partir de uma tecnologia eminentemente digital. Buscou-se também analisar os *smart contracts* como parte integrante do referido modelo. A principal conclusão do estudo é que a DAO, como forma organizacional de sociedades, é considerada uma tendência. As suas vantagens, destacadas ao longo do trabalho, parecem bem atraentes, mas, não se pode deixar de considerar seus pontos negativos, como o risco de ataques *hacker* e o contexto de incerteza jurídica.

29. PALHARES, Felipe. O futuro das organizações. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=38. Acesso em: 13 mar. 2023.

30. PALHARES, Felipe. O futuro das organizações. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=38. Acesso em: 13 mar. 2023.

Faz-se necessária uma compreensão mais aprofundada sobre o tema, inclusive sobre os seus requisitos, bem como a sua aplicabilidade no ordenamento jurídico, antes que se faça uma opção por esse modelo, sobretudo no ordenamento pátrio, no qual, como vimos, ela ainda não encontra respaldo legal. Apesar das DAOS demonstrarem um enorme potencial para inúmeras estruturas corporativas, a sua implementação, do ponto de vista jurídico/regulatório, não é tão simples quanto a ótica tecnológica.

Referências

BERENGER, Francis *et al*. **A Análise de um Modelo Organizacional Autônomo e do seu Artefato Digital: O modelo DAO sob a lente das dinâmicas das rotinas**. Disponível em: http://adcont.net/index.php/adcont/adcont2019/paper/view/3380. Acesso em: 27 dez. 2022.

BORGES, Rodrigo. **DAO: um novo modelo de organização**. Disponível em: https://mittechreview.com.br/dao-um-novo-modelo-de-organizacao/. Acesso em: 28 dez. 2022

CAMPINO, José, BROCHADO, Ana, ROSA, Álvaro. **Fatores de sucesso das *Initial Coin Offerings* (ICOS) - A importância do capital Humano.** Disponível em: article_83059.pdf (iscte-iul.pt). Acesso em: 20 dez. 2022.

DECENTRALISED AUTONOMOUS ORGANISATION. ***Internet Policy Review***. Disponível em: https://policyreview.info/open-abstracts/decentralised-autonomous-organisation. Acesso em: 26 dez. 2022.

DUPONT, Q. ***Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization***. In: CAMPBELL-VERDUYN, M. (ed.). Bitcon and Beyond - Cryptocurrencies, Blockchains and Global Governance. Nova York: Routledge, 2018.

ETHEREUM ORG. ***Ethereum Whitepaper***. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 26 dez. 2022.

ETHEREUM ORG. ***What are DAOS?*** Disponível em: https://ethereum.org/en/dao/#:~:text=A%20DAO%20is%20a%20collectively,manage%20the%20funds%20or%20operations. Acesso em 27 dez. 2022.

FALKON, Samuel. ***The Story of the DAO — Its History and Consequences***. Disponível em: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee. Acesso em: 03 Jan. 2023.

FRAZÃO, Ana. **O que são contratos inteligentes ou *smart contracts*?** Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-04-11-O_que_sao_contratos_inteligentes_ou_smart_contracts_Quais_sao_suas_principais_repercussoes_para_a_regulacao_juridica.pdf. Acesso em: 27 dez. 2022.

LAURENCE, Tiana. I***ntroduction to blockchain technology: the many faces of blockchain technology in the 21st century***. Países Baixos: Van haren Publishing, 2019.

LEMOS, Ronaldo. **O Impacto de NFT é maior do que se pensa**. Disponível em: https://itsrio.org/pt/artigos/impacto-de-nft-e-maior-do-que-se-pensa/. Acesso em: 20 dez. 2022.

MONEYTIMES. **O que são DAOs e qual papel elas cumprem no universo dos criptoativos?** Disponível em: https://www.moneytimes.com.br/conteudo-de-marca/o-que-sao-daos-e-qual-papel-elas-cumprem-no-universo-dos-criptoativos/. Acesso em: 27 dez. 2022.

PALHARES, Felipe. **O futuro das organizações**. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=38. Acesso em: 13 mar. 2023.

SHARMA, Rakesh. ***What Is Decentralized Finance (DeFi) and How Does It Work?*** Disponível em : https://www.investopedia.com/decentralized-finance-defi-5113835#:~:text=Decentralized%20finance%20(DeFi)%20is%20an%20emerging%20financial%20technology%20that%20challenges,peer%2C%20or%20P2P%2C%20transactions. Acesso em: 3 de Jan 2023.

SIEGEL, David. ***Understanding The DAO Attack***. Disponível em: https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/. Acesso em: 28 dez. 2022

VALEONTI, F. *et al*. ***Crypto collectibles, museum funding and openglam: Challenges, opportunities, and the potential of non-fungible tokens (NFTS)***. Disponível em: https://www.mdpi.com/2076-3417/11/21/9931. Acesso em: 03 de

Jan 2023.

VIANA, Fernanda Vilela. ***Smart Contracts* e a problemática frente às relações complexas das DAOs**. Disponível em: https://publicacoes.bmalaw.com.br/books/iqdq/?utm_campaign=e-#p=35. Acesso em: 13 mar. 2023.

WATSON, Andy. What is Initial Coin Offering (ICO)? Disponível em: https://www.coinspeaker.com/guides/what-is-initial-coin-offering/. Acesso em: 26 dez. 2019.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

6

Smart contracts e gestão de risco: uma análise da relação entre contratos inteligentes e cláusula resolutiva expressa

LUCAS CESAR PESSÔA DE MELLO LAVOGADE

Sumário: Introdução. 1. Os contratos inteligentes (smart contracts) como (r)evolução do direito dos contratos. 2. Blockchain e suas contribuições para os smart contracts. 3. Contrato e risco: delineando o problema. 4. A cláusula resolutiva expressa nos smart contracts: tentativas de compatibilização. Considerações finais. Referências.

Introdução

Quando se fala em direito dos contratos, é preciso atribuir uma especial atenção às circunstâncias econômicas, uma vez que "falar de contrato significa sempre remeter – explícita ou implicitamente, directa ou mediatamente – para a ideia de operação económica"[2]. E, ainda que o contrato, como fenômeno jurídico, não se resuma à operação econômica que lhe subjaz, inclusive podendo vir a influenciá-la e não somente formalizá-la, é verdade que sua existência se justifica em função dessa operação[3].

Os contratos, em economia, são muitas vezes vistos como promessas baseadas em salvaguardas institucionais (poder coercitivo do Estado), voltadas para a coordenação de transações, permitindo planejamento dos agentes econômicos[4]. O direito dos contratos visa a garantir que haja confiança entre as partes – ao menos das partes em relação às instituições jurídicas –, de forma a mitigar os riscos de descumprimento ou cumprimento inadequado de promes-

1. Pós-graduado em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) em conjunto com a Universidade do Estado do Rio de Janeiro (UERJ), graduado pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e membro do Grupo de Estudos Processuais do Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (GEP PUC-Rio).

2. ROPPO, Enzo. O contrato. Tradução de Ana Coimbra e M. Januário C. Gomes. Coimbra: Edições Almedina S.A., 2009, p. 8. Paula Forgioni chega a afirmar que "o mercado identifica-se com um emaranhado de relações contratuais, tecido pelos agentes econômicos" (FORGIONI, Paula A. Contratos empresariais: teoria geral e aplicação. 2. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2016, p. 24). Em mesmo sentido, afirma Thiago Barcik Lucas de Oliveira que: "as transações econômicas (relações contatuais) são a forma através da qual há interação entre os agentes econômicos, os quais se relacionam com o propósito de alocar eficientemente seus bens e serviços disponíveis, maximizando seus interesses próprios" (OLIVEIRA, Thiago Barcik Lucas de. A economia dos custos de transação e o novo modelo proposto pelos smart contracts. Revista Jurídica Luso-Brasileira, Ano 8, n. 3, p. 1651-1679, 2022, p. 1668. Disponível em: <https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1651_1679.pdf>. Acesso em: 27.12.2022).

3. ROPPO, Enzo. Op. cit., p. 9.

4. SZTAJN, Rachel; ZYLBERSZTAJN, Decio; e AZEVEDO, Paulo Furquim de. Economia dos contratos. In SZTAJN, Rachel; e ZYLBERSZTAJN, Decio (Org.). Direito e economia: análise econômica do direito e das organizações. Rio de Janeiro: Elsevier, p. 107-136, 2005, p. 103-105.

sas feitas entre os sujeitos dentro de uma relação[5].

No entanto, em sua interlocução com a vida das relações econômicas, é preciso lembrar que o contrato encontra desafios, diante dos mais diversos fatores. Não há contrato que consiga impedir o inadimplemento ou resista à má-fé[6]. Risco de inadimplemento – que, quando há contrato, é reduzido, mas não desaparece –; custos de transação com as negociações, assinatura e mesmo acompanhamento do cumprimento do contrato[7]; atuação oportunista dos agentes[8]; e assimetria informacional[9] são alguns problemas com os quais o direito dos contratos esbarra em seu papel de regulação das transações. Diante de todas as possibilidades de intercorrências, o contrato se consagra como um instrumento de atribuição de confiança e segurança, bem como de alocação de riscos[10]. Mas, por evidente, ele não é capaz de impedir, de maneira absoluta, a ocorrência de toda e qualquer adversidade.

Com o intuito de solucionar alguns desses problemas, a tecnologia surge trazendo novos formatos de contratação e apresentando opções aos desafios vislumbrados na prática contratual. Exemplo claro de tal intenção tecnológica reside nos smart contracts (ou contratos inteligentes), que visam a atribuir maior confiança ao cumprimento dos contratos, bem como solucionar problemas relativos aos custos de transação. No entanto, em seu caminho para buscar soluções, os contratos inteligentes se deparam com seus próprios desafios, especialmente os relativos à operacionalização de institutos classicamente usados no direito dos contratos, como a cláusula resolutiva expressa.

O presente trabalho tem como escopo a análise de uma possível relação entre os smart contracts e a cláusula resolutiva expressa, com foco para aplicação de ambos os institutos na gestão de riscos contratuais. A principal fon-

5. FANDL, Kevin J. Can smart contracts enhance firm efficiency in emerging markets. Northwestern Journal of International Law and Business, Vol. 40, Issue 3, p. 333-362, Spring 2020, p. 339. Disponível em: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1857&context=njilb>. Acesso em 29.11.2022.

6. FORGIONI, Paula. Op. Cit., p. 73. A lição é proferida no âmbito de análise dos contratos empresariais, mas vale para todo tipo de contrato.

7. Para maiores aprofundamentos sobre a noção de custos de transação, cf. FORGIONI, Paula. Op. cit., p. 141-144; OLIVEIRA, Thiago Barcik Lucas de. Op. cit., p. 1663-1668.

8. AZEVEDO, Miguel Gomes. A eficiência econômica dos princípios do direito contratual brasileiro. Rio de Janeiro: Lumen Juris, 2019, p. 48-51; FORGIONI, Paula. Op. cit., p. 150.

9. SZTAJN, Rachel; ZYLBERSZTAJN, Decio; e AZEVEDO, Paulo Furquim de. Op. cit., p. 121-126.

10. Sobre contrato como instrumento de alocação de riscos: FORGIONI, Paula. Op. Cit., p. 145-147. MAYER FEITOSA, M. L. P. de A. O contrato como regulador e como produtor de riscos. Prim@ Facie, [S. l.], v. 4, n. 6, p. 62–85, 2010. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/4507. Acesso em: 14.12.2022.

te de estudo, para tanto, consistiu na pesquisa doutrinária sobre ambos os institutos.

1. Os contratos inteligentes (smart contracts) como (r)evolução do direito dos contratos

Os smart contracts, mencionados pela primeira vez por Nick Szabo[11], têm como objetivo resolver diversos problemas verificados nos contratos tradicionais, possibilitando redução de custos de transação, diminuição da necessidade de confiança entre as partes contratantes e mitigação da dificuldade interpretativa decorrente das ambiguidades da linguagem humana, entre outros benefícios[12].

O conceito de contratos inteligentes é muitas vezes utilizado como sinônimo de contratos autoexecutáveis[13], mesmo porque tais mecanismos, fundados na aplicação de softwares, impõem a execução automática de obrigações previamente definidas pelas partes[14]. A título exemplificativo são lembradas as máquinas de venda (vending machines), encontradas em metrôs e hospitais, por exemplo, nas quais, após a inserção do valor e escolha do alimento pelo consumidor, disponibilizam o bem comprado sem a necessidade de intervenção humana. Além desse caso, muitos outros indicam a proliferação de contratos inteligentes e para citar alguns exemplos podemos mencionar: a transferência automática de valores por instituições financeiras, mediante a programação pelo titular da conta, sem a necessidade de atuação dos

11. SZABO, Nick. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 1997. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>. Acesso em: 25.11.2022.

12. Sobre possíveis usos e benefícios dos smart contracts, confira-se: SKLAROFF, Jeremy M. Smart contracts and the costs of inflexibility. University of Pennsylvania Law Review, Vol. 166, p. 263-303, 2017, p. 275. Disponível: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1009&context=prize_papers>. Acesso em: 27.12.2022; O'SHIELDS, Reggie. Smart contracts: legal agreements for the blockchain. North Carolina Banking Institute, Vol. 21, Issue 1, p. 177-194, March 2017, p. 181-183. Disponível em: <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1435&context=ncbi>. Acesso em: 26.11.2022; COHN, Alan; WEST, Travis; e PARKER, Chelsea. Smart after all: blockchain, smart contracts, parametric insurance, and smart energy grid. Georgetown Law Technology Review, Vol. 1, Issue 2, p. 273-304, April 2017, p. 290-303. Disponível em: <https://perma.cc/TY7W-Q8CX>. Acesso em: 25.11.2022; TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Op. cit., p. 388.

13. COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 280. No mesmo sentido, Max Raskin, que afirma que "[a] smart contract is an agreement whose execution is automated" (RASKIN, Max. The law and the legality of smart contracts. Georgetown Law Technology Review, Vol. 1, Issue 2, p. 305-341, April 2017, p. 309. Disponível em: <https://perma.cc/673G-3ANE>. Acesso em: 25.11.2022).

14. Nas palavras de Aline Terra e Deborah Santos, "o que define os smart contracts é, em primeiro lugar, o fato de sua execução ser automatizada" (TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. Do pacta sunt servanda ao code is law: breves notas sobre a codificação de comportamentos e os controles de legalidade nos smart contracts. In TEPEDINO, Gustavo; e SILVA, Rodrigo da Guia (Coord.). O direito civil na era da inteligência artificial. 1. ed. São Paulo: Thomson Reuters Brasil, p. 397-409, 2020, p. 399).

funcionários do banco; o bloqueio do sistema de ignição de veículo alienado fiduciariamente uma vez constatado inadimplemento do devedor; e o bloqueio automático de portas de apartamento, diante do não pagamento do aluguel pelo locatário.

Os smart contracts consistem em softwares que permitem a execução automática de determinadas funções previamente definidas em seu programa[15]. Para possibilitar essa autoexecutoriedade, esses programas, chamados por alguns de contractware[16], funcionam de acordo com uma lógica condicional de "se X, então Y"[17], onde X é a situação, fato ou condição que, uma vez verificada pelo software, impõe seu funcionamento automático para atingir o resultado Y.

A tecnologia smart contract pode ser utilizada em qualquer ato ou função digitalmente realizável, ou seja, não há necessidade de que exista um contrato para aplicação dessa tecnologia[18]. Os "contratos inteligentes" se traduzem em uma tecnologia que não precisa necessariamente estar vinculada a contratos jurídicos. Assim, esses softwares inteligentes podem ser utilizados para automatizar o cumprimento de outro tipo de negócio jurídico, como um testamento (negócio jurídico unilateral)[19]; ou mesmo um ato que sequer configure negócio jurídico, como a atuação de um objeto ligado à rede a partir da captura de informações que demonstrem a ocorrência de condição necessária para sua

15. CIEPLAK, Jenny; e LEEFATT, Simon. Smart contracts: a smart way to automate performance. Georgetown Law Technology Review, Vol. 1, Issue 2, p. 417-427, April 2017, p. 417-418. Disponível em: <https://perma.cc/EUT6-RL6P>. Acesso em: 25.11.2022. No mesmo sentido: COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 280; O'SHIELDS, Reggie. Op. cit., p. 179.

16. Nesse sentido, cf. Max Raskin, que define contractware da seguinte forma: "I will define contractware as the physical instantiation of a computer-decipherable contract" (RASKIN, Max. Op. cit., p. 312).

17. CANTALI, Rodrigo Ustárroz. Smart contracts e o direito contratual: primeiras impressões sobre suas vantagens e limites. Revista Jurídica Luso-Brasileira, Ano 8, n. 3, p. 1529-1566, 2022, p. 1536. Disponível em: <https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1529_1566.pdf>. Acesso em: 25.11.2022; TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência artificial, smart contracts e gestão do risco contratual. In TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. O direito civil na era da inteligência artificial. 1. ed. São Paulo: Thomson Reuters Brasil, p. 373-396, 2020, p. 384.

18. Esse é o posicionamento claro de Giusella Finocchiaro e Chantal Bomprezzi, para quem "[a] smart contract per se is a computer code that, upon the occurrence of a specific condition, is capable of running automatically. This code can be stored and processed on a blockchain and any change is recorded in the blockchain. In theory, smart contracts can automate everything" (FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. A legal analysis of the use of blockchain technology for the formation of smart legal contracts. medialaws.eu – Rivista di Diritto dei Media, Itália, Vol. 2, p. 111-135, Maggio 2020, p. 115-116. Disponível em: <https://www.medialaws.eu/wp-content/uploads/2020/07/RDM_2_2020-Finocchiaro.pdf>. Acesso em: 25.11.2022).

19. Nesse sentido, Max Raskin nos proporciona o exemplo de utilização da tecnologia de smart contracts para automatizar obrigações de testamento (inspirado no caso Ricketts v. Scothorn), no qual um avô deixa para sua neta determinada quantia em dinheiro em conjunto com uma orientação em código no sentido de que ele não poderia mudar decisão (revogar a determinação de pagar a quantia à neta) (RASKIN, Max. Op. cit., p, 323). Olhando para a questão de maneira objetiva, o autor do testamento poderia simplesmente indicar, utilizando o código de computador, que a quantia fosse transferida para a neta automaticamente a partir da verificação de seu falecimento.

atividade (e.g., termostato que altera a temperatura ao perceber a ocorrência, no ambiente, de um fato predefinido)[20].

A partir disso, logo se percebe que estes "contratos" não traduzem modalidade ou tipo contratual novo.[21] Os smart contracts são programas de computador (softwares) utilizados para automatizar determinadas soluções, a partir da constatação de uma condição previamente definida, e, por isso, não se configuram como novo tipo contratual, mas sim como instrumento apto a automatizar obrigações componentes de contratos típicos ou atípicos.

Como o contrato inteligente é um software ou programa de computador, a linguagem que utiliza não é a linguagem humana, mas sim códigos de computador (computer codes)[22], o que traz alguns benefícios e prejuízos para sua aplicação no direito dos contratos.

A utilização da linguagem de computador reduz a ocorrência das ambiguidades presentes na linguagem humana[23]. O que está descrito no código ocorrerá na forma previamente definida, não há ambiguidade ou espaço para interpretação, pois se trata de linguagem objetiva.

Em contrapartida, a utilização de computer codes limita aquilo que pode ser previsto como obrigação de um smart contract[24]. Dificilmente um contrato inteligente poderá tratar de obrigações que envolvam a interpretação e aplicação de conceitos jurídicos indeterminados ou cláusula gerais, como alguns deveres decorrentes da boa-fé objetiva (desde que não estejam previamente estipulados pelas partes) ou o cumprimento de uma obrigação que envolva a análise das "práticas do mercado" ou "costumes mercantis" (se as partes não tiverem predeterminado em que consistem objetivamente os atos representativos dessas "práticas" ou "costumes", em um modelo "se X, então Y")[25].

20. O exemplo é fornecido por Giusella Finocchiaro e Chantal Bomprezzi (FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 116).

21. CANTALI, Rodrigo Ustárroz. Op. cit., p. 1541. TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Op. cit., p. 385.

22. FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 113. No mesmo sentido: O'SHIELDS, Reggie. Op. cit., p. 181.

23. RASKIN, Max. Op. cit., p. 324-326; TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. Op. cit., p. 400.

24. FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 125-126.

25. Nesse sentido, a crítica formulada por Jeremy Sklaroff aos smart contracts, ao afirmar que "[p]erformance standards present further difficulties by creating a logical gap or undefined term in the contract. A term like 'commercial reasonableness' will mean different things to different parties, in different transactions, at different times" (SKLAROFF, Jeremy M. Op. cit., p. 293). Em mesmo sentido: FANDL, Kevin J. Op. cit., p. 351-352. Igualmente, Gustavo Tepedino e Rodrigo da Guia afirmam que: "a objetividade da linguagem computacional não propicia a consideração de normas de textura mais aberta, tam-

A respeito do exercício da função de execução automática das prestações pelos smart contracts, é preciso distinguir algumas situações, visto que os contratos inteligentes podem ser aplicados para automatizar todas as obrigações principais ou somente as de uma parte[26].

O primeiro caso, execução automatizada de todas as principais obrigações, só pode acontecer, por óbvio, quando ambas as partes têm obrigações autoexecutáveis, como obrigações de transferência de valores. Exemplo claro seria a execução de contrato de swap[27] através de smart contract cujo código prevê a transmissão automática dos valores ou riscos trocados pelas partes, sem que haja atuação humana no ato de transferência. No caso, o ingresso do valor de rendimento do título de cada parte em sua respectiva conta seria identificado pelo software, que já determinaria a transferência imediata à conta da contraparte, operacionalizando a troca de riscos, sem a necessidade de intervenção humana na realização da transferência de recursos.

Por outro lado, o smart contract pode automatizar somente a prestação devida por uma das partes, relegando a prestação da outra ao cumprimento por ato humano[28]. Seria o caso de um contrato em que uma das partes venha a receber um pagamento automático a partir da conta bancária da outra, desde que verificado o cumprimento da contraprestação consistente em entregar bem ou prestar serviço – obrigação que precisaria de atividade humana direta.

No entanto, essa distinção entre smart contracts que automatizam as prestações de ambas as partes ou de apenas uma delas pode perder relevância diante de contratos unilaterais, nos quais apenas uma das partes tem pres-

---

pouco a consideração de circunstâncias que não haviam sido prévia e expressamente reguladas pelas partes" (TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Op. cit., p. 391).

26. Fala-se em uso do código de computador para automatizar a performance (execução/cumprimento) do acordo total ou parcialmente (FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 116).

27. O contrato de swap é um tipo de derivativo em que "as partes constituem direitos e obrigações entre si, sem transferirem as respectivas posições contratuais" (CAVALCANTE, Henrique Haruki Arake. A natureza jurídica dos contratos futuros. Revista da Procuradoria-Geral do Banco Central, Brasília: Banco Central do Brasil, vol. 3, n. 2, p. 135-172, dez. 2009, p. 142. Disponível em: <https://revistapgbc.bcb.gov.br/revista/issue/view/20/Revista%20PGBC%20-%20V.3%20-%20N.2%20%282009%29>. Acesso em: 26.11.2022). Neste contrato, "existe a troca de fluxos financeiros referenciados no mesmo ativo subjacente, sendo que tais fluxos são ajustados por indexadores distintos. Ocorre também no contrato de swap a transferência de risco, característica inerente a todos os contratos derivativos" (FERREIRA, Kenneth Antunes. Contrato derivativo não padronizado: a impropriedade de sua classificação como valor mobiliário. Dissertação (Mestrado em Direito) – Mestrado em Direito Comercial, Pontifícia Universidade Católica de São Paulo, São Paulo, 147 p., 2008, p. 49. Disponível em: <https://tede2.pucsp.br/bitstream/handle/8206/1/Kenneth%20Antunes%20Ferreira.pdf>. Acesso em: 26.11.2022).

28. Segundo Aline Terra e Debora Pereira Pinto dos Santos, "nada impede, como já se deixou transparecer nas linhas anteriores, que uma mesma relação contratual tenha apenas algumas de suas obrigações constantes de smart contract, enquanto as demais observem o formato tradicional do direito das obrigações" (TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. Op. cit., p. 400).

tação a cumprir em favor da outra[29], como ocorre com o contrato de doação e o de depósito.

Os contratos inteligentes podem também ser utilizados para automatizar, não a prestação em si, mas uma sanção prevista contratualmente para casos de mora ou inadimplemento, ou mesmo uma medida de retorno ao status quo ante, em face do não prosseguimento do negócio. Alguns exemplos seriam: o caso do carro com dispositivo que permita sua desativação, ou impeça a ignição, uma vez reconhecido o não pagamento por parte do locador devedor fiduciante (contratos de alienação fiduciária em garantia); e o caso do retorno automático de valores colocados por uma das partes em um fundo escrow e que seriam destinados ao cumprimento do contrato, em caso de inadimplemento da contraparte, ou mesmo de impossibilidade superveniente do objeto da contraprestação.

Para que os contratos inteligentes funcionem, é necessário o preenchimento de ao menos dois requisitos: (i) previsão em seu código de uma relação condicional "se X, então Y"; e (ii) meios que possibilitem ao software ter acesso à informação sobre a concretização ou não da condição ensejadora de sua atuação (condição "X"). Sobre a informação da ocorrência da condicionante, podem ser diversos os meios utilizados pelos smart contracts para acessá-la. Nesse sentido, podem as partes indicar a ocorrência do fato, fazendo o input da informação ou a própria inteligência do contrato pode estar ligada a meios que disponibilizem esse dado, os oráculos, que são agentes externos ou fontes confiáveis[30], como outros programas que realizam leituras na rede e em bancos de dados ou estão vinculados a sensores para captação de informações do ambiente. Nas palavras de Jenny Cieplak e Simon Leefatt, "[a]n oracle is a third-party information services provider that will digitally 'sign' a transaction, attesting to the occurrence of specific conditions"[31].

A partir de suas características, é possível aferir que os smart contracts apresentam uma série de vantagens e benefícios para o direito dos contratos. Os contratos inteligentes podem reduzir os custos relativos ao acompanha-

29. Caio Mário da Silva Pereira afirma: "define-se como unilateral o contrato que cria obrigações para um só dos contratantes" (PEREIRA, Caio Mário da Silva. Instituições de direito civil – V. III: Contratos, declaração unilateral de vontade e responsabilidade civil. 20. ed. rev. e atual. Rio de Janeiro: Forense, 2016, p. 59).

30. COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 283.

31. CIEPLAK, Jenny; e LEEFATT, Simon. Op. cit., p. 423. Tradução livre: Um oráculo é um terceiro provedor de serviços de informação que irá "assinar" digitalmente uma transação, atestando a ocorrência de condições específicas.

mento e ao adimplemento do contrato, pois há certa garantia de que as obrigações automatizadas serão cumpridas, e as partes não precisarão despender tempo e dinheiro com métodos voltados para a supervisão do negócio, pois os oráculos poderão exercer essa função.

Ademais, com tal tecnologia reduz-se consideravelmente a necessidade de investimento de confiança de uma parte na outra. Como a execução é automatizada, as partes não precisam mais confiar uma na outra para dar cumprimento às obrigações contratuais – ao menos dentro de condições previstas e desde que atendidas as circunstâncias presentes no software. Situação que decorre dessa questão é a geração de eficiência no adimplemento contratual, onde se evitam custos com processos judiciais ou outros meios de resolução de conflitos para casos de inadimplemento, uma vez que o incumprimento é improvável na presença de um contrato inteligente. Igualmente não se faz necessário buscar as Cortes em caso de impossibilidade de prestação ou outro fator para o qual uma resposta do software possa ser programada.

Por fim, outro benefício decorrente dos smart contracts é justamente a precisão da linguagem de computador, que dificilmente admite interpretações ambíguas como a linguagem humana, impedindo conflitos originados da maneira como as ideias foram formuladas[32].

Os smart contracts não trazem, porém, somente benefícios. É preciso lembrar da crítica feita linhas acima acerca da impossibilidade de utilizar essa tecnologia para automatizar obrigações que envolvem conceitos jurídicos indeterminados ou mesmo cláusulas gerais. Outro problema é a questão da capacidade de compreensão do indivíduo acerca da linguagem de código, pois não é possível afirmar que um cidadão sem conhecimentos técnicos específicos tenha condições de ler, compreender e interpretar um código de computador, se a tradução do referido código não estiver disponível para ele[33].

Além dessas questões, muitas outras referentes ao preenchimento de requisitos para a validade jurídica dos smart contracts são objeto de questionamento e análise[34]. Mas, uma das mais alarmantes questões é a falta de flexibi-

32. Nesse sentido, cf.: RASKIN, Max. Op. cit., p. 324-325; CANTALI, Rodrigo Ustárroz. Op. cit., p. 1549.

33. FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 123.

34. A título de exemplo, pode-se mencionar a dúvida sobre a validade da forma adotada para o contrato (códigos de computador) e a dificuldade de aferir se houve efetivo consentimento em determinados contextos. Apesar de serem diversas as questões abordadas em doutrina acerca da validade dos contratos inteligentes, não nos deteremos nelas, especialmente por não envolverem o objeto do presente trabalho. Por isso, para maiores aprofundamentos, confira-se: FINOCCHIARO, Giusella;

lidade de tais softwares para tratar do desequilíbrio superveniente da relação ou de causas ulteriores que venham a extinguir o vínculo contratual.

Se é certo que as partes podem prever antecipadamente respostas para eventuais fatos supervenientes, como uma causa de impossibilidade de cumprimento da obrigação ou mesmo uma causa ensejadora de onerosidade excessiva, também é verdadeiro afirmar que as partes não têm como prever toda e qualquer possível situação futura que venha a afetar o equilíbrio da relação[35]. A capacidade preditiva do ser humano é considerável, mas não é perfeita, o indivíduo age de acordo com uma racionalidade limitada[36], seja pela falta de informações suficientes (assimetria informacional), seja por outras razões.

A inflexibilidade dos smart contracts, aliada à blockchain – solução tecnológica muitas vezes empregada em conjunto com os contratos inteligentes –, dificulta a atuação dos tradicionais recursos utilizados pelo direito, como decisões judiciais, bem como os demais meios adequados de resolução de disputas. Isso porque a inflexibilidade dos smart contracts e a imutabilidade da rede blockchain tornam impraticáveis as soluções entendidas como mais adequadas sob a ótica desses outros meios. Nesse sentido, por exemplo, os smart contracts, na blockchain, não poderiam ter sua execução interrompida ou revertida por uma ordem judicial, mesmo que o Poder Judiciário reconheça uma hipótese de aplicação de resolução por onerosidade excessiva (art. 478, CC), caso a mesma não tenha sido prevista pelas partes e incluída no código do contrato inteligente.

2. Blockchain e suas contribuições para os smart contracts

Blockchain pode ser definida como uma tecnologia que permite o registro e compartilhamento de dados de maneira descentralizada[37] e segura, a par-

---

e BOMPREZZI, Chantal. Op. cit., p. 115-135; CANTALI, Rodrigo Ustárroz. Op. cit., p. 1542-1548.

35. CANTALI, Rodrigo Ustárroz. Op. cit., p. 1550.

36. Nesse sentido, Jeremy Sklaroff afirma que pode ser impossível para as partes definir inteira e precisamente todas as futuras situações e eventos que poderão afetar a relação contratual (SKLAROFF, Jeremy M. Op. cit., p. 277 e 280). Sobre a noção de racionalidade limitada, confira-se: AZEVEDO, Miguel Gomes de. Op. cit., p. 27; FORGIONI, Paula. Op. cit., p. 150-153.

37. COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 277. Nesse sentido, Fredie Didier Jr. e Rafael Alexandria afirmam que "[b]lockchain é uma base de dados distribuída" (DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. O uso da tecnologia blockchain para arquivamento de documentos eletrônicos, particulares ou públicos, e negócios probatórios segundo a Lei de Liberdade Econômica e seu regulamento. In ROQUE, Andre Vasconcelos; e OLIVA, Milena Donato (Coord.). Direito na era digital: aspectos negociais, processuais e registrais. São Paulo: JusPodivm, p. 189-212, 2022, p. 200).

tir da utilização de meios de verificação e execução de transações[38]. A blockchain se configura como uma espécie de Distributed Ledger Technology (DLT)[39] e foi utilizada inicialmente com o intuito de servir como rede de suporte para a criptomoeda bitcoin, inventada por uma pessoa ou grupo de pessoas autodenominadas Satoshi Nakamoto[40]. No entanto, hoje, o uso da blockchain ultrapassa o registro de transações com bitcoin. Empresas como a Ethereum passaram a utilizar a tecnologia para diferentes funções, como o registro de smart contracts[41].

As transações na blockchain (e.g., uma transferência de bitcoins, um upload de arquivo ou a execução de uma função de smart contracts) são transmitidas para uma rede de computadores, também chamados "nós"[42]. Nessa rede, existe a necessidade de validação de cada transação, o que é pode ser feito através da adoção de diversos métodos de validação[43], sendo a prova de trabalho – proof of work (POW) – o mais conhecido, em razão de ser adotado pela rede que sustenta as transações de Bitcoins. No modelo de PoW, os "mineradores", ao resolverem problemas matemáticos que demandam substancial poder de computação, validam a transação realizada pelos usuários da

38. CANTALI, Rodrigo Ustárroz. Op. cit., p. 1537.

39. VERÍSSIMO, Levi Borges de Oliveira. Repercussões concorrenciais das Distributed Ledger Technologies (DLTS). In FRAZÃO, Ana; e CARVALHO, Angelo Gamba Prata de (Coord.). Empresa, mercado e tecnologia. Belo Horizonte: Fórum, p. 255-267, 2019, p. 255. No mesmo sentido: CHAVES, Iara. Blockchain e criptomoedas. Curitiba: InterSaberes, 2021, p. 146.

40. NAKAMOTO, Satoshi. Bitcoin: a peer-to-peer electronic cash system. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 26.12.2022. Afirmam que o Bitcoin foi criado por Satoshi Nakamoto, além de ressaltarem a importância do desenvolvimento da blockchain nessa criação: KOLBER, Adam J. Not-so-smart blockchain contracts and artificial responsibility. Stanford Technology Law Review, Vol. 21, Issue 2, p. 198-234, September 2018. Disponível em: <https://law.stanford.edu/wp-content/uploads/2018/09/Kolber_LL_20180910.pdf>. Acesso em: 28.11.2022, p. 206; O'SHIELDS, Reggie. Op. cit., p. 179-180; FANDL, Kevin J. Op. cit., p. 345.

41. Tecnicamente, a blockchain pode ser utilizada para cumprir outras funções, como registro de documentos de empresas, registros de transações envolvendo imóveis, entre outras. Nesse sentido, William Mougayar arrola e desenvolve brevemente diversos usos e funções dessa tecnologia, entre as quais menciona: a atuação como infraestrutura de moedas digitais, como infraestrutura computacional, como plataforma de transações, como banco de dados descentralizados, como registro contábil distribuído, como plataforma de desenvolvimento de softwares e aplicações, entre outras (MOUGAYAR, William. Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books, 2017, p. 18-24).

42. KOLBER, Adam J. Op. cit., p. 206.

43. Além da prova de trabalho (proof of work ou PoW) mencionada no presente trabalho, a literatura especializada também indica como métodos de validação usados por redes blockchain a prova de participação (proof of stake ou PoS), a prova de participação delegada (delegated proof of stake ou DPoS) e a prova de importância (proof of importance ou PoI), todas com formas de funcionamento distinto da prova de trabalho, e não dependentes do poder de computação para resolução de um desafio matemático por tentativa e erro. Nesse sentido, confira-se: LYRA, João Guilherme. Blockchain e organizações descentralizadas: conheça a tecnologia por trás do bitcoin. Rio de Janeiro: Brasport, 2019, p. 16-18.

rede[44], em troca de uma recompensa – normalmente criptomoedas –[45], o que funciona como estímulo ao processo de validação adequada. Nesse método, a resolução do quebra-cabeças matemático é um processo computacionalmente caro[46], o que desestimula o cometimento de fraudes, a validação incorreta ou outros abusos dos validadores[47].

A validação é realizada de acordo com a verificação das características da transação e da identidade digital dos usuários que participaram da mesma[48]. Essa verificação é possível porque os usuários da blockchain são detentores de carteiras (wallets) que contêm uma chave pública e uma chave privada para assinatura das transações[49]. A existência de tais chaves para assinar as transações possibilita o uso da criptografia assimétrica, que permite identificar as identidades digitais das partes e a autenticidade das informações e da operação, atribuindo maior segurança à rede e às operações[50]. Se pela resolução do problema matemático for encontrada uma combinação de chaves que corresponda às chaves usadas na transação, a operação é transmitida para os computadores participantes da rede[51].

Uma vez validada a operação, ela é inscrita em um novo bloco na cadeia da blockchain, um novo registro imutável, que é transmitido para todos os computadores ("nós") participantes da rede (descentralização do registro)[52]. Dessa forma, a blockchain funciona como uma espécie de Diário[53] ou Livro-

44. Segundo Orna Rabinovich-Einy e Ethan Katsh, "[o] 'hash puzzle' [solucionado pelos mineradores] serve como protocolo para garantir aos usuários que aquela transação foi analisada, sendo utilizado como 'proof of work' (POW)" (RABINOVICH-EINY, Orna; e KATSH, Ethan. Blockchain e a inevitabilidade das disputas: o papel da resolução de disputas on-line. Tradução de Felipe Delle Diatczuk. In NUNES, Dierle; WERNECK, Isadora; e LUCON, Paulo Henrique dos Santos (Org.). Direito processual e tecnologia: os impactos da virada tecnológica no âmbito mundial. São Paulo: JusPodivm, p. 613-656, 2022, p. 617).

45. COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 279; RABINOVICH-EINY, Orna; e KATSH, Ethan. Op. cit., p. 617; DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. Op. cit., p. 202-203.

46. DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. Op. cit., p. 202.

47. RABINOVICH-EINY, Orna; e KATSH, Ethan. Op. cit., p. 618; DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. Op. cit., p. 204.

48. RABINOVICH-EINY, Orna; e KATSH, Ethan. Op. cit., p. 617.

49. FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. Op. cit., p. 114; FANDL, Kevin J. Op. cit., p. 347-348.

50. Nesse sentido, Alan Cohn et. al. afirmam que "[c]ryptography is the science behind protecting and securing information, typically in an insecure environment" (COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 278).

51. O'SHIELDS, Reggie. Op. cit., p. 180.

52. KOLBER, Adam J. Op. cit., p. 206; RASKIN, Max. Op. cit., p. 308; FANDL, Kevin J. Op. cit., p. 346.

53. A comparação é feita por Fredie Didier Jr. e Rafael Alexandria de Oliveira (DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexan-

-Razão[54] compartilhado, e os blocos são como acréscimos de novas páginas a esse documento. A rede funciona à base de adições, e não de revisões de transações já validadas, ou seja, para haver uma alteração, ela será traduzida em um acréscimo de bloco indicando que houve uma mudança de determinada transação, e não na forma de uma efetiva revisão ou anulação da transação já validada e incluída[55].

Em suma, a validação da solução pela própria comunidade e a sincronização de registros nos diversos "nós" participantes da rede, previnem o registro de transações inválidas[56], garantindo segurança e confiança na rede. Nesse sentido, a confiança das partes dos negócios realizados e registrados na cadeia não é depositada uma na outra ou nas instituições jurídicas, mas na própria blockchain e na validação realizada pelos usuários[57].

A blockchain tem como uma de suas principais características a imutabilidade[58]. A imutabilidade decorre da irreversibilidade ou inviabilidade prática de revisão de blocos já adicionados[59]. Isso se dá ao fato de que, para alterar um bloco da cadeia, seria necessário alterar também todos os blocos subse-

---

dria de. Op. cit., p. 202).

54. A alusão à noção de livro-razão é comum na literatura especializada, mesmo porque o blockchain, como afirmado é uma espécie de DLT (distributed ledger technology), sendo a palavra ledger traduzida para o português como "livro-razão". Nesse sentido: CHAVES, Iara. Op. cit., p. 146; LYRA, João Guilherme. Op. cit., p. 20.

55. Nesse sentido: VALENCIA RAMÍREZ, Juan Pablo. Contratos inteligentes. Revista de Investigación en Tecnologías de la Información: RITI, Espanha, v. 7, n. 14, p. 1-10, julio/diciembre 2019, p. 3. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=7242766>. Acesso em: 26.12.2022. Em mesmo sentido, Aline Terra e Deborah Pereira Pinto dos Santos afirmam que "a interação do contrato [smart contract] com usuários na rede blockchain ou a realização de nova operação econômica permite sua alteração, mas somente para o futuro" (TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. Op. cit., p. 401-402). Isso decorre da dificuldade ou até mesmo impossibilidade prática de alterar transações já registradas.

56. COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 277-278.

57. Igor Pejic se vale da frase "confiamos no código" (ou, no inglês, "in code we trust") como um jogo de palavras com a expressão presente nas cédulas de dólar ("In God We Trust"), na medida em que identifica que a confiança, no sistema blockchain é depositada no próprio sistema e no processo de validação pelo consentimento (procedimento descentralizado), e não nas instituições centrais, como Deus, bancos centrais ou qualquer outro banco (PEJIC, Igor. Blockchain: revolução para uma nova era financeira? Tradução de UBK Publishing House. Rio de Janeiro: Ubook Editora, 2021, p. 20). No mesmo sentido, destacando que o blockchain muda o foco da confiança depositada de seres humanos e entidades centralizadas para entes descentralizados, o que inclusive funciona como medida para reduzir os custos da confiança: MOUGAYAR, William. Op. cit., p. 31-38. Ao falar sobre smart contracts na blockchain, Aline de Miranda Valverde Terra e Deborah Pereira Pinto dos Santos, citando Ana Frazão, afirmam que "há a transferência, em certa medida, da confiança entre as partes contratantes para a confiança distribuída entre todos os usuários da blockchain" (TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. Op. cit., p. 405). Para Alan Cohn et. al., a característica de abertura e distribuição da blockchain permite transações de alta confiabilidade, sem a necessidade de um intermediário (COHN, Alan; WEST, Travis; e PARKER, Chelsea. Op. cit., p. 279). No mesmo sentido: OLIVEIRA, Thiago Barcik Lucas de. Op. cit., p. 1669-1670.

58. DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. Op. cit., p. 205. Nas palavras de Igor Pejic, a irreversibilidade dos registros "garantiu ao blockchain a reputação de um 'registrador irrepreensível'" (PEJIC, Igor. Op. cit., p. 14).

59. RABINOVICH-EINY, Orna; e KATSH, Ethan. Op. cit., p. 623.

quentes a ele, já que estes mantêm os registros dos blocos que os precedem[60]. Esse fator gera confiança e segurança nas transações a partir do próprio processo de funcionamento da blockchain.

No entanto, essa característica apresenta um inconveniente que pode agravar pontos negativos dos smart contracts. A imutabilidade da blockchain, aliada à inflexibilidade dos smart contracts pode acarretar prejuízos para as partes contratantes, na medida em que fiquem impedidas de recorrer a outra medida que entendam mais adequada para lidar com eventual adversidade surgida após a celebração do negócio (e.g., uma renegociação)[61].

Essas características de ambas as tecnologias dificultam o cumprimento de ordens judiciais e a própria gestão de riscos contratuais pelas partes a posteriori – apesar de sua função se voltar justamente para administrar os riscos da relação contratual em um exercício de previdência das partes.

3. Contrato e risco: delineando o problema

O problema do risco está hoje especialmente presente em todas as sociedades[62]. O risco envolve a noção de incerteza, uma incerteza quanto a prejuízos futuros (projeção futura)[63] ou quanto a situação já verificada, porém desconhecida pelo indivíduo[64].

Sempre existiu uma relação entre o risco e o contrato. Como se viu, os contratos são instrumentos voltados a mitigar riscos e atribuir segurança às relações[65]. Mas não se pode descurar que "[c]ontratar é, em si, uma potencial

60. DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. Op. cit., p. 204.

61. Nesse sentido, é preciso notar que a tecnologia também produz riscos e que a noção de risco se relaciona com a noção de tempo, ideia bem sintetizada por Rafaela Viola ao afirmar que "o desenvolvimento tecnológico projeta riscos (conhecidos e desconhecidos) para o futuro" (VIOLA, Rafael. Risco e causalidade. Indaiatuba: Editora Foco, 2023, p. 31)

62. Nesse sentido, confira-se: BECK, Ulrich. Risk Society: towards a new modernity. London: Sage Publications, 1992. Para maiores aprofundamentos sobre o risco no âmbito jurídico, confira-se: VIOLA, Rafael. Risco e causalidade. Indaiatuba: Editora Foco, 2023).

63. BECK, Ulrich. Op. cit., p. 33-34.

64. BANDEIRA, Paula Greco. Contratos aleatórios no direito brasileiro. Rio de Janeiro: Renovar, 2010, p. 7.

65. O ato de contratar envolve tomar algum conhecimento sobre o risco envolvido na prestação e consentir quanto a uma solução para tratar este risco, e "quanto maior o conhecimento e o consenso sobre determinado risco, mais simples será a solução com a consequente redução dos riscos" (VIOLA, Rafael. Op. cit., p. 66). Inclusive, o próprio conceito de risco contratual relaciona-se diretamente com a noção de equilíbrio da relação contratual, na medida em que as partes estabelecem a repartição de riscos, no âmbito do contrato, como forma de definir o equilíbrio do ajuste (TERRA, Aline de Miranda Valverde; e BANDEIRA, Paula Greco. A cláusula resolutiva expressa e o contrato incompleto como instrumentos de gestão de risco nos contratos. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 6, n. 4, p. 9-25, out./dez. 2015, p. 11. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/80/183>. Acesso em: 27.04.2023).

situação de risco".[66]

Os mais diversos tipos de problemas podem recair sobre uma relação obrigacional: inadimplemento, desequilíbrio ou impossibilidade do objeto da prestação, entre outros. Por isso, são apostas, nos contratos, cláusulas voltadas a lidar com tais riscos, disposições relativas à gestão de riscos contratuais. A gestão de riscos pode ser positiva, quando as partes preveem de antemão a maneira de distribuição de determinado risco específico, ou negativa, quando as partes não preveem antecipadamente uma solução ou forma de distribuição do risco, deixando lacuna contratual proposital a ser preenchida posteriormente[67]. Assim, usam-se técnicas eminentemente jurídicas, como as cláusulas resolutivas expressas, as cláusulas de hardship e a técnica de incompletude contratual (inclusão de cláusulas "abertas" ou "lacunosas")[68] para prever problemas futuros e desenhar soluções ou orientações a serem seguidas pelas partes[69].

Uma das principais cláusulas direcionadas para o tratamento de riscos é a cláusula resolutiva expressa. O instituto, previsto e regulado nos arts. 474 e 475 do Código Civil, é instrumento jurídico que "permite que o credor, diante da verificação do evento nela contemplado, opte entre exigir a execução do contrato pelo equivalente ou resolvê-lo extrajudicialmente, desvinculando-se de relação jurídica incapaz de promover sua função econômico-individual"[70]. A cláusula possibilita a atuação extrajudicial[71] do credor de determinada obrigação no desfazimento do vínculo, em verdadeiro exercício de autotutela[72], o que não difere muito da execução automática de funções previstas nos smart

66. MAYER FEITOSA, M. L. P. de A. Op. cit., p. 63. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/4507. Acesso em: 14.12.2022.

67. TERRA, Aline de Miranda Valverde; e BANDEIRA, Paula Greco. Op. cit., p. 13-14.

68. Sobre cláusulas de hardship e incompletude contratual, cf.: MARTINS-COSTA, Judith. A cláusula de hardship e a obrigação de renegociar nos contratos de linga duração. Revista de Arbitragem e Mediação, Ano 7, n. 25, p. 11-39, São Paulo: Editora Revista dos Tribunais, abr./jun. 2010. Para maiores aprofundamentos sobre incompletude contratual, cf. BANDEIRA, Paula Greco. Contrato incompleto. São Paulo: Atlas, 2015.

69. TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Op. cit., p. 380-382.

70. TERRA, Aline de Miranda Valverde. Cláusula resolutiva expressa. 1. ed. 1. reimpressão. Belo Horizonte: Fórum, 2017, p. 36. No mesmo sentido: TEPEDINO, Gustavo; BARBOZA, Heloísa Helena; e MORAES, Maria Celina Bodin de. Código civil interpretado conforme a Constituição da República. Rio de Janeiro: Renovar, 2012, p. 118.

71. FERNANDES, Micaela Barros Barcelos. Distinção entre a condição resolutiva e a cláusula resolutiva expressa: repercussões na falência e na recuperação judicial. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 20, p. 183-207, abr./jun. 2019, p. 191. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/417/298>. Acesso em: 19.12.2022.

72. TERRA, Aline de Miranda Valverde. Op. cit., p. 55-56.

contracts, salvo pelo automatismo destes últimos.

A mencionada cláusula, que encontra seu fundamento na autonomia privada[73], visa a lidar com o surgimento do inadimplemento, mas não apenas, na medida em que autoriza a redistribuição, entre as partes, de riscos decorrentes de eventos supervenientes ou de fatos que já estão previamente regulados pelo legislador, mas que admitem conformação pela autonomia privada, ou seja, eventos que seriam ordinariamente abarcados pela teoria do risco[74].

A título de exemplo, mencione-se sua utilização para definir quem suportará os custos da impossibilidade ocasionada por fortuito ou para possibilitar a resolução do contrato em razão da constatação de vício redibitório, afastando-se as soluções tipicamente previstas pelo legislador: ação redibitória ou abatimento do preço[75]. Nesse sentido, a cláusula resolutiva expressa tem utilidade mais ampla do que apenas resolver o vínculo diante de inadimplemento, apresentando-se como instrumento maleável na gestão de riscos.

Além dos problemas que decorrem da operação econômica, é preciso notar que a partir do próprio contrato podem surgir riscos[76], como os danos decorrentes de uma não intervenção do Poder Público, facilitando o exercício de poder de uma parte mais forte sobre uma parte mais débil, ou prejuízos advindos de uma intervenção excessiva do Estado sobre o contrato[77].

No cenário contratual repleto de adversidades, os smart contracts surgem como mais uma solução a um problema de controle dos riscos, ao lado dos institutos jurídicos já mencionados (cláusulas contratuais voltadas a tratar de riscos). As diferenças entre uns e outros somente se evidenciam nas suas formas de atuação e na origem dos smart contracts (tecnologia, e não direito).

73. Ibid., p. 47.

74. Ibid., p. 86.

75. Sobre essas hipóteses de utilização da cláusula resolutiva expressa, confira-se: TERRA, Aline de Miranda Valverde; e BANDEIRA, Paula Greco. Op. cit., p. 14-21; TERRA, Aline de Miranda Valverde; e NANNI, Giovanni Ettore. A cláusula resolutiva expressa como instrumento privilegiado de gestão de riscos contratuais. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 31, n. 1, p. 135-165, jan./mar. 2022, p. 141-156. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/837/518>. Acesso em: 27.04.2023.

76. Nesse sentido, Aline Terra e Giovanni Ettore Nanni afirmam que “a relação entre contrato e risco é ambivalente: de um lado, o contrato, consentindo à autonomia privada regular os interesses no tempo, é considerado um dos instrumentos mais consonantes à gestão dos riscos; de outro, próprio à estipulação contratual, vinculando as partes a determinado arranjo de interesses, as expõe a novos riscos, suscitados de eventos que não foram exatamente regulados e que incidem, às vezes de maneira determinante, na atuação do programa negocial ou, ao menos, nas expectativas de cada um dos contraentes” (TERRA, Aline de Miranda Valverde; NANNI, Giovanni Ettore. Op. cit., p. 139).

77. MAYER FEITOSA, M. L. P. de A. Op. cit., p. 76.

Em razão de ambos serem institutos voltados a lidar com incertezas nas relações, as cláusulas resolutivas expressas e os smart contracts poderiam, em tese, vir a ser inseridos em uma mesma avença. Por isso, é preciso compreender como se daria essa relação entre os instrumentos e se ela seria legítima e juridicamente viável.

4. A cláusula resolutiva expressa nos smart contracts: tentativas de compatibilização

A cláusula resolutiva expressa, como se disse, permite ao credor de uma obrigação, diante do inadimplemento, optar entre resolver o vínculo obrigacional ou exigir o cumprimento pelo equivalente[78], havendo, em ambos os casos, a possibilidade de se pleitear perdas e danos[79]. Ademais, ainda possibilita a redistribuição de riscos decorrentes da aplicação da teoria do risco no direito dos contratos, autorizando o delineamento de solução diversa daquela prevista originariamente pelo legislador.

Por sua vez, os smart contracts permitem a execução automática de funções ou medidas previamente definidas, diante da ocorrência de um evento igualmente previsto pelas partes.

Ante tais considerações, um primeiro questionamento que surge é se a automação dos contratos inteligentes poderia ser empregada para executar uma cláusula resolutiva expressa. A princípio poderia parecer óbvia uma resposta afirmativa. No entanto, é necessário levar em conta algumas características da cláusula resolutiva.

A referida cláusula opera de pleno direito, produz efeitos sem a necessidade de determinação judicial[80]. Contudo, para a produção de efeitos, é preciso que o credor da obrigação informe ao devedor acerca de sua escolha[81] pela re-

78. A distinção entre ambos os casos, resolução e cumprimento pelo equivalente, reside no fato de que, enquanto o primeiro extingue a relação obrigacional, transformando-a em relação de liquidação; o segundo mantém a relação original, que deixa de perseguir o programa contratual originalmente pactuado, ou seja, o cumprimento pelo equivalente, na medida em que mantém a relação, altera o objeto da prestação, que deixa de ser o orginalmente pactuado e passa a ser o pagamento de seu valor em dinheiro (prestação genérica). Por esse motivo, a opção do credor por uma ou outra hipótese acarretará para o mesmo efeitos diversos. Nesse sentido, confira-se: TERRA, Aline. Execução pelo equivalente como alternativa à resolução: repercussões sobre a responsabilidade civil. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 18, p. 49-73, out./dez. 2018. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/305/246>. Acesso em: 28.04.2023.

79. TERRA, Aline de Miranda Valverde. Op. cit., p. 73; FERNANDES, Micaela Barros Barcelos, Op. cit., p. 198.

80. TERRA, Aliena de Miranda Valverde; NANNI, Giovanni Ettore. Op. cit., p. 157.

81. Aline Terra e Giovanni Ettore Nanni aduzem que "[o]perar de pleno direito não significa que a relação contratual é mecanicamente extinta, independentemente de qualquer outra providência. Na realidade, representa, a partir da consumação de

solução ou pelo cumprimento pelo equivalente, ou mesmo se deseja dar continuidade ao contrato, tratando o caso como se fosse hipótese de mora – quando não será possível optar pelo caminho da resolução[82] –, e não inadimplemento absoluto[83]. A cláusula resolutiva expressa, uma vez verificada sua hipótese de incidência, faz surgir para o credor o direito potestativo (formativo extintivo) de resolver o vínculo, mas para exercer tal direito o credor precisa emitir uma declaração receptícia de vontade[84]. Existe, então, uma atuação humana por parte do credor, a fim de definir o caminho a ser seguido: resolução ou manutenção do vínculo.

Em um contrato de transporte de cargas, por exemplo, de uma empresa A, fornecedora de determinada matéria prima, para uma empresa B, que produz bens a partir daquela matéria prima, as partes podem incluir no contrato de transporte a previsão de cláusula resolutiva expressa, em caso de a empresa A não realizar a entrega a tempo ou realizar a entrega apenas de parte da matéria adquirida pela empresa B, em situação na qual a empresa B teria que observar determinado prazo de produção (seja por que a produção foi encomendada pelo comprador para data definida ou por razões de mercado). O inadimplemento da obrigação por A, que em abstrato pareceria apenas relativo (mora), tornar-se-ia absoluto e ensejaria para B a possibilidade de resolver o

---

seu suporte fático, isto é, do inadimplemento do que arrolado na cláusula resolutiva, que à parte inocente é conferido o direito potestativo de decidir, segundo seu interesse, se aciona ou não o dispositivo em epígrafe. A resolução do liame contratual não se perpetra automaticamente. Depende de ser colocada em funcionamento, por ato do credor, que deve manifestar ao devedor a decisão" (TERRA, Aliena de Miranda Valverde; NANNI, Giovanni Ettore. Op. cit., p. 157).

82. TERRA, Aline de Miranda Valverde. Op. cit., p. 139. Nessa hipótese, a autora ressalta que deve haver interesse e utilidade no cumprimento da prestação, a qual também não pode ter sido tornada impossível. Na hipótese de mora não se resolve a prestação, "persiste ao devedor a possibilidade de realizar a prestação, desde que indenize os danos a que a mora deu causa" (CAVALLI, Cássio. Mora e utilidade: os standards da utilidade no modelo jurídico da mora do devedor. Rio de Janeiro: Editora FGV, 2011, p. 34 – grifos nossos).

83. Essa terceira hipótese, por óbvio, só será possível se ainda resistir algum interesse do credor na prestação e o cumprimento da mesma não tiver sido impossibilitado para o devedor, o que impede qualquer forma de resolução do contrato (por cláusula resolutiva expressa ou tácita). Nesse sentido: BICHARA, Maria Carolina. O interesse do credor na prestação como critério de distinção entre as hipóteses de execução específica e execução pelo equivalente pecuniário. In TERRA, Aline de Miranda Valverde; e GUEDES, Gisela Sampaio da Cruz. Inexecução das obrigações: pressupostos, evolução e remédios – Vol. I. Rio de Janeiro: Editora Processo, p. 29-50, 2020; AGUIAR JÚNIOR, Ruy Rosado de. A extinção dos contratos por incumprimento do devedor: resolução. 2. ed. rev. e atual. Rio de Janeiro: AIDE Editora, 2003, p. 93-143. Giovanni Ettore Nanni, por sua vez, entende que os critérios para configuração do inadimplemento são a perda de interesse da prestação para o credor e a definitividade do incumprimento, e repudia o critério da impossibilidade da prestação: NANNI, Giovanni Ettore. Inadimplemento absoluto e resolução contratual: requisitos e efeitos. São Paulo: Thomson Reuters Brasil, 2021, p. 91-103.

84. SALLES, Raquel Bellini de Oliveira. A autotutela pelo inadimplemento nas relações contratuais. 2011. Tese (Doutorado) – Universidade do Estado do Rio de Janeiro, Faculdade de Direito, Rio de Janeiro, 2011, p. 189-190. Disponível em: <https://www.bdtd.uerj.br:8443/handle/1/9225>. Acesso em: 20.12.2022. No mesmo sentido, Ruy Rosado de Aguiar Júnior ressalta o caráter de voluntariedade do ato de resolução (seja resolução legal ou convencional – cláusula resolutiva expressa): AGUIAR JÚNIOR, Ruy Rosado de. Op. cit., p. 32.

contrato[85]. No entanto, a empresa B, a depender das circunstâncias da relação contratual concreta, poderia ainda vislumbrar alguma utilidade na cobrança de cumprimento pelo equivalente ou na continuidade da cobrança de cumprimento da obrigação por A, com a entrega do restante dos materiais em momento posterior (e.g., aumento do prazo de B para a entrega do produto final). Nesse caso, o contrato não seria simplesmente resolvido por aplicação automática da cláusula resolutiva expressa através da atuação do smart contract. Ao contrário, deveria ser aberta a B a oportunidade para, diante dos elementos presentes na relação contratual concreta e na finalidade econômico-individual do contrato, escolher entre resolver o contrato, exigir o cumprimento pelo equivalente ou mesmo dar continuidade ao contrato exigindo a entrega do restante do material, tratando a hipótese como caso de mora.

Se o smart contract atuar de forma a, diante do inadimplemento, não apenas impedir o cumprimento da contraprestação, mas restituir às partes os valores e bens que prestaram e se encontravam custodiados em registros digitais (e.g., contratos de compra de títulos)[86], haveria a operacionalização de uma resolução cujo procedimento violaria a disciplina da cláusula resolutiva expressa, em razão da falta de oportunidade ao credor de escolher entre resolução, cumprimento pelo equivalente ou cumprimento da obrigação principal com incidência dos efeitos da mora.

Apesar de parecer contraintuitivo, porém, nessa última hipótese aventada não se deve considerar de pronto inválida a cláusula resolutiva expressa automatizada, mesmo porque ela apenas está a ser executada de acordo com a própria forma de gestão de riscos escolhida previamente pelas partes. Para que seja possível ao credor, ou mesmo ao devedor, questionar a validade ou a legitimidade da cláusula em juízo de merecimento de tutela, é preciso que se analise as circunstâncias do caso concreto, onde haverá de se verificar que o descumprimento não foi tão gravoso a ponto de ensejar a aplicação da cláusula (ex.: entrega parcial que constitui adimplemento substancial)[87] ou que o

85. Estar-se-ia diante de caso de termo essencial, que uma vez inobservado enseja inadimplemento absoluto. Veja-se: NANNI, Giovanni Ettore. Op. cit., p. 95. Sobre a essencialidade do tempo no cumprimento da prestação: CAVALLI, Cássio. Op. cit., p. 118-119.

86. Trata-se do efeito restitutório da resolução. Sobre o tal efeito: AGUIAR JÚNIOR, Ruy Rosado de. Op. cit., p. 259-265; TERRA, Aline de Miranda Valverde. Op. cit., p. 183-200.

87. Um inadimplemento mínimo, a possibilidade de cumprimento pelo devedor, bem como a existência de interesse do credor em receber a prestação, ensejam a configuração de mora, a qual, assim como a ocorrência de adimplemento substancial, torna o exercício do direito potestativo de resolução abusivo. Veja-se: AGUIAR JÚNIOR, Ruy Rosado de. Op. cit., p. 59; ASSIS, Araken de. Resolução do contrato por inadimplemento. 6. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019, p.

exercício do direito potestativo à resolução não ataca a boa-fé nem seu próprio fim econômico social[88]. Em tal situação, entende-se pela possibilidade de invalidar ou tornar ineficaz a cláusula em juízo de merecimento de tutela, mas em razão da automatização pelo smart contract a solução ao problema – se tecnicamente possível – seria dada a posteriori, com a reversão dos efeitos da resolução já verificada.

Diante dos riscos de uma aplicação automática de cláusula resolutiva expressa, a solução mais adequada consistiria no software inteligente, no momento da ocorrência do suporte fático da cláusula, deixar de automatizar o contrato, para permitir ao credor a escolha entre resolver a obrigação e pedir o cumprimento pelo equivalente. Nesse caso, o software deve automatizar o envio da decisão ao devedor, após a escolha do credor, bem como a aplicação da solução definida pelo credor, após a notificação.

Outra questão relevante na aplicação da cláusula resolutiva expressa é a consideração da importância da cláusula na concreta economia contratual. Se é certo que a aposição de cláusula resolutiva expressa pelas partes em determinado contrato faz presumir a relevância da obrigação cujo inadimplemento permitiria sua aplicação[89], também é verdade que o credor não pode utilizá-la de maneira abusiva para justificar a resolução contratual pelo descumprimento de qualquer obrigação a ela relacionada, vez que a obrigação que enseja a aplicação de cláusula resolutiva deve ser essencial na realização da função econômico-individual do negócio[90]. Nesse sentido, e especialmente diante da racionalidade limitada das partes na confecção do contrato e da cláusula[91], tanto se poderá atribuir concretamente, em momento futuro, relevância a obrigações acessórias[92], quanto se pode afastá-la de obrigações consideradas, em abstrato, essenciais, diante de alteração nas circunstâncias fáticas da relação[93].

93; SALLES, Raquel Bellini de Oliveira. Op. cit., p. 220-221.

88. TERRA, Aline de Miranda Valverde. Op. cit., p. 159-161.

89. CAVALLI, Cássio. Op. cit., p. 107.

90. TERRA, Aline de Miranda Valverde. Op. cit., p. 75.

91. CAVALLI, Cássio. Op. cit., p. 108-112.

92. TERRA, Aline de Miranda Valverde. Op. cit., p. 76.

93. Ibid., p. 79-80.

Diante de tais considerações, e do fato de, como já se viu, ser a aplicação dos smart contracts em combinação com a blockchain inflexível e imutável, se faz ainda mais necessário considerar como solução a abertura de oportunidade ao credor para tomar sua decisão antes do prosseguimento automático de efeitos da resolução.

Uma última reflexão que se coloca a respeito da relação entre os institutos é a capacidade de o contrato inteligente retirar a eficiência da aplicação da cláusula resolutiva expressa em determinadas circunstâncias. Explica-se: imagine-se um contrato de permuta de non-fungible tokens (NFTs) com automação inteligente que prevê que, desde que C transfira seu ativo para D (prestação principal de C), será realizada uma transferência automática do ativo de D para C (contraprestação de D). Imagine-se também que, no contrato que rege essa relação, consta cláusula resolutiva expressa prevendo que caso C deixe de entregar, em conjunto com o bem, determinada documentação relativa ao mesmo, D poderá resolver o contrato. Na data da transação, C entrega somente o bem, sem a documentação que o acompanha. Nesse caso, a transferência do ativo de D para C será automática, não dando tempo a D para que faça a escolha entre aplicar a cláusula resolutiva para resolver o contrato ou buscar a execução pelo equivalente antes da execução da prestação automatizada.

Nesse caso, o smart contract impossibilitaria o exercício do direito de resolução por D antes do cumprimento de sua respectiva obrigação. Esse cenário gera ineficiência na aplicação da cláusula resolutiva, eis que a resolução consiste não só em não cumprir a contraprestação – quando o beneficiário da resolução vier a prestar depois –, como também em buscar o retorno ao status quo ante. Nesse caso, é como se fosse instituída uma cláusula solve et repete pela automatização do cumprimento da obrigação principal[94], impondo ao credor a busca pela resolução a posteriori, através da restituição de sua prestação, o que poderia inclusive ser tecnicamente impossível, em razão das já mencionadas características de inflexibilidade e imutabilidade dos smart contracts e da rede blockchain.

Considerações finais

94. Abordando o tema da aproximação do smart contract à natureza da cláusula solve et repete, em nota de rodapé, onde citam entendimento de Daniela Di Sabato: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Op. cit., p. 392.

No presente trabalho, buscou-se analisar se seria possível e como ocorreria eventual interação entre um instituto eminentemente tecnológico, os smart contracts, e um instituto de natureza jurídica, a cláusula resolutiva expressa, considerando a função comum de ambos de gerir os riscos contratuais.

Para tanto, analisou-se os smart contracts e sua maneira de funcionamento, baseada em um formato de encadeamento lógico a partir da aplicação da sentença "se X, então Y", onde X é o evento que, uma vez ocorrido, enseja a ativação do elemento de automação do contrato para alcançar o resultado Y. A partir dessa forma de funcionamento foram extraídas as principais características dos contratos inteligentes (automação e inflexibilidade), bem como alguns benefícios e prejuízos decorrentes de sua utilização. Foi igualmente trabalhada a relação entre os smart contracts e a blockchain, cadeia de registros de transações caracterizada, entre outras coisas, pela imutabilidade de seus registros, elemento que pode tornar ainda mais difícil a revisão de uma decisão automatizada com base no funcionamento de um smart contract.

Em seguida, passou-se a um breve exame da relação entre o contrato enquanto instituto e os riscos, sob as perspectivas jurídica e econômica. A partir disso, viu-se que os contratos são instrumentos para a redução de riscos, mas que eles próprios podem trazer consigo certos riscos, como aqueles que decorrem do desenho das relações reguladas ou da excessiva ingerência do Estado sobre a ferramenta de regulação de interesses. Além disso, viu-se como instrumentos como a cláusula resolutiva expressa são usados na gestão das relações e dos riscos contratuais.

Enfim, chegou-se à análise da interação entre contratos inteligentes e cláusula resolutiva expressa, donde se concluiu que os contratos inteligentes podem ser utilizados para automatizar o funcionamento de tais cláusulas, porém devem respeitar os limites impostos pelo ordenamento à atuação da cláusula resolutiva expressa, como o exercício abusivo do direito potestativo de resolução ou a ausência de preenchimento de suporte fático para a atuação da cláusula – hipótese em que não há inadimplemento, pois resiste interesse do credor na prestação, utilidade da mesma e possibilidade de cumprimento para o devedor.

Assim, a primeira sugestão que se faz é que o contrato inteligente não automatize a aplicação da cláusula resolutiva, mas, em vez disso, ao verificar a ocorrência do evento que enseja para o credor a faculdade de escolha entre resolver o contrato ou exigir o cumprimento da obrigação pelo equivalente, cesse sua atuação e notifique o credor para que efetue sua escolha, e somen-

te após isso, retome sua automação na execução da cláusula, caso essa tenha sido a opção do credor.

Por fim, ressaltou-se o risco de o contrato inteligente vir a afetar o funcionamento da cláusula resolutiva expressa de maneira a impedir sua aplicação eficiente, visto que a automação do cumprimento da obrigação principal não permitiria que o credor optasse por resolver o contrato antes de cumprir sua própria prestação, criando situação similar à cláusula solve et repete.

Fato é que os contratos inteligentes podem servir para operacionalizar a disposição de uma cláusula resolutiva expressa. No entanto, devem ser sempre observadas as peculiaridades de cada caso, em especial o sensível equilíbrio econômico do contrato, levando em consideração situações que deslegitimariam a aplicação do software inteligente, como a configuração de adimplemento substancial ou mora, em lugar de inadimplemento absoluto; a perda de relevância da obrigação para fins de aplicação da cláusula resolutiva; ou mesmo a configuração de hipótese de resolução por descumprimento de obrigação secundária ou acessória que o software venha a deixar de levar em consideração.

Referências

AGUIAR JÚNIOR, Ruy Rosado de. **A extinção dos contratos por incumprimento do devedor: resolução**. 2. ed. rev. e atual. Rio de Janeiro: AIDE Editora, 2003.

ASSIS, Araken de. **Resolução do contrato por inadimplemento**. 6. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019.

AZEVEDO, Miguel Gomes. **A eficiência econômica dos princípios do direito contratual brasileiro**. Rio de Janeiro: Lumen Juris, 2019.

BANDEIRA, Paula Greco. **Contrato incompleto**. São Paulo: Atlas, 2015.

BANDEIRA, Paula Greco. **Contratos aleatórios no direito brasileiro**. Rio de Janeiro: Renovar, 2010.

BECK, Ulrich. ***Risk Society: towards a new modernity***. London: Sage Publications, 1992.

BICHARA, Maria Carolina. **O interesse do credor na prestação como critério de distinção entre as hipóteses de execução específica e execução pelo equivalente pecuniário**. *In* TERRA, Aline de Miranda Valverde; e GUEDES, Gisela Sampaio da Cruz. Inexecução das obrigações: pressupostos, evolução e remédios – Vol. I. Rio de Janeiro: Editora Processo, p. 29-50, 2020.

CANTALI, Rodrigo Ustárroz. ***Smart contracts* e o direito contratual: primeiras impressões sobre suas vantagens e limites**. Revista Jurídica Luso-Brasileira, Ano 8, n. 3, p. 1529-1566, 2022. Disponível em: <https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1529_1566.pdf>. Acesso em: 25.11.2022.

CAVALCANTE, Henrique Haruki Arake. **A natureza jurídica dos contratos futuros**. Revista da Procuradoria-Geral do Banco Central, Brasília: Banco Central do Brasil, vol. 3, n. 2, p. 135-172, dez. 2009. Disponível em: <https://revistapgbc.bcb.gov.br/revista/issue/view/20/Revista%20PGBC%20-%20V.3%20-%20N.2%20%282009%29>. Acesso em: 26.11.2022.

CAVALLI, Cássio. **Mora e utilidade: os *standards* da utilidade no modelo jurídico da mora do devedor**. Rio de Janeiro: Editora FGV, 2011.

CHAVES, Iara. **Blockchain e criptomoedas**. Curitiba: InterSaberes, 2021

CIEPLAK, Jenny; e LEEFATT, Simon. ***Smart contracts: a smart way to automate performance***. Georgetown Law Technology Review, Vol. 1, Issue 2, p. 417-427, April 2017. Disponível em: <https://perma.cc/EUT6-RL6P>. Acesso em: 25.11.2022.

COHN, Alan; WEST, Travis; e PARKER, Chelsea. ***Smart after all: blockchain, smart contracts, parametric insurance, and smart energy grid***. Georgetown Law Technology Review, Vol. 1, Issue 2, p. 273-304, April 2017. Disponível em: <https://perma.cc/TY7W-Q8CX>. Acesso em: 25.11.2022.

DIDIER JR., Fredie; e OLIVEIRA, Rafael Alexandria de. **O uso da tecnologia blockchain para arquivamento de documentos eletrônicos, particulares ou públicos, e negócios probatórios segundo a Lei de Liberdade Econômica e seu regulamento**. In ROQUE, Andre Vasconcelos; e OLIVA, Milena Donato (Coord.). Direito na era digital: aspectos negociais, processuais e registrais. São Paulo: JusPodivm, p. 189-212, 2022.

FANDL, Kevin J. ***Can smart contracts enhance firm efficiency in emerging markets***. Northwestern Journal of International Law and Business, Vol. 40, Issue 3, p. 333-362, Spring 2020. Disponível em: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1857&context=njilb>. Acesso em 29.11.2022.

FERNANDES, Micaela Barros Barcelos. **Distinção entre a condição resolutiva e a cláusula resolutiva expressa: repercussões na falência e na recuperação judicial**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 20, p. 183-207, abr./jun. 2019. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/417/298>. Acesso em: 19.12.2022.

FERREIRA, Kenneth Antunes. **Contrato derivativo não padronizado: a impropriedade de sua classificação como valor mobiliário**. Dissertação (Mestrado em Direito) – Mestrado em Direito Comercial, Pontifícia Universidade Católica de São Paulo, São Paulo, 147 p., 2008. Disponível em: <https://tede2.pucsp.br/bitstream/handle/8206/1/Kenneth%20Antunes%20Ferreira.pdf>. Acesso em: 26.11.2022.

FINOCCHIARO, Giusella; e BOMPREZZI, Chantal. ***A legal analysis of the use of blockchain technology for the formation of smart legal contracts***. medialaws.eu – Rivista di Diritto dei Media, Itália, Vol. 2, p. 111-135, Maggio 2020. Disponível em: <https://www.medialaws.eu/wp-content/uploads/2020/07/RDM_2_2020-Finocchiaro.pdf>. Acesso em: 25.11.2022.

FORGIONI, Paula A. **Contratos empresariais: teoria geral e aplicação**. 2. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2016.

KOLBER, Adam J. ***Not-so-smart blockchain contracts and artificial responsibility***. Stanford Technology Law Review, Vol. 21, Issue 2, p. 198-234, September 2018. Disponível em: <https://law.stanford.edu/wp-content/uploads/2018/09/Kolber_LL_20180910.pdf>. Acesso em: 28.11.2022.

LYRA, João Guilherme. **Blockchain e organizações descentralizadas: conheça a tecnologia por trás do bitcoin**. Rio de Janeiro: Brasport, 2019.

MARTINS-COSTA, Judith. **A cláusula de *hardship* e a obrigação de renegociar nos contratos de linga duração**. Revista de Arbitragem e Mediação, Ano 7, n. 25, p. 11-39, São Paulo: Editora Revista dos Tribunais, abr./jun. 2010.

MAYER FEITOSA, Maria Luiza Pereira de Alencar. **O contrato como regulador e como produtor de riscos**. Prim@ Facie, [S. l.], v. 4, n. 6, p. 62–85, 2010. Disponível em: https://periodicos.ufpb.br/index.php/primafacie/article/view/4507. Acesso em: 14.12.2022.

MOUGAYAR, William. ***Blockchain* para negócios: promessa, prática e aplicação da nova tecnologia da internet**. Rio de Janeiro: Alta Books, 2017.

NAKAMOTO, Satoshi. ***Bitcoin: a peer-to-peer electronic cash system***. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 26.12.2022.

NANNI, Giovanni Ettore. **Inadimplemento absoluto e resolução contratual: requisitos e efeitos**. São Paulo: Thomson Reuters Brasil, 2021.

OLIVEIRA, Thiago Barcik Lucas de. **A economia dos custos de transação e o novo modelo proposto pelos *smart contracts***. Revista Jurídica Luso-Brasileira, Ano 8, n. 3, p. 1651-1679, 2022. Disponível em: <https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1651_1679.pdf>. Acesso em: 27.12.2022.

O'SHIELDS, Reggie. ***Smart contracts: legal agreements for the blockchain***. North Carolina Banking Institute, Vol. 21, Issue 1, p. 177-194, March 2017. Disponível em: <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1435&context=ncbi>. Acesso em: 26.11.2022.

PEJIC, Igor. ***Blockchain*: revolução para uma nova era financeira?** Tradução de UBK Publishing House. Rio de Janeiro: Ubook Editora, 2021.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil – V. III: Contratos, declaração unilateral de vontade e responsabilidade civil**. 20. ed. rev. e atual. Rio de Janeiro: Forense, 2016.

RABINOVICH-EINY, Orna; e KATSH, Ethan. ***Blockchain* e a inevitabilidade das disputas: o papel da resolução de disputas on-line**. Tradução de Felipe Delle Diatczuk. In NUNES, Dierle; WERNECK, Isadora; e LUCON, Paulo Henrique dos Santos (Org.). Direito processual e tecnologia: os impactos da virada tecnológica no âmbito mundial. São Paulo: JusPodivm, p. 613-656, 2022.

RASKIN, Max. ***The law and the legality of smart contracts***. Georgetown Law Technology Re-

view, Vol. 1, Issue 2, p. 305-341, April 2017. Disponível em: <https://perma.cc/673G-3ANE>. Acesso em: 25.11.2022.

ROPPO, Enzo. **O contrato**. Tradução de Ana Coimbra e M. Januário C. Gomes. Coimbra: Edições Almedina S.A., 2009.

SALLES, Raquel Bellini de Oliveira. **A autotutela pelo inadimplemento nas relações contratuais**. 2011. Tese (Doutorado) – Universidade do Estado do Rio de Janeiro, Faculdade de Direito, Rio de Janeiro, 2011. Disponível em: <https://www.bdtd.uerj.br:8443/handle/1/9225>. Acesso em: 20.12.2022.

SKLAROFF, Jeremy M. ***Smart contracts and the costs of inflexibility***. University of Pennsylvania Law Review, Vol. 166, p. 263-303, 2017. Disponível: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1009&context=prize_papers>. Acesso em: 27.12.2022.

SZABO, Nick. ***The idea of smart contracts***. Nick Szabo's Papers and Concise Tutorials, 1997. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>. Acesso em: 25.11.2022.

SZTAJN, Rachel; ZYLBERSZTAJN, Decio; e AZEVEDO, Paulo Furquim de. **Economia dos contratos**. In SZTAJN, Rachel; e ZYLBERSZTAJN, Decio (Org.). Direito e economia: análise econômica do direito e das organizações. Rio de Janeiro: Elsevier, p. 107-136, 2005.

TEPEDINO, Gustavo; BARBOZA, Heloísa Helena; e MORAES, Maria Celina Bodin de. **Código civil interpretado conforme a Constituição da República**. Rio de Janeiro: Renovar, 2012.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **Inteligência artificial, smart contracts e gestão do risco contratual**. In TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. O direito civil na era da inteligência artificial. 1. ed. São Paulo: Thomson Reuters Brasil, p. 373-396, 2020.

TERRA, Aline de Miranda Valverde. **Cláusula resolutiva expressa**. 1. ed. 1. reimpressão. Belo Horizonte: Fórum, 2017.

TERRA, Aline. **Execução pelo equivalente como alternativa à resolução: repercussões sobre a responsabilidade civil**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 18, p. 49-73, out./dez. 2018, p. 58-59. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/305/246>. Acesso em: 28.04.2023

TERRA, Aline de Miranda Valverde; e BANDEIRA, Paula Greco. **A cláusula resolutiva expressa e o contrato incompleto como instrumentos de gestão de risco nos contratos**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 6, n. 4, p. 9-25, out./dez. 2015. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/80/183>. Acesso em: 27.04.2023.

TERRA, Aline de Miranda Valverde; NANNI, Giovanni Ettore. **A cláusula resolutiva expressa como instrumento privilegiado de gestão de riscos contratuais**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 31, n. 1, p. 135-165, jan./mar. 2022. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/837/518>. Acesso em: 27.04.2023.

TERRA, Aline de Miranda Valverde; e SANTOS, Deborah Pereira Pinto dos. **Do *pacta sunt servanda ao code is law*: breves notas sobre a codificação de comportamentos e os controles de legalidade nos smart contracts**. In TEPEDINO, Gustavo; e SILVA, Rodrigo da Guia (Coord.). O direito civil na era da inteligência artificial. 1. ed. São Paulo: Thomson Reuters Brasil, p. 397-409, 2020.

VALENCIA RAMÍREZ, Juan Pablo. **Contratos inteligentes**. Revista de Investigación en Tecnologías de la Información: RITI, Espanha, v. 7, n. 14, p. 1-10, julio/diciembre 2019. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=7242766>. Acesso em: 26.12.2022

VERÍSSIMO, Levi Borges de Oliveira. **Repercussões concorrenciais das *Distributed Ledger Technologies* (DLTS)**. In FRAZÃO, Ana; e CARVALHO, Angelo Gamba Prata de (Coord.). Empresa, mercado e tecnologia. Belo Horizonte: Fórum, p. 255-267, 2019.

VIOLA, Rafael. **Risco e causalidade**. Indaiatuba: Editora Foco, 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

7

Os desafios da tributação na economia digital

RICARDO GODOY VIDAL DA SILVA PAIVA

Com os avanços da tecnologia e da comunicação, diversos desafios surgem para a tributação da economia digital no mundo, que anteriormente se desenvolveu baseada em uma sociedade industrial. No Brasil não é diferente, onde o sistema tributário nacional desenhou-se a partir de um modelo econômico que vem sendo superado pela digitalização da economia, no qual as ações humanas ou a presença física são cada vez menos necessárias à ocorrência dos fatos econômicos tributáveis.

A transformação digital e a evolução tecnológica experimentaram nos últimos anos uma aceleração em razão da pandemia do coronavírus, resultando em diversos reflexos na economia do país e, consequentemente, tornando a adaptação do sistema tributário nacional uma necessidade.[2]

O mundo evoluiu de tal forma que as empresas mais valiosas, hoje, são as de tecnologia, cujos principais ativos são imateriais ou intangíveis. A era da tecnologia desmaterializa as coisas que possuem valor econômico. Inegavelmente as peças e materiais que compõem um computador possuem valor econômico, no entanto, atualmente, os softwares e as informações nele guardadas ou em nuvem podem valer significativamente mais do que a própria máquina.

As maiores sociedades hoje no Brasil dos setores de transporte, imobiliário e de comercialização de alimentos prestam serviços por meio de aplicativos sem possuir um único automóvel, imóvel, hotel ou restaurante.

No entanto, o sistema tributário nacional construiu-se em cima de uma realidade de objetos materiais, baseado em uma época em que as atividades comerciais seguiam o fluxo econômico da indústria, desde a extração à industrialização, ao comércio atacadista e no varejista, em locais físicos, até chegar no consumidor final.

Como fruto da aceleração da mobilidade causada pela tecnologia, as transações bancárias, que antigamente poderiam demorar dias até se concretiza-

1. Ricardo Godoy Vidal da Silva Paiva é assistente de ensino no módulo de Direito Tributário e Internet da Pós-Graduação em Direito Digital do Instituto de Tecnologia e Sociedade do Rio de Janeiro. Pós-Graduado em Direito Tributário e Financeiro pela Universidade Federal Fluminense. Advogado do escritório Bianca Xavier Sociedade de Advogados. Assistente de pesquisa na Fundação Getúlio Vargas.

2. PEROBA, Luiz Roberto. O digital tax europeu e a reforma tributária no Brasil. <https://www.jota.info/opiniao-e-analise/artigos/o-digital-tax-europeu-e-a-reforma-tributaria-no-brasil-29072019> Disponível em 01 de junho de 2023.

rem, atualmente ocorrem em poucos minutos entre diversas pessoas distintas, várias vezes ao dia, até mesmo sem a intervenção de instituições bancárias, como nas operações envolvendo criptoativos, o que dificulta a rastreabilidade, a identificação dos responsáveis e a mensuração do que deve ser tributado.

As relações econômicas também não mais se limitam a fronteiras geográficas, inclusive entre estados de um mesmo país. É plenamente possível que uma empresa localizada em qualquer país ofereça serviços ou produtos à distância pela internet a pessoas em outros países, a despeito de as normas tributárias restringirem-se à soberania dos seus próprios territórios.

Considerando que a mobilidade dos bens intangíveis e dos usuários geram grandes dificuldades para se determinar o local de criação e o consumo desses bens intangíveis, a OCDE lançou planos para tentar tornar a tributação mais justa no âmbito internacional, a fim de combater a erosão das bases tributárias e a transferências de lucros, dentre as quais destacam-se medidas no âmbito da economia digital.[3]

O sistema tributário nacional, no contexto da economia digital, tem enfrentado grandes dificuldades em acompanhar a evolução tecnológica a fim de qualificar os fatos econômicos à medida em que os elementos de apoio tradicionalmente conceituados não identificam as características das novas operações, resultando em conflitos tão caros aos contribuintes e aos próprios entes tributantes, dada a insegurança jurídica e ausência de previsibilidade em relação à tributação.[4]

Embora o Brasil tenha mais *smartphones* do que habitantes e cerca de 75% (setenta e cinco por cento) da população possua celular com *internet*, o sistema tributário nacional ainda tem dispositivos em vigor dispondo sobre a tributação dos serviços de telecomunicação mediante pagamento em ficha telefônica que sequer existe atualmente, o que demonstra a morosidade da legislação tributária em acompanhar a evolução tecnológica.

Por outro lado, em decorrência de regras não tão bem definidas como consequência da economia digital, discutiu-se a inserção do *streaming* na materialidade do imposto sobre serviços, a despeito da inegável relação econômica

3. BRIGAGÃO, Gustavo. O Beps e os desafios da tributação eletrônica internacional. <https://www.conjur.com.br/2017-dez-06/consultor-tributario-beps-desafios-tributacao-eletronica-internacional#_ftn6> Disponível em 01 de junho de 2023.

4. GRECO, Marco Aurélio, FARIA, Renato; Silveira, Ricardo; Monteiro, Alexandre (coords). Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas. São Paulo: Saraiva Educação: 2018, p. 781.

envolvendo tais atividades, por suposta ausência de expressa previsão legal para tributação.

Apesar disso, mesmo com a inclusão do serviço na lei complementar de competência dos municípios, uma nova discussão deve se iniciar, posto que os estados buscam trazer a tributação para o seu campo de incidência, sob a justificativa de que inexiste obrigação de fazer na operação, o que seria pressuposto para o tributo municipal, em que pese os serviços de *streaming* sejam disponibilizados pela internet sem cessão definitiva para o consumidor e sem mudança de titularidade do bem. A tendência é que a matéria seja definida pelo Supremo Tribunal Federal.

O problema da "servicização" gerado pelos modelos de negócios implementados na economia digital podem causar dificuldades financeiras para os estados, competentes para arrecadar os tributos sobre circulação de mercadorias, propriedade de veículos automotores e doação e transmissão causa mortis, uma vez que a tributação dos serviços se concentra nos municípios, resultando em perda de arrecadação dos entes estatais.

O conflito gerado por força da economia digital disruptiva é bem demonstrado no julgamento dos *softwares* de computador pela Suprema Corte. Num primeiro momento, a Corte decidiu pela incidência do imposto de competência estadual, incidente sobre a circulação de mercadorias, na comercialização de "*software de prateleira*" e pela incidência do imposto sobre serviços dos municípios na venda de "*software customizado*".

A justificativa seria que no *software de prateleira*, desenvolvido em série para um número indefinido de pessoas, predominaria a venda do suporte físico, ao passo que no *software customizado*, a preponderância existiria na prestação do serviço, por se tratar de produto desenvolvido especificamente para um determinado cliente, conforme as solicitações e especificações do produto.

Contudo, vinte e dois anos depois, a Corte alterou seu entendimento original, estabelecendo a incidência do imposto sobre serviços em todas as operações relativas aos *softwares*, seja padronizado ou customizado, por se tratar de programas de computador, portanto, utilitários e imateriais, não havendo que se falar em mercadoria.

Inobstante a modulação de efeitos no julgamento em referência para salvaguardar as operações ocorridas no passado, a decisão afastou a tributação dos entes estaduais sobre a circulação de mercadorias dos *softwares de prateleira*, acarretando perda de arrecadação projetada para custear as despesas

dos estados.

Para o futuro, certo é que novos conflitos serão gerados em razão da aplicação do modelo de tributação da industrialização atual em face das novas tecnologias, como por exemplo no enquadramento dos elementos na impressão 3D, que permitem a criação de objetos tridimensionais a partir de um arquivo digital.[5]

Tendo em vista a competência material do imposto sobre produtos industrializados da União, da circulação de mercadorias pelos estados e dos serviços pelos municípios, será necessário definir sobre qual (ou quais) incide a tributação em consequência da atividade, se trata-se de industrialização com circulação de mercadorias ou se se está diante de uma prestação de serviços. A discussão ganha contornos ainda mais complexos se considerado que a impressão 3D pode ser padronizada ou customizada.

A substituição dos homens pelas máquinas, a massificação da utilização da inteligência artificial, da internet das coisas e da robotização, no futuro também pode gerar problemas tributários, visto que grande parte da arrecadação, no Brasil e no mundo, advém da tributação da renda e da folha de salários dos funcionários das empresas.

Assim é que, eventualmente, o desemprego causado pela robotização acompanhada da internet das coisas e da inteligência artificial também pode causar efeitos negativos bastante significativos no financiamento dos sistemas de seguridade social. Daí porque avalia-se, como forma de minimizar os impactos causados pela automação, propostas para criação de um novo *robot tax*.[6]

Diante de tais mudanças sucedem-se os desafios da tributação da economia digital, pelas dificuldades de se identificar onde estão a renda, o consumo e o patrimônio das pessoas físicas e jurídicas, as relações econômicas, bem como do ordenamento jurídico no Brasil e no mundo acompanhar as modificações derivadas do modelo atual disruptivo, tendo em vista a insuficiência dos mecanismos preexistentes.

A incompatibilidade do modelo econômico digital repercute diretamen-

5. CUNICO, Marlon Wesley Machado. Impressoras 3D: o novo meio produtivo. Curitiba: Concep3D Pesquisas Científicas LTDA, 2014. p. 2

6. SEGUNDO, Hugo de Brito Machado. Tributação e inteligência artificial. <https://www.cidp.pt/revistas/rjlb/2020/1/2020_01_0057_0077.pdf> Disponível em 01 de junho de 2023.

te nas regras da tributação construídas sob uma realidade antiga, hoje em transformação, razão pela qual discussões sobre o tema são absolutamente relevantes na tentativa de solucionar os problemas decorrentes da economia digital em escala global.

Por força disso, em virtude da ruptura do no cenário econômico, considerando que o momento é propício para isso, sobretudo porque se discute a tributação da economia digital no mundo, é relevante que seja debatida uma reforma tributária nacional como tentativa de antecipar a solução para os problemas que já existem e os que surgirão.

Bibliografia

BRIGAGÃO, Gustavo. **O Beps e os desafios da tributação eletrônica internacional**. <https://www.conjur.com.br/2017-dez-06/consultor-tributario-beps-desafios-tributacao-eletronica-internacional#_ftn6> Disponível em 01 de junho de 2023.

CUNICO, Marlon Wesley Machado. **Impressoras 3D: o novo meio produtivo**. Curitiba: Concep3D Pesquisas Científicas LTDA, 2014.

FARIA, Renato; Silveira, Ricardo; Monteiro, Alexandre (coords). **Tributação da economia digital: desafios no Brasil, experiência internacional e novas perspectivas**. São Paulo: Saraiva Educação: 2018.

FARIA, Renato; Silveira, Ricardo; Monteiro, Alexandre. **Os desafios da tributação dos negócios desenvolvidos na economia digital**. <https://www.conjur.com.br/2018-out-11/opiniao-desafios-tributacao-economia-digital#_edn4> Disponível em 01 de junho de 2023.

GOMES, Eduardo. **Tributação da impressão 3D: *blueprint*, *software* e impressora 3D**. São Paulo: Thomson Reuters, Revista dos Tribunais: 2021.

LEITE, Luiza; SCWARTZ, Rodrigo; FEIGELSON, Bruno. **Tax 4.0: tributação na realidade exponencial**. São Paulo: Thomson Reuters, 2021.

MACHADO SEGUNDO, Hugo de Brito (coord). **Tributação e novas tecnologias: software, criptomoedas, disponibilização de conteúdos e inteligência artificial**. São Paulo: Editora Foco, 2021.

SEGUNDO, Hugo de Brito Machado. **Tributação e inteligência artificial**. <https://www.cidp.pt/revistas/rjlb/2020/1/2020_01_0057_0077.pdf> Disponível em 01 de junho de 2023.

OLVIEIRA, Gustavo da Gama; LIVIO, Marcus; ROCHA, Sergio André (coords). **Tributação da economia digital**. Rio de Janeiro: Lumen Juris, 2019.

PEROBA, Luiz Roberto. **O digital tax europeu e a reforma tributária no Brasil**. <https://www.jota.info/opiniao-e-analise/artigos/o-digital-tax-europeu-e-a-reforma-tributaria-no-brasil-29072019> Disponível em 01 de junho de 2023.

PEROBA, Luiz Roberto. **Os desafios da tributação da economia digital**. <https://valor.globo.com/legislacao/coluna/os-desafios-da-tributacao-da-economia-digital.ghtml> Disponível em 01 de junho de 2023.

PISCITELLI, Tathiane; SILVEIRA, Daniela (coords). **Tributação da economia digital**. São Paulo: Thomson Reuters, 2022.

PISCITELLI, Tathiane (org). **Tributação da Nuvem: conceitos tecnológicos, desafios internos e internacionais**. São Paulo: Thomson Reuters, 2018.

RENAULT, Felipe. **Competência tributária internacional e economia digital**. Rio de Janeiro: Lumen Juris, 2020.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO 2

Proteção de dados pessoais e novas tecnologias

AUTORES

Carolina Fiorini Ramos Giovanini

Tatiana Chagas dos Santos Coutinho

Rayanne Conceição de Almeida Santos

Nice Siqueira do Amaral

Vanessa Vargas dos Santos

Bianca Alves Batista

Janaina Costa

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

8

Telessaúde, proteção de dados pessoais e direito ao corpo: reflexões à luz do ordenamento jurídico brasileiro

CAROLINA FIORINI RAMOS GIOVANINI

CAROLINA FIORINI RAMOS GIOVANINI[1]

Sumário: Introdução. 1. Regulamentação da telessaúde no Brasil. 2. Aplicação de controles de proteção de dados à telessaúde. 3. Dados pessoais de saúde e direito ao corpo. 4. Consentimento para tratamento de dados pessoais em aplicações de telessaúde. Considerações finais. Referências.

Introdução

Ao longo dos últimos anos, observou-se um crescente uso de tecnologias da informação e comunicação (TIC) no setor de saúde. Aplicativos de saúde, prescrições médicas eletrônicas e consultas por videochamada são alguns exemplos que passaram a fazer parte das rotinas de cuidados médicos. Durante o contexto da pandemia de COVID-19, duas particularidades fizeram com que o uso de tecnologias fosse ainda maior: (i) o alto número de casos gerou maior demanda sobre o sistema de saúde; e (ii) a necessidade de isolamento e distanciamento social fez com que a prática da telemedicina ganhasse destaque.

Para além das consultas remotas, a pandemia de COVID-19 impulsionou o desenvolvimento de uma série de aplicações de saúde. Na Itália, a partir do uso de *chatbots* orientados por inteligência artificial, pacientes sintomáticos puderam avaliar seu estado de saúde e receber recomendações sobre como proceder[2]. Outro exemplo foi o projeto suíço-italiano COVID-Guide[3], que funciona a partir de um chatbot e coleta dados pessoais como gênero, faixa etária, informações sobre gravidez ou amamentação, localização, sintomas e histórico de saúde para apresentar recomendações sobre o que deve ser feito e breve explicação sobre o racional adotado.

Nesse sentido, estudos demonstram que houve um crescimento de cerca de 372% entre março de 2020 e setembro de 2021, sendo que 83% dos pacientes entrevistados afirmaram que gostariam de continuar usando a telemedici-

1. Mestranda em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF) e graduada em Direito pela mesma instituição. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio), em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro). Advogada.

2. NITTAS, Vasileios; VON WYL, Viktor. COVID-19 and telehealth: a window of opportunity and its challenges. Swiss Medical Weekly, [S.L.], v. 150, n. 1920, p. 1-3, 13 maio 2020. SMW Supporting Association. http://dx.doi.org/10.4414/smw.2020.20284. Disponível em: https://pubmed.ncbi.nlm.nih.gov/32400882/. Acesso em: 02 jan. 2023.

3. COVID-GUIDE. Disponível em: https://covidguide.health/en/. Acesso em: 02 jan. 2023.

na após o fim da pandemia[4]. Assim, é importante notar que os avanços no uso de tecnologias na área da saúde não pararam na pandemia. Na verdade, esta área está em constante evolução e expansão.

Especificamente no contexto brasileiro, a pesquisa TIC Saúde 2021, desenvolvida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br)[5], no âmbito do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), demonstrou que 24% dos estabelecimentos de saúde oferecem visualização on-line de resultados de exames, 16% dos estabelecimentos de saúde oferecem interação on-line com a equipe médica e 9% dos estabelecimentos de saúde oferecem visualização on-line do prontuário do paciente.

Evidentemente, tais iniciativas envolvem a circulação de uma série de informações, incluindo dados pessoais, isto é, informações que podem identificar uma pessoa física direta ou indiretamente, como nome, número de documentos, localização geográfica etc. No contexto do setor de saúde, é importante notar que há um relevante fluxo de informações pessoais relacionadas à saúde, como atestados, receitas, exames e laudos.

Por tal razão, o aumento do fluxo de informações relacionadas à saúde suscita diversas preocupações acerca da proteção da personalidade de pacientes, notadamente em relação ao direito ao corpo e à proteção de dados pessoais. Diante desse cenário, surgem regulamentações sobre o tema: em maio de 2022, o Conselho Federal de Medicina (CFM) publicou a Resolução nº 2314/2022, que regulamenta a telemedicina no Brasil e, posteriormente, em dezembro de 2022, foi publicada a Lei nº 14.510/2022, que regulamenta a prática da telessaúde em todo o território nacional.

Diante desse cenário, mostra-se importante refletir acerca dos impactos técnicos, éticos e jurídicos decorrentes do uso de dados pessoais em práticas de telessaúde. O presente artigo pretende, portanto, analisar o uso de dados pessoais na telessaúde tendo em vista o fato de que o ordenamento jurídico brasileiro apresenta regime específico para tratamento de dados de saúde e dispositivos acerca do direito ao corpo. O trabalho adota metodologia baseada em abordagem exploratória, uma vez que o contexto regulatório brasileiro

4. ALTMAN, Rachael. 2022 Trends in Telemedicine and Hybrid Healthcare. 2022. Disponível em: https://www.g2.com/articles/telemedicine-and-hybrid-healthcare-trends-2022. Acesso em: 2 jan. 2023.

5. CETIC.BR. TIC Saúde 2021. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124124231/resumo_executivo_tic_saude_2021.pdf. Acesso em: 2 jan. 2023.

da telessaúde é incipiente e sua relação com as normas de proteção de dados ainda está em desenvolvimento. Assim, busca-se alcançar maior proximidade com o objeto de estudo, de modo a torná-lo evidente e compreensível, a partir do levantamento bibliográfico e análise das disposições da Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018, abreviada por "LGPD") e demais legislações pertinentes ao tema.

Em primeiro lugar, apresenta-se o atual estado da regulamentação da telessaúde no Brasil, posteriormente, analisa-se a aplicação de controles de proteção de dados em tais práticas. Em seguida, busca-se estabelecer relação entre o regime jurídico de proteção de dados de saúde e o direito ao corpo. Por fim, investiga-se os limites do consentimento de pacientes para o tratamento de dados pessoais, tendo em vista o uso de dados sensíveis e eventuais vulnerabilidades do titular.

Regulamentação da telessaúde no Brasil

Em maio de 2022, o Conselho Federal de Medicina (CFM) publicou a Resolução nº 2314/2022, que regulamenta a telemedicina no Brasil. Nesse sentido, a telemedicina é definida como o exercício da medicina mediado por Tecnologias Digitais, de Informação e de Comunicação (TDICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde, podendo ser realizada em tempo real on-line (síncrona) ou off-line (assíncrona).

Vale destacar que a 51ª Assembleia Geral da Associação Médica Mundial6, realizada em 1999, gerou o documento denominado "Declaração de Tel Aviv", no quão são delimitadas cinco modalidades e diretrizes para emprego da telemedicina: (i) teleassistência; (ii) televigilância; (iii) teleconsulta; (iv) interação entre dois médicos; e (v) teleintervenção.

A partir de tal definição, Faleiros Junior, Nogaroli e Cavet[7] ressaltam que é possível verificar que a prática da telemedicina apresenta diferentes graus de complexidade, de adequação e de necessidade das instituições de saúde

6. ASSEMBLEIA GERAL DA ASSOCIAÇÃO MÉDICA MUNDIAL. Declaração de Tel Aviv sobre responsabilidades e normas éticas na utilização da telemedicina. Disponível em: http://www.dhnet.org.br/direitos/codetica/medica/27telaviv.html. Acesso em: 29 abr. 2023.

7. FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da Covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. Revista dos Tribunais, Brasília, v. 109, n. 1016, jun. 2020. Disponível em: https://juslaboris.tst. jus.br/handle/20.500.12178/173660. Acesso em: 2 jan. 2023.

e das comunidades a que se destina. Por tal razão, Garcia e Costa8 apontam que a regulação da telemedicina não deve se centrar na figura do médico individual, mas sim nos impactos e transformações que o uso de tecnologias de informação e comunicação acarreta.

Por outro lado, em dezembro de 2022, foi publicada a Lei nº 14.510/2022, que autoriza e disciplina a prática da telessaúde em todo o território nacional. Nota-se que referida norma afasta o uso do termo "telemedicina" e adota a denominação "telessaúde", que abrange a prestação remota de serviços relacionados a todas as profissões da área da saúde regulamentadas pelos órgãos competentes do Poder Executivo federal.

Nesse sentido, a telessaúde é definida como a modalidade de prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação, que envolve, entre outros, a transmissão segura de dados e informações de saúde, por meio de textos, de sons, de imagens ou outras formas adequadas. Assim, trata-se de definição que abrange a prestação de serviços de saúde em geral, não somente o exercício da medicina. Em razão de sua maior abrangência, este trabalho adota a terminologia "telessaúde" para tratar do tema.

Embora as normas mencionadas apresentem diferenças conceituais, ambas se assemelham ao ressaltar a importância da proteção de dados pessoais. A Resolução nº 2.314/2022 estabelece que os dados pessoais e clínicos do teleatendimento médico devem seguir as definições da Lei Geral de Proteção de Dados (Lei nº 13.709/2018, abreviada por "LGPD"). Na mesma direção, a Lei nº 14.510/2022 determina que a prática da telessaúde deve observar as disposições da LGPD.

Nesse sentido, vale destacar que os dados pessoais são quaisquer informações que possam identificar, direta ou indiretamente, uma pessoa física, seja ela determinada ou determinável, nos termos do art. 5º, I, da LGPD. Além disso, a LGPD apresenta categoria específica de dados pessoais, denominada "dados sensíveis", que são definidos como informações pessoais 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

8. GARCIA, Marco Aurélio Fernandes; COSTA, José Augusto Fontoura. O (novo) marco civil da telemedicina: a construção de um ambiente regulatório saudável para as novas práticas telemédicas. Revista de Direito Sanitário, [S.L.], v. 22, n. 2, p. 1-17, 12 set. 2022. Universidade de São Paulo, Agência USP de Gestão da Informação Acadêmica (AGUIA). http://dx.doi.org/10.11606/issn.2316-9044.rdisan.2022.173191. Disponível em: https://www.revistas.usp.br/rdisan/article/view/173191/186235. Acesso em: 02 jan. 2023.

ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme o art. 5º, II, da referida norma.

A prática de telessaúde, por vezes, irá envolver o tratamento de dados pessoais, inclusive de natureza sensível (como exames médicos, receitas e laudos). Conforme apontam Faleiros Junior, Nogaroli e Cavet[9], esse cenário requer especial atenção quanto à garantia de sigilo da informação e privacidade do paciente, pela ampliação da circulação, conexão e coordenação de dados pessoais sensíveis estruturadas, o que potencializa os riscos de vazamento. Por tal razão, a Lei nº 14.510/2022 prevê a confidencialidade dos dados como um dos princípios a serem observados durante a prática de telessaúde.

Sobre o tema, o Código de Boas Práticas de Proteção de Dados para Prestadores Privados em Saúde publicado pela Confederação Nacional de Saúde[10] aponta que as medidas de segurança relacionadas aos dados gerados em consultas via telemedicina devem ser reforçadas em razão dos riscos cibernéticos externos e internos.

Desse modo, as diversas atividades que envolvem tratamento de dados pessoais no contexto da telemedicina devem ser analisadas sob a ótica das disposições da LGPD, que prevê, por exemplo, princípios que devem orientar o uso lícito e seguro de dados pessoais. Assim, como forma de melhor ilustrar referido cenário, o presente trabalho busca analisar as práticas de telessaúde à luz de controles de proteção de dados.

Aplicação de controles de proteção de dados à telessaúde

Em análise comparativa entre a Resolução nº 2314/2022 e a Lei nº 14.510/2022, é possível observar que a Resolução que regulamenta a telemedicina traz disposições mais específicas acerca de controles de proteção de dados pessoais, prevendo, por exemplo, que os dados e imagens dos pacientes constantes no registro do prontuário devem ser preservados, em observância aos preceitos de integridade, veracidade, confidencialidade, privacidade e garantia do sigilo profissional.

---

9. FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da Covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. Revista dos Tribunais, Brasília, v. 109, n. 1016, jun. 2020. Disponível em: https://juslaboris.tst. jus.br/handle/20.500.12178/173660. Acesso em: 2 jan. 2023.

10. CONFEDERAÇÃO NACIONAL DE SAÚDE. Código de Boas Práticas de Proteção de Dados para Prestadores Privados em Saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 29 abr. 2023.

Além disso, a Resolução nº 2314/2022 apresenta regras para o armazenamento de dados pessoais, estabelecendo que em caso de contratação de serviços terceirizados de arquivamento, a responsabilidade pela guarda de dados de pacientes e do atendimento deve ser contratualmente compartilhada entre o médico e a contratada. Ainda, a norma estabelece parâmetros para interoperabilidade de dados e garante ao paciente ou ao ser representante legal o direito de solicitar e receber cópia em mídia digital e/ou impressa dos dados de seu registro.

Por outro lado, a Lei nº 14.510/2022, que disciplina a telessaúde, redireciona o tema para as disposições da LGPD, que prevê regras para o tratamento de dados pessoais e direitos aos titulares de dados. No entanto, a ausência de regras específicas na Lei nº 14.510/2022 não significa que a prática de telessaúde está imune à implementação de controles de proteção de dados. Nesse caso, faz-se necessário traçar uma interpretação sistemática entre as normas, o que pode ser feito a partir dos princípios previstos pela LGPD, que orientam o tratamento de dados pessoais.

No âmbito da LGPD, os princípios da finalidade e da adequação (art. 6º, I e II, da LGPD) indicam que é necessário definir, previamente, um objetivo concreto para o tratamento de dados pessoais do paciente, garantindo-se que as informações coletadas no contexto da prática de telessaúde não serão utilizadas para finalidades secundárias incompatíveis com as que as justificaram o tratamento de dados.

A partir do princípio da necessidade (art. 6º, III, da LGPD) é possível concluir que os dados pessoais coletados para viabilizar a prática da telemedicina devem se limitar ao mínimo necessário, evitando-se a coleta excessiva de dados pessoais. Além disso, é importante estabelecer um prazo de retenção para os dados pessoais, de modo a limitar o tempo de armazenamento das informações.

A partir dos princípios do livre acesso e da transparência (art. 6º, IV e V, da LGPD), verifica-se que as informações acerca do tratamento de dados pessoais no contexto da prática da telessaúde devem ser disponibilizadas aos pacientes de maneira clara e acessível. Além disso, é importante considerar as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos pacientes, adaptando o formato de disponibilização das informações conforme necessário. Para além do fornecimento de informações, é importante assegurar a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Considerando-se o princípio da qualidade (art. 6º, V, da LGPD), verifica-se que o uso de dados pessoais no contexto da telessaúde deve observar padrões de qualidade que assegurem a obtenção de diagnósticos corretos e prescrições adequadas. Por tal razão, é necessário garantir que as informações pessoais utilizadas sejam verídicas e atualizadas.

Além disso, nota-se a possibilidade de transferências de informações pessoais por meio de plataformas e armazenamento de alto volume de dados, motivo pelo qual é essencial avaliar as medidas técnicas e administrativas de segurança adotadas durante a prática de telessaúde, de modo a garantir que acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão não ocorram, conforme prevê o princípio da segurança (art. 6º, VII, da LGPD).

Por fim, destaca-se o princípio da não discriminação (art. 6º, IX, da LGPD), que assume especial relevância considerando-se o potencial discriminatório das informações pessoais fornecidas ou geradas no contexto das práticas de telessaúde. Nesse sentido, faz-se necessário assegurar que não ocorram privações relacionadas a direitos fundamentais e limitações de acesso a direitos e/ou serviços, uma vez que o tratamento de dados para fins discriminatórios ilícitos ou abusivos é vedada.

Desse modo, nota-se que, ainda que a Lei nº 14.510/2022 não tenha estabelecido regras específicas para o tratamento de dados pessoais no âmbito da telessaúde, as disposições da LGPD são plenamente aplicáveis e devem ser consideradas em tal contexto. Para além dos princípios que orientam o tratamento de dados pessoais, é essencial notar que a prática de telessaúde atrai regime setorial específico para uso de dados pessoais de saúde e envolve diferentes agentes deste sistema.

A título de exemplificação, é possível citar as resoluções normativas da Agência Nacional de Saúde (ANS) sobre proteção ao fluxo de informações relativas à assistência prestada aos beneficiários de planos de saúde privados (Resolução Normativa nº 255, de 18 de maio de 2011 e Resolução Normativa nº 389, de 26 de novembro de 2015). Tais normas estabelecem a necessidade de designação de Responsável pela Área Técnica da Saúde, responsável por zelar pelo fluxo de informações relativas à assistência prestada aos beneficiários, e regras sobre transparência e disponibilização de informações no âmbito da saúde suplementar.

Assim, verifica-se que o setor de saúde está sujeito a normas e regulamentações específicas que, por vezes, também envolvem regras sobre o uso

de informações pessoais. Considerando as particularidades do setor, o volume estimado de dados envolvidos e a natureza das informações, a implementação de medidas para garantir a proteção e privacidade dos dados é essencial.

Dados pessoais de saúde e direito ao corpo

Os dados pessoais relacionados à saúde são classificados como dados pessoais sensíveis e, consequentemente, recebem tutela jurídica diferenciada em razão do potencial discriminatório gerado por atividades de tratamento que utilizam tais dados. Nesse sentido, Maria Celina Bodin de Moraes[11], em apresentação à obra de Rodotà, aponta que os dados pessoais sensíveis são aqueles relacionados às características basilares da persona, sendo aptos a gerar situações de discriminação e desigualdades.

Negri e Korkmaz[12] explicam que a natureza sensível de um dado também pode ocorrer a partir de uma associação intrínseca à autodeterminação individual, como é o caso das convicções políticas, religiosas ou filosóficas, filiação sindical, a própria orientação sexual, entre outros, porque existem inúmeros contextos em que uma pessoa pode ser objeto de práticas incompatíveis com a dignidade da pessoa humana.

No âmbito da União Europeia, o *Article 29 Data Protection Working Party*[13] (órgão consultivo europeu que tratava de questões relacionadas ao tema de privacidade e proteção de dados, atualmente substituído pelo *European Data Protection Board – EDPB*) já esclareceu que a lógica por trás da regulamentação de categorias específicas de dados de uma maneira diferente decorre da presunção de que o uso indevido desses dados pode ter consequências mais graves sobre os direitos fundamentais do indivíduo.

11. RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

12. NEGRI, Sergio 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, [S.L.], v. 5, n. 1, p. 63-85, 22 out. 2019. Conselho Nacional de Pesquisa e Pos--Graduacao em Direito - CONPEDI. http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2019.v5i1.5479. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 02 jan. 2023.

13. ARTICLE 29 DATA PROTECTION WORKING PARTY. Advice paper on special categories of data (“sensitive data”). Disponível em: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Acesso em: 02 jan. 2023.

Na mesma direção, a *Information Commissioner's Office*[14] (autoridade britânica de proteção de dados) destaca que dados pessoais sensíveis merecem proteção específica porque o uso desses dados pode criar riscos significativos para os direitos e liberdades fundamentais do indivíduo, uma vez que tais informações estão diretamente relacionadas à liberdade de expressão, liberdade religiosa, liberdade de associação, direito à integridade corporal e livre discriminação.

Assim, verifica-se que a proteção especial direcionada aos dados pessoais sensíveis é uma forma de proteger e efetivar outros direitos para além do direito à proteção de dados, por exemplo, o direito ao corpo. No contexto de uso de dados pessoais de saúde, Rodotà[15] aponta que estes sempre exigem atenção especial, não só porque as legislações assim determinam, mas também porque representam a condição humana, de modo a retratar a pessoa em seus momentos de maior fragilidade e revelar as fraquezas do corpo.

Por tal razão, nota-se que o uso de dados de saúde, por vezes, ocorre em um contexto de vulnerabilidade do titular de dados. Em relação à vulnerabilidade, Konder e Konder[16] esclarecem que o conceito de vulnerabilidade busca demonstrar como determinados grupos, em razão de características específicas, estão mais suscetíveis a certos riscos relacionados à ameaça de lesão a aspectos existenciais da pessoa humana.

Especificamente no contexto de tratamento de dados pessoais de saúde, a vulnerabilidade pode ser ilustrada a partir do cenário relatado por Sarlet e Caldeira[17], que alertam para o fato de que a saúde passou a ser afetada por fatores como (i) a implementação desordenada de inovações biotecnológicas; (ii) a estruturação de um mercado rentável e muito atuante; (iii) a aplicação irresponsável da tecnologia da informação e da comunicação; e (iv) os novos paradigmas voltados para a imortalização e para o enaltecimento da ideia de

14. INFORMATION COMMISSIONER'S OFFICE. What is special category data? Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/. Acesso em: 02 jan. 2023.

15. RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

16. KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza. Da vulnerabilidade à hipervulnerabilidade: exame crítico de uma trajetória de generalização. Interesse Público [Recurso Eletrônico]. Belo Horizonte, v.23, n.127, maio/jun. 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/41221. Acesso em: 02 jan. 2023.

17. SARLET, G. B. S.; CALDEIRA, C. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. Civilística, v. 8, n. 1, p. 1-27, 29 abr. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 02 jan. 2023.

perfeição em um contexto de saúde preventiva.

No âmbito da LGPD, os dados pessoais de saúde são classificados como dados pessoais sensíveis, porém, não há uma definição sobre o que seriam dados de saúde. Por outro lado, no âmbito da União Europeia, verifica-se que o *General Data Protection Regulation* (GDPR) – norma do direito comunitário europeu que regulamenta o uso de dados pessoais – estabelece que dados pessoais relativos à saúde são dados pessoais relacionados com a física ou mental de pessoa natural, incluindo a prestação de serviços de saúde que revelem informações sobre o seu estado de saúde.

O Considerando 35 do GDPR estabelece que deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Desse modo, são considerados dados de saúde informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre a saúde, por exemplo, uma doença, deficiência, um risco de doença, histórico clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico.

Por tal razão, o *Article 29 Data Protection Working Party*[18] considera que, devido à grande variedade de dados pessoais que podem se enquadrar na categoria de dados relacionados à saúde, essa categoria representa uma das áreas mais complexas de dados sensíveis. Além disso, é importante notar que existem grandes diferenças no grau de criticidade dos dados relacionados à saúde, pois podem variar, por exemplo, de informações sobre um resfriado simples a informações estigmatizantes sobre doenças ou deficiências.

No contexto brasileiro, apesar da legislação não estabelecer uma definição para os dados pessoais de saúde, existem regras específicas para o tratamento de tais informações. Em primeiro lugar, nota-se que a LGPD, a partir da interpretação conjunta dos parágrafos 4º e 5º do art. 11, apresenta duas proibições relacionadas ao tratamento de dados pessoais de saúde: (i) é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais

18. ARTICLE 29 DATA PROTECTION WORKING PARTY. Advice paper on special categories of data ("sensitive data"). Disponível em: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Acesso em: 02 jan. 2023.

sensíveis referentes à saúde com objetivo de obter vantagem econômica; e (ii) é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

No entanto, a tratamento de dados pessoais de saúde não será vedado quando realizado para (i) prestação de serviços de saúde, (ii) prestação de serviços de assistência farmacêutica; (iii) prestação de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados; (iv) viabilizar a portabilidade de dados quando solicitada pelo titular; e (v) permitir as transações financeiras e administrativas decorrentes do uso e da prestação de tais serviços.

Tais hipóteses de prestação de serviços de saúde podem ocorrer a distância por meio da utilização das tecnologias da informação e da comunicação, o que caracteriza a prática de telessaúde, nos termos da Lei nº 14.510/2022. Nesse contexto, observa-se que o corpo humano ganha uma dimensão eletrônica, para além do corpo físico. Korkmaz[19] destaca que os dados de saúde são, a rigor, condições relativas ao corpo físico, elevadas ao patamar do corpo eletrônico diante das potencialidades tecnológicas.

Em relação à tutela jurídica do corpo humano, o pensamento moderno compreende a integridade corporal como parte da autonomia da pessoa, de modo que o regime jurídico brasileiro busca instituir garantias contra interferências externas, seja por parte do Estado, seja por parte de particulares. Nesse sentido, o Código Civil Brasileiro (Lei nº 10.406/2022) prevê disposições acerca do direito à integridade psicofísica sob a perspectiva dos atos de disposição do corpo, determinando regras para a relação entre a proteção ao corpo e a vontade da pessoa humana.

No entanto, em tempos de crescente circulação de dados de uso e uso massivo de aplicações tecnológicas durante a prestação de assistência médica, Rodotà[20] já apontava a importância de que o direito à proteção do corpo

19. KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. 2019. 119 f. Dissertação (Mestrado) - Curso de Mestrado em Direito e Inovação, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11438. Acesso em: 02 jan. 2023.

20. RODOTÀ, Stefano. Transformações do corpo. Trad. Maria Celina Bodin de Moraes. Revista trimestral de direito civil. v. 19, julho/setembro, 2004, p. 91.

também fosse debatido na esfera eletrônica. Nesse sentido, para Rodotà[21], os corpos físico e eletrônico devem ser tutelados na sua unidade, de modo que a violação de qualquer um dos componentes do corpo deve ser entendida como uma violação enquanto unidade e, consequentemente, uma violação à personalidade.

Portanto, considerando a evolução e popularização das práticas de telessaúde, o tratamento de dados pessoais relacionados à saúde deve levar em consideração o fato de que tais informações são, de um lado, projeções do corpo físico, e, de outro, elementos que constituem o corpo eletrônico. Nesse sentido, Basan e Faleiros Júnior[22] destacam que é necessário reconhecer que a ampliação do fluxo informacional também ampliou as possibilidades de lesão às pessoas e que a integridade humana não mais se limita ao corpo físico, tendo repercussão em elementos virtuais ou eletrônicos da pessoa humana.

Assim, para efetivação da proteção integral da pessoa humana, deve-se considerar a expansão da tutela dos direitos da personalidade ao denominado "corpo eletrônico", formado por informações pessoais - inclusive relacionadas à saúde - que individualizam a pessoa humana e revelam elementos inerentes à sua personalidade.

Consentimento para tratamento de dados pessoais em aplicações de telessaúde

> Conforme mencionado anteriormente, o Código Civil trata do direito ao corpo a partir da previsão de regras para os atos de disposição do corpo, determinando a relação entre a proteção ao corpo e a vontade da pessoa humana. Vale destacar que parte da doutrina critica essa abordagem restritiva, uma vez que a tutela da integridade psicofísica abrange outros aspectos para além dos atos de disposição do próprio corpo[23].

Procurando regular tal questão, o Código Civil estabelece que é proibido dispor do próprio corpo, quando importar diminuição permanente da integri-

21. RODOTÀ, Stefano. Transformações do corpo. Trad. Maria Celina Bodin de Moraes. Revista trimestral de direito civil. v. 19, julho/setembro, 2004, p. 91.

22. BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura. A tutela do corpo eletrônico como direito básico do consumidor. Revista dos Tribunais [Recurso Eletrônico]. São Paulo, n.1021, nov. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/39001. Acesso em: 02 jan. 2023.

23. Nesse sentido, destaca-se SCHREIBER, Anderson. Direitos da Personalidade: Revista e Atualizada, 3ª edição. Rio de Janeiro: Grupo GEN, 2014. E-book. ISBN 9788522493449.

dade física, ou contrariar os bons costumes, exceto em casos de exigência médica. Além disso, o Código Civil prevê que ninguém poderá ser constrangido a submeter-se, com risco de vida, a tratamento médico ou intervenção cirúrgica. Embora a redação do dispositivo levante a possibilidade de interpretação no sentido de que, em não havendo risco de vida, uma pessoa poderia ser constrangida a tratamento médico ou intervenção cirúrgica, tal leitura é incompatível com os valores fundamentais de proteção da dignidade da pessoa humana, devendo ser afastada.

Assim, verifica-se a necessidade de obtenção de autorização do paciente em qualquer tipo de tratamento médico. Conforme esclarece Schreiber[24], não se trata de uma obtenção genérica de concordância, mas de consentimento informado em relação aos procedimentos médicos a serem adotados, bem como acerca de toda informação relevante sobre o tratamento, seus potenciais impactos e eventuais alternativas disponíveis.

No âmbito da telessaúde, a Lei nº 14.510 estabelece que a prática deve ser realizada por consentimento livre e esclarecido do paciente, ou de seu representante legal, e sob responsabilidade do profissional de saúde. Além disso, ainda em relação aos dados de saúde, a Lei nº 14.289/2022 estabelece que o sigilo profissional sobre a condição de pessoa que vive com infecção pelos vírus da imunodeficiência humana (HIV) e das hepatites crônicas (HBV e HCV) e de pessoa com hanseníase e com tuberculose somente poderá ser quebrado nos casos determinados por lei, por justa causa ou por autorização expressa da pessoa acometida ou, quando se tratar de criança, de seu responsável legal, mediante assinatura de termo de consentimento informado, observado o disposto no art. 11 da LGPD.

Nota-se, portanto, que a obtenção do consentimento é tema de extrema importância para a prestação de serviços de saúde. Nesse contexto, em relação ao corpo eletrônico, o consentimento para tratamento de dados pessoais também assume especial relevância. Considerando-se que os dados de saúde são categorizados como dados pessoais sensíveis, atrai-se um regime jurídico específico, no qual as hipóteses legais que autorizam o tratamento de dados estão previstas no art. 11 da LGPD. Trata-se de rol distinto daquele que autoriza o tratamento de dados pessoais comuns.

---

24. SCHREIBER, Anderson. Direitos da Personalidade: Revista e Atualizada, 3ª edição. Rio de Janeiro: Grupo GEN, 2014. E-book. ISBN 9788522493449.

A LGPD estabelece uma maior qualificação do consentimento para o tratamento de dados sensíveis, determinando que a manifestação deve se dar de forma específica e destacada, para finalidades específicas. Para Rodotà[25], o consentimento qualificado se justifica em razão do fato de que se trata de "contratante vulnerável", permeado pela ausência de liberdade substancial no momento da determinação da vontade.

No ordenamento jurídico brasileiro, a validade do consentimento para tratamento de dados pessoais sensíveis depende das seguintes qualificações: (i) informado; (ii) livre; (iii) inequívoco; (iv) específico; e (v) destacado.

Em relação ao adjetivo "informado", Bioni[26] aponta que é necessário analisar o dever-direito de informação sob duas perspectivas: qualidade e quantidade. Desse modo, a informação disponibilizada ao titular para fins da tomada de decisão deve ser útil, imprevisível e original, equalizando a disparidade informacional. Sob a perspectiva quantitativa, as informações devem ser fornecidas em quantidade suficiente para despertar uma compreensão adequada acerca do tratamento de dados.

Sobre o elemento "livre", nota-se que está relacionado a uma escolha genuína do titular de dados, isto é, a manifestação de livre-arbítrio que caracteriza a tomada de decisão. Por isso, a LGPD veda o tratamento realizado mediante vício de consentimento (art. 8º, § 3º). Além disso, vale destacar que a caracterização do consentimento como livre está diretamente relacionada à vulnerabilidade do titular de dados, uma vez que tal fato impacta o nível de assimetria de poder presente na relação estabelecida entre agente de tratamento e titular. Acerca do adjetivo "inequívoco", o objetivo da LGPD é indicar que o consentimento deve ser uma ação afirmativa clara por parte do titular de dados.

Em relação ao tratamento de dados pessoais sensíveis, a LGPD prevê camada adicional de proteção, estabelecendo que o consentimento deve ser "específico". Vale destacar que Bioni (2019)[27] aponta que, do ponto de vista de técnica legislativa, o uso da expressão "específico" é redundante, uma vez que

25. RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

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

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

qualquer tratamento de dados pessoais deve ser realizado para propósitos específicos e explícitos, conforme previsto pelo princípio da finalidade (art. 6º, I, da LGPD). Assim, o autor entende que uma melhor opção teria sido utilizar o termo "expresso", sendo visto como um vetor para que haja mais assertividade do titular.

Sobre a qualificação do consentimento como "destacado", nota-se que se trata de disposição acerca da forma de coleta da manifestação de vontade do titular, de modo a exigir que a informação seja colocada em posição de destaque, chamando atenção do titular. Por fim, em relação ao elemento "para finalidade específica", nota-se que demanda que o agente de tratamento disponibilize informações exatas que discriminam os objetivos do tratamento de dados pessoais.

Assim, em que pese a carga máxima de participação exigida para o tratamento de dados sensíveis é importante considerar os desafios gerados pela implementação do consentimento, especialmente tendo em vista o fato de que, por vezes, o titular (paciente) será um indivíduo em situação de vulnerabilidade, o que pode afetar sua manifestação de vontade no caso concreto. Desse modo, observa-se que, por vezes, o enquadramento da atividade de tratamento de dados na base legal do consentimento será inviável.

Diante de tais desafios, também é importante assegurar a implementação de outros mecanismos que buscam garantir a conformidade do tratamento de dados pessoais. Tendo em vista que, na maior parte das vezes, o tratamento de dados pessoais de saúde será realizado em um contexto de condição de vulnerabilidade do titular e levando-se em consideração a assimetria de poderes que marca a relação médica, os agentes de tratamento também devem ser preocupar com a construção de rotinas de governança efetivas, que não deixem o peso da garantia da proteção dos dados pessoais somente na autorização do titular.

Além disso, não se deve perder de vista o fato de que o consentimento do titular de dados não é a única hipótese legal que autoriza o tratamento de dados pessoais, tampouco assume posição hierarquicamente superior às demais. Inclusive, especificamente no setor da saúde, as bases legais de tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, VII e art. 11, II, alínea "f", ambos da LGPD) e proteção da vida ou da incolumidade física do titular ou de terceiro (art.7º, VII e art. 11, II, alínea "e", ambos da LGPD) podem desempenhar papéis relevantes.

Portanto, é necessário que agentes de tratamento envolvidos em práticas de telessaúde, por vezes amparadas na obtenção do consentimento, busquem o equilíbrio entre assegurar que o titular tenha capacidade de controlar seus dados pessoais e endereçar esforços para redução da assimetria de poderes e implementação efetiva de rotinas de governança, uma vez que a situação de vulnerabilidade dos titulares demanda especial atenção.

Considerações finais

Nota-se que, na sociedade de informação, as práticas de telemedicina evoluíram e se tornaram cada vez mais complexas e dinâmicas, juntamente com o desenvolvimento da análise de dados de pacientes, o que gerou um grande fluxo de informações, por vezes, de natureza sensível. Diante do cenário de utilização de dados pessoais em práticas de telessaúde, procurou-se demonstrar que o ordenamento jurídico brasileiro busca assegurar a proteção dos dados pessoais envolvidos em tais atividades, especialmente em relação aos dados pessoais de saúde.

A partir da análise da Lei Geral de Proteção de Dados (Lei n° 13.709/2018), da Lei nº 14.510/2022, da Lei nº 14.289/2022 e do Código Civil Brasileiro, foi possível demonstrar que o consentimento do titular assume especial relevância no contexto de uso de dados pessoais de saúde e proteção da integridade psicofísica.

No entanto, a efetivação da proteção da personalidade as assimetrias já existentes na relação entre agentes econômicos e titulares de dados, motivo pelo qual é necessário reconhecer a condição de vulnerabilidade dos pacientes e identificar, em cada caso concreto, sua real liberdade para realizar uma escolha genuína acerca do tratamento de dados pessoais.

Evidentemente, não se trata de inviabilizar o uso da base legal do consentimento ou banir práticas de telessaúde, mas de assegurar que a utilização de dados pessoais em tal contexto seja acompanhada de rotinas e procedimentos de governança eficientes. Portanto, é importante que agentes de tratamento implementem controles de proteção de dados que efetivamente contribuam para a mitigação de eventuais riscos identificados no tratamento de dados pessoais decorrente de práticas de telessaúde, evitando que tal responsabilidade recaia exclusivamente sobre o titular, simplesmente em razão de sua manifestação de vontade.

Referências

ALTMAN, Rachael. ***2022 Trends in Telemedicine and Hybrid Healthcare***. 2022. Disponível em: https://www.g2.com/articles/telemedicine-and-hybrid-healthcare-trends-2022. Acesso em: 02 jan. 2023.

ARTICLE 29 DATA PROTECTION WORKING PARTY. ***Advice paper on special categories of data ("sensitive data")***. Disponível em: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Acesso em: 02 jan. 2023.

ASSEMBLEIA GERAL DA ASSOCIAÇÃO MÉDICA MUNDIAL. **Declaração de Tel Aviv sobre responsabilidades e normas éticas na utilização da telemedicina**. Disponível em: http://www.dhnet.org.br/direitos/codetica/medica/27telaviv.html. Acesso em: 29 abr. 2023.

BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura. **A tutela do corpo eletrônico como direito básico do consumidor**. Revista dos Tribunais [Recurso Eletrônico]. São Paulo, n.1021, nov. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/39001. Acesso em: 02 jan. 2023.

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

CETIC.BR. **TIC Saúde 2021**. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124124231/resumo_executivo_tic_saude_2021.pdf. Acesso em: 02 jan. 2023.

CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de Boas Práticas de Proteção de Dados para Prestadores Privados em Saúde**. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 29 abr. 2023.

COVID-GUIDE. Disponível em: https://covid-guide.health/en/. Acesso em: 02 jan. 2023.

FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. **Telemedicina e proteção de dados: reflexões sobre a pandemia da Covid-19 e os impactos jurídicos da tecnologia aplicada à saúde**. Revista dos Tribunais, Brasília, v. 109, n. 1016, jun. 2020. Disponível em: https://juslaboris.tst. jus.br/handle/20.500.12178/173660. Acesso em: 02 jan. 2023.

GARCIA, Marco Aurélio Fernandes; COSTA, José Augusto Fontoura. **O (novo) marco civil da telemedicina: a construção de um ambiente regulatório saudável para as novas práticas telemédicas**. Revista de Direito Sanitário, [S.L.], v. 22, n. 2, p. 1-17, 12 set. 2022. Universidade de São Paulo, Agência USP de Gestão da Informação Acadêmica (AGUIA). http://dx.doi.org/10.11606/issn.2316-9044.rdisan.2022.173191. Disponível em: https://www.revistas.usp.br/rdisan/article/view/173191/186235. Acesso em: 02 jan. 2023.

INFORMATION COMMISSIONER'S OFFICE. ***What is special category data?*** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/. Acesso em: 02 jan. 2023.

KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza. **Da vulnerabilidade à hipervulnerabilidade: exame crítico de uma trajetória de generalização**. Interesse Público [Recurso Eletrônico]. Belo Horizonte, v.23, n.127, maio/jun. 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/41221. Acesso em: 02 jan. 2023.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade**. 2019. 119 f. Dissertação (Mestrado) - Curso de Mestrado em Direito e Inovação, Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/11438. Acesso em: 02 jan. 2023.

NEGRI, Sergio 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, [S.L.], v. 5, n. 1, p. 63-85, 22 out. 2019. Conselho Nacional de Pesquisa e Pos-Graduacao em Direito - CONPEDI. http://dx.doi.org/10.26668/indexlawjournals/2526-0049/2019.v5i1.5479. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 02 jan. 2023.

NITTAS, Vasileios; VON WYL, Viktor. ***COVID-19 and telehealth: a window of opportunity and its challenges***. Swiss Medical Weekly, [S.L.], v. 150, n. 1920, p. 1-3, 13 maio 2020. SMW Supporting Association. http://dx.doi.org/10.4414/smw.2020.20284. Disponível em: https://pubmed.ncbi.nlm.nih.gov/32400882/. Acesso em: 02 jan. 2023.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Transformações do corpo**. Trad. Maria Celina Bodin de Moraes. Revista trimestral de direito civil. v. 19, julho/setembro, 2004, p. 91.

SAMPAIO, Carolina Vasques; DE MENEZES, Joyceane Bezerra. **Autonomia da pessoa com deficiência e os atos de disposição do próprio corpo**. Revista Jurídica Cesumar-Mestrado, v. 18, n. 1, p. 133-157, 2018. Disponível em: https://repositorio.ufc.br/handle/riufc/54316. Acesso em: 02 jan. 2023.

SARLET, G. B. S.; CALDEIRA, C. **O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana**. Civilística, v. 8, n. 1, p. 1-27, 29 abr. 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 02 jan. 2023.

SCHREIBER, Anderson. **Direitos da Personalidade: Revista e Atualizada, 3ª edição**. Rio de Janeiro: Grupo GEN, 2014. E-book. ISBN 9788522493449

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

9

Pilares do Programa de Compliance em Proteção de Dados

TATIANA CHAGAS DOS SANTOS COUTINHO

TATIANA CHAGAS DOS SANTOS COUTINHO[1]

Introdução

O desenvolvimento socioeconômico e cultural, resultante da globalização, propôs um novo modelo de sociedade, com a informação, a hiperconectividade, a acessibilidade, a interatividade e o armazenamento contínuo de dados pessoais[2] como ponto central[3]. A tendência é que o plano físico migre para o plano virtual[4], fundamentando-se, cada vez mais, em ações que compõem a personalidade do indivíduo.

Na era *data-driven*, os dados dos indivíduos ou grupo de indivíduos têm grande relevância, sobretudo, para empresas que manipulam dados pessoais e criam perfis ("*profiling*") que podem ser utilizados para diversas finalidades, como a tomada de decisões negociais, concessão de crédito, estabelecimento de contrato, entre outras.

Como efeito, as novas tecnologias surgem a partir da necessidade de se atender a dinâmica social frente aos novos desafios da modernidade. No entanto, definir um ponto de equilíbrio entre o respeito à privacidade, o desenvolvimento econômico-tecnológico e a inovação, é medida urgente e necessária.

Com objetivo de proteger os direitos fundamentais de liberdade e de pri-

1. Advogada especializada em Processo Civil, Governança em Tecnologia da Informação, Privacidade, Proteção de Dados Pessoais, Cybersecurity, Regulação e Novas Tecnologias no escritório Lima Feigelson Advogados. Certified Data Protection Officer e Information Privacy Management. Auditora interna do Sistema de Gestão de Segurança da Informação - SGSI ISO 27001:2013 e 27001:2019. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro).

2. MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Editora, 2018, p. 21.

3. GOUVEIA, Luís Manuel Borges, 2004. Notas de contribuição para uma definição operacional. Disponível em http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf - Acesso em 31.12.2022.

4. RODOTÀ, Stefano. Palestra. Tradução de Myriam de Filippis. Disponível em: http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf. Acesso em: 13 jul. 2022.

vacidade e o livre desenvolvimento da personalidade da pessoa natural[5], foi promulgada a Lei Federal 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD"), surgindo para as organizações a obrigatoriedade da adoção de um conjunto de medidas capazes de "comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas", tal como previsto no princípio da responsabilização e prestação de contas, disposto no artigo 6º, X, da LGPD.

A abrangência destas medidas demanda a elaboração de um Programa de Compliance em Proteção de Dados, cuja forma, para fins deste artigo, inspirar-se-á nos 5 (cinco) principais parâmetros que compõem os programa de integridade dispostos no artigo 57 do Decreto n.º 11.129/2022, que regulamentou a Lei n.º 12.846/20136, combinado com as determinações dispostas nos artigos 46 e 50 da LGPD e melhores práticas exigidas pelo mercado.

Os pilares de um Programa de Compliance em Proteção de Dados são princípios básicos que norteiam o tratamento de dados pessoais pela organização e estimulam a adoção de medidas preventivas e corretivas que ajudam a garantir que os direitos de privacidade dos indivíduos sejam respeitados e protegidos, e que os dados pessoais sejam tratados de forma justa e transparente.

Conforme as melhores práticas exigidas de mercado, entende-se que um Programa de Compliance em Proteção de Dados deve incluir os seguintes pilares: i) comprometimento da alta administração; ii) gestão adequada de riscos; iii) políticas e procedimentos de conformidade; iv) treinamento e conscientização; e v) monitoramento e avaliação. A seguir, haverá breve exposição sobre cada um deles.

1.Pilares do programa de compliance a proteção de dados

Os pilares de conformidade são elementos fundamentais que devem ser considerados e seguidos para garantir que a organização esteja conforme às leis, normas e regulamentos que envolvem temas relacionados à privacidade e proteção de dados pessoais. Esses pilares podem variar conforme o setor em que a empresa está inserida e o tipo de regulamentação a que está sujeita. Em geral, os pilares de conformidade incluem:

5. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: L13709 (planalto.gov.br). Acesso em: 12 abr. 2023.

6. BRASIL. Decreto nº 11.129/2022 que regulamenta a Lei n.º 12.846/2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm. Acesso em 31.12.2022

1.1. Comprometimento da alta administração

O pilar de comprometimento da alta administração é fundamental para a garantia do efetivo desenvolvimento do programa de Compliance a Proteção de Dados, pois o engajamento da alta administração transmite de forma clara o entendimento de que Privacidade e Proteção de Dados Pessoais fazem parte da estratégia de negócio da organização.

Compete à alta administração deliberar sobre a destinação de recursos para a implementação do programa, nomear o Encarregado de Dados, mas conhecido por DPO, sigla para *Data Protection Officer* -, nomear o grupo de trabalho e/ou comitê de proteção de dados, composto por líderes das principais áreas da organização, tais como, Recursos Humanos, Sistema da Informação, Departamento Jurídico e Marketing, que dentre outras atribuições, reportará ao Conselho de Administração, órgão responsável pela gestão de riscos cibernéticos, os assuntos relacionados à proteção de dados pessoais, inclusive, quanto aos riscos identificados nas operações de tratamento de dados pessoais[7].

Ainda sobre as formas através das quais a alta administração pode apoiar o Programa de Compliance em Proteção de Dados, destacamos:

Demonstrar compromisso pessoal: A alta administração deve demonstrar compromisso pessoal com a conformidade, cumprindo as políticas e procedimentos de conformidade da organização e agindo com integridade em todas as suas decisões.

Estabelecer políticas e procedimentos de conformidade: A alta administração deve definir as expectativas de conformidade e criar políticas e procedimentos claros e bem documentados para garantir que todos na organização entendam o que é esperado.

Investir em treinamento de conformidade: A alta administração deve assegurar que todos na organização recebam treinamento adequado sobre as políticas de conformidade, a proteção de dados pessoais e as leis e regulamentos aplicáveis. Isso pode incluir treinamentos presenciais ou *online* e deve ser atualizado regularmente para refletir as mudanças nas leis ou regulamentos.

7. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). LGPD: Lei geral de proteção de dados comentada. São Paulo: Revista dos Tribunais, 2019.

Promover uma cultura de conformidade: A alta administração deve criar uma cultura em que a conformidade é valorizada e incentivada em toda a organização. Isso pode incluir recompensar os funcionários pelo cumprimento das políticas de conformidade e punindo aqueles que as violam.

Não obstante o poder de decisão da alta administração, é essencial que liderança nomeada para as funções de encarregado tenha autonomia e acesso às instâncias superiores, a fim de que possa desempenhar as suas funções de forma mais imparcial e independente o possível, viabilizando o bom desenvolvimento do Programa de Compliance em Proteção de Dados.

1.2. Gestão adequada de riscos

Uma das formas mais conservadoras de gerir os riscos é a implementação de boas práticas ou protocolos a serem seguidos por toda a organização. Para tanto, é fortemente recomendável a adoção de uma abordagem consistente na análise sistêmica, incluindo, mas não se limitando ao:

1.3. Levantamento das áreas de negócio

Etapa relevante que viabiliza a compreensão do modelo de negócio, o mercado que a organização está inserida, público-alvo, processos que envolvem dados pessoais, fluxo e ciclo de vida dos dados, bem como a identificação dos ativos de tecnologia da informação e estrutura dos departamentos de Compliance, Jurídico, Segurança da Informação, Comercial, Recursos Humanos e Marketing.

1.4. Registro das Operações de Tratamento de dados pessoais

Documento obrigatório que deve ser mantido por controladores e operadores, nos termos do artigo 37 da LGPD, viabilizando o mapeamento dos possessos, fluxos e ciclo de vida dos dados pessoais e o arbitramento de base legal adequada.

1.5. Apontamento de eventuais riscos regulatórios, de segurança da informação e à privacidade

Esta etapa permite que a organização compreenda suas potencialidades e fraquezas no que tange as suas capacidades de proteção de dados pessoais,

segurança da informação e privacidade, que passa essencialmente por conhecer as melhores práticas internacionais exigidas pelo mercado, a legislação e as regulamentações setoriais, bem como os riscos à privacidade e liberdades individuais do titular, o que permitirá o conhecimento do nível de maturidade de seus processos, indicador que deve ser considerado no ecossistema de gerenciamento de riscos.

1.6. Definição de plano de ação

Para essa etapa, é necessária uma colaboração entre as equipes jurídica, de privacidade e de tecnologia da informação, que trabalharão juntas para identificar as medidas a serem adotadas pela organização, em compliance com a LGPD, leis setoriais e melhores práticas internacionais adotadas pelo mercado. Essas práticas podem incluir, mas não se limitam a:

Elaboração de Avaliação de Impacto à Proteção de Dados Pessoais: documento preliminar, não obrigatório e sem previsão expressa na LGPD, que objetiva avaliar a necessidade de elaboração do Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"). Em síntese, consiste em medida de boas práticas que visa à descrição da atividade de tratamento, tanto da perspectiva contextual, quanto técnica e na definição de critérios baseados na natureza, contexto e finalidade do tratamento de dados pessoais. Ao encerrar a avaliação, caso não seja indicado a elaboração de RIPD, é recomendável a elaboração de justificativa que fundamente a ausência de impacto relevante aos direitos e liberdades fundamentais dos indivíduos.

Elaboração de Teste do Legítimo Interesse: ainda que não se trate de obrigação legal expressa na LGPD, recomendamos a elaboração do LIA — (*Legitimate Interests Assessment*), quando da atribuição da base legal do legítimo interesse. O teste possui 4 fases delineadas a seguir: **i) Legitimidade (Art. 10, *Caput* e Inciso I, da LGPD):** esta fase conta com o juízo de valor do controlador e / ou terceiros, objetivando descrever o contexto real em que se dará o tratamento e finalidade legítima de utilização dos dados pessoais; **ii) necessidade (10, §1º, da LGPD):** o controlador demonstrará se o tratamento se dá de forma adequada, necessário, ou seja, se os dados pessoais tratados são estritamente para atingir a finalidade pretendida, e se outras bases legais poderiam se enquadrar na operação; **iii) balanceamento (Art. 6º, I, 7º, IX, e art. 10, II, da LGPD):** nesta fase, o controlador demonstrara que há legítima expectativa, que se traduz pela compatibilidade do tratamento realizado com as

expectativas do titular de dados pessoais; e **iv) salvaguardas (10, §2º e §3º da LGPD):** fase final, em que serão descritas as medidas necessárias para garantia dos direitos dos titulares, como medidas de transparência, direito de oposição e medidas de mitigação dos riscos (pseudonimização, entre outras). Não há formato padrão para realização do LIA. No entanto, é recomendável que a organização documente o teste, gerando evidências de que a empresa tem processos adequados de tomada de decisão, demonstrando, assim, o interesse do controlador em prever riscos e aplicar o maior número possível de ações que busquem salvaguardar e proteger os titulares, mitigando potenciais riscos do tratamento.

Elaboração de Relatório de Impacto à Proteção de Dados Pessoais[8]: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco[9]. O Relatório de Impacto à Proteção de Dados Pessoais visa identificar e minimizar os riscos à proteção de dados pessoais que objetiva a realização de uma análise sistemática e abrangente da atividade de tratamento, a fim de demonstrar a diligência e a transparência no tratamento dos dados pelo Controlador.

Conforme os artigos 10, §3º, e 38, da LGPD, a Autoridade Nacional de Proteção de Dados ("ANPD") poderá solicitar que o controlador elabore relatórios de impacto à proteção de dados, referente a suas operações de tratamento, inclusive de dados sensíveis. Ainda que o dispositivo legal não especifique a necessidade de confecção de RIPD para todas as operações, por demonstração de boa-fé e medida que oferece maior segurança jurídica, recomenda-se que os Controladores elaborem tais documentos. Nesse contexto, toda operação, baseada no legítimo interesse e / ou que possua risco de violação aos princípios dispostos no artigo 6º da LGPD deverá ser acompanhada de RIPD.

A experiência europeia baseada no *General Data Protection Regulation* ("GDPR") nos traz diretrizes sobre operações que podem vir a apresentar riscos aos direitos dos titulares. O art. 35 do GDPR determina que o *Data Protection Impact Assessment* ("DPIA") será necessário quando o tratamento represen-

8. Este tema carece de regulamentação por parte da Autoridade Nacional de Proteção de Dados – ANPD.

9. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jan. 2023.

tar risco para direitos e liberdades e utilizar tecnologias inovadoras, sempre levando em conta sua natureza, âmbito, contexto e finalidade. O GDPR determina ainda, que a elaboração do DPIA será obrigatória quando envolver: *i)* tratamento automatizado; *ii)* definição de perfis; *iii)* operações em grande escala e controle sistemático de zonas acessíveis ao público.

Além disso, a diretriz WP 248 do Article 29 Working Party[10], que foi endossada posteriormente pelo European Data Protection Board ("EDPB")[11], estabelece diversas situações que justificam a elaboração de um DPIA, incluindo: perfilamento, tratamento automatizado, monitoramento sistemático, tratamento sobre dados sensíveis, tratamento em larga escala, tratamento sobre dados de pessoas vulneráveis, uso de tecnologia inovadora, transferência internacional de dados e operações que podem restringir direitos de um titular de dados[12].

As recomendações do Information Commissioner's Office ("ICO")[13] são igualmente relevantes e estabelecem que um DPIA deve ser realizado antes do início de qualquer tipo de processamento que possa resultar em um risco elevado. Além disso, o ICO orienta os agentes de tratamento a considerarem as diretrizes europeias relevantes, como o WP 248, que define nove critérios de operações de processamento que podem resultar em um alto risco.

A ICO também exige que o agente de tratamento faça um DPIA se planeja: usar tecnologia inovadora (em combinação com qualquer um dos critérios das diretrizes europeias); usar perfis ou dados de categoria especial para decidir sobre o acesso aos serviços; traçar perfis de indivíduos em grande escala; processar dados biométricos (em combinação com qualquer um dos critérios das diretrizes europeias); processar dados genéticos (em combinação com qualquer um dos critérios das diretrizes europeias); combinar dados ou combinar conjuntos de dados de diferentes fontes; coletar dados pessoais de uma fonte

10. Grupo de trabalho independente que tratou de questões relacionadas com a proteção da privacidade e dos dados pessoais até a entrada em vigor do GDPR.

11. Endorsement 1/2018. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 2017. Disponível em https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf. Acesso em 30.abr.2023.

12. Article 29 WP 248 – Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236/en. Acesso em 30. abr. 2023.

13. Avaliações de Impacto e proteção de dados. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em 30.abr.2023.

diferente do indivíduo sem fornecer a eles um aviso de privacidade (em combinação com qualquer um dos critérios das diretrizes europeias); rastrear a localização ou o comportamento dos indivíduos (em combinação com qualquer um dos critérios das diretrizes europeias); criar perfis de crianças ou direcionar marketing ou serviços online para elas; processar dados que possam colocar em risco a saúde física ou a segurança do indivíduo em caso de violação de segurança; ou qualquer outro processamento que seja em larga escala, envolva criação de perfil ou monitoramento, decida sobre o acesso a serviços ou oportunidades ou envolva dados confidenciais ou indivíduos vulneráveis[14]

Recentemente a ANPD, disponibilizou em seu sítio eletrônico uma nova página destinada a esclarecimentos sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), com 15 (quinze) perguntas e respostas sobre o tema[15]. A iniciativa tem como objetivo orientar os controladores de dados pessoais a agir em prol da segurança dos dados dos titulares sob sua responsabilidade.

Entre os principais pontos abordados, destaca-se a responsabilidade do controlador pela elaboração do RIPD antes de iniciar o tratamento de dados pessoais, a possibilidade de divulgação do relatório e a recomendação de consulta ao Encarregado. Além da Autoridade facultar aos controladores a escolha do formato e a estrutura do RIPD, desde que a análise dos fatores de risco seja documentada e justificada. Também é destacado o dever de encaminhar o RIPD apenas quando solicitado pela ANPD e a recomendação de adoção da Resolução CD/ANPD nº 2 [16] para a conceituação de alto risco.

> **Adoção de controles internos:** Os controles internos são mecanismos, formalizados por meio de políticas e procedimentos da organização que minimizam riscos operacionais e de compliance, sobretudo, assegurando que as políticas reflitam as operações da organização. Consideram-se controles internos eficientes aqueles que conferem à Alta administração a segurança, em certa medida, que: **i)** os objetivos das operações da organização estão sendo alcançados; **ii)** os relatórios financeiros são confiáveis; e **iii)** as leis e regulamentos aplicáveis estão sendo cumpridos.

---

14. INFORMATION COMMISSIONER'S OFFICE. Data Protection Impact Assessments. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em 30.abr.2023.

15. RELATÓRIO DE IMPACTO. ANPD divulga página com perguntas e respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Disponível em:https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-pagina-com-perguntas-e-respostas-sobre-o-relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em 30.abr.2023.

16. BRASIL. RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - DOU - Imprensa Nacional.

> ***Privacy by design e by default***: conceito desenvolvido por Ann Cavoukian[17], nos anos 90, que se propôs a abordar os crescentes e sistêmicos efeitos das Tecnologias de Informação e Comunicação (TICs) e dos sistemas de dados em rede em larga escala. A Privacidade desde a concepção, *by design*, promove a visão de que o futuro da privacidade não pode ser assegurado apenas pelo cumprimento de estruturas regulatórias. Em vez disso, a garantia da privacidade deve idealmente se tornar o modo de operação padrão, *by default,* de uma organização.

O *Privacy by default* propõe a implementação de medidas técnicas e organizacionais apropriadas para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento18. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Além disso, o conceito reúne 7 princípios, a saber: i) medidas protetivas e não reativas; ii) privacidade por default; iii) privacidade sob design; iv) funcionalidade completa; v) segurança de ponta a ponta; vi) visibilidade e transparência; e vii) respeito à privacidade do usuário.

> **Gestão de Terceiros:** gestão de riscos de fornecedores é meio de eliminação, redução e / ou controle dos impactos às ameaças relacionadas à cadeia de suprimentos da organização. Entre os tipos de risco envolvendo fornecedores destacamos, para fins deste artigo, os legais, de compliance, reputacionais e de segurança da informação.

Importante mencionar que em eventual due diligence de fornecedores a organização deve se atentar quanto à forma de análise, armazenamento, coleta, compartilhamento, eliminação, processamento, adotada por terreiros quando do tratamento de dados pessoais, sendo recomendável a coleta de evidências quanto às políticas e procedimentos adotados. Construir confiança digital alinhada a uma forte visão de segurança, integridade, privacidade de dados, gerenciamento de riscos, governança, qualidade, garantia, resiliência

---

17. CAUVOKIAN, Ann. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Disponível em: Privacidade por Design (PbD): Os 7 Princípios Fundamentais – Cavoukian (psu.edu). Acessado em 31.12.2022

18. ABNT. ABNT NBR ISO/IEC 27701 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação. Associação Brasileira de Normas Técnicas, Rio de Janeiro, dez. 2019.

e ética são elementos fortes para o desenvolvimento de parcerias confiáveis à medida que as empresas continuam a estabelecer as bases para a transformação digital e a inovação[19]. Desse modo, investir em meios que viabilizem a gestão de terceiros é medida que se impõe.

Elaboração e/ou revisão de minutas contratuais, manuais e guia de boas práticas: Não obstante a definição de direitos, obrigações e responsabilidades pela lei, as finalidades precípua da realização de contrato é de instrumento de atribuição de responsabilidades e demonstração de boas práticas[20]. Na prática, é recomendável que a elaboração e/ou revisão contratual considere a análise de 3 (três) pontos: i) se há tratamento de dados pessoais em determinado contrato; ii) qual o papel desempenhado pelas partes, enquanto agente de tratamento (Controlador, Controlador conjunto, Controlador independente ou Operador); e iii) a definição das medidas adotadas para que o contrato atenda aos preceitos da LGPD, bem como a definição da cláusula ou anexo de privacidade adequado.

Implementação do canal de comunicação: de acordo com o artigo 18, da LGPD, o titular de dados pessoais tem os seguintes direitos: **i)** confirmação da existência de tratamento; **ii)** acesso aos dados; **iii)** correção de dados incompletos, inexatos ou desatualizados; **iv)** anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade a LGPD; **v)** portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; **vi)** eliminação dos dados pessoais tratados com o consentimento do titular exceto nas hipótese de cumprimento de obrigação legal ou regulatória, transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD, ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que os dados estejam anonimizados; **vii)** informação das entidades públicas e privadas com as quais o controlador realizou compartilhamento de dados; **viii)** informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e **ix)** revogação do consentimento. Deste modo, para viabilizar o aten-

19. Relatório sobre o estado da confiança digital de 2022. Disponível em: state-of-digital-trust-2022-report-final.pdf (isaca.org). Acesso em 31.12.2022

20. TEIXEIRA, Tarcísio; ARMELIN, Ruth M. G. F. Responsabilidade Civil e Ressarcimento de Danos por Violação às Regras Previstas na LGPD: Um cotejamento com o CDC. In: LIMA, Cíntia R. P. (Org.) Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, p. 297-326, 2020.

dimento às requisições do titular e/ou da Autoridade Nacional de Proteção de Dados, é recomendável a implementação de canal de atendimento gratuito e de fácil acesso, que viabilize contato com o Encarregado de Dados, que nos termos do artigo 5º, VIII é pessoa indicada para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a ANPD.

Plano de Respostas a Incidentes: documento que visa detalhar as ações a serem tomadas no gerenciamento de incidentes ou suspeita de incidentes. Deve contar com mecanismos que garantam o acionamento da equipe de respostas a incidentes, grupo consultivo e colaborativo previamente definido para atuar na gestão de incidentes de segurança. De acordo com a estrutura de segurança cibernética proposta pelo *National Institute of Standards and Technology* - NIST[21], um plano de respostas a incidentes deve conter os seguintes tópicos[22]: Planejamento de respostas, comunicações, análise, mitigação, melhorias.

1.7. Políticas e Procedimentos

O sucesso de um programa de *Compliance* em Proteção de Dados passa pelo estabelecimento de uma estratégia de privacidade e proteção de dados pessoais, o que se dará através da construção e implementação de políticas e normas.

As políticas criam um sistema de princípios e normas, enquanto as normas criam procedimentos de comando e controle que oferecem instruções claras e inequívocas que norteiam as decisões dos colaboradores quanto às melhores práticas de proteção de dados pessoais.

De acordo com a LGPD e melhores práticas internacionais sobre o tema, as principais políticas que compõem o programa são: i) aviso de Privacidade, ii) Política de Privacidade; iii) Política de Cookies; iv) Política de Segurança da Informação e normas de apoio, como controle e segregação de acesso, BYOD, uso de mensagens instantâneas e redes sociais, dentre outras; v) Política de Retenção de Dados; vi) Política e Procedimento de Direitos dos Titulares de

21. NIST. National Institute of Standards and Technology.

22. NIST. National Institute of Standards and Technology (2020) Privacy Framework, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). Disponível em https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018pt.pdf. Acessado em 31. dez.2022.

Dados, vii) Política de *Privacy by Design*; viii) Política de *Due Diligence* em Proteção de Dados em Fornecedores, dentre outras.

Por fim, é importante mencionar que as políticas mencionadas somente serão implementadas através da divulgação, treinamento e conscientização contínua de toda organização.

1.8. Treinamento e conscientização

Medida educativa prevista nos artigos 41, § 2º, e 50, *caput*, da LGPD, o treinamento e conscientização contínua de toda a organização é ferramenta relevante para a implementação do Programa de Compliance em Proteção de Dados.

É relevante destacar a necessidade de processos contínuos de treinamento para que o time de colaboradores esteja sempre pronto e preparado para administrar situações que envolvam o tema de proteção de dados pessoais.

Para a implementação eficaz de uma cultura de proteção de dados pessoais é importante tornar os colaboradores verdadeiros aliados, e o caminho mais indicado para obtenção deste resultado é através das iniciativas de treinamento como seminários, campanha de divulgação, carta do presidente, entre outras.

1.9. Monitoramento e avaliação

O Programa de Compliance em Proteção de Dados é um processo contínuo. Desta forma, é preciso planejar e reavaliar periodicamente a eficácia das políticas e controles implementados. Uma das melhores formas de avaliação da eficácia do programa é a auditoria, que objetiva determinar o grau de conformidade da tecnologia, dos processos e das pessoas com as políticas e práticas de proteção de dados.

A auditoria pode, ainda, medir a eficácia dos procedimentos de segurança da informação, privacidade e proteção de dados pessoais, demonstrar a conformidade, aumentar o nível de conscientização sobre o tema e revelar eventuais lacunas e fornecer um embasamento para o planejamento de remediação.

A auditoria também é aplicável para a gestão de mudanças, quer seja por inobservância, atualização e/ou manutenção das políticas e/ou sistemas de suporte a operação, quer seja pela ocorrência de eventos e/ou violações a proteção de dados pessoais, solicitação dos órgãos reguladores, novos fornece-

dores, novas linhas de negócios, entre outros.

Para as hipóteses de não conformidade, os casos devem ser documentados, evidenciados e comunicados aos *stakeholders*, demonstrando os riscos, os planos de remediação e os custos associados para a efetiva implementação das melhorias.

Considerações Finais

Vive-se, nos últimos tempos, o ápice da economia de dados no Brasil e no mundo. Diante da complexidade do cenário, em que os processos de inovação dão o tom, cada vez mais, demanda-se das organizações uma estratégia permanente para promover a proteção e o uso ético dos dados pessoais.

O tratamento inadequado ou ilegal dos dados pessoais podem culminar em incidentes de segurança e afetar a reputação, as finanças, as operações e os ativos das organizações.

Neste contexto, o desenvolvimento de um Programa de Compliance em Proteção de Dados Pessoais mostra-se fundamental para a minimização dos riscos e impactos inerentes ao negócio, proporcionando às organizações a oportunidade de usufruírem plenamente de todos os benefícios decorrentes dos avanços tecnológicos.

Referências

ABNT. ABNT NBR ISO/IEC 27701 – **Técnicas de segurança** — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação. Associação Brasileira de Normas Técnicas, Rio de Janeiro, dez. 2019.

Article 29 WP 248 – ***Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679***. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236/en. Acesso em 30. abr. 2023.

Avaliações de Impacto e proteção de dados. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.Acesso em 30.abr.2023.

Baldin, Paulo e Cilurzo, André. **Avaliação de riscos e mapeamento de dados**, 2020, São Paulo, artigo, 102-108. In: Apostila de Curso de Compliance em Proteção de Dados. Coordenação de Alessandra Gonçalves, Gianfranco Fogaccia Cinelli e Tae Young Cho.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jan. 2023.

BRASIL. **Decreto nº 11.129/2022 que regulamenta a Lei n.º 12.846/2013**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm. Acesso em 31.dez.2022.

BRASIL. **RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022** - DOU - Imprensa Nacional.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2ª Ed., 2021.

CAUVOKIAN, Ann. ***Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices***. Disponível em: Privacidade por Design (PbD): Os 7 Princípios Fundamentais – Cavoukian (psu.edu). Acessado em 31.12.2022

Endorsement 1/2018. ***Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679***. 2017. Disponível em https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf. Acesso em 30.abr.2023.

INFORMATION COMMISSIONER'S OFFICE. ***Data Protection Impact Assessments***. Disponívelem:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em 30.abr.2023.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018, p. 21.

MALDONADO, Viviane Nóbrega. **A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação**. Lei Geral de Proteção de Dados Pessoais: manual de implementação. São Paulo: Revista dos Tribunais, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD: Lei geral de proteção de dados: comentada**. São Paulo: Revista dos Tribunais, 2019.

NIST. ***National Institute of Standards and Technology (2020) Privacy Framework, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD)***. Disponível em https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018pt.pdf. Acessado em 31.dez.2022.

RELATÓRIO DE IMPACTO. **ANPD divulga página com perguntas e respostas sobre o relatório de impacto à proteção de dados pessoais (RIPD)**. Disponível em: https://www.

gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-pagina-com-perguntas-e-respostas-sobre-o-relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em 30.abr.2023.

RELATÓRIO - **ESTADO DA CONFIANÇA DIGITAL DE 2022**. Disponível em: state-of-digital-trust-2022-report-final.pdf (isaca.org). Acesso em 31.dec.2022.

RODOTÀ, Stefano. **Palestra**. Tradução de Myriam de Filippis. Disponível em: http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoeoDireito.pdf. Acesso em: 13 jul. 2022.

TEIXEIRA, Tarcísio; ARMELIN, Ruth M. G. F. **Responsabilidade Civil e Ressarcimento de Danos por Violação às Regras Previstas na LGPD: Um cotejamento com o CDC**. In: LIMA, Cíntia R. P. (Org.) Comentários à Lei Geral de Proteção de Dados. São Paulo: Almedina, p. 297-326, 2020.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

10

Reconhecimento facial e torcidas: uma análise dos riscos e medidas de proteção de dados

ANA CLARA GONÇALVES FLAUZINO

ANA CLARA GONÇALVES FLAUZINO[1]

Sumário: Introdução. 1. Reconhecimento Facial e motivação para sua utilização. 2. Riscos e medidas protetivas necessárias à proteção de dados. 3. Normatização do tema na Lei Geral de Proteção de Dados. Considerações finais. Referências.

Introdução

O reconhecimento facial é uma tecnologia que se baseia no mapeamento e processamento de dados biométricos da face através da identificação de padrões semelhantes entre a imagem capturada e aquelas presentes nos bancos de dados utilizados como base. Conforme Teffé e Fernandes[2], a maior parte das tecnologias de reconhecimento facial modernas trabalham basicamente, por meio de dois passos: (I) registro (*enrollment*) e (II) correspondência ou reconhecimento (*matching*). Essa ferramenta tem sido progressivamente desenvolvida e aplicada no Brasil em diversos locais e contextos, que abrangem desde a segurança pública até a iniciativa privada, como no metrô de São Paulo, nas ruas de Copacabana, bairro da cidade do Rio de Janeiro e no Estádio Allianz Parque, de propriedade da Sociedade Esportiva Palmeiras.

Fato é que, em que pese os diversos benefícios que ela provê, há sérios riscos atrelados ao seu uso, que devem ser considerados durante todo o processo de sua aplicação. Dada a velocidade no desenvolvimento tecnológico e a ainda existente ausência de familiaridade com a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/18) por parte dos agentes de tratamento e dos próprios titulares de dados, o emprego da tecnologia em comento tem sido permeado por problemáticas.

No dia sete de dezembro de 2022, a Sociedade Esportiva Palmeiras divulgou em seu site[3] a instalação de sistema de reconhecimento facial nas entradas do seu clube social. Anteriormente, ainda em 14 de novembro de 2022,

1. Advogada. Bacharel em Direito pela Universidade Federal Fluminense (UFF). Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio), em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro).

2. TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O Direito civil na era da inteligência artificial. 1ª. ed. São Paulo: Thomson Reuters Brasil, 2020. cap. 15, p. 283-315.

3. Palmeiras instala sistema de reconhecimento facial em entradas do clube social. São Paulo: Departamento de Comunicação, 7 dez. 2022. Disponível em: https://www.palmeiras.com.br/noticias/palmeiras-instala-sistema-de-reconhecimento-facial-em-entradas-do-clube-social/. Acesso em: 12 jan. 2023.

conforme notícia divulgada no mesmo portal[4], a presidente do Palmeiras, Leila Pereira, declarou que o objetivo do clube era ter a tecnologia disponível para entrada no estádio até o fim de janeiro de 2023.

Em que pese o tom inovador, o Palmeiras não é o primeiro a utilizar dados sensíveis para viabilizar o ingresso de torcedores no estádio. Em 2017, antes mesmo da entrada em vigor da Lei Geral de Proteção de Dados brasileira, o Athletico Paranaense já havia implementado o uso de catracas com sistema biométrico para todo o público que frequentava a Arena da Baixada, estádio de propriedade do mencionado clube[5].

Do lado de fora dos campos, o Estado do Rio de Janeiro já operacionalizava o uso de reconhecimento facial nas intermediações do estádio do Maracanã no ano de 2019[6], destacando-se, neste último local, a realização de 11 detenções durante uma partida de futebol, dentre as quais sete revelaram-se falsos positivos[7].

Sendo certo que para o funcionamento do reconhecimento facial é necessário tratar dados biométricos, torna-se essencial a adequação dos agentes de tratamento à Lei Federal nº 13.709/18 ("LGPD"), especialmente porque tal classe de dado é considerada, pela Lei, como sensível.

Logo, dada a relevância do mencionado tratamento e de sua progressiva disseminação, bem como a contemporânea aplicação desta tecnologia, é fundamental investigar quais são os riscos atrelados ao seu uso, especialmente dentro dos estádios, e as possíveis medidas de proteção de dados a serem tomadas pelos agentes de tratamento.

Reconhecimento facial e motivação para sua utilização

O uso de biometria para reconhecer pessoas é histórico. Em 1894 Alphon-

---

4. Leila reforça importância do Avanti para títulos e projeta reconhecimento facial em 2023. São Paulo: Departamento de Comunicação, 14 nov. 2022. Disponível em: https://www.palmeiras.com.br/noticias/leila-reforca-importancia-do-avanti-para-titulos-e-projeta-reconhecimento-facial-em-2023/. Acesso em: 12 jan. 2023.

5. Biometria na Arena da Baixada completa um ano e vira referência: Para coibir e inibir a violência, o Atlético-PR agiu por conta própria, investiu em infraestrutura e colocou em prática serviço pioneiro no Brasil: a biometria. LANCE!, Curitiba/PR, 10 set. 2018. Disponível em: https://www.lance.com.br/atletico-paranaense/biometria-arena-baixada-completa-ano-vira-referencia.html. Acesso em: 11 abr. 2023.

6. SILVA, Mariah Rafaela; NUNES, Pablo; OLIVEIRA, Samuel R. de. Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. 26 p. ISBN 978-85-5969-014-9. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 11 abr. 2023.

7. Idem

se Bertillon já utilizava impressões digitais como meio de complementar a identificação humana[8]. A tecnologia de reconhecimento facial, em especial, tem raízes que alcançam a década de 1960,

> quando uma empresa chamada Panoramic Research Inc., em Palo Alto, Califórnia, realizava investigações financiadas pelo Departamento de Defesa dos Estados Unidos, além de outras agências de inteligência, em um contexto de busca pela superioridade tecnológica na Guerra Fria.[9]

Porém, em que pese o histórico de mais de 50 anos de desenvolvimento, é sabido que tal meio tecnológico ainda está se aperfeiçoando, uma vez que seu mecanismo de operação é complexo e enseja a avaliação de diversas variáveis, como os riscos a ela atrelados e os bancos de dados utilizados como base para seu funcionamento.

A autoridade britânica Information Commissioner's Office (ICO) divulgou em 26 de outubro de 2022 o relatório "Biometrics: insight", no qual traz uma análise do que entende como biometria, com olhar técnico para além da definição trazida pelo Regulamento Geral de Proteção de Dados do Reino Unido. Conforme a ICO[10], em tradução livre, a biometria pode ser dividida em dois aspectos: a biometria rígida (*hard biometrics*) e a biometria suave (*soft biometrics*). A primeira diz respeito a características fisiológicas, como padrões faciais, impressões digitais, padrão de orelha e análise vascular, que não mudam com o passar do tempo, salvo quando há lesão ou incapacitação. Por sua vez, a segunda se refere a aspectos fisiológicos e psicológicos, que podem ser mudados com o tempo, circunstância ou ambos, como, por exemplo, a análise de marcha: jovens caminham diferente de idosos.

Apesar da existência de diversas possibilidades de utilização de biometria, a tecnologia de reconhecimento facial se encontra no centro do debate público brasileiro nos dias atuais, especialmente em razão do destaque tra-

8. SOUZA, Marcos Antonio de. A biometria e suas aplicações. Revista Brasileira de Ciências Policiais, Brasília, v. 11, n. 2, p. 79-102, mai/ago 2020. Disponível em: https://dspace.mj.gov.br/handle/1/7826. Acesso em: 11 abr. 2023.

9. GATES, Kelly. Our biometric future?, cit., p. 28, apud TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad. Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O Direito civil na era da inteligência artificial. 1a. ed. São Paulo: Thomson Reuters Brasil, 2020. cap. 15, p. 283-315. ISBN 978-65-5614-218-0.

10. INFORMATION COMMISSIONER 'S OFFICE (ICO) (Reino Unido). Biometrics: insight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf. Acesso em: 11 abr. 2023.

zido pela sua implementação no estádio Allianz Parque. Sobre essa forma de identificação biométrica, Teffé e Fernandes[11] explicam que

> A maior parte das tecnologias de reconhecimento facial modernas trabalham, basicamente, por meio de dois passos: (I) registro (*enrollment*) e (II) correspondência ou reconhecimento (*matching*). Essas fases podem ser divididas em quatro passos: captura, desconstrução, armazenamento e comparação, a depender da finalidade para a qual a tecnologia será utilizada.

Adicionalmente, ensinam Ferreira, Silva e Pinheiro[12] no projeto de bilheteria por reconhecimento facial por eles desenvolvido:

> O reconhecimento facial tem como base pegar uma foto de uma pessoa e extrair dados dessa foto. Desta forma, é bem comum o uso de matrizes, à álgebra linear, mas especificamente que consiste em reorganizar esses dados extraídos da foto em um vetor e assim colocando outros rostos temos uma matriz com esses vetores.

Em tradução livre, o *European Data Protection Board* (EDPB) define o reconhecimento facial como uma tecnologia probabilística que consegue reconhecer indivíduos automaticamente com base em sua face, a fim de autenticá-los ou identificá-los[13].

O processo é feito através de *software* específico, que "decompõe a imagem (rosto de uma pessoa) nas suas componentes vermelho, verde e azul, onde cada uma das cores é uma matriz 3x3. Em seguida ele cria uma imagem média das apresentadas, organizando os espaços vetoriais em olhos, nariz, boca, entre outros.". Resumidamente, após este processo o *software* refina os resultados, determinando relações de ausência ou presença de variáveis em relação aos dados inseridos, no caso, imagens. Ao fim, é gerada uma imagem média que será comparada com outras imagens, com o objetivo de encontrar semelhança ou diferença entre elas.

---

11. Idem

12. FERREIRA, Mitson D. G.; SILVA, Lucas V. F.; PINHEIRO, Jocivania. Proceeding Series of the Brazilian Society of Computational and Applied Mathematics. Projeto Ticket Face: Bilheteria por Reconhecimento Facial, [s. l.], p. 1-2, 2022. Disponível em: https://proceedings.sbmac.emnuvens.com.br/sbmac/article/view/3971/4021. Acesso em: 12 jan. 2023

13. EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2022. 49 p. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en. Acesso em: 11 abr. 2023.

Segundo o EDPB[14], a partir da imagem da face de um indivíduo, que se nomeia "amostra" biométrica, é possível extrair a representação de características distintas da face, chamadas de "modelo". Com isso, o processo de reconhecimento facial se realizaria em duas etapas: a coleta da imagem da face e sua transformação em modelo, seguida por seu reconhecimento e comparação do "modelo" com um ou mais "modelos".

Este fluxo pode ser automatizado através do aprendizado de máquinas ("*machine learning*"), fazendo com que, a partir do uso de inteligência artificial, a aplicação realize todo o processo de forma autônoma, cruzando dados e gerando resultados a partir de uma fonte pré-definida. Assim, a forma como o algoritmo é desenvolvido, desde a sua concepção até o acompanhamento de seu desempenho, é relevante. Se os dados inicialmente inseridos e os parâmetros definidos forem eivados de características discriminatórias, seus resultados (*outputs*) assim também serão.

Outrossim, se a avaliação dos possíveis resultados for precária, como se vê quando há ausência pela equipe desenvolvedora de problematização e antevisão de reprodução de estigmas sociais, os resultados provenientes da máquina poderão violar direitos fundamentais, acentuando discriminações e prejudicando as liberdades fundamentais.

Caso relevante que exemplifica falha na tecnologia de reconhecimento facial foi o vivenciado na segurança pública do Rio de Janeiro em 2019, nos entornos do estádio do Maracanã. Segundo o estudo desenvolvido no projeto "O panóptico", pelo Centro de Estudo de Segurança e Cidadania – CESeC[15], durante a segunda fase do projeto-piloto realizado no Rio de Janeiro foram utilizadas 95 câmeras para monitorar e vigiar indivíduos que eram procurados pela polícia. Durante uma partida de futebol, 11 pessoas foram detidas no entorno do Maracanã, sendo sete delas falsos positivos, ou seja, apenas três pessoas de fato possuíam mandado de prisão em aberto.

Outros casos de destaque foram a detenção indevida de uma mulher no

14. Idem

15. SILVA, Mariah Rafaela; NUNES, Pablo; OLIVEIRA, Samuel R. de. Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. 26 p. ISBN 978-85-5969-014-9. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 11 abr. 2023.

Rio de Janeiro, em 2019, através de identificação por reconhecimento facial[16] e, ainda, o impedimento do uso da tecnologia pelo Poder Judiciário no metrô da cidade de São Paulo por não atender a LGPD[17]. Em regra, as inovações tecnológicas surgem para solucionar um problema, melhorar algo que já existe ou criar uma nova realidade, de forma paulatina ou disruptiva. Nesse contexto, a implementação de tecnologias de identificação biométrica nos estádios de futebol teria como objetivo dar maior segurança aos frequentadores, seja através da identificação de pessoas condenadas pelo Poder Judiciário ou pela Justiça Desportiva ou da probidade na aquisição dos ingressos para assistir às partidas.

A exemplo, a Sociedade Esportiva Palmeiras afirma ter enfrentado, ao longo dos últimos anos, problemas com cambistas que "utilizavam o programa de sócio torcedor para vender ingressos de forma irregular para os jogos do time como mandante"[18], estes ocorridos no Allianz Parque.

Diante disso, o clube alega ter encontrado como solução utilizar o reconhecimento facial para entrada em seu estádio, realizando testes anteriormente a tal liberação, como a implementação da tecnologia no clube social[19] e eventos teste, tais como acesso a jogos-treino[20]. Ciente dos riscos atrelados ao uso da mencionada tecnologia, o Palmeiras divulgou uma série de perguntas e respostas[21] para esclarecer ao torcedor de que forma a adaptação seria realiza-

16. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano: Secretaria reconheceu o erro e lamentou o fato. Segundo a corporação, a pessoa foi levada para a delegacia, onde foi confirmado que não se tratava da criminosa procurada. [S. l.]: G1 Rio, 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 12 jan. 2023.

17. Metrô de SP inicia operação de sistema de reconhecimento facial; TJ chegou a impedir instalação: De acordo com entidades que entraram com ação, sistema não atendia aos requisitos legais previstos na Lei Geral de Proteção de Dados, entre outros. O sistema custou o total de R$ 58 milhões e utilizará cerca de 5 mil câmeras de monitoramento quando estiver 100% implementado. Por ora, 18 estações da Linha 3-Vermelha receberam 1.381 câmeras. [S. l.], 21 nov. 2022. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtml. Acesso em: 12 jan. 2023.

18. Leila reforça importância do Avanti para títulos e projeta reconhecimento facial em 2023. São Paulo: Departamento de Comunicação, 14 nov. 2022. Disponível em: https://www.palmeiras.com.br/noticias/leila-reforca-importancia-do-avanti-para-titulos-e-projeta-reconhecimento-facial-em-2023/. Acesso em: 12 jan. 2023.

19. Palmeiras instala sistema de reconhecimento facial em entradas do clube social. São Paulo: Departamento de Comunicação, 7 dez. 2022. Disponível em: https://www.palmeiras.com.br/noticias/palmeiras-instala-sistema-de-reconhecimento-facial-em-entradas-do-clube-social/. Acesso em: 12 jan. 2023.

20. Exclusivo Avanti: palmeiras realiza primeiro evento-teste da biometria facial em jogo-treino no Allianz Parque. São Paulo: Departamento de Comunicação, 5 jan. 2023. Disponível em: https://www.palmeiras.com.br/noticias/exclusivo-avanti-palmeiras-realiza-primeiro-evento-teste-da-biometria-facial-em-jogo-treino-no-allianz-parque/. Acesso em: 12 jan. 2023.

21. Perguntas e respostas sobre o sistema de reconhecimento facial. São Paulo: Departamento de Comunicação, 5 jan. 2023. Disponível em: https://www.palmeiras.com.br/noticias/perguntas-e-respostas-sobre-o-sistema-de-reconhecimento-facial/. Acesso em: 12 jan. 2023.

da. No documento, informa que o titular deverá obrigatoriamente cadastrar sua face através de site próprio. Ainda, explica que crianças e idosos também deverão ter sua biometria cadastrada.

Relevante mencionar que não somente os torcedores do Palmeiras deverão realizar o processo de cadastro e ter sua biometria coletada. Também os torcedores visitantes, ou seja, aqueles que torcem para outros times e cujos jogos serão realizados no Allianz Parque. O Clube informa, ainda, que "todo e qualquer tratamento de seus dados pessoais pela SEP observará a Lei Geral de Proteção de Dados"[22] e indica contato para comunicar-se com o Encarregado de Dados da instituição. Além da seção de perguntas e respostas, o Time possui política de privacidade disponibilizada em seu portal eletrônico a qualquer usuário que o acesse. Para fins desta pesquisa, o documento foi acessado no dia 12 de abril de 2023.

Anteriormente, no ano de 2017, o Athletico Paranaense já havia iniciado o processo de implementação da entrada do público na Arena da Baixada, estádio que comporta até 42 mil pessoas em jogos de futebol[23], através de biometria, com coleta de impressões digitais. O Athletico também possui política de privacidade em seu site, consultada na mesma data supracitada, 12 de abril de 2023.

Fato é que o uso de reconhecimento facial não é uma exclusividade do Palmeiras. No ano de 2019, quando o Brasil sediou a Copa América, a Confederação Sul-Americana de Futebol (Conmebol) anunciou que o reconhecimento facial seria utilizado como medida de segurança nos estádios que receberiam as partidas da competição[24], sendo eles o Estádio do Morumbi (de propriedade do São Paulo Futebol Clube); a então NeoQuímica Arena, antiga Arena Corinthians (pertencente ao Sport Club Corinthians Paulista); a Arena Fonte Nova, localizada em Salvador, no estado da Bahia; o Maracanã, no estado do Rio de Janeiro; o Mineirão, situado em Belo Horizonte, no estado de Minas Gerais (de propriedade do Cruzeiro Esporte Clube) e a Arena do Grêmio, localizada em

22. Idem

23. Biometria na Arena da Baixada completa um ano e vira referência: Para coibir e inibir a violência, o Atlético-PR agiu por conta própria, investiu em infraestrutura e colocou em prática serviço pioneiro no Brasil: a biometria. LANCE!, Curitiba/PR, 10 set. 2018. Disponível em: https://www.lance.com.br/atletico-paranaense/biometria-arena-baixada-completa-ano-vira-referencia.html. Acesso em: 11 abr. 2023

24. Copa América 2019 terá reconhecimento facial em estádios brasileiros: O torneio, que vai de 14 de junho a 7 de julho, será o primeiro evento no país com este tipo de sistema de segurança. Placar, [S. l.], 25 abr. 2019. Disponível em: https://placar.abril.com.br/placar/copa-america-2019-tera-reconhecimento-facial-em-estadios-brasileiros/. Acesso em: 12 abr. 2023.

Porto Alegre, no estado do Rio Grande do Sul. Após a realização do evento, o reconhecimento facial foi mantido no Estádio do Morumbi[25], na NeoQuímica Arena[26], no Mineirão[27] e na Arena do Grêmio[28].

O que se vê, portanto, é uma grande motivação na implementação de funcionalidades para reconhecimento facial em mais estádios, principalmente através da iniciativa do poder público. No estado do Ceará, está em discussão pelo Ministério Público do Estado o uso da tecnologia na Arena Castelão[29], além de tramitar na Assembleia Legislativa do Estado do Ceará o Projeto de Lei nº 380/2023, de autoria do deputado David Durand, objetivando a "fiscalização do acesso das pessoas nos estádios de futebol, e, ao mesmo tempo evitar a presença de torcedores violentos, que estão impedidos de frequentar jogos de futebol"[30].

Atualmente, em sede nacional, o Projeto de Lei nº 10089/18 aguarda o parecer da Comissão de Constituição e Justiça e de Cidadania (CCJC), na Câmara dos Deputados. Ele visa alterar o Estatuto de Defesa do Torcedor "para obrigar a entidade responsável pela organização do evento a instalar aparelhos de identificação biométrica que identifiquem os torcedores impedidos judicialmente de frequentar estádios esportivos"[31], demonstrando que o debate

---

25. SÃO PAULO FUTEBOL CLUBE. Morumbi: um palco em constante evolução: Casa do Tricolor abre a Copa América recheada de modernizações importantes. São Paulo, 13 jun. 2019. Disponível em: http://www.saopaulofc.net/noticias/noticias/morumbi/2019/6/13/morumbi-um-palco-em-constante-evolucao. Acesso em: 12 abr. 2023.

26. OLIVEIRA, Maurício. Arena Corinthians e Morumbi terão reconhecimento facial também após a Copa América: Sistema será usado para impedir entrada de "barra-bravas" fichados e de torcedores com mandados de prisão decretados. O Globo, São Paulo, 14 jun. 2019. Disponível em: https://ge.globo.com/futebol/copa-america/noticia/arena-corinthians-e-morumbi-terao-reconhecimento-facial-tambem-apos-a-copa-america.ghtml. Acesso em: 12 abr. 2023.

27. DIRETORIA DE COMUNICAÇÃO INSTITUCIONAL – DIRCOM. Juizado do Torcedor do Mineirão inaugura reconhecimento facial: Três torcedores foram flagrados em atos ilícitos dentro e no entorno do estádio. Minas Gerais, 7 mar. 2022. Disponível em: https://www.tjmg.jus.br/portal-tjmg/noticias/juizado-do-torcedor-do-mineirao-inaugura-reconhecimento-facial.htm#.ZDcNy3ZBxD8. Acesso em: 12 abr. 2023.

28. ARENA PORTO-ALEGRENSE S.A. Política de Privacidade: política de privacidade e proteção de dados. Porto Alegre, jan. 2021. Disponível em: https://arenapoa.com.br/politicas-de-privacidade/. Acesso em: 12 abr. 2023.

29. ASSESSORIA DE IMPRENSA DO MINISTÉRIO PÚBLICO DO ESTADO DO CEARÁ. MPCE discute uso de reconhecimento facial para identificação de pessoas envolvidas em ilícitos na Arena Castelão. Ceará, 4 nov. 2022. Disponível em: http://www.mpce.mp.br/2022/11/mpce-discute-uso-de-reconhecimento-facial-para-identificacao-de-pessoas-envolvidas-em-ilicitos-na-arena-castelao/. Acesso em: 12 abr. 2023.

30. CEARÁ. Assembleia Legislativa. Projeto de Lei nº 380/2023, de 15 de março de 2023. Dispõe sobre a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios de futebol, ou eventos esportivos, e dá outras providências. Disponível em: https://www2.al.ce.gov.br/legislativo/tramit2023/pl380_23.htm. Acesso em: 12 abr. 2023.

31. BRASIL. Câmara dos Deputados. Projeto de Lei nº 10089, de 19 de abril de 2018. Altera a Lei nº 10.671, de 15 de maio de 2003, que dispõe sobre o Estatuto de Defesa do Torcedor, para obrigar a entidade responsável pela organização do evento a instalar aparelhos de identificação biométrica que identifiquem os torcedores impedidos judicialmente de frequentar estádios esportivos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2172779. Acesso em: 12 abr. 2023.

acerca da utilização de tecnologias de reconhecimento facial é urgente e necessário.

Riscos e medidas protetivas necessárias à proteção de dados

Verifica-se, portanto, que a percepção de riscos é indissociável do tema do tratamento de dados biométricos, especialmente no contexto do reconhecimento facial, ensejando a aplicação de medidas protetivas aos titulares de dados.

Considerando seu caráter imutável, salvo em exceções extremamente específicas, o dado biométrico resta vinculado ao titular por toda a sua vida, logo, qualquer violação a esses dados é inegavelmente danosa. A ICO[32] aponta três principais riscos no tratamento dessa espécie de dado, quais sejam: se houver uma perda, roubo ou uso inapropriado, o dado não pode simplesmente ser substituído; o potencial para conduzir a inferências imprecisas e inapropriadas; e quando há processamento de dados biométricos em conjunto com processamento algorítmico, há possibilidade de impacto por um viés sistêmico subjacente.

Adicionalmente, o EDPB[33] entende que o uso de tecnologias de reconhecimento facial, que usualmente utiliza componentes de inteligência artificial, traz também os riscos de discriminação e falsos resultados, gerando impacto negativo especialmente em minorias sociais.

No tema, Bioni e Luciano[34] destacam que:

> As incertezas quanto aos benefícios e os riscos pelo emprego de tecnologias de reconhecimento facial formaram uma arena regulatória efervescente, a qual está formatada em três eixos. O que lhes permite comparar é justamente carga de atribuição de obrigações precaucionárias diante das incertezas quanto aos benefícios

32. INFORMATION COMMISSIONER'S OFFICE (ICO) (Reino Unido). Biometrics: insight. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf. Acesso em: 11 abr. 2023.

33. EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. 2022. 49 p. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en. Acesso em: 11 abr. 2023.

34. BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?, Disponível em: https://brunobioni.com.br/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: 12 jan. 2023.

> e riscos em jogo decorrentes do emprego de tecnologias de reconhecimento facial.

Os três referidos eixos se localizariam, de um lado, na autorregulação; de outro, no banimento da tecnologia; e, ao centro, uma posição que defende o desenvolvimento da tecnologia com precauções e mitigação de riscos.

Nesse sentido, verificam-se como riscos relevantes, além dos anteriormente mencionados, a ausência de transparência com o usuário, possibilitando que tratamentos ilegais sejam promovidos, como o compartilhamento abusivo; o *output* de resultados maculados por preconceitos raciais e sociais, que ferem os direitos fundamentais dos titulares de dados; e a opacidade algorítmica, que afeta não só os titulares, mas toca também os próprios desenvolvedores. E, assim sendo, resta claro que ao implementar tal tecnologia é indispensável uma análise compromissada com os direitos dos titulares de dados, tomando-se todos os cuidados necessários para proteger seus direitos, inclusive, constitucionalmente garantidos.

Vale ressaltar, em complemento, a problemática da opacidade algorítmica. Conforme leciona Zuboff[35], vivemos na era do capitalismo de vigilância, no qual os hábitos humanos são rastreados, capturados e tratados como mercadoria, analisando-se o passado e predizendo o futuro. É nesse contexto que os agentes de tratamento utilizam seu poder enquanto classe dominante do sistema capitalista para atuar de forma obscura, principalmente ao usar algoritmos.

Nesse sentido, afirma Ana Frazão[36]:

> Cathy O'Neil chega a se referir aos algoritmos como armas matemáticas de destruição, na medida de que, longe de serem neutros e objetivos, embutem em seus códigos uma série de decisões e opiniões que não podem ser contestadas, até porque não são conhecidas. Daí o seu potencial de destruição silenciosa, na medida em que podem basear seus julgamentos em preconceitos e padrões passados que automatizam o status quo e ainda podem ser utilizados para toda sorte de discriminações e violações de direitos.

35. SHOSHANA, Zuboff. A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira de poder. 1ª. ed. Rio de Janeiro: Intrínseca, 2021. 823 p. ISBN 978-65-5560-145-9. E-book.

36. FRAZÃO, Ana; GOETTNAUER, Carlos. Black Box e o Direito Face à Opacidade Algorítmica. Direito Digital e Inteligência Artificial, [s. l.], p. 27-42, 2021. Disponível em: https://www.academia.edu/45811453/Black_Box_e_o_direito_face_%C3%A0_opacidade_algor%C3%ADtmica. Acesso em: 12 jan. 2023.

Por vezes, a opacidade é tão significativa que nem ao menos os próprios desenvolvedores das aplicações conseguem identificar o ponto causador da violação de direitos, impedindo-os de, caso necessário, realizar as modificações específicas para que tais danos sejam evitados ou remediados.

Torna-se pilar fundamental, portanto, a transparência. Sua ausência dá espaço para que agentes de tratamento mal-intencionados utilizem os dados para atingir objetivos ilícitos ou abusivos, impossibilitando ao titular sequer contestar as ações tomadas, uma vez que este muitas vezes desconhece a forma como os seus dados estão sendo tratados e, até mesmo, por quem eles estão sendo manejados.

Por isso, em que pese compreensível, se questiona se esta é, realmente, a maneira mais segura contra cambistas e menos arriscada sob o olhar da proteção de dados, tendo em vista o peso que o dado biométrico possui e que, em caso de vazamento de dados, o dano ao titular pode ser irreversível e inestimável, sendo certo que, a princípio, o dado biométrico não comporta a possibilidade de alteração, por estar vinculado a características fisiológicas de seu titular e, portanto, um incidente pode significar danos existenciais a ele. Deste modo, medidas protetivas devem ser tomadas pelos agentes que desejam implementar tal tecnologia nos estádios por eles geridos, observando os riscos atinentes a ela e as melhores práticas definidas pelas autoridades no tema.

Conforme já mencionado, promover a transparência ao titular de dados acerca de como seu dado biométrico será tratado é essencial. A informação deve estar clara, precisa e facilmente acessível, nos termos do artigo 6º, inciso VI, da Lei Geral de Proteção de Dados, viabilizando que o torcedor compreenda como seus dados serão tratados e, assim, opte por submetê-los ou não ao agente de tratamento, bem como frequentar ou não o estádio em questão.

Outro ponto de destaque é a coleta e tratamento de dados de crianças e adolescentes, que também poderão ser condicionados a cadastrar sua biometria para acessar os estádios. Aqui, é fundamental a presença de disposições específicas voltadas para tais sujeitos nas políticas de privacidade do gestor do estádio, uma vez que estes titulares são considerados indivíduos hipervulneráveis e devem ter sempre observado o seu melhor interesse, conforme dispôs a ANPD em seu Estudo Preliminar[37]:

37. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. Brasília, 25 p., 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: 12 abr. 2023.

> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da Lei Geral de Proteção de Dados (LGPD), desde que observado o seu melhor interesse, a ser avaliado no caso concreto, nos termos do caput do art. 14 da Lei.

Ademais, revela-se importante permitir que o torcedor tenha alternativas à coleta de dados biométricos pelo agente de tratamento, sendo-lhe garantido o direito ao lazer sem violar seus direitos de privacidade.

Adicionalmente, o detalhamento acerca da existência ou não do compartilhamento de dados deve ser fornecido ao titular de dados. Dados biométricos interessam a diversos agentes, principalmente quando se trata de políticas de segurança pública. Ante a ausência de regulação da proteção de dados voltada para a seara penal, a utilização de tais dados por instituições como as Polícias Civil e Militar ainda é nebulosa, contudo, tem sido fomentada por todo o Brasil. Logo, eventual compartilhamento entre o gestor do estádio em que há tecnologia de reconhecimento facial e as forças policiais, por exemplo, poderia configurar conduta abusiva, que ultrapassa os limites da finalidade para qual o titular forneceu seus dados, qual seja, ingressar no estádio para assistir a um jogo de futebol, além de ferir diretamente o preceituado pela Lei Geral de Proteção de Dados.

Ressalte-se que a LGPD prevê, no artigo 4º, inciso III, a sua inaplicabilidade ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Complementarmente, o §1º do artigo 4º da mesma Lei determina que

> O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei

Assim, considerando a inexistência de lei específica que verse sobre o tratamento de dados na esfera penal, a insegurança jurídica é notável, sendo improrrogável o preenchimento do vácuo legislativo. O Projeto de Lei nº

1515/2022[38] busca sanar o problema, criando a chamada "LGPD Penal", e ainda resta pendente de análise pelas comissões específicas da Câmara dos Deputados.

Outrossim, a ausência de informação sobre o tempo de retenção dos dados e forma de descarte destes também se mostra relevante, uma vez que o dado não deve ser armazenado por tempo indeterminado, sob risco de seu tratamento fugir à finalidade que este se propôs. Em adição, a manutenção de dados sem necessidade aumenta o risco em caso de incidentes de segurança e vazamentos, temas que aparentemente não encontram menção na referida Política. Sabe-se que esta é uma ameaça constante entre toda a comunidade que se conecta digitalmente, afetando desde os indivíduos enquanto pessoa natural até empresas privadas e o poder público. Nesse sentido, é de grande interesse do titular de dados ter conhecimento acerca de como a instituição que tratará seus dados se preocupa e atuará no caso de um incidente.

Não obstante, o alto volume de dados também deve ser salientado neste estudo. A exemplo, o Allianz Parque comporta cerca de 44 mil pessoas[39]. Logo, no caso de acesso aos jogos integralmente biometrizado, ou seja, utilizando-se do

Decerto, a iniciativa dos gestores dos estádio brasileiros e dos agentes públicos é interessante e objetiva garantir maior segurança ao espaço e aos torcedores. Contudo, percebe-se que esta é circundada por diversos riscos e exige que medidas de proteção sejam seriamente implementadas.

Normatização do tema na Lei Geral de Proteção de Dados

Matéria-prima para o funcionamento da tecnologia de reconhecimento facial, a biometria se destaca como dado cada vez mais utilizado. Sob o olhar da Lei Geral de Proteção de Dados, este é classificado como um dado pessoal sensível. Chiara de Teffé destaca que a Lei, apesar de trazer o rol supramencionado, não define expressamente o conceito de dado sensível. Para a autora, "entende-se que a identificação dos dados sensíveis pode variar a depender

38. BRASIL. Câmara dos Deputados. Projeto de Lei nº 1515 de 7 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022. Acesso em: 12 abr. 2023.

39. Palmeiras. Allianz Parque. Disponível em: https://www.palmeiras.com.br/allianz-parque/. Acesso em: 12 abr. 2023.

da forma como eles forem compreendidos em cada legislação e cultura."[40].

Sendo certo que o uso de dados biométricos é indispensável à operacionalização do reconhecimento facial, e que estes são considerados como dados sensíveis à luz da Lei Geral de Proteção de Dados, vide seu artigo 5º, inciso II, é inegável que exigem maior proteção.

Conforme leciona Teffé,

> Embora seja possível afirmar que alguns dados, especialmente em certos usos e contextos, sejam mais sensíveis que outros, historicamente, mostrou-se difícil encontrar consenso sobre quais tipos de dados deveriam ser considerados sensíveis e como os tratados e as legislações deveriam ser redigidos para protegê-los. [41]

Ainda, Bioni[42] entende que dados sensíveis podem ser conceituados como "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação". Nas palavras de Doneda[43],

> (...) seriam determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação.

Observando-se o contexto europeu, que muito influenciou na elaboração da norma brasileira de proteção de dados, percebe-se que o legislador estrangeiro optou por caracterizar tais tipos de dados como uma categoria especial. O Regulamento Geral de Proteção de Dados ("GDPR") traz, em seu artigo 9º, parágrafo primeiro, a proibição de tratamento de dados que revelem origem

---

40. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. Indaiatuba: Editora Foco, 2022. 304 p. ISBN 978-65-5515-582-2.

41. TEFFÉ, Chiara Spadaccini de. A categoria especial dos dados sensíveis: fundamentos e contornos. In: SCHREIBER, Anderson; FILHO, Carlos Edison do Rêgo Monteiro; OLIVA, Milena Donato (org.). Problemas de Direito Civil: Homenagem aos 30 anos de cátedra do Professor Gustavo Tepedino por seus orientandos e ex-orientandos. 1. ed. Rio de Janeiro: Forense, 2021. cap. 6, p. 97-123. ISBN 978-65-596-4205-2.

42. BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense, 10/2018 Apud MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Coluna Migalhas de Vulnerabilidade, [s. l.], 22 jun. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 25 jul. 2022.

43. DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2020. ISBN 978-65-5065-030-8.

racial ou étnica, opinião política, crenças religiosas ou filosóficas, filiação a sindicato, bem como o processamento de dados genéticos ou biométricos para o propósito único de identificar pessoa natural, dados concernentes a saúde ou dados relativos à vida sexual ou orientação sexual de pessoa natural. Em adição, é válido destacar o Considerando 51 do Regulamento, que dispõe, em seu primeiro item, que "os dados pessoais que são, pela sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais merecem proteção específica, pois o contexto do seu tratamento pode criar riscos significativos para os direitos e liberdades fundamentais"[44].

Especialmente quanto aos dados biométricos, o artigo 4º, item 14, do GDPR[45] os conceitua como

> dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos

Assim, entende-se que não somente câmeras de vigilância são instrumentos que levam ao reconhecimento facial, podendo as imagens serem usadas para este propósito e serem consideradas dados pessoais sensíveis, apesar de inicialmente não serem compreendidas desta maneira, consoante o Considerando 51 do GDPR[46], que entende que

> o tratamento de fotografias não deve ser sistematicamente considerado como tratamento de categorias especiais de dados pessoais, uma vez que são abrangidos pela definição de dados biométricos apenas quando tratados através de um meio técnico específico que permita a identificação ou autenticação única de uma pessoa singular.

44. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: General Regulation Data Protection (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 27 abr. 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 11 abr. 2023.

45. Idem

46. Idem

No tema, a ICO reforça o entendimento do GDPR[47], argumentando que estas não são automaticamente consideradas dados biométricos, logo, não seriam dados sensíveis, contudo, nos casos em que se utilizam processamentos técnicos específicos, a imagem pode adquirir caráter sensível.

Nesse sentido, a LGPD possui princípios norteadores de sua interpretação, que devem, por óbvio, orientar o destinatário da Lei, sendo ele agente de tratamento ou o próprio titular de dados. Estes estão dispostos no artigo 6º da referida legislação e são: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (*accountability*). Ao realizar o tratamento de dados o agente deverá levar todos estes princípios em consideração, sob risco de tomar medidas abusivas, ilegítimas ou ilegais, principalmente quando o dado envolvido for considerado sensível.

Para Mulholland, "dos princípios previstos, dois são de especial relevância quando do tratamento de dados sensíveis, quais sejam, o princípio da finalidade e o princípio da não discriminação" [48]. O primeiro refere-se à "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[49] e o segundo à "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos"[50].

Aqui, a divulgação de políticas de privacidade transparentes e inteligíveis pelo titular de dados mostra-se um instrumento fundamental à efetivação de direitos. A partir desta disponibilização, os princípios expostos na Lei Geral de Proteção de Dados encontram verdadeira aplicação, em especial os da finalidade e da transparência, provendo-se ao titular de dados informações verdadeiras e legítimas sobre como seus dados são tratados pelo agente em questão e asseguram que limites não serão ultrapassados quando do tratamento, sob pena do agente estar violando suas próprias políticas.

---

47. INFORMATION COMMISSIONER'S OFFICE (ICO) (Reino Unido). What is special category data?. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd1. Acesso em: 11 abr. 2023.

48. MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018.

49. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 abr. 2023.

50. Idem

O uso de ferramentas de *visual law* destaca-se como um grande aliado na operacionalização desta medida, possibilitando alcançar todos os públicos a quem se destinam as declarações fornecidas pela empresa. Quando se fala em dados sensíveis, a base legal para o tratamento encontra-se no artigo 11 da Lei 13.709/18. As hipóteses trazidas são a do consentimento pelo titular de forma específica e destacada; para cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário para execução, pela administração pública, de políticas públicas previstas em lei ou regulamento; para realização de estudos por órgãos de pesquisa; para exercício regular de direitos; para proteção da vida ou da incolumidade física; para tutela da saúde e para garantia da prevenção à fraude e à segurança do titular.

No caso em comento, percebe-se grande probabilidade de uso das bases legais do consentimento do titular ou de seu responsável legal "de forma específica e destacada, para finalidades específicas"[51], ou da garantia da prevenção à fraude e à segurança do titular para fundamentar a operacionalização do reconhecimento facial nos estádios. Na íntegra, o artigo 11, inciso II, alínea g[52], dispõe:

> garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Ademais, a Constituição Federal é mais um instrumento de proteção ao titular de dados, tendo em seu rol de direitos fundamentais, previsto pelo artigo 5º da Carta Magna, a proteção dos dados pessoais, nos meios físico e digital. Logo, não há dúvidas de que a observância de medidas protetivas deve ser tema de destaque dentro das organizações.

Destaque-se que, ainda que o agente de tratamento opte por não utilizar a base legal do consentimento para fundamentar o tratamento por ele realizado, tal fato não o isenta de dar publicidade às medidas de proteção e divulgar como e por que o tratamento é realizado, expondo as bases legais e finalidades legítimas que estão atreladas ao ato.

---

51. Idem

52. Idem

Adicionalmente, rememore-se que o tratamento de dados impõe ao agente de tratamento diversas obrigações, especialmente quando estes são considerados sensíveis. Dentre elas, a LGPD prevê que a Autoridade Nacional de Proteção de Dados ("ANPD") "poderá determinar ao controlador que elabore relatório de impacto, inclusive de dados sensíveis", nos termos do artigo 38 da Lei. A ANPD poderá, também, "considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis", dispor de padrões técnicos mínimos para tornar aplicáveis as "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", consoante o artigo 46 da LGPD.

No tema, destacam-se os ensinamentos de Teffé[53], que manifesta que:

Como forma de concretização da dignidade da pessoa humana, e figurando como direito da personalidade, a proteção de dados pessoais revela-se fundamental, sendo condição para que o sujeito se realize e de relacione em sociedade. Como apresentado, tutelar dados sensíveis e tratamentos de caráter sensível significa proteger a pessoa contra discriminações abusivas ou ilícitas, assegurar igualdade material no seu tratamento e permitir o livre desenvolvimento da sua personalidade, levando-se em conta suas diferenças e características particulares.

Logo, verifica-se que a proteção aos dados pessoais sensíveis encontra respaldo na legislação e na constituição brasileiras, devendo ser alvo de grande atenção dos agentes de tratamento, como é o caso dos gestores dos estádios brasileiros, como a Sociedade Esportiva Palmeiras e o Grêmio Foot-Ball Porto Alegrense.

Considerações finais

Conclui-se, portanto, a partir do caso concreto vivenciado atualmente em diversos estádios de futebol brasileiros, que o reconhecimento facial é uma tecnologia valiosa nos dias atuais, que traz benefícios, mas, ao mesmo tempo, apresenta riscos ao agente de tratamento e principalmente aos torcedores, titulares de dados.

53. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. Indaiatuba: Editora Foco, 2022.

O reconhecimento facial funciona através da programação de algoritmos que, a partir da inserção de dados, são capazes de gerar análises e consequentemente resultados. Os dados em questão são imagens, as quais, após a aplicação de métodos técnicos, tornam-se um dado biométrico e, portanto, um dado pessoal sensível, que adquire maior proteção jurídica pela norma de proteção de dados brasileira.

A proteção conferida aos dados pessoais sensíveis encontra justificativa, dentre outros fatores, em seu potencial discriminatório. Assim, os dados elencados no artigo 5º, inciso II, da Lei Geral de Proteção de Dados brasileira, quando não tratados com a devida diligência, podem gerar ao titular situações em que este correrá riscos de ser discriminado ilicitamente. Nesse sentido, garante-se maior proteção e exigem-se medidas mais cautelosas ao se tratar os referidos dados.

Assim, é preciso atentar-se não somente à base de dados utilizada como combustível ao algoritmo, mas também quais parâmetros de análise serão definidos e por quem o serão. Uma equipe diversa, constituída por pessoas de lugares, cores e gêneros diferentes, por exemplo, é extremamente benéfica ao desenvolvimento deste tipo de tecnologia, uma vez que a antevisão de possíveis problemáticas se torna muito mais palpável.

Verificou-se, a partir deste estudo, que é necessário que os gestores dos estádios realizem a implementação da tecnologia de reconhecimento facial de forma controlada, promovendo eventos teste e situações de mais fácil manejo, objetivando verificar o desempenho deste novo meio de acesso ao estádio, a exemplo do realizado pelo Palmeiras na entrada de seu clube social.

A ausência de disposições acerca do compartilhamento de dados, retenção, exclusão, ações em caso de incidentes de segurança e medidas protetivas voltadas para crianças e adolescentes não podem ser negligenciados, principalmente porque o projeto promovido nos estádios é ambicioso e contará com o tratamento de um alto volume de dados pessoais sensíveis.

Outrossim, é extremamente relevante que os agentes de tratamento tomem as medidas necessárias para tornar transparente ao titular de dados a forma como a tecnologia a ser utilizada foi desenvolvida e será aplicada, de modo a não gerar um meio capaz de causar danos ao torcedor, os quais, por vezes, são irreversíveis.

O caminho à compreensão plena do funcionamento dos sistemas de inteligência artificial ainda é longo e, talvez, infindável. Contudo, é essencial que os agentes de tratamento se comprometam a realizar as melhores práticas

de modo a utilizar tal tecnologia de forma saudável e sustentável. Assim, com a observância de todas as medidas de proteção e cuidados, casos como o da Sociedade Esportiva Palmeiras poderá servir de parâmetro a ser seguido pelos demais clubes do Brasil, transformando a tecnologia, antes ameaça, em aliada.

Referências

ARENA PORTO-ALEGRENSE S.A. **Política de Privacidade: política de privacidade e proteção de dados**. Porto Alegre, jan. 2021. Disponível em: https://arenapoa.com.br/politicas-de-privacidade/. Acesso em: 12 abr. 2023.

ASSESSORIA DE IMPRENSA DO MINISTÉRIO PÚBLICO DO ESTADO DO CEARÁ. **MPCE discute uso de reconhecimento facial para identificação de pessoas envolvidas em ilícitos na Arena Castelão**. Ceará, 4 nov. 2022. Disponível em: http://www.mpce.mp.br/2022/11/mpce-discute-uso-de-reconhecimento-facial-para-identificacao-de-pessoas-envolvidas-em-ilicitos-na-arena-castelao/. Acesso em: 12 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. Brasília, 25 p., setembro 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em: 12 abr. 2023.

BASAN, Arthur Pinheiro; JÚNIOR, José Luiz de Moura Faleiros. **A tutela do corpo eletrônico como direito básico do consumidor**. Revista dos Tribunais, [s. l.], v. 1021, p. 133-168, novembro 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/ewp-m/documents/brazil/pt/pdf/other/rt-1021-a-tutela-do-corpo-eletronico-como-direito-basico-do-consumidor.pdf. Acesso em: 12 jan. 2023.

Biometria na Arena da Baixada completa um ano e vira referência: Para coibir e inibir a violência, o Atlético-PR agiu por conta própria, investiu em infraestrutura e colocou em prática serviço pioneiro no Brasil: a biometria. LANCE!, Curitiba/PR, 10 set. 2018. Disponível em: https://www.lance.com.br/atletico-paranaense/biometria-arena-baixada-completa-ano-vira-referencia.html. Acesso em: 11 abr. 2023.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada?**, Disponível em: https://brunobioni.com.br/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: 12 jan. 2023.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 10089, de 19 de abril de 2018. Altera a Lei nº 10.671, de 15 de maio de 2003, que dispõe sobre o Estatuto de Defesa do Torcedor, para obrigar a entidade responsável pela organização do evento a instalar aparelhos de identificação biométrica que identifiquem os torcedores impedidos judicialmente de frequentar estádios esportivos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2172779. Acesso em: 12 abr. 2023.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 1515 de 7 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022. Acesso em: 12 abr. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jan. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 abr. 2023.

CEARÁ. Assembleia Legislativa. **Projeto de Lei nº 380/2023, de 15 de março de 2023**. Dispõe sobre a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios de futebol, ou eventos esportivos, e dá outras providências. Disponível em: https://www2.al.ce.gov.br/legislativo/tra-

mit2023/pl380_23.htm. Acesso em: 12 abr. 2023.

Copa América 2019 terá reconhecimento facial em estádios brasileiros: O torneio, que vai de 14 de junho a 7 de julho, será o primeiro evento no país com este tipo de sistema de segurança. Placar, [S. l.], 25 abr. 2019. Disponível em: https://placar.abril.com.br/placar/copa-america-2019-tera-reconhecimento-facial-em-estadios-brasileiros/. Acesso em: 12 abr. 2023.

DIRETORIA DE COMUNICAÇÃO INSTITUCIONAL – DIRCOM. **Juizado do Torcedor do Mineirão inaugura reconhecimento facial: Três torcedores foram flagrados em atos ilícitos dentro e no entorno do estádio**. Minas Gerais, 7 mar. 2022. Disponível em: https://www.tjmg.jus.br/portal-tjmg/noticias/juizado-do-torcedor-do-mineirao-inaugura-reconhecimento-facial.htm#.ZDcNy3ZBxD8. Acesso em: 12 abr. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2ª. ed. rev. e atual. São Paulo: Thomson Reuters Brasil, 2020. ISBN 978-65-5065-030-8.

EUROPEAN DATA PROTECTION BOARD. ***Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement***. 2022. 49 p. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en. Acesso em: 11 abr. 2023.

Exclusivo Avanti: palmeiras realiza primeiro evento-teste da biometria facial em jogo-treino no Allianz Parque. São Paulo: Departamento de Comunicação, 5 jan. 2023. Disponível em: https://www.palmeiras.com.br/noticias/exclusivo-avanti-palmeiras-realiza-primeiro-evento-teste-da-biometria-facial-em-jogo-treino-no-allianz-parque/. Acesso em: 12 jan. 2023.

FERREIRA, Mitson D. G.; SILVA, Lucas V. F.; PINHEIRO, Jocivania. ***Proceeding Series of the Brazilian Society of Computational and Applied Mathematics***. Projeto Ticket Face: Bilheteria por Reconhecimento Facial, [s. l.], p. 1-2, 2022. Disponível em: https://proceedings.sbmac.emnuvens.com.br/sbmac/article/view/3971/4021. Acesso em: 12 jan. 2023

FRAZÃO, Ana; GOETTNAUER, Carlos. **Black Box e o Direito Face à Opacidade Algorítmica. Direito Digital e Inteligência Artificial**, [s. l.], p. 27-42, 2021. Disponível em: https://www.academia.edu/45811453/Black_Box_e_o_direito_face_%C3%A0_opacidade_algor%C3%ADtmica. Acesso em: 12 jan. 2023.

INFORMATION COMMISSIONER'S OFFICE (ICO) (Reino Unido). ***Biometrics: insight***. Disponível em: https://ico.org.uk/media/about-the-ico/documents/4021972/biometrics-insight-report.pdf. Acesso em: 11 abr. 2023.

INFORMATION COMMISSIONER'S OFFICE (ICO) (Reino Unido). ***What is special category data?***. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd1. Acesso em: 11 abr. 2023.

Leila reforça importância do Avanti para títulos e projeta reconhecimento facial em 2023. São Paulo: Departamento de Comunicação, 14 nov. 2022. Disponível em: https://www.palmeiras.com.br/noticias/leila-reforca-importancia-do-avanti-para-titulos-e-projeta-reconhecimento-facial-em-2023/. Acesso em: 12 jan. 2023.

Metrô de SP inicia operação de sistema de reconhecimento facial; TJ chegou a impedir instalação: De acordo com entidades que entraram com ação, sistema não atendia aos requisitos legais previstos na Lei Geral de Proteção de Dados, entre outros. O sistema custou o total de R$ 58 milhões e utilizará cerca de 5 mil câmeras de monitoramento quando estiver 100% implementado. Por ora, 18 estações da Linha 3-Vermelha receberam 1.381 câmeras. [S. l.], 21 nov. 2022. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtml. Acesso em: 12 jan. 2023.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Coluna Migalhas de Vulnerabilidade, [s. l.], 22 jun. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 12 jan. 2023.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)**. Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018.

NEGRI, Sergio 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. 63-85, 2019.

NETTO, Milton Pereira de França; JÚNIOR, Marcos Ehrhardt. **Os riscos da discriminação algorítmica na utilização de aplicações de inteligência artificial no cenário brasileiro**. Revista jurídica luso-brasileira, Portugal, ano 8, n. 3, p. 1271-1318, 2022. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/3/2022_03_1271_1318.pdf. Acesso em: 12 jan. 2023.

OLIVEIRA, Maurício. **Arena Corinthians e Morumbi terão reconhecimento facial também após a Copa América: Sistema será usado para impedir entrada de "barra-bravas" fichados e de torcedores com mandados de prisão decretados**. O Globo, São Paulo, 14 jun. 2019. Disponível em: https://ge.globo.com/futebol/copa-america/noticia/arena-corinthians-e-morumbi-terao-reconhecimento-facial-tambem-apos-a-copa-america.ghtml. Acesso em: 12 abr. 2023.

Palmeiras. **Allianz Parque**. Disponível em: https://www.palmeiras.com.br/allianz-parque/. Acesso em: 12 abr. 2023.

Palmeiras instala sistema de reconhecimento facial em entradas do clube social. São Paulo: Departamento de Comunicação, 7 dez. 2022. Disponível em: https://www.palmeiras.com.br/noticias/palmeiras-instala-sistema-de-reconhecimento-facial-em-entradas-do-clube-social/. Acesso em: 12 jan. 2023.

Palmeiras instala sistema de reconhecimento facial em entradas do clube social. Site do Palmeiras: Departamento de Comunicação, 7 dez. 2022. Disponível em: https://www.palmeiras.com.br/noticias/palmeiras-instala-sistema-de-reconhecimento-facial-em-entradas-do-clube-social/. Acesso em: 12 jan. 2023.

Perguntas e respostas sobre o sistema de reconhecimento facial. São Paulo: Departamento de Comunicação, 5 jan. 2023. Disponível em: https://www.palmeiras.com.br/noticias/perguntas-e-respostas-sobre-o-sistema-de-reconhecimento-facial/. Acesso em: 12 jan. 2023.

SÃO PAULO FUTEBOL CLUBE. **Morumbi: um palco em constante evolução: Casa do Tricolor abre a Copa América recheada de modernizações importantes**. São Paulo, 13 jun. 2019. Disponível em: http://www.saopaulofc.net/noticias/noticias/morumbi/2019/6/13/morumbi-um-palco-em-constante-evolucao. Acesso em: 12 abr. 2023.

SHOSHANA, Zuboff. **A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira de poder**. 1ª. ed. Rio de Janeiro: Intrínseca, 2021. 823 p. ISBN 978-65-5560-145-9. E-book.

SILVA, Mariah Rafaela; NUNES, Pablo; OLIVEIRA, Samuel R. de. **Um Rio de câmeras com olhos seletivos: uso do reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022. 26 p. ISBN 978-85-5969-014-9. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 11 abr. 2023

SILVA, Tarcízio. **Racismo algorítmico em plataformas digitais: Microagressões e discriminação em código**. In: SILVA, Tarcízio (org.). Comunidades, Algoritmos e Ativismos Digitais: Olhares Afrodiaspóricos. São Paulo: LiteraRua,

2020. p. 121-137. ISBN 978-65-86113-01-3.

Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano: Secretaria reconheceu o erro e lamentou o fato. Segundo a corporação, a pessoa foi levada para a delegacia, onde foi confirmado que não se tratava da criminosa procurada. [S. l.]: G1 Rio, 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 12 jan. 2023.

SOUZA, Marcos Antonio de. **A biometria e suas aplicações**. Revista Brasileira de Ciências Policiais, Brasília, v. 11, n. 2, p. 79-102, mai/ago 2020. Disponível em: https://dspace.mj.gov.br/handle/1/7826. Acesso em: 11 abr. 2023.

TEFFÉ, Chiara Spadaccini de. **A categoria especial dos dados sensíveis: fundamentos e contornos**. In: SCHREIBER, Anderson; FILHO, Carlos Edison do Rêgo Monteiro; OLIVA, Milena Donato (org.). Problemas de Direito Civil: Homenagem aos 30 anos de cátedra do Professor Gustavo Tepedino por seus orientandos e ex-orientandos. 1. ed. Rio de Janeiro: Forense, 2021. cap. 6, p. 97-123. ISBN 978-65-596-4205-2.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. Indaiatuba: Editora Foco, 2022. 304 p. ISBN 978-65-5515-582-2.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad. **Tratamento de dados sensíveis por tecnologias de reconhecimento facial: proteção e limites**. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (coord.). O Direito civil na era da inteligência artificial. 1ª. ed. São Paulo: Thomson Reuters Brasil, 2020. cap. 15, p. 283-315. ISBN 978-65-5614-218-0.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: General Regulation Data Protection (Regulamento Geral sobre a Proteção de Dados)**. Bruxelas, 27 abr. 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 11 abr. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

11

Além da formalidade: as dificuldades reais na obtenção do consentimento válido à luz da LGPD

RAYANNE CONCEIÇÃO DE ALMEIDA SANTOS

RAYANNE CONCEIÇÃO DE ALMEIDA SANTOS[1]

Sumário: Introdução. 1. Consentimento: contextualização conceitual 2. Autodeterminação informativa e a sua relevância para o consentimento. 3. A coleta do consentimento e a real autonomia do titular. Considerações finais. Referências.

Introdução

Um dos principais objetivos da Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais (LGPD) é garantir ao titular (aquele a quem pertencem as informações) o real controle sobre seus dados pessoais. Nesse sentido, a legislação impõe aos agentes de tratamento (aqueles que fazem uso das informações pessoais), limites para sua atuação.

Considerando esse cenário, dentre as bases legais previstas nos artigos 7º e 11 da LGPD, a obtenção de consentimento do titular, em certos casos, tem sido colocada em posição de destaque pelo mercado, especialmente por possibilitar que a pessoa aja previamente ao tratamento de seus dados pessoais, de forma que só então estaria o controlador autorizado a atingir a finalidade para qual foi dado o consentimento.

O consentimento, além de ser obtido com atenção às exigências da LGPD, devendo ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, poderá ser revogado pelo titular a qualquer momento. Diante disso, há responsabilidades diretas ao coletá-lo, dentre elas a de se certificar de que o indivíduo compreende claramente o que está outorgando.

O presente trabalho busca demonstrar as dificuldades de se coletar o consentimento válido do titular, nos moldes atuais do mercado, pois se mostra raro que a metodologia vigente cumpra sua razão de ser, sendo pouco eficiente na prática e apresentando lacunas visíveis de aplicabilidade.

Para tanto, a pesquisa será organizada em três capítulos. Em um primeiro momento, serão abordados os conceitos iniciais e a contextualização necessária ao entendimento da temática. Após, será apresentado um breve histórico da concepção da autodeterminação informativa e a sua definição. Por último, serão elencados expressamente os motivos que trazem dificuldades para

1. Advogada. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro). Graduada em Direito pela UNESA (Universidade Estácio de Sá).

a coleta válida do consentimento, sendo apontados, inclusive, os Termos de Consentimento como um mecanismo a ser ressignificado e repensado, a fim de se promover a privacidade do titular e a proteção dos dados pessoais fornecidos.

1. Consentimento: contextualização conceitual

Muito embora não exista atualmente uma hierarquia de bases legais imposta pela legislação, interpreta-se que o consentimento foi, inicialmente, concebido para ser o principal fundamento para o tratamento de dados pessoais. Isso porque, em linhas gerais, entende-se o ato de consentir como um exercício do poder de escolha do titular entre aceitar ou recusar a utilização de seus dados.

Assim versava o anteprojeto que deu origem à Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais (LGPD)[2], ao destacar em seu art. 7º que "o tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular"[3]. As demais bases legais, segundo a lógica do anteprojeto, seriam usadas somente quando houvesse a dispensa do consentimento, colocando a autonomia do titular como centro das atividades de tratamento.

Esta linha de raciocínio não foi mantida pelo texto definitivo da LGPD, que equilibrou todas as possibilidades de uso das bases legais no mesmo nível de aplicabilidade. No entanto, ainda se observa uma centralidade da vontade do titular quando colocamos em voga os direitos à revogação do consentimento (art. 18, IX) e à oposição ao tratamento (art. 18, par. 2º).

Além do exposto, o inciso XII do artigo 5º da LGPD estabelece vários requisitos legais que devem ser atendidos para que o consentimento seja considerado válido, enfatizando a importância de uma permissão qualificada. Conforme o texto legal, o consentimento deve ser concedido de forma livre, ou seja, sem que haja qualquer tipo de coação ou pressão, além de ser informado, inequívoco e manifestado por meio de uma afirmação clara, em que o titular concorde com o tratamento de seus dados pessoais para uma finalidade es-

2. BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709/18, de 14 de agosto de 2018.

3. BRASIL. Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ). Anteprojeto da Lei Geral de Proteção de Dados Pessoais. Disponível em < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em 03 jan. 2023

pecífica. É permitido que o consentimento seja concedido por escrito, inclusive em meio eletrônico, ou por outro meio que demonstre a manifestação de vontade do titular, desde que seja possível comprovar que o titular o concedeu (Art. 8º da LGPD).

O legislador brasileiro não determinou o significado de "manifestação livre, informada e inequívoca", contudo, o EDPB (*European Data Protection Board*), órgão consultivo da União Europeia, traz referência explicativa:

> Para ser considerado livre, o consentimento deve ser dado sem coerção, e o titular dos dados deve ter uma escolha real e efetiva. Para ser considerado informado, o titular dos dados deve ser informado sobre a identidade do controlador de dados, as finalidades para as quais os dados serão processados, os tipos de dados que serão processados, o direito de retirar o consentimento, e as informações básicas sobre outras questões relevantes, como transferências internacionais de dados. Para ser inequívoco, o consentimento deve ser claro e afirmativo, e não pode ser inferido de silêncio, inatividade ou pré-seleção de opções [4]

Outrossim, mais especificamente de acordo com o Guia de Consentimento da EDPB (*Guidelines* 06/2021), o GDPR exige que o consentimento seja dado da seguinte forma:

> O consentimento deve ser dado livremente, de forma específica, informada e inequívoca, indicando os desejos do titular dos dados por meio de uma declaração ou ação afirmativa clara, pela qual ele ou ela concorda com o processamento dos dados pessoais relacionados a ele ou a ela. (tradução nossa)[5][6]

Em outras palavras, os três requisitos estão interligados, a "manifestação livre" deve implicar uma escolha real do titular dos dados, sendo desprovida

4. COMITÊ EUROPEU DE PROTEÇÃO DE DADOS (EDPB). *Guidelines 06/2021 on the application of Article 6(1)(b) of Regulation 2016/679 for processing of personal data in the context of provision of online services to data subjects*. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202105_article_6_1_b_online_services_en.pdf. Acesso em: 26 abr. 2023.

5. No original: "*The GDPR requires that consent is freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or he.*"

6. EUROPEAN DATA PROTECTION BOARD. *Guidelines on Consent under Regulation 2016/679, Version 2.0. 2020*. Disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-70/2020/guidelines-052020-consent-under-regulation-2016679_en.> Acesso em: 20 abr. 2023.

de obrigações acessórias ou condicionadas, com o condão de ensejar consequências ruins ao titular que não as desejar conceder. Além disso, se o titular não possuir informações suficientes para compreender com o que concorda ou se seu aceite for usado para fins diferentes do que foi consentido, não haverá de se falar em consentimento livre.

Nessa perspectiva, Bruno Bioni acrescenta:

> O adjetivo livre nos remete à ideia de uma ação espontânea que não é objeto de pressão, mas, pelo contrário, de livre-arbítrio caracterizado pela tomada de uma escolha em meio a tantas outras que poderiam ser feitas por alguém. Por isso, o ponto central do qualificador livre é investigar qual é o nível de assimetria de poder em jogo. Deve-se verificar qual é o "poder de barganha" do cidadão com relação ao tratamento de seus dados pessoais, o que implica considerar quais são as opções do titular com relação ao tipo de dado coletado até os seus possíveis usos. Em síntese, o "cardápio de opções" à disposição do cidadão calibrará o quão é o seu consentimento, na exata medida em que esse "menu" equaliza tal relação assimétrica.[7]

Caso o consentimento seja concedido por escrito, é necessário que seja destacado das demais cláusulas contratuais ou documentos, podendo ser utilizadas soluções textuais ou gráficas. No entanto, é preciso evitar a inclusão de autorizações superficiais, uma vez que essas serão consideradas nulas.

É o que reforça Chiara de Teffé e Gustavo Tepedino:

> Não se deve confundir a validade do consentimento, especialmente de seus requisitos formais, com a sua prova. Todavia, é aconselhável ao agente de tratamento que tenha registrado em documento escrito o consentimento dado pelo titular. Isso porque, como dispõe o art. 8º, §2º, da LGPD, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na lei, o que é influência direta do princípio da responsabilização e prestação de contas (art. 6º, X).[8]

7. BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2019. p. 197.

8. TEPEDINO, Gustavo; DE TEFFÉ, Chiara Spadaccini. O Consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil – RBDCivil , Belo Horizonte, v. 25, 2020, p.98. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/521/389/1918. Acesso em: 7 jan. 2023.

Percebe-se que o consentimento não deve ser tácito. Portanto, o silêncio não configurará aceite. Resta indubitável a importância de que o titular tenha compreensão sobre como e por qual motivo seus dados pessoais estão sendo tratados, para assim ter condições de consentir, mesmo porque a coleta de consentimento está condicionada à observância dos princípios elencados no art. 6º da LGPD, especialmente os da transparência e da finalidade. [9]

Por esse contexto, justifica-se o tema do presente trabalho. A legislação de proteção de dados traz regras de outorga do consentimento que, na prática, não vêm sendo cumpridas adequadamente. O que se vê, muitas vezes, é a banalização de termos de consentimento apresentados ao titular em formatos que cumprem requisitos técnicos, mas não alcançam seus objetivos ou, ainda, checkboxes que confirmam disposições não lidas.

2. Autodeterminação informativa e a sua relevância para o consentimento

Em se tratando de privacidade e proteção de dados pessoais, a autodeterminação informativa é, sem dúvidas, um dos princípios mais importantes a serem compreendidos. Sua definição integra os pilares fundamentais da LGPD, junto da necessidade de proteção à intimidade do cidadão titular dos dados.

O direito à autodeterminação informativa surgiu e se desenvolveu ao longo de décadas de jurisprudência alemã, sendo reconhecido de forma expressa no ano de 1983, em decisão proferida pelo Tribunal Constitucional Alemão, no processo referente ao recenseamento da população[10]. No caso mencionado, como em todo censo, o Poder Público tinha a intenção de inventariar a população por meio da coleta de dados pessoais, incluindo onde moravam e com quem viviam.

Nas palavras de Laura Schertel, o cerne do julgamento se encontrava no processamento dos dados pessoais requeridos pelo censo, senão vejamos:

9. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; [..] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

10. MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. Migalhas de Proteção de Dados, 30 out. 2022. Disponível em: < https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa.> Acesso em: 8 jan. 2023.

> O ponto de partida do acórdão é o processamento eletrônico de dados que, em virtude do moderno desenvolvimento tecnológico, possibilitou o processamento ilimitado, o armazenamento e a transmissão de dados pessoais em proporções até então desconhecidas. De acordo com o Tribunal, as novas condições tecnológicas e sociais requerem o desenvolvimento continuado da interpretação dos direitos fundamentais para garantir a proteção do indivíduo na sociedade da informação. [11]

Nota-se que a decisão do tribunal alemão também demonstra um progresso significativo na conceituação da privacidade, pois, ao longo da história, ela vem sendo entendida como direito do indivíduo, titular de dados, de controlar e autodeterminar suas informações pessoais[12]. Ressaltamos outra vez as palavras de Schertel:

> Na evolução do conceito de privacidade, a decisão do Tribunal Constitucional alemão, no julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 25-3-1982, é considerada uma referência. Nesse julgamento histórico, o Tribunal radicalizou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade e decidiu pela inconstitucionalidade parcial da referida lei, ao argumentar a existência de um direito à "autodeterminação informativa" (*informationelle Selbstbestimmung*) com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade, respectivamente, Art. 1, I, GG e Art. 2, I, GG.[13]

Fica claro que a autodeterminação informativa visa a promover a participação ativa do titular no processamento de seus dados pessoais, daí o porquê de a base legal do consentimento estar tão intimamente ligada ao seu conceito. Por outro lado, não há dúvidas quanto à superestima do consentimento em promover ao titular o controle total de seus dados pessoais, o que, na prática, muitas vezes, não é observado nos atuais formatos "li e concordo" aos quais os titulares são expostos.

---

11. MENDES, Laura S. F. Autodeterminação informativa: a história de um conceito. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 03 jan. 2023

12. "Historicamente, a proteção dos dados pessoais tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais: autodeterminação informacional". (BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2019. p. 28.)

13. MENDES, Laura S. F. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Edição do Kindle.

Sobre o tema, Bioni leciona:

> O principal vetor para alcançar tal objetivo é franquear ao cidadão o controle sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade.[14]

Importante ressaltar que atrelada a suposta autonomia do titular em consentir está a legitimidade das decisões sobre o tratamento de dados que o controlador recebe. Existe uma inegável posição de vulnerabilidade do titular, que nem sempre é totalmente protegida pelos requisitos formais do consentimento. Isso acontece porque, ao dar o aceite em termos, o titular expressa o consentimento sem reservas e, a partir de então, o controlador de dados pessoais tem autorização legítima para tratar informações. Conforme explicam Ruaro e Rodriguez:

> Se por um lado [no consentimento] está presente o caráter de autodeterminação, funcionando como condição de acesso à esfera privada [do indivíduo], também há o aspecto da legitimação propriamente dita quando da inserção de dados em algum tipo de mercado, seja ele qual for. Desvela-se, por estes argumentos, o problema do consentimento e seus matizes – autodeterminação e legitimação – no âmbito da proteção de dados pessoais, buscando sempre um equilíbrio entre ambos.[15]

Dessa forma, a autodeterminação informativa vai além do consentimento. É necessário que o titular conheça verdadeiramente os benefícios e possíveis malefícios no tratamento de seus dados pessoais e, ainda, que possa estabelecer os limites desse tratamento. Outrossim, faz-se necessário enfatizar que informar ao titular sobre a possibilidade de retirada do consentimento nada mais é do que o cumprimento de um dos requisitos de validade da outorga. É preciso que o indivíduo compreenda sobre a retirada e saiba os meios pelos

14. BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2019.

15. RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. Direito, estado e sociedade, Rio de Janeiro, n. 36, p. 178-199, jan/jun. 2010. Disponível em: <https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212 >. Acesso em: 08 jan. 2023.

quais poderá fazê-la antes de oferecer a autorização.

São questões como essas que insurgem questionamentos a respeito da forma como o consentimento é coletado atualmente. Diante dos itens abordados até o momento, mostra-se necessário pensar em alternativas para garantir a efetiva autodeterminação informativa e proteção de dados pessoais, assunto que será mais bem discutido no capítulo a seguir.

3. A coleta do consentimento e a real autonomia do titular

Os "termos de consentimento" representam a principal metodologia empregada por agentes de tratamento para coletar o consentimento dos indivíduos. O documento, normalmente, traz texto explicativo sobre quem são as agentes de tratamento, quais dados pessoais serão tratados, a finalidade da atividade, o contato do Encarregado e o canal para exercício dos direitos dos titulares.

O objetivo do presente artigo não é o de ignorar a importância de fornecer tais informações ao titular, mesmo porque, conforme abordado anteriormente, a transparência é não apenas um princípio da LGPD, mas uma obrigatoriedade para a validade do consentimento coletado. Porém, não se pode ignorar que esse documento muitas vezes apresenta lacunas e raramente atinge o proposto, sendo tão somente uma exigência legal.

Ana Frazão reforça que, mesmo havendo a possibilidade de retirar o consentimento oferecido de maneira não-clara, existiria uma assimetria informacional pela qual o agente de tratamento sempre estaria em posição de vantagem quanto à atividade de tratamento. Vejamos:

> Não deixa de ser uma ficção achar que os consumidores podem e irão barganhar por privacidade ou simplesmente deixarem de contratar quando entenderem que seus direitos não estão sendo assegurados (o chamado *opt out*). Pelo contrário, em contextos de ausência de rivalidade e em que a aceitação da política de privacidade é condição sine qua non para o acesso ao serviço (as chamadas cláusulas *take it or leave it*), a legitimidade do consentimento sempre será discutível, mesmo que ele tenha sido informado. Por essa razão, diante da assimetria informacional que parece ser insolúvel, indaga-se em que medida vale a pena ainda valorizar tanto

> o consentimento [...].[16]

Em primeiro lugar, temos como realidade prática a adoção de termos genéricos. O que se vê atualmente é uma padronização dos termos de consentimento, com redações idênticas ou poucas alterações para diferenciá-los uns dos outros. De forma sucinta, Ronaldo Macedo Júnior aborda como o indivíduo absorve grandes quantidades de informação:

> Segundo o paradigma econômico neoclássico, quanto maior o número de informações que um consumidor puder obter para orientar suas decisões, maior será seu grau de liberdade para realizar suas escolhas racionais. [...] Caberia, contudo, perguntar: Até que ponto o mero aumento de informação serve atualmente de elemento para a efetiva ampliação do poder decisório do consumidor, ou ainda, para aumento de sua consciência no momento em que atua no mercado? Estudos sobre o conceito de racionalidade limitada ("*bounded rationality*") e sobrecarga de informações ("*overload information*") têm evidenciado que a equação: maior informação = maior capacidade de decisão consciente (e portanto, livre) frequentemente não corresponde à realidade. [17]

Ademais, a forma padronizada de termos de consentimento ignora as diferenças de público do documento. Sabe-se que o nível de instrução dos titulares não será o mesmo, assim como cada pessoa tem níveis de educação acadêmica distintos na sociedade. Isso sem mencionar as pessoas com deficiência, que a depender da situação podem precisar de adaptações capazes de atender a sua necessidade.

Sobrevém de igual modo a granularidade do consentimento, sendo certo que este não deve ser coletado na forma do "*take it or leave it*" ou "tudo ou nada". Critica-se, portanto, o modelo de consentimento em massa, no qual os termos de consentimento com finalidades pouco transparentes são apenas apresentados e a manifestação do titular é coletada por meio de uma assinatura ou outro método de verificação, incluindo o uso de caixas de seleção.

Para ser coletado de forma granulada, o titular, em regra, deveria concor-

16. FRAZÃO, Ana. Objetivos e alcance da Lei Geral de proteção de dados e suas repercussões no direito brasileiro. Revista dos Tribunais, São Paulo, 2019 p. 124.

17. MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. Justitia, São Paulo, v. 61, n. 185/188, p. 245-259, jan./dez. 1999. Disponível em: <https://core.ac.uk/download/pdf/79074338.pdf>. Acesso em: 8 jan. 2023

dar separadamente com as atividades de tratamento, não estando o aceite de uma atividade condicionado ao aceite de outra. Na mesma linha de raciocínio, entendem Tepedino e Teffé:

> Regula-se, assim, a lógica binária das chamadas políticas de tudo ou nada (*take-it-or-leave-it choice*) em que o usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo. Não se trata apenas de consentir ou não, mas fundamentalmente da possibilidade de fazê-lo de forma livre, informada e racional, mesmo havendo desequilíbrio de forças entre os contratantes. Sabe-se que não são todos os sujeitos que têm a habilidade de negociar ou a possibilidade concreta de rejeitar a condição imposta nos termos de serviços e políticas de privacidade das plataformas. Assim, ao invés de realmente concordar com o uso dos próprios dados, o que se verifica na prática é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais. Dessa forma, mostra-se necessário realizar mudanças significativas tanto na maneira pela qual o consentimento é implementado nos termos e políticas, quanto no desenho e arquitetura das plataformas.[18]

Diante disso, é possível notar que para realmente possibilitar a autodeterminação informativa os termos de consentimento precisam ser pormenorizados para além da inserção de dados de identificação do titular nas minutas padronizadas, observando as suas particularidades caso a caso, organizando as informações de modo a facilitar sua compreensão.

O *visual law* seria uma técnica possível de ser implementada. A aplicabilidade de elementos visuais e, principalmente, de um design capaz de atender aos diversos tipos de público é cada vez mais latente e evidencia a recomendação de que as questões relacionadas à proteção de dados e privacidade não sejam cercadas de formalidades jurídicas e linguagem rebuscada, possibilitando o acesso à informação de forma igualitária.

Muitas vezes sem levar em consideração a experiência do usuário e a forma como ele recebe e compreende os termos que lê, as disposições que deveriam garantir transparência acabam representando um conjunto de parágrafos extensos e repetitivos, como ilustra Camila Telles:

---

18. TEPEDINO, Gustavo; DE TEFFÉ, Chiara Spadaccini. O Consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil – RBDCivil , Belo Horizonte, v. 25, p. 83-116, 2020. DOI 10.33242/rbdc.2020.03.005. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/521/389/1918. Acesso em: 7 jan. 2023.

> Experiências são claramente subjetivas, já que cada usuário tem uma diferente experiência ao usar um produto, serviço ou objeto. Isso acontece porque a experiência é influenciada por diversos fatores humanos (visão, capacidade de leitura, habilidade etc.) e fatores externos (temperatura, ambiente, horário do dia). Todas as vivências de uma pessoa com uma marca, produto ou serviço, seja no momento de compra ou no de uso, incluindo a parte emocional, são definidas como experiência do usuário.[19]

O *Privacy by Design*, ou seja, a privacidade desde a concepção é igualmente um aspecto a ser levado em conta, em se tratando da coleta de consentimento. Considerando a sua doutrina[20], todo novo produto deve ser orientado pelo viés da proteção de dados, facilitando o controle de dados pessoais pelo titular. É sabido que existem esforços a serem despendidos para o emprego dessas técnicas, todavia oferecer soluções sem inovação para problemas que envolvem tecnologia é um erro a ser evitado.

Em paralelo ao *Privacy by Design* está o *Privacy by Default*, cujas bases principiológicas estão interligadas, que nada mais é senão a privacidade como um padrão. Nas palavras de Rafael Zanatta:

> *Privacy by Design* é a tradução prática do respeito à privacidade desde o projeto de sistemas, redes, aplicativos e equipamentos, enquanto o Privacy by Default é a obrigatoriedade de estabelecimento de configurações de privacidade mais restritivas possíveis como parâmetro padrão em todo o ciclo de vida do produto ou serviço [21]

Assim, uma vez priorizada a privacidade, pode-se pensar em padrões de programação que, apesar de não solucionarem a tendência do indivíduo de ignorar leituras ditas como complexas, servem como tentativa de garantir um comportamento ativo. A demonstração de atuação energética por parte do titular é, inclusive, um realce fundamental trazido pelo ICO (*Information Commissioner's Office*), conforme se verifica no trecho destacado abaixo:

---

19. TELLES, Camilla. Experiência do usuário (user experience) e legal design. In: FALEIROS JÚNIOR, José Luiz de Moura; CALAZA, Tales (coord.). Legal design: teoria e prática. 2. ed. Indaiatuba: Foco, 2023, p. 231.

20. CAVOUKIAN, Ann. *Privacy by design: the 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada*, 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-sec.pdf. Acesso em: 24 abr. 2023.

21. ZANATTA, Rafael. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Revista dos Tribunais, 2019

> O consentimento deve ser livre, específico, informado e não ambíguo. Existem altos padrões para a obtenção do consentimento. O consentimento deve ser dado por meio de uma ação afirmativa clara e positiva. Isso significa que uma pessoa deve tomar uma ação ativa para dar seu consentimento, em vez de ter que retirar seu consentimento posteriormente. As empresas não podem usar caixas pré-marcadas ou qualquer outra forma de consentimento implícito. O consentimento deve ser documentado e incluir quem deu o consentimento, quando, como e para o quê.[22]

Exemplos de ações relacionadas ao aceite de termos, *Privacy by Design* e *Privacy by Default* são a anonimização de dados, a criptografia, ou até mesmo a coleta de assinatura com certificado digital, visto que para o usuário comum, existe certa seriedade atribuída a assinaturas, ao contrário do notado no caso de uma *checkbox*. Pelo entendimento de Sunstein:

> A conclusão é que, em matéria de privacidade na Internet, muito se depende da regra do padrão. Caso um navegador de internet torne padrão configurações que protegem a privacidade, o resultado será muito diferente daquele em que os indivíduos necessitem selecioná-las a cada acesso. Considere, por exemplo, a recente estrutura de escolha do Google Chrome. As pessoas podem selecionar "navegação anônima", mas ela não constitui a configuração padrão, e os usuários não podem facilmente torná-la padrão; a tecnologia não o facilita. Usuários precisam escolher selecionar a "navegação anônima" a cada acesso. Como resultado, as pessoas navegam anonimamente muito menos.[23] [24]

Em harmonia ao explicado por Sunstein, reforça-se que não há a expectativa de eliminar os riscos de coleta ineficaz de consentimento, visto que onde há tratamento de dados pessoais sempre haverá riscos, porém mitigar as falhas nítidas da metodologia empregada pelo mercado de dados atual é um compromisso legal e ético.

---

22. INFORMATION COMMISSIONER'S OFFICE (ICO). *Guidance on Consent*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/. Acesso em: 26 abr. 2023.

23. Do original: "*The upshot is that in the domain of privacy on the Internet, much depends on the default rule. If a web browser defaults people into privacy-protective settings, the outcomes will be very different from what they will be if people have to select privacy settings every time. Consider, for example, the recent choice architecture on Google Chrome. People are allowed to select "Incognito," but it is not the default, and users cannot easily make it into the default; the technology does not facilitate that. Users must choose to select "go Incognito" every time they log on. As a result, people go Incognito a lot less.*"

24. SUNSTEIN, Cass R. *Choosing not to choose: understanding the value of choice*. New York: Oxford University Press, 2015.

Considerações finais

O estudo em tela buscou expor o panorama das dificuldades em se coletar a real manifestação de vontade do titular de dados pessoais. Por todo o material demonstrado, concluiu-se que ressignificar os termos de consentimento atualmente difundidos e rever os padrões atuais no mercado digital representam evolução significativa no avanço da cultura de privacidade na internet.

A proteção de dados tem por característica exigir um acompanhamento cíclico e, portanto, é importante considerar a aplicabilidade prática dos métodos de tratamento dos dados pessoais para garantir segurança adequada ao titular. Ignorar essa consideração pode levar ao descumprimento de princípios e pilares que são essenciais à privacidade. Proporcionar meios eficazes de compreensão das informações faz parte da adequação das atividades de tratamento à legislação pertinente.

Constatou-se que existe um longo caminho a ser percorrido até que se alcancem as técnicas ideais de coleta, sendo improvável atingir perfeição, porém já existe tecnologia e recursos a serem implementados, inclusive arcabouço teórico de grande valia para viabilizar a compreensão do titular, expressar suas intenções verdadeiras e, por consequência, promover autodeterminação informativa.

Referências

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – A função e os limites do consentimento**. 1ª ed. Rio de Janeiro: Editora Forense, 2019. p. 197.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Lei nº 13.709/18, de 14 de agosto de 2018.

BRASIL. Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ). **Anteprojeto da Lei Geral de Proteção de Dados Pessoais**. Disponível em < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em 03 jan. 2023

CAVOUKIAN, Ann. ***Privacy by design: the 7 foundational principles***. Information and Privacy Commissioner of Ontario, Canada, 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-sec.pdf. Acesso em: 24 abr. 2023.

COMITÊ EUROPEU DE PROTEÇÃO DE DADOS (EDPB). ***Guidelines 06/2021 on the application of Article 6(1)(b) of Regulation 2016/679 for processing of personal data in the context of provision of online services to data subjects***. Disponível em: <https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202105_article_6_1_b_online_services_en.pdf>. Acesso em: 26 abr. 2023.

DIAS, Amanda Damasceno; SOARES, Luiz Henrique de Souza; COSTA, Marilia Ramos. **Consentimento na LGPD e os desafios para sua implementação: uma revisão sistemática da literatura**. Revista de Direito, Tecnologia e Inovação, v. 8, n. 1, p. 1-22, 2021. DOI: 10.5335/rdti.8.1.11758.

DRUMOND, Thomaz Carneiro. **LGPD e a administração pública: alguns desafios**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 27, n. 7119, 28 dez. 2022. Disponível em: https://jus.com.br/artigos/100332. Acesso em: 8 jan. 2023.

EUROPEAN DATA PROTECTION BOARD. ***Guidelines on Consent under Regulation 2016/679, Version 2.0***. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-70/2020/guidelines-052020-consent-under-regulation-2016679_en.> Acesso em: 20 abr. 2023.

FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de proteção de dados e suas repercussões no direito brasileiro**. Revista dos Tribunais, São Paulo, 2019 p. 124.

INFORMATION COMMISSIONER'S OFFICE. ***Guide to the General Data Protection Regulation (GDPR): Consent. 2018***. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/.> Acesso em: 24 abr. 2023.

INFORMATION COMMISSIONER'S OFFICE (ICO). ***Guidance on Consent***. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/. Acesso em: 26 abr. 2023.

MACEDO JÚNIOR, Ronaldo Porto. **Privacidade, mercado e informação**. Justitia, São Paulo, v. 61, n. 185/188, p. 245-259, jan./dez. 1999. Disponível em: <https://core.ac.uk/download/pdf/79074338.pdf>. Acesso em: 8 jan. 2023

MENDES, Laura S. F. **Autodeterminação informativa: a história de um conceito**. Rev. de Ciências Jurídicas Pensar, v. 25, n. 4, 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em 03 jan. 2023

MENDES, Laura S. F. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. – (Série IDP: linha pesquisa acadêmica). E-book. Edição do Kindle.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Migalhas de Proteção de Dados, 30 out. 2022. Disponível em: < https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significa-

do-da-autodeterminacao-informativa.> Acesso em: 8 jan. 2023.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade da informação**. Direito, estado e sociedade, Rio de Janeiro, n. 36, p. 178-199, jan/jun. 2010. Disponível em: <https://revistades.jur.puc-rio.br/index.php/revista-des/article/view/212>. Acesso em: 08 jan. 2023.

SILVA, Flávia Lages de Castro; MARTINS, Guilherme Magalhães. **Consentimento como base legal para o tratamento de dados pessoais: aspectos gerais e análise crítica à luz da LGPD**. Revista de Direito, Tecnologia e Inovação, v. 7, n. 2, p. 109-127, 2020. DOI: 10.5335/rdti.7.2.10492.

STEINMÜLLER, Wilhelm. ***Das informationelle Selbstbestimmungsrecht: Wie es entstanden ist und was man daraus lernen kann***, p. 17. Disponível em: <https://dipbt.bundestag.de/doc/btd/06/038/0603826.pdf>. Acesso em 07 jan. 2023

SUNSTEIN, Cass R. ***Choosing not to choose: understanding the value of choice***. New York: Oxford University Press, 2015.

TELLES, Camilla. ***Experiência do usuário (user experience) e legal design***. In: FALEIROS JÚNIOR, José Luiz de Moura; CALAZA, Tales (coord.). Legal design: teoria e prática. 2. ed. Indaiatuba: Foco, 2023, p. 231.

TEPEDINO, Gustavo; DE TEFFÉ, Chiara Spadaccini. **O Consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil – RBDCivil , Belo Horizonte, v. 25, p. 83-116, 2020. DOI 10.33242/rbdc.2020.03.005. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/521/389/1918. Acesso em: 7 jan. 2023.

UNIÃO EUROPEIA. **Guidelines on consent under Regulation 2016/679 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. 28 de novembro de 2017. Disponível em: <http:ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>. Acesso em: 06 jan. 2023.

ZANATTA, Rafael. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Revista dos Tribunais, 2019

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

12

A transferência internacional de dados pessoais e o consentimento: um olhar para o artigo 33, inciso VIII, da Lei Geral de Proteção de Dados

NICE SIQUEIRA DO AMARAL

NICE SIQUEIRA DO AMARAL[1]

Sumário: Introdução. 1. A Transferência Internacional de Dados Pessoais: contexto e definição. 2. O Consentimento. 3. O Consentimento aplicado na Transferência Internacional de Dados (LGPD, art. 33, VIII). Considerações finais. Referências.

Introdução

Por onde "andam" os seus dados pessoais? É com esse questionamento inicial que foram delimitados os objetivos do presente estudo. Tendo em vista o atual estágio de desenvolvimento tecnológico, é facilmente possível considerar que embora uma pessoa nunca tenha saído do espaço físico de uma nação, os seus dados, ao revés, tenham sido transportados para diversos países.

Sabe-se que a Lei Geral de Proteção de Dados (LGPD), ao disciplinar a matéria de privacidade e proteção de dados pessoais, buscou garantir aos titulares o exercício de seus direitos e promover mais controle sobre os seus próprios dados. Uma espécie de controle, cercada de amplos debates, é o consentimento do titular, que aparece na lei como uma das hipóteses que autoriza o tratamento de dados pessoais.

E como, num contexto em que as fronteiras virtuais não possuem limites territoriais aparentemente definidos, trazer mais controle para os indivíduos sobre o translado dos seus dados pessoais? Seria o consentimento uma forma viável para atingir esse controle? Qual a intenção do legislador ao prever essa hipótese no artigo 33, inciso VIII, da LGPD?

Buscando responder às indagações acima, essa pesquisa percorrerá as definições de transferência internacional de dados pessoais e consentimento, examinando-as em especial com o Regulamento Europeu de Proteção de Dados (*General Data Protection Regulation* - GDPR) e o arcabouço bibliográfico disponível. Ao final, a pesquisa discorrerá sobre a convergência desses dois institutos, resultando no exame do artigo 33, inciso VIII, da LGPD.

1. A Transferência Internacional de Dados Pessoais: contexto e definição

Considerando os avanços tecnológicos ocorridos desde a democratização

1. Advogada. Pós-Graduada em Direito Digital pelo ITS, em parceria com o CEPED/UERJ. Mestranda em Direito Internacional pelo Programa de Pós-Graduação em Direito da Universidade do Estado do Rio de Janeiro (UERJ).

do acesso à internet, por meio de equipamentos domésticos e *smartphones*, nota-se, de forma cada vez mais clara, modelos econômicos baseados no tratamento de dados[2] As formas de consumo pela sociedade vêm se mostrando as mais diversas possíveis, como, por exemplo, o cadastro em redes sociais de interação interpessoal, o armazenamento de dados em nuvem (*cloud service*), a tecnologia *blockchain* e as ferramentas que apresentam aplicações de inteligência artificial.

Nisso, as barreiras geográficas parecem não mais importar, visto que esse trânsito de informações se dá a nível global percorrendo e suscitando o aparato de diferentes jurisdições. Com impactos a nível político, econômico, social e cultural, mostrou-se necessária a regulamentação da transferência transfronteiriça de dados pessoais que garanta ao mesmo tempo a proteção necessária à privacidade dos dados pessoais dos indivíduos e o contínuo desenvolvimento tecnológico da humanidade.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define os "fluxos transfronteiriços de dados pessoais" como sendo as movimentações de dados pessoais através das fronteiras nacionais[3]. Em torno dessa situação, diversas legislações foram criadas ao redor do globo. No Brasil, a Lei Geral de Proteção de Dados (LGPD)[4] trouxe a disciplina da transferência internacional de dados em seu capítulo V, entre os artigos 33 a 36. Sabe-se que, como um todo, a lei pátria apresenta inequívoca influência da regulação europeia na matéria. E, no tópico em comento, essa influência é ainda maior, haja vista o interesse em ser o Brasil reconhecido pela União Europeia como "país de nível adequado" para transferência de dados oriundos do território europeu.

A título de exemplo, e considerando os vizinhos da América do Sul[5], países

---

2. Segundo artigo 5º, inciso I, da LGPD, dados pessoais são qualquer informação relacionada a pessoa natural identificada ou identificável;

3. OCDE. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 28/04/2023.

4. BRASIL. 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). D.O.U de 15/08/2018, pág. nº 59. Lei nº 13.853 de 08 de julho de 2019. D.O.U. de 09/07/2019, P. 1.

5. Até a presente data, a Comissão Europeia reconheceu as seguintes nações e localidades como adequadas para a transferência internacional de dados: Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido sob o GDPR e Uruguai. Ver mais em: COMISSÃO EUROPEIA. Adequacy decisions. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em 28/04/2023.

como a Argentina[6], que possui uma lei em matéria de proteção de dados pessoais desde 2000, e o Uruguai[7], cuja legislação análoga data de 2008, foram declarados adequados pela Comissão Europeia, estando assim aptos para receber dados pessoais da União Europeia sem garantias adicionais, enquanto o Brasil ainda não foi objeto de uma decisão de adequação[8].

Quando a LGPD ainda tramitava no Congresso Nacional, a Comissão Especial da Câmara dos Deputados divulgou um parecer[9], que atualmente remete ao artigo 45 do General Data Protection Regulation (GDPR)[10], trazendo de forma expressa que a diretiva europeia em vigor à época[11] não permitia a transferência internacional de dados para países que não possuíssem legislação que garantisse a mesma proteção dada pela Lei Europeia[12].

Indo mais além, o parecer fundamentou-se também no acordo existente entre os EUA e a União Europeia, conhecido como *Safe Harbour*, assinado em 2000 e sob a égide da Diretiva 95/46/EC, que estabelecia princípios visando a garantia da proteção dos dados pessoais nas relações comerciais e demais transações internacionais ocorrida entre eles. Em que pese as legislações setoriais ou estaduais e alguns projetos de lei sobre o tema[13], é notória a ausência de uma legislação geral em matéria de proteção de dados que vigore em todo território norte-americano. A solução encontrada foi reconhecer, por meio

---

6. ARGENTINA. Ley Nº 25.326/2000. Proteccion de los Datos Personales. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion. Acesso em: 28/04/2023 .

7. URUGUAI. Ley Nº 18.331/2008. Protección de Datos Personales y Acción de “habeas data” Disponível em: https://parlamento.gub.uy/documentosyleyes/leyes/ley/18331 . Acesso em: 28/04/2023.

8. Ver mais em:: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt. Acesso em 28/04/2023.

9. BRASIL. Comissão Especial da Câmara dos Deputados. Parecer ao Projeto de Lei Nº 4060/2012. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012. Acesso em 28/04/2023

10. PARLAMENTO EUROPEU. Regulamento (UE) 2016/679 de 27 de abril de 2016. relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia L 119/1.

11. Explica-se: A Diretiva 95/46/CE foi revogada pelo GDPR, que em relação ao presente tópico pouco inovou.

12. GDPR. Artigo 45o. Transferências com base numa decisão de adequação. 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.

13. A saber: Driver’s Privacy Protection Act (DPPA); Children’s Online Pivacy Protection Act (COPPA); Fair Credit Reporting Act (FCRA); Telemarketing Sales Rules (TSR); Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM); Health Insurance Portability and Accountability Act (HIPAA); Family Educational Rights and Privacy (FERPA); California Consumer Privacy Act (CCPA); New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD); Virginia Consumer Data Protection Act (CDPA); Colorado Privacy Act (CPA); Data Protection Act (2021).

desse acordo, que os EUA garantiam as proteções legais europeias quando o tratamento de dados pessoais provenientes da UE ocorresse em seu território.

Havia verdadeira discrepância entre a forma de tratamento dada aos EUA e aos demais países, visto que a regra é a adoção pela Comissão Europeia de uma decisão de adequação autorizando o fluxo de dados pessoais para fora do território europeu. Eis que, em 2013 houve a divulgação dos escândalos de espionagem envolvendo Edward Snowden, ex-agente da *National Security Agency* (NSA), responsável pelo alerta mundial envolvendo o uso de dados pessoais em programas de vigilância do governo norte-americano.

Em 2014, no caso conhecido como Schrems I, um cidadão austríaco postulou perante a autoridade de proteção de dados de seu país (*The Data Protection Commissioner*) diversos questionamentos envolvendo o tratamento de dados pessoais pela subsidiária do Facebook na Europa (Facebook Ireland Ltd), como o envio para a matriz (Facebook Inc), localizada nos Estados Unidos, e a conservação dos dados em servidores situados nesse país. Tratando-se, assim, de hipótese de transferência internacional de dados. Um ano após, o caso chegou à Corte de Justiça da União Europeia (CJEU), que ao analisar os argumentos trazidos no litígio, decidiu pela invalidação do *Safe Harbour*[14].

Em 2016, os EUA e a Comissão Europeia firmaram um outro acordo, dessa vez conhecido como *Privacy Shield*, estabelecendo tantos outros princípios e quesitos de proteção. Assim, as empresas e os organismos norte-americanos, aderentes ao acordo, estariam aptos a receber dados pessoais provenientes da União Europeia, sem a necessidade de autorizações suplementares por parte das autoridades de proteção de dados de cada um dos países-membros da União Europeia.

Novamente, o ativista Max Schrems (caso Schrems II) compareceu ao litígio anterior e suscitou que o Facebook suspendesse a transferência de dados pessoais aos EUA, visto que o arcabouço legislativo americano ainda não oferecia a proteção necessária, equiparável à Europeia, para a realização desse tratamento. Em 2020, a Corte da União Europeia decidiu pela invalidade do *Privacy Shield*[15] e, com isso, mais de 5 mil empresas aderentes ao acordo fo-

14. CORTE DE JUSTIÇA DA UNIÃO EUROPEIA (CJEU). Julgamento C362/14. Maximillian Schrems vs Data Protection Commissioner. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362. Acesso em 28/04/2023.

15. CORTE DE JUSTIÇA DA UNIÃO EUROPEIA (CJEU). Julgamento C-311/18. Data Protection Commissioner vs. Facebook Ireland Ltd e Maximillian Schrems. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62018CJ0311. Acesso em 28/04/2023.

ram impactadas[16].

Essa decisão, no entanto, foi além, e se manifestou sobre as cláusulas-padrão de proteção de dados (*standard contractual clauses – SCC*), pré-aprovadas pela Comissão Europeia e previstas no artigo 46 do GDPR. A Corte definiu que, para serem consideradas garantidoras de uma transferência internacional adequada, não seria suficiente a mera assinatura, havendo a necessidade do efetivo cumprimento dessas cláusulas na prática.

Nesse cenário, e reforçando que a LGPD se inspirou no regulamento europeu, deve-se olhar com mais atenção para a disciplina, em especial o artigo 33, inciso II, que também atrela a transferência internacionais à hipótese de existência de cláusulas contratuais padrão, [17], cujos modelos deverão ser disponibilizados pela ANPD. Observando o ocorrido, é incontestável que não basta a mera existência e assinatura de cláusulas-padrão, sem que haja o seu efetivo cumprimento prático e a garantia ao titular do controle e do acesso a informações claras e precisas sobre como os seus dados serão tratados.

Atualmente, mais precisamente no final de 2022, a União Europeia deu início à avaliação da decisão de adequação do quadro legal dos EUA (*Data Privacy Framework*), que abordará as questões levantadas pela CJUE no caso Schrems II. Assim, as transferências transatlânticas poderão contar com um arcabouço mais robusto envolvendo, entre outros, (i) limitações e salvaguardas relativas ao acesso de dados pelas autoridades públicas norte-americanas; (ii) mecanismos de resolução de litígios sobre violações de direitos; e (iii) revisões periódicas pela Comissão Europeia e fiscalização quanto a efetividade das medidas do framework[18]. Não obstante essas melhorias, alguns pontos de atenção foram enfatizados no parecer do Comitê Europeu para a Proteção de Dados (European Data Protection Board – EDPB), que ainda deverão ser avaliados pela Comissão Europeia em sua tomada de decisão[19].

---

16. Ver mais em https://www.privacyshield.gov/list. Acesso em 28/04/2023.

17. LGPD, Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos;(-grifos da autora)

18. COMISSÃO EUROPEIA. Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631. Acesso em 28/04/2023.

19. EDPB. EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain. Disponível em: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en Acesso em: 28/04/2023.

O Brasil, por sua vez, deve estar atento às discussões internacionais, tendo em vista o interesse em ser considerado, pela Comissão Europeia, como adequado para transferências de dados e sua tentativa de ingressar oficialmente na Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

A partir desse panorama, é preciso definir o que de fato vem a ser a transferência internacional de dados pessoais. A LGPD traz essa definição em seu artigo 5º, inciso XV, ao expor que transferência internacional de dados é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Esse conceito não é de todo perfeito, sendo por vezes impreciso. Logo, é necessário aprofundar a análise e diferenciar algumas situações que possam parecer confusas. É o caso, por exemplo, da diferenciação entre transferência e trânsito internacional de dados pessoais. Trazendo a lume essa distinção e citando orientações da ICO (*Information Commissioner's Office*), a autoridade de proteção de dados do Reino Unido[20], tem-se que:

> As regras de transferência se aplicam quando o destinatário é um controlador ou processador separado e legalmente distinto do remetente. O destinatário pode ser empresário individual, parceiro, empresa, companhia, autoridade pública ou outra organização, incluindo empresas distintas do mesmo grupo econômico.
> As regras de transferência não se aplicam quando o destinatário é um funcionário do remetente ou quando o remetente e o destinatário fazem parte da mesma pessoa jurídica, da mesma empresa.[21] (tradução livre)

Analisar essa situação revela o escopo territorial de aplicação da norma e as regras específicas de transferência internacional de dados[22]. Nisso, Luis

20. Válido mencionar que embora o Reino Unido tenha saído da União Europeia por meio do "Brexit", a Comissão Europeia se posicionou numa decisão de adequação sobre as transferências de dados para o seu território, demostrando que a legislação de proteção de dados da UE continua a ter influência nesse país. O GDPR foi mantido na legislação doméstica, sendo chamado de "GDPR do Reino Unido" Ver mais em: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html. Acesso em 28/04/2023.

21. No original: The transfer rules apply where the receiver is a separate controller or processor and legally distinct from the sender. The receiver can be a separate sole trader, partnership, company, public authority or other organisation, and includes separate companies in the same group. The transfer rules do not apply where the receiver is an employee of the sender, or the sender and receiver are part of the same legal entity, such as a company. In: ICO. International Transfers. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/. Acesso em 28/04/2023.

22. Para se aprofundar sobre o aparente conflito – ou uma necessidade de harmonização – entre o escopo (âmbito) territorial do GDPR (art. 3) e a aplicação das regras de transferência internacional de dados (capítulo V), ver: KUNER, Cristopher. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850. Acesso em 28/04/2023.

Prado Chaves, reflete o seguinte entendimento:

> Isso significa dizer, por exemplo, que, se para viabilizar a troca de e-mails entre diferentes áreas de uma organização 100% brasileira (no contexto de um tratamento de dados pessoais sujeito à LGPD), por uma questão meramente de infraestrutura tecnológica, dados pessoais transitam momentaneamente por um servidor localizado na Índia, tal atividade, por si só, não deveria ser considerada uma transferência internacional de dados àquele país.

Indo além, novamente traduzindo os entendimentos europeus do ICO à realidade brasileira, temos que o mero envio de dados pessoais por um controlador a seu próprio empregado localizado no exterior não deveria configurar transferência internacional de dados, enquanto que, por outro lado, a comunicação de dados (no âmbito internacional) ocorrida entre diferentes empresas de um mesmo grupo empresarial, indubitavelmente, entra na regra do regime especial criado pela legislação[23].

Trazer as informações expostas acima é relevante principalmente para não se esvaziar o instituto. Ou seja, é preciso definir e delimitar quais as hipóteses estão abrangidas pelo regramento dado às transferências internacionais de dado. Inclusive, a LGPD, em seu artigo 3º[24], explica o âmbito de aplicação da norma, e informa que, para que seja aplicada a lei, não é necessária a análise do país sede ou de onde estejam localizados os dados, bastando que esteja presente uma das seguintes hipóteses, não cumulativas: (i) operação de tratamento realizada em território brasileiro; (ii) a atividade de tratamento com objetivo de oferta ou de fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (iii) a coleta de dados tenha ocorrido em território nacional.

Portanto, não será considerada uma transferência internacional de dados a hipótese em que uma pessoa no Brasil crie cadastro em uma plataforma online, gerenciada por empresa estrangeira e com o envio de dados para o exte-

23. Capítulo V, Da Transferência Internacional de Dador por Luis Fernando Prado Chaves. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020. P 330.

24. LGPD, Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (grifos da autora)

rior. A LGPD não considera essa situação como transferência internacional, mas sim como âmbito de aplicação direta da legislação brasileira. A empresa de outra nação, ao disponibilizar a oferta do seu serviço em território nacional, deverá cumprir os deveres de controlador e garantir todos os direitos aos titulares tal como rege a LGPD. Situação diferente ocorre, como visto no caso Schrems, quando a empresa que disponibiliza o serviço localmente ("exportadora"), transmite os dados para fora do país a outra empresa ("importadora"), independentemente de pertencerem ou não ao mesmo grupo econômico.

O Comitê Europeu para a Proteção de Dados (*European Data Protection Board* – EDPB), em sua diretriz (*guideline*) 5/2021[25] , externalizou o seguinte entendimento para a configuração de uma transferência internacional:

> O EDPB identificou os três critérios cumulativos seguintes que qualificam um processamento como uma transferência:
> 1) Um controlador ou um processador sujeito ao GDPR para o processamento dado.
> 2) Este controlador ou processador ("exportador") divulga por transmissão ou por outro meio disponibiliza dados pessoais, sujeitos ao processamento, a outro controlador, controlador conjunto ou processador ("importador").
> 3) O importador se encontra em país terceiro ou é uma organização internacional, independentemente de estar ou não este importador está sujeito ao GDPR em relação ao processamento do dado de acordo com o artigo 3.[26] (Tradução livre)

Sabendo que a Autoridade Nacional brasileira, ao se debruçar sobre o assunto, poderá recorrer a fontes europeias, é necessário estar atento a tal definição. Inclusive, não deverá demorar muito para que se tenha maiores detalhes sobre o tema em território nacional, pois o tema "Transferência Internacional de dados pessoais" foi incluído na agenda regulatória da ANPD para o biênio 2023/2024[27], bem como foi iniciado o processo de tomada de subsídios para

25. EDPB. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. Disponível em: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf. Acesso em 28/04/2023.

26. No original: The EDPB has identified the three following cumulative criteria that qualify a processing as a transfer: 1) A controller or a processor is subject to the GDPR for the given processing. 2) This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"). 3) The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

27. Para mais informações, acessar ANPD publica Agenda Regulatória 2023-2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024. Acesso em:28/04/2023.

coleta de colaborações da sociedade na elaboração do regulamento sobre transferências internacionais de dados pessoais[28].

Portanto, tem-se que para a transferência internacional é necessária a presença de dois agentes – exportador e importador – e a transmissão de dados entre eles. De uma forma geral, essa hipótese é vislumbrada em diversas situações cotidianas na atualidade conectada, como nos exemplos a seguir: quando a rede social de preferência envia dados para a matriz; o provedor de e-mail da empresa é localizado no exterior e/ou quando essa empresa em que se trabalha utilizar de armazenamento em nuvem (*data center*) localizado fora do Brasil; caso o pagamento do serviço de *streaming* de áudio e/ou de audiovisual seja processado por uma empresa terceira no exterior; a terceirização de um serviço de marketing para o consumidor; entre outros.

Analisando o cenário, mostra-se, dessa forma, inevitável não ter seus dados em algum momento transferidos para além do território nacional e, mais do que isso, sujeitos à disciplina da transferência internacional de dados. Ocorre que a proteção e a privacidade de dados pessoais é um direito fundamental, tanto no Brasil, pela introdução do inciso LXXIX no artigo 5º da Constituição Federal, quanto fora, tal como previsto na Carta dos Direitos Fundamentais da União Europeia[29]. O ponto sensível dessa questão é: como garantir aos titulares o controle sobre os seus próprios dados e o livre exercício de seus direitos, em cenários de transferência internacional de dados?

2. O Consentimento na Proteção de Dados Pessoais

A fim de analisar se seria (ou não) o consentimento uma melhor opção para sanar os desafios da transferência internacional de dados, se impõe percorrer a sua definição, os seus usos na LGPD e, ao fim, destrinchar o mencionado inciso VIII do artigo 33 da lei protetiva nacional.

Levando em consideração a interpretação sistemática da LGPD, é possível observar que qualquer operação de tratamento de dados pessoais deverá estar atrelada a uma justificativa. Nos ensinamentos de Chiara de Teffé e Mario Viola, “deverá ocorrer o encaixe perfeito do tratamento realizado em pelo me-

28. Para mais informações, acessar ANPD. Tomada de subsídios sobre transferências internacionais de dados pessoais inicia nesta quarta-feira. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/tomada-de-subsidios-sobre-transferencias-internacionais-de-dados-pessoais-inicia-nesta-quarta-feira.Acesso em:28/04/2023.

29. UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12016P%2FTXT. Acesso em 28/04/2023.

nos uma das hipóteses legais para que ele seja considerado legítimo e lícito."[30].

Essas hipóteses, também conhecidas como bases legais, estão dispostas na lei no art. 7, dedicado aos dados pessoais em sentido amplo, e no art. 11, específico para os dados pessoais sensíveis. Em se tratando de consentimento, afirmam os mesmos autores, que

> [o] consentimento do titular dos dados recebeu tutela destacada na LGPD, ainda que não seja, vale lembrar, a única hipótese legal para o tratamento de dados pessoais nem hierarquicamente superior às demais contidas no rol do art. 7º. Aliás, em determinados casos a obtenção do consentimento poderá ser até mesmo inadequada, tendo em vista a existência de outra base legal mais precisa para o tratamento em questão.[31]

Como definição, a LGPD traz no artigo 5º, inciso XII, que consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Portanto, é uma ação do titular, por meio da qual ele expressa sua concordância ativa com determinado tratamento dos seus dados pessoais.

O consentimento é, portanto, uma expressão do controle pelo titular dos usos aos quais seus dados serão submetidos. Veja-se também que um dos fundamentos da norma de proteção é a autodeterminação informativa (LGPD, art. 2, II), que tal como definido por Stefano Rodotà é um "poder permanente de controle sobre seus próprios dados".[32]

Por um outro lado, atrelar o tratamento dos dados ao consentimento do titular impõe certos riscos. Deve-se ter em mente que a norma protetiva existe em razão da discrepância econômica, política, social e informacional entre o controlador de dados e o titular. Ao analisar os contornos do consentimento, sintetiza Bruno Bioni que

> o consentimento do titular dos dados continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a

30. VIOLA, Mario e DE TEFFÉ, Chiara Spadaccini. Tratamento de Dados Pessoais na LGPD: Estudo Sobre as Bases Legais dos Artigos 7º e 11. In: Tratado de Proteção de Dados Pessoais. Coordenação Danilo Doneda [et al.] 2ª ed. Rio de Janeiro: Forense, 2023. P. 116.

31. VIOLA, Mario e DE TEFFÉ, Chiara Spadaccini. Op.cit. p. 119.

32. RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Ed. Renovar, 2008.

> atuação de atores coadjuvantes importantes: i) novas formas para operacionalizá-lo, levando-se em conta a arquitetura (de vulnerabilidade) da rede; ii) o relato normativo complementar da privacidade contextual que o limita e o readapta diante de um solo epistemológico que esfacela a técnica tradicional da autodeterminação baseada de declaração de vontade do titular dos dados; e iii) o cidadão também exerce domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas. Portanto, o conteúdo jurídico-normativo de autodeterminação informacional vai além do consentimento.[33]

Nesse sentido também se posicionou Danilo Doneda ao afirmar que "a autodeterminação estaria concentrada no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, e assim poderia se prestar ao afastamento da matéria do âmbito dos direitos da personalidade"[34].

Compreendidos os riscos em torno do consentimento, nota-se na LGPD que diversos são os seus usos. Como visto, aparece como base legal, no já informado no art. 7º, inciso I, e nas situações em que ocorrer o compartilhamento com outros controladores (§5º). O artigo 8º, por sua vez, traz mais regras e reforça a ideia de que esse consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. E mais, o ônus da prova de que o consentimento foi obtido em conformidade com a lei é do controlador (§2º), podendo ser anulado se for obtido mediante vício (§3º). Além disso, o consentimento deverá estar atrelado a uma finalidade específica de tratamento, sendo vedado autorizações genéricas (§4º), e caso alterada posteriormente essa finalidade, o controlador deverá informar ao titular, que poderá revogar o consentimento, caso discorde da alteração (6º). Por fim, sendo interesse do titular, ele pode a qualquer momento, de forma gratuita e facilitada, revogar o seu consentimento (§5º), hipótese essa também encontrada no rol dos direitos do titular disposto no artigo 18.

O consentimento também está presente na disciplina dos dados pessoais sensíveis, que são aqueles dados que constituem o "núcleo duro" da privacidade, pois em razão do tipo e da natureza dessa informação, são ainda mais rele-

33. BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. P. 345

34. DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 161.

vantes para a intimidade e podem levar à discriminação do titular[35]. Segundo o artigo 11, o tratamento dos dados pessoais sensíveis somente poderá ocorrer quando o titular ou o responsável consentir (inciso I) ou sem o fornecimento de consentimento do titular em hipóteses indispensáveis (inciso II).

Outro grupo de dados considerados merecedores de uma maior proteção à luz da LGPD são os dados pessoais de crianças e adolescentes. E, mais uma vez, a lei apresenta o consentimento (§1º do artigo 14) como uma das bases legais para o tratamento de dados dos referidos sujeitos, sendo ele aqui específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Em suma, é inegável a relevância do consentimento na LGPD, no entanto, é necessário ir além e compreender os objetivos que esse instituto visa a garantir. Estabelecido o alinhamento entre o consentimento e a autodeterminação informativa, tem-se que a mera obtenção daquele não basta, é imperioso se atentar, por exemplo, se as informações são passadas de forma clara e precisa ao titular, tal como preconiza o princípio da transparência (art. 6, VI), e que seja garantido de forma enfática o controle dos dados pelo titular por meio do exercício dos seus direitos garantidos na lei.

E em se tratando de transferência internacional, o afastamento, principalmente o informacional, entre os agentes de tratamento e o titular é ainda mais expressivo. Portanto, cuida-se de examinar em que medida o consentimento se relaciona com o instituto da transferência internacional de dados.

3. O Consentimento aplicado na Transferência Internacional de Dados (LGPD, art. 33, VIII)

A LGPD traz a disciplina da transferência internacional em seu capítulo V, sendo que a regra seria não permitir a transferência, de forma que as hipóteses de sua ocorrência seriam por exceção. Cumpre observar que a Lei estrutura três regimes de transferência internacional de dados: (i) quando países ou organismos internacionais proporcionam grau de proteção de dados pessoais adequado à LGPD e chancelado pela ANPD (art. 33, I, c/c art. 34); (ii) quando os controladores ofereçam garantias de cumprimento dos preceitos da LGPD

35. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro [livro eletrônico] – Gustavo Tepedino; Ana Frazão; Milena Donato Oliva (Coord) - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2019. p. 307.

(art. 33, II); quando há situações específicas autorizativas (art. 33, III a IX).

Na primeira hipótese, o art. 34 estabelece os parâmetros a serem observados pela ANPD em sua avaliação do nível de proteção de dados do país ou da organização estrangeira, a saber: as normas gerais e setoriais em vigor; a natureza dos dados; a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD; a adoção de medidas de segurança previstas em regulamento; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e outras circunstâncias específicas relativas à transferência.

A segunda hipótese considera que, ainda que o país ou organização internacional não tenha recebido o "salvo-conduto" anterior, poderá o controlador oferecer e comprovar a adesão ao arcabouço protetivo da LGPD, conforme previsto nas alíneas do inciso II do art.33, por meio de cláusulas contratuais específicas para determinada transferência; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos.

Por fim, na terceira hipótese, a LGPD elenca situações excepcionais autorizativas da transferência internacional de dados, sendo elas: para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (III); para a proteção da vida ou da incolumidade física do titular ou de terceiro (IV); quando a autoridade nacional autorizar a transferência (V); quando a transferência resultar em compromisso assumido em acordo de cooperação internacional (VI); quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público (VII); quando o titular tiver fornecido o seu consentimento (VIII); ou quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD (respectivamente: cumprimento de obrigação legal ou regulatória, execução de contrato e exercício regular de direitos) (IX).

Portanto, uma dessas situações específicas vem a ser o objeto de análise, isto é, tal como previsto no inciso VIII, do art. 33, a transferência internacional de dados pessoais é permitida nos casos em que "o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades".

Consubstanciando o art. 5º, XII, com o art. 33, VIII, percebe-se que o consentimento da transferência internacional é diferenciado, pois além de ser uma

"manifestação livre, informada e inequívoca" deverá ser também "específico e em destaque". Para Bruno Bioni, esse consentimento qualificado se justifica para "estabelecer uma "camada adicional" de proteção por entender que tais cenários apresentam um risco anormal. O fiel dessa balança é a obtenção de um consentimento especial por parte do cidadão em que ele assente deliberadamente com tais riscos elevados[36]."

E os riscos, como já explicado, são elevadíssimos, segue o autor dizendo que nem mesmo o compartilhamento de dados implica "no mesmo risco que a transferência internacional para um país sem um nível adequado de proteção. Parece-nos que eventual regulação por parte do órgão fiscalizador será de extrema relevância para fins de segurança jurídica e não vulgarização desse consentimento especial.[37]" E de fato a ANPD já anunciou que no biênio 2023/2024 irá se debruçar sobre a transferência internacional de dados.

É válido ressaltar que as hipóteses de transferência internacional amparadas pelo consentimento sejam difíceis de exemplificar, visto que não serão abarcadas pela hipótese de existência de chancela da ANPD sobre o nível de adequação do país ou organismo internacional (regime 1), pela garantia oferecida pelo controlador de adesão à LGPD (regime 2) ou pelas demais hipóteses excepcionais do artigo 33 (regime 3).

No entanto, seja como for, a hipótese está prevista na lei e deve ser pensada levando em consideração todo o arcabouço jurídico estabelecido nacional e internacional, inclusive pensando nas jurisdições envolvidas nesse processo. Na prática, o exercício de autorizar uma transferência internacional somente com base no consentimento do titular, poderá implicar na ausência de informações precisas sobre para quais usos e finalidades os dados pessoais são tratados, sobre quais agentes e organismos estarão envolvidos no processo, sobre os mecanismos de segurança e proteção contra violações e sobre os meios efetivos de tutela de direitos. Em última análise, essa hipótese pode levar ao afastamento de toda lógica protetiva da LGPD, que em termos gerais, busca, por meio do equilíbrio informacional entre titular e agentes de tratamento, garantir a autodeterminação informativa, ou seja, o controle sobre os próprios dados, para atendimento de um direito fundamental ligado à dignidade humana.

---

36. BIONI, Bruno Ricardo. Op. cit. p. 250.

37. BIONI, Bruno Ricardo. Op. cit. p. 289.

A respeito dos meandros dessa disciplina, Christopher Kuner é cirúrgico ao detalhar como deve ser pensada a disciplina de transferência internacional de dados:

> Maior transparência também precisa ser criada para os indivíduos. Isso significa que os avisos de privacidade que fornecem as informações sobre fluxos de dados transfronteiriços devem ser redigidas em linguagem mais clara; que o uso do consentimento para transferir dados deve ser limitado; e que a cooperação regulatória transfronteiriça deve ser aumentada, para que os indivíduos possam mais facilmente fazer valer seus direitos em relação aos dados que foram transferidos para outros países. Os controladores de dados também precisam fornecer maior transparência no que diz respeito à localização e identidade das entidades envolvidas no processamento e armazenamento dos dados pessoais. (tradução livre)[38]

Corrobora-se com a ideia de que a transferência internacional deve ser pensada tanto como política pública por meio da cooperação entre as nações, quanto como mecanismos privados de boas práticas e governança sobre privacidade e proteção de dados pessoais. Acerca da regulação transnacional, a OCDE aborda que "os países membros têm um interesse comum em promover e proteger os valores fundamentais da privacidade, das liberdades individuais e do livre fluxo global de informações"[39]. Nesse sentido, além dos acordos estabelecidos entre a União Europeia e os EUA, abordados anteriormente, outros países vêm se articulando para definir regras para seus fluxos transfronteiriços de dados pessoais, a título de exemplo: Acordo sobre o Comércio Eletrônico do Mercosul; Acordo Bilateral de Livre Comércio entre Brasil e Chile; Mercado Comum e Comunidade do Caribe (CARICOM); Convenção 108 do Conselho da Europa; Cooperação Econômica Ásia-Pacífico (APEC); Acordos Estados Unidos-México-Canadá (USMCA); Associação das Nações do Sudes-

38. No original: Greater transparency also needs to be created for individuals. This means that privacy notices giving information about transborder data flows should be drafted in clearer language; that the use of consent to transfer data should be limited; and that cross-border regulatory co-operation should be increased, so that individuals can more easily assert their rights with regard to data that have been transferred to others countries. Data controllers also need to provide greater transparency with regard to the location and identity of entities they use to process and store personal data. KUNER, Cristopher. Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, OECD Digital Economy Papers, No. 187, OECD Publishing, Paris. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en. Acesso em 28/04/2023.

39. OCDE. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 28/04/2023.

te Asiático (ASEAN); Convenção sobre Segurança Cibernética e Proteção de Dados Pessoais da União Africana; Acordo de Comércio e Cooperação (EU--R.U.); Acordo de Parceria Econômica (EU-Japão); Acordo de Livre Comércio Singapura-Austrália; Acordo de Parceria da Economia Digital (Chile, Nova Zelândia e Singapura)[40].

Sobre as possibilidades privadas, em 2005, Ann Cavoukian[41] presidiu um grupo de trabalho de especialistas em privacidade que resultou no desenvolvimento do *Global Privacy Standard*[42], e possuía como objetivo a formação de "um conjunto de princípios universais de privacidade[43], harmonizando aqueles encontrados em vários conjuntos de práticas informacionais atualmente existentes.", tendo como base "o conhecimento coletivo e a sabedoria prática da comunidade internacional de proteção de dados". Outro expoente ator na condução de padronizações globais, é a ISO (*International Organization for Standardization*), que possui diversas normas técnicas em matéria de privacidade e segurança da informação que podem ser utilizadas pelas instituições privadas e públicas na condução das transferências internacionais de dados[44].

Sintetizando as ideias expostas, Ângelo Prata de Carvalho tece os seguintes comentários:

> o desafio referente à garantia da efetividade da LGPD passa tanto pelo fortalecimento da autoridade nacional de proteção de dados – inclusive mediante a celebração de tratados internacionais – quando pela difusão dos ideais de proteção da privacidade e dos dados pessoais entre os *players* do cenário econômico internacional, por intermédio da introjeção da privacidade aos seus próprios processos produtivos.[45]

---

40. Válido citar que os acordos citados embora autorizem as transferências internacionais de dados, oscilam quanto aos parâmetros regulatórios em meio a um grande espectro de regras rígidas e flexíveis. Ver mais em: GUEIROS, Pedro. Relatório: Tratados e Acordos para Transferências Internacionais de Dados. Disponível em: https://itsrio.org/pt/publicacoes/tratados-e-acordos-para-transferencias-internacionais-de-dados/. Acesso em: 28/04/2023.

41. Idealizadora do conceito Privacy By Design, que versa sobre a aplicação de 7 (sete) princípios no tratamento de dados pessoais. Ver mais em: CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em 28/04/2023.

42. CAVOUKIAN, Ann. Creation of a Global Privacy Standard. Disponível em: http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf. Acesso em 28/04/2023.

43. Consentimento; Responsabilidade; Finalidade; Limitação de coleta; Limitação de uso, retenção e divulgação; Precisão.

44. A título exemplificativo: ISO 29100, ISO 29101, ISO 29134, ISO 29184, ISO 29190; ISO 27000 family.

45. CARVALHO, Ângelo Prata de. Transferência internacional de dados na lei geral de proteção de dados – Força normativa e efetividade diante do cenário transnacional. In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito

Dessa forma, conclui-se, que embora seja de enorme relevância na LGPD, o consentimento não se mostra como instituto chave, em termos garantistas, para a transferência internacional de dados. Cercada de riscos, tais como o nível de proteção no país que irá receber os dados pessoais e a disparidade informacional do titular perante os agentes de tratamento, a transferência transfronteiriça merece a devida atenção da autoridade nacional brasileira. Deverá a ANPD, por meio da celebração de tratados internacionais ou não, e a partir da experiência das demais nações, retirar as lições válidas para exercer seu papel na fiscalização e no cumprimento da LGPD.

Considerações finais

A Lei Geral de Proteção de Dados (LGPD) conferiu à pessoa natural papel de centralidade, tanto é assim, que a própria expressão titular remete à propriedade. Ou seja, os dados são de titularidade da pessoa natural e ela deve ter o controle sobre como eles são utilizados. O consentimento aparece como um instituto cercado de nuances, por um lado expressa a manifestação voluntária do titular, mas por outro pode ser facilmente esvaziado se não forem dadas ao titular as condições necessárias para a tomada de sua decisão.

No mundo altamente tecnológico, e sendo os dados o combustível da economia do presente século, inúmeras são as situações em que os dados pessoais possam ser transferidos internacionalmente. Grandes potências econômicas e políticas travam emblemáticos debates acerca desse tema, sendo um ponto positivo a ampliação das discussões entre as nações, por meio de tratados bi e multilaterais que visam articular regras sobre o tema. Organismos privados também podem contribuir ativamente para a questão por meio do estabelecimento de boas práticas e de standards de governança voltados à privacidade e a proteção de dados pessoais.

Ocorre que há muito mais a ser discutido e debatido, e as respostas são meramente provisórias. Há um aparente conflito de interesses: garantir a proteção fundamental ao indivíduo sobre a privacidade de seus dados pessoais de um lado e a atual revolução tecnológica do mundo digital do outro, um progresso jamais visto na história de forma tão grandiosa, dinâmica, efêmera, e, enfim, tão feroz.

---

brasileiro [livro eletrônico] – Gustavo Tepedino; Ana Frazão; Milena Donato Oliva (Coord) - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2019.

O consentimento pensado na transferência internacional de dados tem pouco espaço e apresenta uma gama enorme de riscos. Devem as autoridades nacionais, portanto, pensar em outros mecanismos para elevar a proteção de dados, não permitindo discrepância normativa e informativa entre as nações, e principalmente entre os organismos privados e/ou públicos que tratam os dados e os maiores interessados na questão – os titulares de dados pessoais. A ANPD certamente terá um grande exercício nos próximos anos.

Referências

ANPD. **ANPD publica Agenda Regulatória 2023-2024**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024. Acesso em:28/04/2023.

ANPD. **Tomada de subsídios sobre transferências internacionais de dados pessoais inicia nesta quarta-feira**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/tomada-de-subsidios-sobre-transferencias-internacionais-de-dados-pessoais-inicia-nesta-quarta-feira.Acesso em:28/04/2023.

ARGENTINA. Ley 25.326/2000. **Proteccion de los Datos Personales**. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion. Acesso em 28/04/2023.

BRASIL. Comissão Especial da Câmara dos Deputados. **Parecer ao Projeto de Lei Nº 4060/2012**. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=Tramitacao-PL+4060/2012. Acesso em 28/04/2023.

BRASIL. **Constituição da República Federativa do Brasil - 1988**. D.O.U de 05/10/1988, pág. nº 1.

BRASIL. 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). D.O.U de 15/08/2018, pág. nº 59. Lei nº 13.853 de 08 de julho de 2019. D.O.U. de 09/07/2019, P. 1.

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

CARVALHO, Ângelo Prata de. **Transferência internacional de dados na lei geral de proteção de dados – Força normativa e efetividade diante do cenário transnacional**. In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro [livro eletrônico] –Gustavo Tepedino; Ana Frazão; Milena Donato Oliva (Coord) - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2019.

CAVOUKIAN, Ann. ***Creation of a Global Privacy Standard***. Disponível em: http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf. Acesso em 28/04/2023.

CAVOUKIAN, Ann. ***Privacy by Design: The 7 Foundational Principles***. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em 28/04/2023.

COMISSÃO EUROPEIA. ***Adequacy decisions***. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em 28/04/2023.

COMISSÃO EUROPEIA. ***Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US***. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631. Acesso em 28/04/2023.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA (CJEU). Julgamento C362/14. ***Maximillian Schrems vs Data Protection Commissioner***. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362. Acesso em 28/04/2023.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA (CJEU). Julgamento C-311/18. ***Data Protection Commissioner vs. Facebook Ireland Ltd e Maximillian Schrems***. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:-62018CJ0311. Acesso em 28/04/2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

EDPB. EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but con-

cerns remain. Disponível em: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en Acesso em: 28/04/2023.

EDPB. ***Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR***. Disponível em: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf. Acesso em 28/04/2023.

GUEIROS, Pedro. **Relatório: Tratados e Acordos para Transferências Internacionais de Dados**. Disponível em: https://itsrio.org/pt/publicacoes/tratados-e-acordos-para-transferencias-internacionais-de-dados/. Acesso em: 28/04/2023.

ICO. ***International Transfers***. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/. Acesso em 28/04/2023.

KUNER, Cristopher. ***Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future***, OECD Digital Economy Papers, No. 187, OECD Publishing, Paris. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en. Acesso em 28/04/2023.

KUNER, Cristopher. ***Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection***. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850. Acesso em 28/04/2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]** – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

OCDE. ***Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data***. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 28/04/2023.

PARLAMENTO EUROPEU. ***European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom***. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html. Acesso em 28/04/2023

PARLAMENTO EUROPEU. **Regulamento (UE) 2016/679 de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia L 119/1.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Ed. Renovar, 2008.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **Consentimento e proteção de dados pessoais na LGPD**. In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro [livro eletrônico] – Gustavo Tepedino; Ana Frazão; Milena Donato Oliva (Coord) - 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12016P%2FTXT. Acesso em 28/04/2023.

URUGUAI. Ley Nº 18.331/2008. ***Protección de Datos Personales y Acción de "habeas data"*** Disponível em: https://parlamento.gub.uy/documentosyleyes/leyes/ley/18331. Acesso em: 09/01/2023.

VIOLA, Mario; DE TEFFÉ, Chiara Spadaccini.

Tratamento de Dados Pessoais na LGPD: Estudo Sobre as Bases Legais dos Artigos 7º e 11. In: Tratado de Proteção de Dados Pessoais. Coordenação Danilo Doneda [et al.] 2ª ed. Rio de Janeiro: Forense, 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

13

Tratamento de dados pessoais do trabalhador: aplicação das bases legais

VANESSA VARGAS DOS SANTOS

VANESSA VARGAS DOS SANTOS[1]

Sumário: Introdução. 1. Implementação da LGPD e seus impactos nas relações de trabalho. 2. Hipóteses autorizadoras para o tratamento de dados pessoais.3. Análise crítica da aplicação das bases legais no âmbito trabalhista. 3.1. O consentimento como base legal para o tratamento de dados de trabalhadores: análise crítica e pressupostos para a sua validação. 3.2 Aplicabilidade do legítimo interesse no âmbito das Relações Trabalhistas. 3.3 Hipóteses para o tratamento de dados pessoais sensíveis: análise do artigo 11 da LGPD. Considerações Finais. Referências.

Introdução

Com a expansão da Indústria 4.0, os processos produtivos foram ampliados, gerando novas formas de trabalho, como o trabalho *on-demand*, executado por meio de aplicativos, e o *crowdwork*. Os trabalhos plataformizados são organizados e controlados por programação algorítmica. Os comandos pré-ordenados pela programação da plataforma conduzem a uma reação do trabalhador, que se mantém mobilizado, para reagir aos comandos, subordinando-se ciberneticamente[2].

Assim, subordinado à vigilância constante de seu empregador e diante dessa conexão digital acentuada, o trabalhador cede seus dados pessoais e sua privacidade. Os dados pessoais dos cidadãos passaram a ditar uma nova lógica de acumulação de capital[3]. A cada segundo, o compartilhamento de dados se dá de forma incalculável[4]. Tendo em vista o uso excessivo de dados pessoais, gerou-se uma necessidade de regulamentação emergente para esse novo cenário, com a finalidade de resguardar os dados dos indivíduos, para que os titulares dos dados pessoais não sejam expostos sem sua ciência, pre-

1. Advogada, mestre no PPGD UERJ na área de concentração: Pensamento Jurídico e Relações Sociais. Direito do Trabalho e Previdenciário, pós-graduada em Direito Digital na UERJ/CEPED em parceria com ITS e pós-graduada em processo civil pela Cândido Mendes. Experiência profissional de quase três anos no Siqueira Castro Advogados e dois anos no IBMEC, dentro da coordenadoria do curso de Direito. Foi assistente de ensino e de pesquisa na pós-graduação em Direito Empresarial na Fundação Getúlio Vargas (FGV LAW PROGRAM). Também coordenou a pós-graduação em Direito Digital do ITS em parceria com a UERJ-CEPED. Atualmente é coordenadora da área de educação do ITS. Está cursando pós-graduação de Design Educacional na UNIVALI.

2. FONSECA, Vanessa Patriota. O crowdsourcing e os desafios do sindicalismo em meio à crise civilizatória. In: CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (Org.). Futuro do Trabalho: os efeitos da revolução digital na sociedade. Brasília: ESMPU, 2020. p. 360.

3. BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 3ª ed. Rio de Janeiro: Forense, 2021. p.11

4. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 25, p. 84, jul./set. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521>. Acesso em: 14 jan. 2022.

servando dessa maneira sua intimidade e privacidade[5].

Sendo assim, foi aprovada a Lei nº 13.709 (Lei Geral de Proteção de Dados – LGPD), que entrou em vigor em 18 de setembro de 2020. De acordo com o artigo 1º da LGPD, a lei tem a finalidade de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa humana[6]. A Lei Geral de Proteção de Dados admite aos seus titulares a proteção dos próprios dados e o direito ao acesso a todas as etapas do tratamento, desde a coleta até o processamento, o arquivamento, o armazenamento, a eliminação e o compartilhamento[7].

Na relação de emprego, não é diferente: são coletadas muitas informações pessoais em diversos cenários, que se iniciam na fase pré-contratual e se encerram no término do contrato.[8]A todo instante, portanto, são tratados dados pessoais e dados sensíveis dos empregados, alguns dos quais podem ser exemplificados como: dados relativos à saúde; biometria; de orientação sexual; dados cadastrais etc.[9] Porém, embora o empregador tenha a justificativa da necessidade de cumprimento da lei, muitos desses são coletados por diversas razões, muitas vezes, não divulgadas[10].

Em consonância com o art. 5º, VI, da LGPD, o empregador tem o dever de guardar, proteger e tratar os dados dos empregados, configurando-se como um "controlador". O tratamento dos dados deve respeitar os princípios constitucionais e os fincados na LGPD, o que tem sido objeto de debates, devido ao limite que o empregador deve ter em conhecer e dispor de informações do trabalhador, mesmo no cumprimento de suas prerrogativas e de direitos na

5. PRATTI, Gabriela; SOARES, Mariana Maça. Evolução da tecnologia e a necessidade de criação da Lei Geral de Proteção de Dados no Brasil. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 80.

6. MATOS, Larissa. Princípios da Lei Geral de Proteção de Dados. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 18.

7. NASCIMENTO, Ivan Kaminski do; BOSCATTO, Gianfranco. Proteção de Dados Pessoais nas Relações de Trabalho. São Paulo: Dialética, 2022. p. 15. Edição do Kindle.

8. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 49.

9. CARLOTO, Selma. Manual prático de adequação à LGPD com enfoque nas relações de trabalho. São Paulo: LTR, 2021. p.18.

10. PIERONI, Verissa Coelho Cabral. Noções gerais sobre proteção de dados nas relações de emprego. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 30.

esfera da relação trabalhista[11].

A LGPD estabelece hipóteses que autorizam a realização dos tratamentos de dados pessoais, em seu artigo 7º, e artigo 11, no que se refere ao tratamento de dados sensíveis. A primeira base legal, não mais importante, é a do consentimento, o qual deve ser manifestado de forma: livre, informada e inequívoca[12].

Nas relações de trabalho, todavia, há controvérsias sobre a aplicação da base legal de consentimento, por exemplo, tendo em vista que há uma relação assimétrica de poder, sendo o trabalhador a parte mais fraca da relação[13], já que a subordinação é de caráter basilar da relação de emprego. Nesse sentido, existe um desequilíbrio entre a liberdade de consentimento e o poder direcional do empregador. Sendo assim, é improvável que o titular dos dados recuse o consentimento, devido à relação de subordinação[14].

Neste sentido, o empregador, com o poder diretivo, colhe e trata intensamente os dados do trabalhador, muitas vezes sem o consentimento dele ou sem necessidade, pelo exercício do contrato. Diante disso, indaga-se: Como os dados pessoais e pessoais sensíveis dos trabalhadores devem ser tratados? Quais são os limites do poder diretivo do empregador em função do uso dos dados pessoais dos trabalhadores? Quais bases legais autorizadoras mais adequadas a serem aplicadas nas relações de trabalho?

Diante da grande circulação de dados pessoais em decorrência da Era Digital, na presente pesquisa será analisada a importância do tratamento dos dados em consonância com a LGPD, sobretudo nas relações de trabalho, já que esses são geralmente colhidos desde a contratação até a resolução do contrato. Também serão abordadas as hipóteses autorizadoras para tratamento de dados pessoais e os desafios da utilização do consentimento como base legal na esfera laboral, considerando o contexto do trabalho subordinado.

---

11. GIUNTINI, Adriana et al. LGPD nas relações de trabalho. Salvador, BA: Editora Motres, 2021. E-book (38p.) color. ISBN: 978-65-89765-07-3, p. 7. Disponível em: <https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes--de-Trabalho-1-1.pdf.> Acesso em: 27 jul. 2022.

12. GALLINDO, Sergio Paulo. Economia intensiva em dados, virtudes da LGPD e primeiros desafios quanto à efetividade. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo. Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A caminho da efetividade: contribuições para implementação da LGPD. São Paulo: Revistas dos Tribunais, 2020. p. 155

13. BIONI, Bruno Ricardo. Proteção de Dados Pessoais: A Função e os Limites do consentimento. 3ª ed. Ed. Forense. 2021. p.158

14. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p.108

1. Implementação da LGPD e seus impactos nas relações de trabalho

O avanço da Tecnologia da Informação e Comunicação (TIC) e o consequente uso excessivo de dados pessoais no mercado, geraram a necessidade emergente de regulamentação mais específica sobre a proteção de dados pessoais, notadamente quando versaram sobre dados sensíveis. Neste sentido, a União Europeia aprovou o Regulamento Geral de Proteção de Dados Pessoais (RGPD)[15], que entrou em vigor em 27 de abril de 2018. O RGPD influenciou a Lei Geral de Proteção de Dados Pessoais no Brasil. A LGPD foi aprovada em 2018, a qual entrou em vigor no ano de 2020.

O processo legislativo nacional persistiu por aproximadamente oito anos, enquanto em mais de 100 países já existiam legislações sobre a proteção de dados pessoais.[16] No Brasil, a LGPD foi a primeira legislação a abordar especificamente sobre a proteção de dados pessoais. Porém, a referida lei não consagrou a proteção de dados pessoais no ordenamento brasileiro, pois a regulação nacional havia se estruturado nos instrumentos então existentes:[17]

> A Lei Geral de Proteção de Dados tem a base principiológica ampla e traz no artigo 2º fundamentos de forma plural. Os princípios têm como objetivo limitar o tratamento de dados, além de conferir poder de controle ao indivíduo sobre o tratamento de seus dados.[18] Em consonância com os objetivos e fundamentos da LGPD, em seu artigo 6º, traz princípios que orientam a aplicação e a interpretação da Lei. Esses princípios aparentemente conflitantes, são bases para boas práticas no tratamento de dados pessoais, principalmente no ambiente virtual. Através deles, proporciona-se uma segurança jurídica maior[19] e se evita uma eventual colisão entre os

15. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04. Acesso em 15 de jun. de 2022.

16. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. [S. l.], v. 16, n. 90, 2019. p. 109-131. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 5 set. 2022. p.111.

17. Doneda, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo. Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A caminho da efetividade: contribuições para implementação da LGPD. São Paulo: Revistas dos Tribunais, 2020. p. 245.

18. BIONI, Bruno Ricardo; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. In: BIONI, Bruno Ricardo (org). Proteção de dados: Contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p. 292.

19. MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020.p.18

princípios fundamentais.

O artigo então supracitado, compreende 10 princípios: finalidade; adequação; necessidade ou minimização; livre acesso; qualidade dos dados; transparência; responsabilização; prestação de contas; segurança; prevenção e não discriminação. Esses princípios são igualmente aplicáveis à relação de trabalho contratual, uma vez que se baseiam em uma relação contratual pautada na boa-fé.

Todos esses princípios estão dispostos no Regulamento Europeu, exceto os princípios da segurança, prevenção e não discriminação, que são previstos apenas pela LGPD. Esses princípios novos demonstram a atenção da Lei no que se refere às novas demandas da sociedade sobre os aspectos de proteção de dados.

A principal preocupação da LGPD é resguardar os dados pessoais, concedendo o seu controle aos titulares dos dados[20]. A referida lei tem por finalidade prevenir danos à pessoa humana e propicia a segurança no tratamento de dados pessoais, o que diminui os riscos de violação à privacidade e os dados pessoais, além de impedir tratamentos abusivos.[21] A proteção dos dados pessoais é um direito básico do cidadão, inclusive em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional (EC/115)[22] que passou a ser incluída no rol dos direitos e garantias fundamentais e o direito à proteção de dados com inclusão nos meios digitais.

Na Lei Geral de Proteção de Dados não há expressa disposição referente ao direito do trabalho, porém, é necessário observar as causas legitimadoras do tratamento de dados e as obrigações conferidas pela LGPD.[23] O empregador é considerado “controlador”, tendo em vista que, compete a este o poder decidir sobre o tratamento de dados pessoais, conforme disposto no art. 5º, VI, da LGPD. Portanto, tem a obrigação de resguardar os dados pessoais dos

20. CARLOTO, Selma.Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p.13.

21. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p.9

22. Emenda Constitucional nº 115. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF. 2022. Disponível em: https://www.in.gov.br/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 01 jul. 2022

23. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 49.

empregados.

Cumpre ressaltar que, no GDPR há regras explanadas sobre o tratamento de dados no contexto trabalhista. Em seu artigo 88[24], autoriza a regulamentação mais específica através das convenções coletivas de trabalho com o intuito de garantir a defesa dos direitos e liberdade dos trabalhadores, referente ao tratamento de seus dados pessoais, que abrange os seus efeitos desde o recrutamento a cessação da relação de trabalho.

Apesar da ausência de uma norma brasileira expressa sobre o tratamento de dados pessoais nas relações de trabalho, a negociação coletiva poderá ser utilizada para adequar as empresas à LGPD, desde que observados os limites e princípios amparados pela Constituição Federal de 1988 e o artigo 611-B da CLT. O compliance trabalhista deve iniciar desde a seleção de candidatos à vaga de emprego, durante a execução do contrato de trabalho, até o término da relação trabalhista, assim como o artigo 88 do GDPR.[25]

A LGPD assegura, a toda a pessoa natural, a titularidade de seus dados pessoais, considerando relevante todo dado pessoal.[26] A LGPD tem por desígnio proteger a liberdade e privacidade, além do livre desenvolvimento da pessoa natural.[27] A proteção dessas informações pessoais contribui para que a pessoa desenvolva a sua personalidade de forma livre.[28]

Com a grande circulação de dados pessoais e a consequente vulnerabilidade do titular de tais elementos, foi constituída a categoria de dado pessoal

---

24. Art. 88, GDPR: 1. Os Estados-Membros podem, por lei ou por convenções coletivas, prever regras mais específicas para assegurar a proteção dos direitos e liberdades em matéria de tratamento dos dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, cumprimento do contrato de trabalho, incluindo o cumprimento das obrigações estabelecidas por lei ou por convenções coletivas, gestão, planeamento e organização do trabalho, igualdade e diversidade no local de trabalho, saúde e segurança no trabalho, proteção dos bens do empregador ou do cliente e para a para fins de exercício e gozo, individual ou coletivo, de direitos e benefícios relacionados ao emprego, e para fins de extinção do vínculo empregatício.
2. Essas regras devem incluir medidas adequadas e específicas para salvaguardar a dignidade humana, os interesses legítimos e os direitos fundamentais do titular dos dados, nomeadamente no que diz respeito à transparência do tratamento, à transferência de dados pessoais no seio de um grupo de empresas ou de um grupo de empresas que exerçam uma atividade econômica conjunta e sistemas de monitoramento no local de trabalho. Disponível em: <https://gdpr-info.eu/art-88-gdpr/>. Acesso em 16 set. 2022.

25. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 33.

26. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p. 11.

27. NASCIMENTO, Ivan Kaminski do; BOSCATTO, Gianfranco. Proteção de Dados Pessoais nas Relações de Trabalho. São Paulo: Dialética, 2022. p. 10. Edição do Kindle.

28. BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 83.

sensível, segundo o artigo 5º, inciso II, da LGPD de 2018.[29]Com a circulação de alguns dados pessoais poderá ocasionar maior potencial lesivo aos seus titulares em um contexto social e político. Sendo assim, a proteção de dados sensíveis tem por objetivo prevenir a discriminação em face dos titulares dos dados.[30]

A utilização dos dados pessoais, indevidamente, poderá impulsionar a discriminação em atividades bancárias, financeiras, de saúde e de seguro, por exemplo. Se não observadas as garantias de maneira adequada, seja pelos empregadores, recrutadores, companhias seguradoras e planos de saúde poderão aumentar a violação aos direitos[31].

Nas relações de trabalho, os dados pessoais quando são utilizados para traçar perfis comportamentais, por exemplo, pode ocasionar situações discriminatórias ou tendenciosas que venham a onerar oportunidades de emprego às pessoas, baseadas em suas opiniões ou informações lançadas no mundo virtual.

No tocante aos dados sensíveis, nos departamentos pessoais das empresas são coletados dados de empregados a partir da fase inicial do contrato, como por exemplo, perguntas em entrevistas sobre pretensão de filhos, prática de alguma religião ou filiação de partido político. Durante a vigência do contrato, outros dados sensíveis são coletados, tais como: origem racial e filiação sindical, além dos dados biométricos para controle de jornada, entre outros.[32] Além disso, através da utilização de inteligência artificial, os cruzamentos de alguns dados sensíveis poderão ser utilizados para averiguar o estado de saúde e a moral dos trabalhadores.[33]

Ademais, o empregador, por meio da observação de dados sensíveis do

29. "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.

30. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p. 21-23.

31. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p. 20.

32. PIERONI, Verissa Coelho Cabral. Noções gerais sobre proteção de dados nas relações de emprego. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 38.

33. MOREIRA, Teresa Coelho. Algumas considerações sobre segurança e saúde dos trabalhadores no trabalho 4.0. In: CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (Org.). Futuro do Trabalho: os efeitos da revolução digital na sociedade. Brasília: ESMPU, 2020. p. 283.

trabalhador e a sua vida privada, poderá encerrar o contrato de trabalho, sem o trabalhador perceber que a exposição de seus dados pessoais motivou a sua demissão. Por haver a necessidade de ter mais cuidado no tratamento dos dados pessoais sensíveis, tendo em vista que tem um potencial discriminatório, as hipóteses autorizadoras de tratamento pela legislação de proteção de dados devem ser observadas, incluindo-se as relações de trabalho.[34] Essas hipóteses autorizadoras para tratamento prevista em lei, serão tratadas adiante.

2. Hipóteses autorizadoras para o tratamento de dados pessoais

Na LGPD estão previstas 10 bases legais para o tratamento de dados pessoais. As bases legais são hipóteses que permitem a realização do tratamento, que ocorre em diversas situações. As hipóteses relacionadas no artigo 7º da LGPD, definem as condições para a licitude do tratamento de dados. No que se refere ao tratamento de dados pessoais sensíveis, as hipóteses deverão ser observadas no artigo 11, da referida Lei.[35]

Nas relações de trabalho, o empregador, que é o controlador dos dados pessoais do empregado, executa o tratamento dos dados geralmente para cumprimento de obrigação legal ou regulatória. Porém, há casos em que poderá tratar dados sensíveis, mediante o consentimento do empregado ou pelo exercício regular de direitos.

O artigo 7º da Lei Geral de Proteção de Dados destina-se ao tratamento de dados de pessoas comuns, e todas as bases apresentam o mesmo grau de importância.[36] O consentimento é a primeira hipótese de tratamento de dados disposto no artigo 7º da LGPD e traz algumas particularidades, assim como a hipótese para atender aos interesses legítimos do controlador ou de terceiros, prevista no inciso IX do aludido artigo. Diante disso, necessita de um maior debate, portanto, serão tratadas a adiante de forma mais detalhada.

A hipótese do cumprimento de obrigação legal ou regulatória pelo controlador, prevista no inciso II do artigo 7º da LGPD, poderá ser utilizada para cui-

34. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 34.

35. MIRAGEM, Bruno; MADALENA, Juliano. Capítulo II – Do tratamento de dados pessoais. I - Dos requisitos para o tratamento de dados pessoais. Art. 7º. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.) Comentários à Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora Foco, 2022. p. 68.

36. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. P. 129.

dar dos dados pessoais quando houver uma determinação legal, que poderá ser por lei federal, estadual ou municipal.[37] Para o autor Ivan Kaminski, esta hipótese de tratamento de dados pessoais é a mais segura ao controlador, tendo em vista que, é amparada por uma necessidade legal extrínseca à relação com o titular.[38]

No inciso III do artigo 7º da Lei em tela, traz o tratamento de dados pessoais pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da lei, que regula o tratamento de dados pessoais pelo Poder Público.

A quarta hipótese prevista no artigo 7º permite o tratamento de dados para a prática de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. O órgão de pesquisa a que se refere este artigo, está previsto no artigo 5º, inciso XVIII, da LGPD. [39] Esta quarta hipótese é uma base legal com aplicação restrita.[40] Essa hipótese é a que oferece maior proteção aos titulares, uma vez que um dado anonimizado refere-se a dados relacionados ao titular que não podem ser identificados. Em outras palavras, quando um dado é anonimizado, deixa de ser considerado pessoal, conforme estabelecido pelo artigo 12 da LGPD.[41]

A quinta hipótese para o tratamento de dados prevista no artigo sétimo, refere-se à execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. Ou seja, a referida base legal só poderá ser utilizada se o titular dos dados for parte

37. NASSIF, Murilo Meneghetti; LINGUANOTTO, Fernanda. A LGPD como norma de inclusão e fomento da diversidade no ambiente laboral brasileiro. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 166-168.

38. NASCIMENTO, Ivan Kaminski do; BOSCATTO, Gianfranco. Proteção de Dados Pessoais nas Relações de Trabalho. São Paulo: Dialética, 2022. p. 31. Edição do Kindle.

39. (...) XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico

40. DIAS, Fernanda Rêgo Oliveira Dias. Limites à utilização do consentimento como base legal adequada para o tratamento de dados pessoais. In: REQUIÃO, Maurício (org.). Proteção de dados pessoais: novas perspectivas. Salvador, Editora: Edufba, 2022. p. 39.

41. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 23, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 dez. 2022.

no contrato.[42] São alguns exemplos de circunstâncias em que esta hipótese é aplicada, quando: Para entregar produtos em que o titular adquiriu, é necessário conhecer o nome completo, o endereço e outras informações de contato do consumidor e, antes de conceder crédito à uma pessoa é necessário levantamentos realizados por instituições financeiras relacionados a mesma.[43]

Cumpre-se ressaltar ainda, sendo lícito o tratamento de dados pessoais, nos casos de diligências pré-contratuais ou preliminares, a assinatura do contrato desde que a pedido do titular dos dados. Como, por exemplo, nos casos de processo seletivo para a vaga de emprego que há envio de currículo pelo candidato ou ficha com o preenchimento dos seus dados. Nesta linha de raciocínio, segundo o artigo 6º, número 1, alínea b), do GDPR, também é lícito o tratamento de dados pessoais nestes moldes. [44]

Esta base legal também poderá ser utilizada após o término da operação, para armazenar os dados, com o intuito de constituir meios de provas de direitos e obrigações, como por exemplo, um empregador mantém os dados do seu ex-empregado que sofreu acidente de trabalho, para produzir provas de defesa em eventual processo judicial.[45]

A sexta hipótese refere-se ao exercício regular de direitos em processo judicial, administrativo ou arbitral. É possível o tratamento de dados pessoais nessa hipótese em virtude dos princípios constitucionais: contraditório e ampla defesa, conforme artigo 5º, inciso LV, da CF/88. Em seguida, o artigo 7º da LGPD apresenta a sétima hipótese, que seria para a proteção da vida ou da incolumidade física do titular ou de terceiros. Esta base legal é utilizada para tratar dados toda vez que for imprescindível para resguardar os interesses vitais do titular dos dados ou de terceiros. [46]

Por conseguinte, verifica-se na oitava hipótese a possibilidade do trata-

---

42. NASSIF, Murilo Meneghetti; LINGUANOTTO, Fernanda. A LGPD como norma de inclusão e fomento da diversidade no ambiente laboral brasileiro. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 169.

43. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 25, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 de dez. 2022.

44. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 128.

45. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p. 169.

46. NASSIF, Murilo Meneghetti; LINGUANOTTO, Fernanda. A LGPD como norma de inclusão e fomento da diversidade no ambiente laboral brasileiro. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022.p.170.

mento para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde. Ou seja, aos profissionais de saúde é permitido o tratamento de dados quando o objetivo for especificamente de tutela da saúde.[47]

A última base legal prevista no artigo em tela, inciso X, é para a proteção do crédito, inclusive, quanto ao disposto na legislação pertinente. Esta hipótese autorizadora para tratamento de dados concede a possibilidade de um levantamento sobre o titular de dados, referente a sua adimplência ou inadimplência, o que influencia na tomada de decisão de conceder ou não um crédito.[48]

Diante das bases legais mencionadas acima, o controlador deve analisar cuidadosamente qual delas se aplica ao tratamento de dados, levando em consideração a natureza dos dados e a finalidade do tratamento. Em caso de várias opções disponíveis, o controlador deve escolher a hipótese mais segura e adequada para a situação específica.[49] Para a LGPD, não há hierarquia entre as bases legais. Neste sentido, a base legal mais adequada deverá ser a opção do responsável pelo tratamento de dados pessoais. [50]

3. Análise crítica da aplicação das bases legais no âmbito trabalhista

Considerando que o empregado é titular dos seus dados e o empregador é o controlador, porquanto trata os dados do trabalhador, devem ser observados os limites de tratamento de dados. A licitude do tratamento de dados pessoais deve ser adequada em uma das bases legais previstas na LGPD.[51] O titular dos dados deverá ter ciência do tratamento, independente da base legal utilizada, pois o titular dos dados poderá tomar decisões, tais como: ter acesso livre aos seus dados, segurança de qualidade, garantia da correção, precisão e a atua-

47. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 130

48. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021, p. 144.

49. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 22, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 de dez. 2022.

50. MONSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022.p.175.

51. MONSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 164.

lização dos seus dados.[52]

No campo das relações de trabalho, as hipóteses que legitimam o tratamento de dados pessoais do empregado mais frequentes para o autor Iuri Pinheiro são: Cumprimento de obrigação legal ou regulatória; execução de contrato ou de procedimentos preliminares relacionados ao contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral.[53]

Já para a autora Selma Carloto, as bases legais mais utilizadas seriam: Em primeiro lugar, cumprimento de obrigação legal ou regulatória, como por exemplo: nos casos de exames admissionais, periódicos e demissionais, exame virtual de ergonomia em teletrabalho e antecedentes para vigilantes. Em segundo lugar, execução de contrato ou de procedimentos preliminares relacionados ao contrato, utilizada para fins de conta salário, direitos decorrentes de acordo coletivo, entre outros. Em terceiro lugar, proteção à vida e integridade física do titular ou terceiro, empregada nos casos de vídeo vigilância, antecedentes para a vaga de babá, por exemplo. Em seguida, a quarta mais utilizada seria o legítimo interesse, aplicada nos casos de revista pessoal na saída, monitoramento de e-mail corporativo, canal de denúncia. E por fim, a base do consentimento, em alguns casos como: vídeo institucional, foto para revista, plano de saúde e bolo de aniversário. [54]

Na fase contratual é solicitado uma grande quantidade de dados que são necessários à execução contratual e para atender a ordens legais. Os dados podem ser relacionados à jornada de trabalho, ao valor do salário, eventuais descontos na folha, faltas, dados sobre saúde, status matrimonial e situações familiares. Já na etapa pós contratual, são necessários dados para a rescisão do contrato trabalhista, o que inclui exame médico demissional.[55]

Compete observar, quando várias bases legais são reveladas adequadas para o mesmo fim, deverá se escolher apenas uma única base legal. Por outro lado, quando o mesmo tratamento de dados possui vários objetivos para cada

52. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 56.

53. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 62.

54. CARLOTO, op. cit., p.134.

55. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 63.

uma das finalidades, deve-se optar por apenas uma base legal.[56] Além disso, as informações coletadas não poderão ser reutilizadas ou alteradas para outras finalidades diferentes do objetivo inicial e, as bases legais deverão ser decididas antes de qualquer operação de tratamento. [57]Cumpre ressaltar, que os incisos III, IV e X, do artigo 7º, da LGPD não cabem na relação de trabalho.[58]

3.1 O consentimento como base legal para o tratamento de dados de trabalhadores: apreciação e pressupostos para a sua validade e aplicação.

O consentimento está entre as 10 bases legais e poderá ser dispensado se as demais bases legais forem utilizadas, não havendo uma hierarquia entre elas. Tanto para a legislação brasileira como a europeia, o consentimento é a primeira hipótese de tratamento de dados pessoais. Apesar disso, o consentimento, em regra, não deve ser a primeira base legal a ser selecionada para tratar os dados pessoais, pois as bases legais são independentes entre si.[59]

De acordo com o artigo 5º, inciso XII, da LGPD, o consentimento, para ser válido deverá ser: de "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade determinada". Para o consentimento ser considerado livre, o titular deve ter como garantia a genuína opção em aceitar, negar ou retirar a sua manifestação de vontade, sem prejuízo. A manifestação de vontade livre presume-se um conhecimento prévio de quem vai consentir. [60] Outrossim, cumpre salientar, que o consentimento não poderá estar atrelado a uma parte não negociável

56. CLIMACO, Emerson. Nascimento, reflexos e reflexões trabalhistas da LGPD. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022.p.175.

57. MONSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 176.

58. ZAVANELLA, Fabiano; JUNIOR, Gilberto Carlos Maistro. Utilização dos dados pessoais do trabalhador e o legítimo interesse do empregador a partir do poder de direção. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 247.

59. SECCO, Monica Cibele Cantoni. Os Desafios do cumprimento da LGPD no ambiente corporativo vinculado ao ambiente remoto de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p.165.

60. MIRAGEM, Bruno; MADALENA, Juliano. Capítulo II – Do tratamento de dados pessoais. Sessão I- Dos requisitos para o tratamento de dados pessoais. Art. 7º. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.) Comentários a Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora Foco, 2022. p.72.

relacionada às condições gerais do contrato. [61]

No que se refere a manifestação informada, de acordo com o artigo 5º, inciso XII, da LGPD, quem busca colher o consentimento, tem o dever de informar ao titular dos dados, de forma completa, ou em termos que sejam compreensíveis e, de forma fácil ao destinatário para que o consentimento colhido seja válido,[62] para que possam indicar a finalidade específica pelo qual concorda que seus dados sejam tratados, como por exemplo, desempenhar o direito de derrogar o consentimento dado.[63]

Sobre a manifestação inequívoca, faz-se necessária a comprovação inconfundível de uma ação positiva pelo titular dos dados pessoais. Além disso, o consentimento do titular dos dados deverá ser vinculado a uma finalidade determinada, ou seja, o tratamento dos dados não poderá ser realizado com a finalidade diversa daquela que se deu o conhecimento antes da coleta do consentimento.[64] Conforme disposto no artigo 8º da Lei Geral de Proteção de Dados, o consentimento deverá ser fornecido por escrito ou qualquer outro meio que demonstre a manifestação de vontade do titular, sendo vedado o tratamento de dados pessoais, quando o consentimento estiver viciado[65].

Ademais, o consentimento poderá ser revogado através da manifestação expressa do titular a qualquer momento. Nas relações de trabalho as informações do empregado que são tratadas pelo empregador são fruto da subordinação inerente à relação de emprego. As relações trabalhistas demandam um grande fluxo de informações pessoais do trabalhador e, na maioria das vezes, o empregado depende economicamente do empregador, e diante do temor de sofrer represálias, o trabalhador não se opõe a determinadas decisões referente ao tratamento de dados.[66]

---

61. SECCO, Monica Cibele Cantoni. Os Desafios do cumprimento da LGPD no ambiente corporativo vinculado ao ambiente remoto de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p.165.

62. MIRAGEM, op. cit., p. 72.

63. MONSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022.p. 168.

64. MIRAGEM, Bruno; MADALENA, Juliano. Capítulo II – Do tratamento de dados pessoais. Sessão I- Dos requisitos para o tratamento de dados pessoais. Art. 7º. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.) Comentários a Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora Foco, 2022. p. 72.

65. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 91

66. GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo:

Além da situação de hipossuficiência do empregado, a autora Manoela Monteiro, ainda pondera que a hipótese do consentimento só deverá ser utilizada, caso as outras bases legais não se enquadrarem, tendo em vista que, o consentimento pode ser revisto a qualquer momento pelo titular dos dados, inviabilizando assim, o tratamento dos dados dos empregados, pois "há obrigações constantes que devem ser enviada ao governo, bem como rotinas de RH que serão inviabilizadas caso tenham que ser moldadas a pedido do titular de dados." [67]

Sendo assim, o consentimento não é válido caso o empregado, que é titular dos dados consentir, devido o receio das futuras consequências negativas que poderá sofrer. Diante dos fatos, o consentimento não seria a melhor hipótese para tratar dos dados pessoais nas relações de trabalho, pois se questiona se o consentimento se dará de maneira livre. Por outro lado, também não se pode afirmar que a hipótese do consentimento jamais deverá ser utilizada nas relações de emprego, como por exemplo, filmagem do empregado no ambiente de trabalho, processo seletivo.[68]

O consentimento ainda pode ser inválido, quando não for necessário o consentimento para a funcionalidade de determinado aplicativo, segundo entendimento do Grupo do Trabalho do Artigo 29. Inclusive no artigo 8º, parágrafo 3º, da LGPD, dispõe que é vedado o tratamento de dados pessoais através de vício de consentimento e, ao controlador lhe é conferido o ônus de provar que o consentimento foi adquirido em conformidade com a Lei.[69] Caso o consentimento seja a hipótese para autorização de tratamento de dados pessoais, este será coletado através de formulários, termos ou cláusulas em destaque no contrato.[70] Toda vez que for identificada essa base legal como tratamento

---

Revistas dos Tribunais, 2020. p. 217.

67. CEZARANI, Manoela Monteiro de Castro Antunes. A LGPD criou mais um passivo trabalhista? In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 128.

68. MAIA, Daniel Azevedo de Oliveira. As hipóteses autorizativas de tratamento de dados pessoais nas relações de trabalho sob a ótica da LGPD e do GDPPR. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 191.

69. GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 218.

70. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 91.

de dados, deverá ser elaborado os termos de consentimento.[71]

3.2 Aplicabilidade do legítimo interesse no âmbito das Relações Trabalhistas

A hipótese legal do legítimo interesse, objetiva possibilitar tratamentos de dados importantes referentes às atividades praticadas pelo controlador, e que possuam justificativa legítima. Os interesses legítimos poderão ser do controlador ou de terceiros, de acordo com o art. 7º, IX, da LGPD, podendo ser de interesses comerciais ou individuais. [72] Sobre o interesse legítimo de terceiros, a LGPD não delibera propriamente sobre a figura do terceiro, ao contrário da regulamentação europeia, que define no GDPR quem é a figura de terceiro, "sendo este a pessoa física ou jurídica, autoridade pública, agência, organismo diferente do titular dos dados, controlador, processador e pessoas que, sob a autoridade direta do controlador ou operador estão autorizadas a tratar dados pessoais."[73]

No tratamento dos dados com a justificativa da hipótese de legítimo interesse, necessita prevalecer os direitos e liberdades fundamentais do titular dos dados pessoais, sem que haja tratamento abusivo, não podendo contrariar o princípio da dignidade da pessoa humana e outros princípios fundamentais, inclusive, referente aos valores sociais do trabalho.[74]

Nos termos do artigo 10, II, §1º, da LGPD, o tratamento de dados deverá se basear somente por necessidades legítimas e consideradas situações concretas, atendendo os princípios da finalidade, necessidade e transparência, evitando o tratamento indiscriminado com fundamento no legítimo interesse.[75] Pois, "quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse."[76].

---

71. Ibidem, p. 109.

72. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 14-23, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 de dez. 2022.

73. BIONI, Bruno Ricardo; RIELLI, Mariana Marques; KITAYAMA, Marina. Colocando em movimento o legítimo interesse. In: BIONI, Bruno Ricardo (org). Proteção de dados: Contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p.162.

74. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 131.

75. CARLOTO, op. cit., p. 133.

76. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 14-15, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 de dez.

Além disso, é imperioso ressaltar que a base legal do legítimo interesse do controlador para tratamento de dados, somente poderá ser aplicada para tratar os dados rigorosamente necessários para o fim pretendido, conforme disposto no parágrafo 1º, do artigo 10 da LGPD.[77]

Quando se trata de relação de trabalho, o legítimo interesse do controlador (neste caso, o empregador), previsto no artigo 7º, inciso IX, da LGPD, combinado com o artigo 10 da mesma legislação, poderá ser a base para o tratamento de dados dos empregados.[78]

Desta forma, Selma Carloto e Marcel Edvar ressaltam que é necessário uma análise prévia acurada do legítimo interesse, necessitando realizar um teste de ponderação, é preferível nas relações de trabalho com vínculo ao consentimento, tendo em vista o desequilíbrio de poder presente nas relações de emprego e, é improvável que o empregado recuse o consentimento.[79] Sendo assim, o consentimento não é necessário em muitas situações, sendo em algumas vezes a hipótese autorizativa do legítimo interesse a mais indicada.[80]

Cumpre-se ressaltar, que o legítimo interesse do controlador não é intrínseco ao poder diretivo patronal, pois esta base legal exige-se uma situação concreta para ter autorização no tratamento dos dados. Esta hipótese autorizadora é aplicada em sentido estrito.[81] Para aplicação da base legal do legítimo interesse, optou-se por um teste prévio, que possui quatro fases: 1-Verificação da legitimidade do interesse: situação concreta e finalidade legítima (artigo 10, caput e I, da LGPD; 2-Necessidade: minimização e outras bases legais (artigo 10°, § 1º, da LGPD); 3-Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (artigo 10, II, da LGPD) e 4-Salvaguardas: transparên-

---

2022.

77. ZAVANELLA, Fabiano; JUNIOR, Gilberto Carlos Maistro. Utilização dos dados pessoais do trabalhador e o legítimo interesse do empregador a partir do poder de direção. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p.243.

78. CARLOTO, Selma. Lei Geral de proteção de Dados: enfoque nas relações de trabalho. 2 ed. São Paulo: LTR, 2021. p. 131.

79. CARLOTO, Selma; SIMÕES, Marcel Edavar. Legítimo interesse na lei geral de proteção de dados e a efetividade dos direitos fundamentais. Ltr Legislação do Trabalho: publicação mensal de legislação, doutrina e jurisprudência, São Paulo, v. 5, n. 85, p. 615. 01 mai. 2021. Mensal.

80. SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. [S. l.], v. 16, n. 90, 2019. p.128. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 10 dez. 2022.

81. Ibidem, p.249

cia e minimização dos riscos ao titular do dado (artigo 10, §§2º e 3º, da LGPD).[82]

Neste sentido, este requisito apenas corrobora o tratamento de dados pessoais exclusivamente no que for imprescindível para a finalidade a qual ele se propõe, devendo o agente de tratamento dos dados pessoais conservar o registro das operações realizadas. Além disso, é necessária a realização de RIPD (Relatório de Impacto à Proteção de Dados), com intuito de diminuir os riscos para ambas as partes da relação.

De acordo com o artigo 38 da LGPD[83], o RIPD poderá ser exigido pela Autoridade Nacional, principalmente quando se tratar de dados sensíveis. Além disso, o artigo 10, II, § 3º, da LGPD, o RIPD também poderá ser solicitado pela autoridade nacional ao controlador, quando o tratamento tiver como base seu interesse legítimo, observados os segredos comercial e industrial. Diante disto, verifica-se que a hipótese do legítimo interesse pode vir a ser a base mais adequada em determinadas ocasiões, em que sua aplicação deverá ser proporcional e limitada, sem causar danos aos direitos e garantias do indivíduo e ainda, sua aplicação poderá dispensar o consentimento para tratamentos. [84]

Contudo, cumpre ressaltar, que a hipótese autorizativa do legítimo interesse para o tratamento de dados pessoais, sem a necessidade do consentimento do titular, só é válida quando não versar sobre dados sensíveis, tendo em vista que, as hipóteses previstas no artigo 11º da LGPD, que trata sobre os dados pessoais sensíveis, não dispõe o legítimo interesse, o que será abordado a seguir.[85]E, com o fim de evitar colher o consentimento do titular, o controlador poderá se utilizar do exercício regular do direito, disposto na alínea d, inciso II do artigo 11, da LGPD.[86]

---

82. BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 244-248.

83. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

84. TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 21, maio 2020. Disponível em:< https://civilistica.emnuvens.com.br/redc/article/view/510 >. Acesso em:.10 de dez. 2022.

85. SOUZA, Carlos Affonso; VIOLA, Mario; PADRAO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. [S. l.], v. 16, n. 90, 2019. p.129. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 10 dez. 2022.

86. ZAVANELLA, Fabiano; JUNIOR, Gilberto Carlos Maistro. Utilização dos dados pessoais do trabalhador e o legítimo interesse do empregador a partir do poder de direção. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 249.

3.3 Hipóteses para o tratamento de dados pessoais sensíveis: análise do artigo 11 da LGPD

O artigo 11, da Lei Geral de Proteção de Dados, refere-se ao tratamento de dados pessoais sensíveis, que são inicialmente taxativos. Devido a relevância que é oferecida aos dados pessoais sensíveis, a LGPD traz hipóteses específicas para o tratamento de dados. Em alguns casos, são complementados pelo artigo 14, que trata de dados pessoais de crianças e adolescentes, e o artigo 23, que versa sobre o tratamento de dados pessoais pela pessoa jurídica de direito público, ambos artigos da Lei em voga.[87] Tais hipóteses autorizativas, que são tratadas no artigo 11 da LGPD, por abordar dados pessoais sensíveis, têm requisitos mais rígidos estabelecidos para autorizar o tratamento dos dados.[88]

As bases legais previstas no artigo 7º da LGPD, se repete em sua maioria no artigo 11°, exceto, a do legítimo interesse do controlador ou de terceiros, que se encontra no inciso IX do artigo 7º e, a hipótese de proteção ao crédito, estabelecida no inciso X, do aludido artigo. Por outro lado, o dispositivo que trata dos dados pessoais sensíveis, traz base mais específica, que tem a finalidade de prevenir fraudes, garantindo a segurança do titular dos dados (Art. 11, II, "g", da LGPD).

Baseado no artigo 11, o consentimento deverá ser apresentado de forma destacada e específica, além de ser livre, informado e inequívoco. Além disso, a Lei em tela, dispõe que se o titular não fornecer consentimento, os dados poderão ser tratados nas hipóteses do artigo 11, II, da LGPD[89]em que for indispensável nessas situações.[90] Porém, conforme já exposto, a base legal do consentimento dificilmente será utilizada nas relações de trabalho, tendo em vista a natureza da relação, pois, a empresa deverá demonstrar que o trabalhador não será prejudicado se não o consentir.[91]

---

87. TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. São Paulo: Editora Foco, 2022. p. 129.

88. SOUZA, Carlos Affonso; VIOLA, Mario; PADRAO, Vinícius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. Direito Público. [S. l.], v. 16, n. 90, 2019. p. 117. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 10 dez. 2022.

89. MONSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 174.

90. Ibidem, p. 174.

91. CARLOTO, Selma. Seção II: Do tratamento de Dados Pessoais Sensíveis. In: ALMIRÃO, Mariana; CARLOTO, Selma (coord.). Lei Geral de proteção de Dados comentada: com enfoque nas relações de trabalho. 1 ed. São Paulo: LTR, 2021. p.66.

No âmbito laboral, por parte dos empregadores ideológicos, há necessidade de tratar determinados dados sensíveis, como por exemplo: convicção religiosa, a opinião política, a filiação ao sindicato ou a organização de caráter religioso, filosófico ou político, tendo em vista que, para o funcionamento das Organizações de Tendência,[92] esses dados se mostram relevantes. Neste sentido, os dados sensíveis poderão ser tratados justificados pela hipótese de tratamento com a finalidade de exercer regularmente os direitos, até mesmo em contrato, processo judicial, administrativo e arbitral (artigo 11, II, alínea d, da LGPD).

A coleta de alguns dados sensíveis se justifica apenas nas organizações ideológicas, em que o empregado tem a função de realizar tarefas de tendências, nos quais os dados coletados têm papel relevante para prestação desses serviços. Porém, para os empregados que exercem tarefas sem conteúdo ideológicos, a coleta de dados não tem legitimidade e não pode se enquadrar na hipótese do artigo 11, II, alínea d, da LGPD.[93]

Considerações finais

Com a evolução tecnológica e os consequentes desafios em proteger os dados pessoais, inclusive, em um contexto trabalhista, muito se questiona sobre a privacidade dos dados pessoais dos trabalhadores, considerando a necessidade da circulação de determinadas informações, em cumprimento às prerrogativas e direitos que a relação de trabalho traz.

Apesar da Lei Geral de Proteção de Dados não abordar diretamente o tratamento de dados no contexto laboral, a aplicabilidade da referida Lei não é afastada, tendo em vista que, o trabalhador é uma pessoa natural, de tal modo, considerado titular de dados. Em contrapartida, o empregador, seja ele pessoa física ou jurídica, ao tratar os dados pessoais do trabalhador, se insere na figura do controlador de dados, o que não resta dúvidas da aplicação da LGPD na relação de trabalho. [94] Outrossim, no artigo 4º da LGPD, em que versa sobre

92. Para melhor entendimento, a autora Gabriela Curi define Organizações de Tendência: “aquelas cuja finalidade é a difusão de determinada ideologia, independentemente do ânimo de lucro, formadas por pessoas (ou apenas por uma pessoa) que se utilizam dessa para expressar seu pensamento, credo, religião ou ideologia” (GASPAR, 2020. p.226.)

93. GASPAR, Gabriela Curi Ramos. LGPD e o tratamento de dados sensíveis nas organizações de tendência. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 225.

94. MOSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno,

hipóteses em que não é aplicada, não fez alusão às relações trabalhistas.

Em contrapartida, com a falta de artigos específicos na Lei sobre o tratamento de dados na relação laboral, a aplicação da LGPD necessitará observar as demais normas existentes no ordenamento jurídico.[95]Nessa linha de raciocínio, as empresas precisam se adequar à LGPD, não só no aspecto consumerista, mas principalmente em todas as fases da relação de trabalho com o objetivo de preservar a privacidade do titular dos dados – seja ele cliente, empregado, consumidor, prestador de serviço – ou tornar os dados de forma anônima, para que não seja possível a sua vinculação aos respectivos titulares.[96]

Contudo, o interesse econômico não pode estar acima dos direitos fundamentais do cidadão. O Relatório de Impacto à Proteção de Dados é uma das ferramentas para adequação à LGPD e ao compliance, pois minimiza o risco de lesionar os direitos fundamentais dos titulares.[97] As relações de trabalho perpassam por diversas fases, que vão desde a candidatura do interessado na vaga de trabalho ou emprego, ao término do contrato trabalhista e a exclusão dos dados pessoais. Nessas fases, há tratamento de dados pessoais e, precisam estar de acordo com alguma base legal prevista na LGPD[98]

É necessário que o controlador dos dados pessoais tenha a ciência e a percepção da aplicação, e qual será a utilidade e finalidade para tratamento dos dados pessoais. As empresas devem reorganizar suas práticas internas introduzindo políticas e regulamentos, se atentando à proteção dos dados pessoais dos empregados. Observando ainda, um prazo de armazenamento e como se dará a exclusão dos dados pessoais dos trabalhadores, com o fim da relação de trabalho.[99]

2022. p. 161.

95. ARAUJO, Adriane Reis. Proteção da informação envolvendo empregados e suas dimensões no direito do trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p.127.

96. JUNIOR, Vicente Vasconcelos; FILHO, Rodolfo Pamplona. A Lei Geral de Proteção de dados e seus reflexos nas relações jurídicas trabalhistas. In: Coni MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020.p.86

97. CARLOTO. Selma. O compliance Trabalhista: E a efetividade dos direitos humanos dos trabalhadores. São Paulo: LTR, 2021.p. 33.

98. MOSELE, Rafael. LGPD: Estudo prático das bases legais nas relações de trabalho. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022. p. 162.

99. PIERONI, Verissa Coelho Cabral. Noções gerais sobre proteção de dados nas relações de emprego. In: MIZIARA, Raphael;

Conforme exposto, na LGPD faltou atenção para a regulação das relações de trabalho, que diante da condição de subordinação e dependência econômica do empregado ao empregador, o conceito de consentimento não é o mais adequado. Sendo assim, essa lacuna tem um amplo potencial danoso para ambas as partes e que exigirão a cautela do Judiciário e da ANPD. Na relação de trabalho, a base legal do consentimento é afastada de um modo geral. O consentimento poderá apenas ser utilizado quando o titular dos dados tem a possibilidade de negar de forma positiva o consentimento, sem sofrer consequências negativas de sua recusa.[100]

Neste sentido, as entidades deverão considerar os casos concretos à luz da LGPD e com alicerce nas garantias fundamentais da Constituição Federal.[101] As empresas necessitam considerar ainda, a hipossuficiência do empregado e avaliar sobre aplicação do consentimento referente aos seus dados pessoais e pessoais sensíveis que foram coletados em virtude da relação de emprego.[102] O GDPR, destacando seu artigo 30, além das experiências já habituadas nas relações de trabalho sob sua vigência, poderá servir de exemplo para indicar a interpretação mais adequada.[103]

Considerando a assimetria de poder entre empregado e empregador, a atenção precisa ser redobrada, sendo necessário verificar a finalidade e a necessidade para o tratamento dos dados pessoais. Além disso, é preciso assegurar a transparência do tratamento aos titulares. Nas relações de trabalho, é imperioso se adequar a LGPD, analisando o auxílio da tecnologia da informação para garantir a segurança dos dados armazenados nas empresas. É necessário considerar a interseção entre a Lei Geral de Proteção de Dados, o

---

MOLLICONE, Bianca; PESSOA, André (org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 45.

100. CARLOTO, Selma; MASSONI, Túlio de Oliveira. Tecnologia, inteligência artificial, robótica e dados nas relações laborais: algumas promessas e muitos perigos. Ltr Legislação do Trabalho: publicação mensal de legislação, doutrina e jurisprudência, São Paulo, v. 1, n. 86, p. 92, 01 jan. 2022. Mensal

101. NASCIMENTO, Ivan. Kaminski do; BOSCATTO, Gianfranco. Proteção de Dados Pessoais nas Relações de Trabalho. São Paulo: Dialética, 2022. Edição do Kindle. pp.113-114.

102. PIERONI, Verissa Coelho Cabral. Noções gerais sobre proteção de dados nas relações de emprego. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020.p.45.

103. ZAVANELLA, Fabiano; JUNIOR, Gilberto Carlos Maistro. Utilização dos dados pessoais do trabalhador e o legítimo interesse do empregador a partir do poder de direção. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 254.

Direito do Trabalho, compliance e tecnologia da informação (TI). [104]

Sendo assim, a empresa deverá assegurar a segurança da informação em todas as fases do tratamento de dados pessoais, que inicia no processo seletivo. O tratamento dos dados pessoais deve ocorrer durante o ciclo de vida dos dados pessoais, que inicia na coleta e termina no descarte. A finalidade do tratamento deve ser determinada e é necessária uma base legal que oriente as operações de tratamento dos dados.[105] Ressalta-se que a autodeterminação informativa é basilar da LGPD, já que os titulares dos dados voltaram a ter controle sobre estes.[106] Ao controlador, caberá discernir entre as bases legais autorizadoras para o tratamento de dados, quando houver mais de uma hipótese, a mais adequada, ou seja, a mais segura e específica, considerando a adequação, necessidade e a finalidade legitimadora.[107]

---

104. MONNAZI, Ricardo Nogueira. Banco de currículos: intersecção e conformidade entre o direito do trabalho pré-contratual e a LGPD. In: PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial. São Paulo: Mizuno, 2022.p.313.

105. QUINELATO, Pietra Daneluzzi. Seção IV: Do término do tratamento de dados. In: ALMIRÃO, Mariana; CARLOTO, Selma (coord.). Lei Geral de proteção de Dados comentada: com enfoque nas relações de trabalho. 1 ed. São Paulo: LTR, 2021. p. 81.

106. CARLOTO, Selma; MASSONI, Túlio de Oliveira. Tecnologia, inteligência artificial, robótica e dados nas relações laborais: algumas promessas e muitos perigos. Ltr Legislação do Trabalho: publicação mensal de legislação, doutrina e jurisprudência, São Paulo, v. 1, n. 86, p. 84-97, 01 jan. 2022. Mensal.

107. PINHEIRO, Iuri; BOMFIM, Vólia. A Lei Geral de Proteção de Dados e seus impactos nas relações de trabalho. In: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo: Revistas dos Tribunais, 2020. p. 62.

Referências

ALMIRÃO, Mariana; CARLOTO, Selma (coord.). **Lei Geral de proteção de Dados comentada: com enfoque nas relações de trabalho**. 1 ed. São Paulo: LTR, 2021.

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

BIONI, Bruno Ricardo (org). **Proteção de dados: Contexto, narrativas e elementos fundantes**. Curitiba: Appris, 2022. p.283.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 09 jun. 2022.

_____. **Decreto-Lei 5452, de 01º de maio de 1943. Consolidação das Leis do Trabalho (CLT)** Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm#art6>. Acesso em: 22 de jun. de 2022.

_____. **Emenda Constitucional nº 115. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília**, DF. 2022. Disponível em: https://www.in.gov.br/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 01 jul. 2022.

_____. **Lei 12.414, de 09 de junho de 2014**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 10 maio 2022.

_____. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 mai. 2022.

_____. **Lei nº 13.467, de 13 de julho de 2017**. Altera a Consolidação das Leis do Trabalho (CLT),

_____. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de dados (LGPD). Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.> Acesso em: 09 jul. 2022.

CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da (Org.). **Futuro do Trabalho: os efeitos da revolução digital na sociedade**. Brasília: ESMPU, 2020.

CARLOTO, Selma. **Lei Geral de proteção de Dados: enfoque nas relações de trabalho**. 2 ed. São Paulo: LTR, 2021.

_____. **Manual prático de adequação à LGPD com enfoque nas relações de trabalho**. São Paulo: LTR, 2021.

_____. **O compliance Trabalhista: E a efetividade dos direitos humanos dos trabalhadores**. São Paulo: LTR, 2021.

CARLOTO, Selma; MASSONI, Túlio de Oliveira. **Tecnologia, inteligência artificial, robótica e dados nas relações laborais: algumas promessas e muitos perigos**. Ltr Legislação do Trabalho: publicação mensal de legislação, doutrina e jurisprudência, São Paulo, v. 1, n. 86, p. 84-97, 01 jan. 2022. Mensal.

CARLOTO, Selma; SIMÕES, Marcel Edavar. **Legítimo interesse na lei geral de proteção de dados e a efetividade dos direitos fundamentais**. Ltr Legislação do Trabalho: publicação mensal de legislação, doutrina e jurisprudência, São Paulo, v. 5, n. 85, p. 611-624. 01 mai. 2021. Mensal.

DONEDA, Danilo; MENDES, Laura Schertel;

CUEVA, Ricardo. **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**. A caminho da efetividade: contribuições para implementação da LGPD. São Paulo: Revistas dos Tribunais, 2020.

EDPB. ***Guidelines 05/2020 on consent under Regulation 2016/679***. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>Acesso em: 10 jan. de 2023.

GIUNTINI, Adriana *et al*. **LGPD nas relações de trabalho**. Salvador, BA: Editora Motres, 2021. E-book (38p.) color. ISBN: 978-65-89765-07-3. Disponível em: <https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf.> Acesso em: 27 jul. 2022..

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.) **Comentários a Lei Geral de Proteção de Dados Pessoais**. São Paulo: Editora Foco, 2022.

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André (Org.). **Reflexos da LGPD no Direito e no Processo do Trabalho**. São Paulo: Revistas dos Tribunais, 2020.

MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18)**. Revista de direitos e garantias fundamentais, v. 19, n. 3, p. 159-180, 2018. Disponível em: < https://doi.org/10.18759/rdgf.v19i3.1603>. Acesso em: 25 de jun. 2022.

NASCIMENTO, Ivan Kaminski do; BOSCATTO, Gianfranco. **Proteção de Dados Pessoais nas Relações de Trabalho**. São Paulo: Dialética, 2022. Edição do Kindle.

PERREGIL, Fernanda; CALCINI, Ricardo. (Org.). **LGPD e compliance trabalhista: Os desafios atuais do direito do trabalho empresarial**. São Paulo: Mizuno, 2022.

REQUIÃO, Maurício (org.). **Proteção de dados pessoais: novas perspectivas**. Salvador, Editora: Edufba, 2022.

RODOTÀ, Stefano. **A Vida na sociedade da vigilância - a privacidade hoje**. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SOUZA, Carlos Affonso; VIOLA, Mario; PADRAO, Vinícius. **Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais**. Direito Público. [S. l.], v. 16, n. 90, 2019. p. 109-131. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 5 set. 2022.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. São Paulo: Editora Foco, 2022.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com, v. 9, n. 1, p. 1-38, maio 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em:.10 de dez. 2022.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **O consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521>. Acesso em: 14 jan. 2022.

UNIÃO EUROPEIA. **Grupo de Trabalho do Artigo 29**.º. Parecer 15/2011 Sobre a definição do consentimento. Disponível em: <https://www.gpdp.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC15_2011%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_PT.pdf>Acesso em: 10 fev. de 2023.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

14

A Lei Geral de Proteção de Dados e a responsabilidade civil das empresas no e-commerce em casos de vazamento de dados

BIANCA ALVES BATISTA

BIANCA ALVES BATISTA[1]

Introdução

O presente estudo tem como escopo a análise da atribuição da responsabilidade civil das empresas quando sofrem vazamentos de dados pessoais de seus usuários de e-commerce, ou seja, consumidores, na internet. Busca-se apresentar a posição da legislação e da Lei Geral de Proteção de Dados (LGPD) sobre o tema, assim como abordar a proteção do consumidor no e-commerce. É preciso que as empresas tenham o aconselhamento do operador do Direito para se adequarem quanto à proteção de dados dos seus clientes. Ao final, apresenta-se a necessidade de adequação das empresas diante do risco do negócio, o e-commerce, e a possibilidade de sofrerem vazamento de dados e serem, no futuro, responsabilizadas por possíveis danos.

Analisa-se a captação de dados na internet diante da coleta e comercialização não autorizada de dados destinados aos anúncios direcionados. O objetivo do artigo é o de verificar o exame da LGPD em razão da disposição sobre o regime de responsabilidade civil que é considerado pela mencionada lei.

A LGPD é uma legislação brasileira que tem como objetivo proteger os dados pessoais de cidadãos, estabelecendo regras claras para a coleta, armazenamento, uso e compartilhamento desses dados por empresas e instituições públicas. A norma se faz importante para a sociedade brasileira nos aspectos político, econômico e social. No aspecto político, a LGPD é uma legislação que garante o direito fundamental à privacidade e proteção de dados pessoais, algo fundamental para o exercício da cidadania e da democracia.

No aspecto econômico, a LGPD é uma lei que traz benefícios para as empresas que respeitam as regras de proteção de dados. Ao proteger os dados pessoais dos seus clientes, uma empresa pode aumentar a confiança e a fidelidade dos seus clientes, além de evitar prejuízos financeiros decorrentes de

1. Advogada. Graduada em Direito pela Pontifícia Universidade Católica de São Paulo em 2018. Pós-graduada em Direito Digital pelo CEPED/UERJ (Universidade do Estado do Rio de Janeiro) em parceria com o ITS (Instituto de Tecnologia e Sociedade do Rio). Certified Data Protection Office (CDPO/BR) e Certified Information Privacy Manager (CIPM) pela IAPP.

vazamentos de dados e possíveis sanções legais. Além disso, a LGPD incentiva a inovação e o desenvolvimento de novas tecnologias de proteção de dados, o que pode gerar novas oportunidades de negócios.

No aspecto social, a LGPD é fundamental para a proteção dos direitos humanos, principalmente no que diz respeito à proteção da privacidade e dos dados pessoais dos cidadãos. A lei também contribui para reduzir a discriminação e o preconceito que podem surgir a partir da utilização inadequada de dados pessoais. A LGPD também pode incentivar o desenvolvimento de políticas públicas mais eficazes, uma vez que as informações coletadas pelos órgãos governamentais estarão protegidas pela legislação.

Em resumo, a Lei Geral de Proteção de Dados é importante para a sociedade brasileira nos aspectos político, econômico e social, uma vez que garante o direito fundamental à privacidade e proteção de dados pessoais, traz benefícios para as empresas que respeitam as regras de proteção de dados, e contribui para a proteção dos direitos humanos e para o desenvolvimento de políticas públicas mais eficazes.

Assim, o que será disposto em três capítulos aborda o vazamento de dados pessoais, o sistema de responsabilidade civil na LGPD e, por fim, a adequação das empresas quanto à LGPD.

1. Vazamento de dados pessoais: qual a responsabilidade das empresas de e-commerce?

O direito do consumidor se mostra como uma conquista da sociedade contemporânea, sendo fundamental para promover a proteção daquele que é mais vulnerável: o consumidor. O equilíbrio das relações jurídicas de consumo precisa ser atualizado a partir das formas mais novas de consumo que surgem e, neste ponto, aborda-se a problemática do presente estudo, que é a questão da captação e do vazamento de dados que podem ocorrer com o uso do *e-commerce* no consumo. A LGPD e as questões do direito do consumidor se fundem neste sentido.

A partir dos avanços tecnológicos que foram inseridos na sociedade, no Direito passaram a se formar discussões voltadas às atividades que ocorrem, principalmente, na *internet*. A *internet*, por sua vez, é aquela que supera fronteiras, que vai além das mudanças do próprio tempo, acompanhou tanto aspectos positivos como os aspectos negativos nas novas configurações da sociedade. Em 2014, entrou em vigor o Marco Civil da Internet. A partir desse Marco, novas discussões no Brasil foram influenciadas por outras novas discussões no

mundo todo. Em 2018, em diálogo com o debate europeu é publicada a LGPD.

Para definições do presente estudo, entende-se *e-commerce* como o comércio eletrônico de produtos e serviços através de compras e vendas na *internet*. É o ramo da atividade econômica que mais cresce – e continua crescendo – no mundo todo. Neste sentido, Forgioni introduz:

> Hoje, podemos paragonar as estradas medievais à Internet. Em determinados setores da economia, seu domínio é o controle do comércio, e o bloqueio do acesso à rede, a expulsão do mercado. Tal como fizeram os glosadores, devemos deter-nos sobre os textos legais disponíveis e, reinterpretando-os, delinear as normas que se prestam a pautar a atuação dos agentes econômicos nesse novo ambiente[2].

Os avanços tecnológicos e o advento da *internet* ultrapassaram os avanços do próprio Direito e das legislações. No entanto, não se pode negar a importância da LGPD atualmente e em como é preciso se adaptar à nova realidade. Godinho[3] explica sobre a questão do armazenamento de dados dos consumidores durante as compras na *internet* e discute a atribuição da responsabilidade de pessoa ou empresa que, por alguma falha na adequação à LGPD, sofre vazamentos de dados de seus consumidores/usuários armazenados em seu *site*.

Explica-se que o armazenamento de dados, antes atrelado a um cartão de memória que para ser destruído bastava ser perfurado, rompeu os padrões a partir do avanço da tecnologia e evoluiu de maneira que, atualmente, é entendido como aquele armazenado na *cloud storage*, em português, "armazenamento na nuvem". Esse armazenamento se volta para abarcar uma quantidade infindável de informações de diversos usuários. Destaca-se: "o armazenamento de dados abrange não só o que encontramos na rede mundial de computadores interligados, mas também os chamados bancos de dados"[4].

2. FORGIONI, Paula. Apontamentos sobre os aspectos jurídicos do e-commerce. São Paulo: RAE – Revista de Administração de Empresas, vol. 40, n. 4, out./dez. 2000, p. 71. Disponível em https://www.scielo.br/j/rae/a/b7jhPyWv6sbVfmpNDvzqKQs/?format=pdf&lang=pt. Acesso em 27 abr. 2023.

3. GODINHO, Adriano Marteleto (et al.). A responsabilidade civil pela violação a dados pessoais. São Paulo: Revista IBERC, vol. 3, n. 1, jan./abr. 2020. Disponível em https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78. Acesso em 10 jan. 2023.

4. Ibidem, p. 3.

Sobre o armazenamento de dados, Schreiber[5] ensina que a responsabilidade de proteção está atribuída tanto para entidades públicas como privadas. Essas empresas se valem da frequência cada vez maior de padronizações a fim de se avaliar uma infinidade de dados individuais, de forma que esses dados de clientes que fornecem se veem "capturados". Por muitas vezes, poderia ocorrer esse armazenamento interno de dados de clientes de forma involuntária.

É a partir do armazenamento e captação de dados dos clientes que os algoritmos utilizados constroem os perfis de consumidores. Ou seja, eles são atribuídos a cada indivíduo a partir do que esses clientes compram, buscam, se interessam na internet e de acordo com o histórico de navegação e compras. Há uma verdadeira personalização para que uma pessoa que tenha interesses em determinados produtos e assuntos tenha mais "acesso" a esse mercado.

Assim, entende-se que o armazenamento de dados – ou o banco de dados – se define da seguinte forma:

> [...] diz respeito a informações pessoais que ficam arquivadas por entes públicos, privados ou pelo próprio indivíduo, para serem acessados posteriormente. Este armazenamento outrora inofensivo, passou a ameaçar direitos e garantias fundamentais, tais quais a privacidade, a imagem e a honra[6].

Além disso, pode-se verificar que a própria LGPD trouxe no seu artigo 5º, inciso IV, a definição de banco de dados: "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico"[7].

Situações de uso e armazenamento de dados podem ser exemplificadas como aquelas em que o anúncio publicitário é feito com base nos dados armazenados das pesquisas realizadas, ou mesmo, em âmbito alheio à internet, com os dados pessoais dos usuários que foram cadastrados em lojas.

Existiram, recentemente, diversas situações em que ocorreram vazamen-

5. SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de dados pessoais. In. BIONI, Bruno Ricardo (Org.). Tratado de Proteção de Dados Pessoais – vol. 1. Rio de Janeiro: Editora Forense, 2020.

6. GODINHO, Adriano Marteleto (et al.). A responsabilidade civil pela violação a dados pessoais. São Paulo: Revista IBERC, vol. 3, n. 1, jan./abr. 2020, p. 3. Disponível em https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78. Acesso em 10 jan. 2023.

7. BRASIL. Lei nº 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 10 jan. 2023.

to de dados dos usuários em face do armazenamento de dados dentro dos bancos das empresas. Em 2014, no aplicativo de comunicação social chamado Snapchat foram vazados dados e mais de cem mil fotos ao público de forma geral, ferindo não somente os direitos de personalidade, mas o direito à proteção dos dados[8]. À época, a empresa e o provedor de hospedagem haviam afirmado que o vazamento somente teria ocorrido devido a um serviço efetuado por terceiros e que se viram proibidos em acessar o aplicativo[9].

O vazamento de dados do Snapchat compreendeu cerca de 13 GB de informações e mais de 100 mil imagens dos usuários do serviço[10]. Alega-se que os dados obtidos por serviços terceirizados prejudicaram o funcionamento do aplicativo, que prometia que as imagens, fotos e informações ali compartilhadas se "autodestruiriam"[11]. Na matéria de Rohr[12] e estudo acadêmico para dissertação de mestrado de Gomes[13], informa-se que esses dados foram publicados no site "viralpop", distribuindo diversos vírus e que foi brevemente retirado do ar.

8. DESLANDES, Suely Ferreira (et al.). Vazamento de nudes: da moralização e violência generificada ao empoderamento. São Paulo: Ciênc. Saúde Coletiva, vol. 27, n. 10, out. 2022. Disponível em https://www.scielo.br/j/csc/a/Fp9zrh6C64Y4DLpx5TdvL8b/abstract/?lang=pt. Acesso em 27 abr. 2023; ROHR, Altieres. Vazamento de dados do Snapchat expõe milhares de fotos na web. São Paulo: G1. Publicado em 10 out. 2014. Disponível em https://g1.globo.com/tecnologia/noticia/2014/10/vazamento-de-dados-do-snapchat-expoe-milhares-de-fotos-na-web.html. Acesso em 10 jan. 2023.

9. SILVA, Walyf Lopes da (et al.). Aspectos jurídicos da exposição de dados pessoais na internet e sua relação com o direito fundamental à privacidade. São Paulo: Revista Ibero-americana de Humanidades, Ciência e Educação, vol. 7, n. 10, 2021. Disponível em https://www.periodicorease.pro.br/rease/article/view/2906. Acesso em 09 mar. 2023.

10. GOMES, Anselmo Lacerda. Mapeamento de incidentes com identidades digitais e estratégias de controle em ambientes virtuais. Pernambuco: Universidade Federal de Pernambuco, Mestrado em Ciência da Computação, ago. 2015. Disponível em https://repositorio.ufpe.br/handle/123456789/16377. Acesso em 09 mai. 2023.

11. O vazamento de dados do Snapchat ocorreu devido a uma vulnerabilidade no sistema de segurança da empresa. Hackers exploraram essa vulnerabilidade para acessar os servidores do Snapchat e roubar informações pessoais, como nomes de usuário, números de telefone e endereços de e-mail. Esses dados foram então postados em um site de compartilhamento de arquivos e disponibilizados publicamente. Esse vazamento de dados teve um impacto significativo na reputação do Snapchat e na confiança dos usuários no aplicativo. A empresa enfrentou críticas por não ter protegido adequadamente as informações dos usuários e por não ter notificado os usuários afetados imediatamente após o vazamento. Além disso, a empresa foi processada pelo Federal Trade Commission (FTC) dos Estados Unidos por ter enganado os usuários sobre a privacidade de suas informações. Esse vazamento de dados do Snapchat é um exemplo claro de como a segurança e a privacidade dos dados pessoais dos usuários são fundamentais para a reputação e o sucesso de uma empresa. As empresas devem tomar medidas adequadas para proteger os dados pessoais de seus usuários e notificar imediatamente os usuários afetados em caso de violação de dados. Essas medidas não só protegem a privacidade dos usuários, mas também podem evitar prejuízos financeiros e de reputação para a empresa (Cf. GOMES, Anselmo Lacerda. Mapeamento de incidentes com identidades digitais e estratégias de controle em ambientes virtuais. Pernambuco: Universidade Federal de Pernambuco, Mestrado em Ciência da Computação, ago. 2015. Disponível em https://repositorio.ufpe.br/handle/123456789/16377. Acesso em 09 mai. 2023).

12. ROHR, Altieres. Vazamento de dados do Snapchat expõe milhares de fotos na web. São Paulo: G1. Publicado em 10 out. 2014. Disponível em https://g1.globo.com/tecnologia/noticia/2014/10/vazamento-de-dados-do-snapchat-expoe-milhares-de-fotos-na-web.html. Acesso em 10 jan. 2023.

13. GOMES, Anselmo Lacerda. Mapeamento de incidentes com identidades digitais e estratégias de controle em ambientes virtuais. Pernambuco: Universidade Federal de Pernambuco, Mestrado em Ciência da Computação, ago. 2015. Disponível em https://repositorio.ufpe.br/handle/123456789/16377. Acesso em 09 mai. 2023.

Outro caso que ainda se discute é a questão do vazamento de dados da rede Yahoo!, que sofreu diversos ataques hackers entre 2013 e 2016, atingindo todas as contas criadas na rede, cerca de três bilhões de contas. Devido às falhas de segurança, ainda seguem sendo discutidos nos Estados Unidos os valores referentes às indenizações que deverão ser pagas pelos provedores de acesso da rede eletrônica de e-mails[14].

Outra situação de vazamento de dados ocorreu com o banco de dados da rede de hotéis Marriot, no ano de 2018, que se estimou afetar quinhentos milhões de clientes. Dados pessoais como nome, número de telefone, data de nascimento, endereço de e-mail, passaporte, tempo e valor da hospedagem foram acessados por terceiros, causando sérios transtornos à rede hoteleira. O ataque hacker que vinha ocorrendo desde 2014, somente foi descoberto em 2018. Um novo vazamento de dados ocorreu em 2020 e afetou 5,2 milhões de hóspedes da rede[15].

De acordo com Bisso[16], no primeiro trimestre de 2019 já se observavam muitos vazamentos de dados de grandes volumes. Um exemplo dado pelo autor em seu artigo trata sobre o vazamento de 2,4 milhões de usuários da rede Blur em março de 2020. A empresa que gerencia senhas e que sofreu o vazamento de dados de seus usuários a terceiros, dados como os *e-mails*, dicas de senhas, endereços de IP dos computadores e celulares, das senhas cifradas, entre outras informações. Entre outras questões de vazamento, estão os 540 milhões de registros do Facebook e as 773 milhões de senhas e dados que foram vazados também entre 2018 e 2019[17].

---

14. GOGONI, Ronaldo. Vazamento expôs dados de mais de 500 milhões de usuários do Yahoo!. São Paulo: Meio Bit, 2018. Disponível em https://meiobit.com/352105/yahoo-vazamento-massivo-pode-ter-comprometido-centenas-de-milhoes-de-contas-de-usuarios/. Acesso em 27 abr. 2023; ANDREW, Scottie. Yahoo could pay you $358 for its massive data breach settlement. Here's how to claim it. Nova Iorque: CNN. Publicado em 15 out. 2019. Disponível em https://edition.cnn.com/2019/10/15/business/yahoo-data-breach-settlement-trnd/index.html. Acesso em 09 mai. 2023; CHACON, Guilherme. Vazamento de dados pessoais: dano presumido ou expectativa não indenizável de dano. São Paulo: Lapin.Org. Publicado em 13 set. 2021. Disponível em https://lapin.org.br/2021/09/13/vazamento-de-dados-pessoais-dano-presumido-ou-expectativa-nao-indenizavel-de-dano/. Acesso em 09 mai. 2023.

15. HÁRAN, Juan Manuel. Marriott sofre novo vazamento de dados que afeta 5,2 milhões de hóspedes. [S.l.]: We Live Security. Publicado em 2 abr. 2020. Disponível em https://www.welivesecurity.com/br/2020/04/02/marriott-sofre-novo-vazamento-de-dados-que-afeta-52-milhoes-de-hospedes/. Acesso em 06 abr. 2022.

16. BISSO, Rodrigo (et al.). Vazamento de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. São Paulo: Revista Eletrônica Argentina-Brasil de Tecnologia da Informação e da Comunicação, vol. 3, n. 1, 2020. Disponível em https://revistas.setrem.com.br/index.php/reabtic/article/view/378. Acesso em 10 jan. 2023.

17. BARAN, Guru. 2.4 Million Blur Password Manager Users Data Exposed Online. [S.l.]: GBHackers on Security. Publicado em 3 jan. 2019. Disponível em https://gbhackers.com/2-4-million-blur-password/. Acesso em 09 mai. 2023; NEOTEL. Global Privacy Control surge como a mais recente tentativa de permitir que os internautas escolham se querem ser rastreados online. [S.l.]: Neotel Segurança Digital. Publicado em 12 out. 2020. Disponível em https://blog.neotel.com.br/2020/10/12/global-privacy-control-surge-como-a-mais-recente-tentativa-de-permitir-que-os-internautas-escolham-se-querem-ser-rastrea-

Explicando: a empresa de segurança cibernética Comparitech divulgou que encontrou um banco de dados desprotegido pertencente à empresa de privacidade online Abine, que é a proprietária do serviço de gerenciamento de senhas e proteção de privacidade chamado "Blur". O banco de dados exposto continha informações de mais de 2,4 milhões de usuários do serviço, incluindo endereços de e-mail, senhas criptografadas, endereços IP e outros dados pessoais[18].

De acordo com a Comparitech[19], o banco de dados estava desprotegido e acessível a qualquer pessoa que soubesse a URL correta. A empresa de segurança cibernética alertou Abine sobre o vazamento e a empresa agiu rapidamente para corrigir o problema. Ainda assim, a exposição das informações pessoais dos usuários do Blur é um exemplo do risco que as empresas correm quando não protegem adequadamente os dados dos seus clientes.

Em 2023, segundo o relatório da companhia de segurança digital Acronis, diversas empresas sofreram com o vazamento de dados dos usuários dos programas e redes sociais como deezer, twitter e paypal[20]. Os custos desses vazamentos podem aumentar ainda mais durante o ano de 2023, atingindo a marca de US$ 5 milhões[21].

Bisso[22] ainda trouxe à tona outros casos de vazamento de dados, como ocorreu no ramo alimentício com a franquia Ceckers and Rally's, em que 103 pontos de venda foram vítimas de malware em seus armazenamentos e permitiram que terceiros criminosos roubassem dados dos clientes, incluindo os dados dos cartões de crédito. Um dos detalhes que, a fim de adicionar um comentário, indica a importância de se manter dentro dos padrões de segurança para a proteção de dados, é que este malware estava ativo há mais de três

---

dos-online/. Acesso em 09 mai. 2023.

18. Idem.

19. Cf. https://www.comparitech.com/blog/information-security/blur-data-leak/. Acesso em 09 mai. 2023.

20. DERMARTINI, Felipe. Custos de vazamento de dados podem ultrapassar R$ 26 mi em 2023. São Paulo: Canal Tech. Publicado em 04 jan. 2023. Disponível em https://canaltech.com.br/seguranca/custos-de-vazamento-de-dados-podem-ultrapassar-r-26-mi-em-2023-234616/. Acesso em 27 abr. 2023.

21. SECURITY REPORT. Vazamento de dados podem ultrapassar R$ 26 mi em 2023. São Paulo: Security Report, Conteúdo Editorial. Publicado em 17 fev. 2023. Disponível em https://www.securityreport.com.br/overview/vazamento-de-dados-podem-ultrapassar-r-26-mi-em-2023/#.ZEqQLnbMLIU. Acesso em 27 abr. 2023.

22. BISSO, Rodrigo (et al.). Vazamento de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. São Paulo: Revista Eletrônica Argentina-Brasil de Tecnologia da Informação e da Comunicação, vol. 3, n. 1, 2020. Disponível em https://revistas.setrem.com.br/index.php/reabtic/article/view/378. Acesso em 10 jan. 2023.

anos dentro do site e armazenamento de dados da empresa e, até então, não havia sido identificado pela equipe de segurança e técnica da informação[23].

Outro exemplo que se verifica foi publicado pela Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD)[24]. Afirma-se que o Biden Cash, mercado da chamada "*dark web*", publicou em 2023 cerca de 2,1 milhões de dados de cartões de crédito e débito de usuários de *e-commerce*. Ainda em 2022 o Biden Cash já tinha vazado gratuitamente cerca de 1,2 milhões de dados de cartões de crédito. O vazamento de 2023 expôs a informação de 811.676 cartões de débito, 740.858 cartões de crédito e 292 cartões de cobrança[25].

A análise feita pelos pesquisadores de segurança mostrou que os dados vazados incluem também informações pessoais dos usuários, como nomes, e-mails, números de telefone e endereços residenciais. No entanto, o que mais se verifica como principal de informações vendidas são os números de cartão de crédito com as datas de vencimento entre 2023 e 2052 e os código CVV[26].

A ANPPD[27] ainda alertou que as informações já estavam na *dark web* há um bom tempo. Além disso, cerca de 70% dos cartões de crédito foram identificados com vencimento em 2023. De toda forma, mesmo que esses cartões já estejam cancelados, o vazamento de informações dos usuários apresenta risco às empresas de *e-commerce* e podem facilitar a aplicação de golpes por cibercriminosos, deixando vulneráveis os usuários a ataques de *phishing*, roubo de identidade e outras práticas fraudulentas.

A partir da apresentação dos exemplos e da real possibilidade de ainda existirem outros vazamentos de dados, o estudo, a seguir, analisará a atribuição da responsabilidade civil às empresas de e-commerce, especialmente nos casos de vazamento de dados de seus usuários.

---

23. KHANDELWAL, Swati. Hackers Stole Customers' Credit Cards from 103 Checkers and Rally's Restaurants. [S.l.]: The Hacker News. Publicado em 31 mai. 2019. Disponível em https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html. Acesso em 09 mai. 2023.

24. ASSOCIAÇÃO NACIONAL DOS PROFISISONAIS DE PRIVACIDADE DE DADOS (ANPPD). Vazamento de dados pessoais continuam aumentando. Brasília: ANPPD. Publicado em 30 mar. 2023. Disponível em https://anppd.org/noticia/vazamentos-de-dados-pessoais-continuam-aumentando-30-03-2023. Acesso em 27 abr. 2023.

25. OLIVEIRA, Damião. Dark Web vaza 2,1 millhões de cartões de crédito e débito. São Paulo: Olhar Digital. Publicado em 30 mar. 2023. Disponível em https://www.linkedin.com/posts/dpodamiaooliveira_protectionday2024-somaxigroup-protecao-dedados-activity-7046828578289651712-DzqY/?utm_source=share&utm_medium=member_android. Acesso em 09 mai. 2023.

26. ASSOCIAÇÃO NACIONAL DOS PROFISISONAIS DE PRIVACIDADE DE DADOS (ANPPD). Vazamento de dados pessoais continuam aumentando. Brasília: ANPPD. Publicado em 30 mar. 2023. Disponível em https://anppd.org/noticia/vazamentos-de-dados-pessoais-continuam-aumentando-30-03-2023. Acesso em 27 abr. 2023.

27. Idem.

O que será discutido e apresentado no próximo capítulo diz respeito à análise da responsabilidade civil dessas empresas: elas devem apresentar provas de que tiveram ou não culpa no vazamento de dados ou, para serem responsabilizadas, basta o cumprimento dos requisitos para a responsabilidade objetiva?

2. Análise do regime de responsabilidade civil na Lei Geral de Proteção de Dados

É preciso, inicialmente, esclarecer e diferenciar os regimes da responsabilidade civil subjetiva e objetiva, para, em seguida, analisar a temática da responsabilidade civil nos casos de vazamento de dados do consumidor em relações de e-commerce. Segundo Barros[28], "realmente, a imposição de sanções administrativas no âmbito da LGPD dispensa qualquer elemento subjetivo (dolo ou culpa)" e, no tocante à responsabilidade civil, existem discussões sobre a aplicação da responsabilidade objetiva ou subjetiva.

A problemática do assunto abordado está disposta no sentido de verificar como podem ser responsabilizadas as pessoas jurídicas perante os problemas relacionados ao tratamento dos dados pessoais de seus usuários. O vazamento de dados, como visto anteriormente, é efetivamente uma das prioridades a se analisar perante a LGPD e a aplicação do Direito Civil e do Código de Defesa do Consumidor em casos mais específicos[29].

Buscando definir o que é a responsabilidade civil objetiva de acordo com a doutrina civilista, será aquela que independe de qualquer critério subjetivo para seu conhecimento, isto é, se provados o dano e o nexo causal, há o dever de reparar. O Código Civil dispõe sobre a matéria no artigo 927, parágrafo único[30].

Outro marco importante no que tange a responsabilidade civil objetiva é o

28. BARROS, Laura Mendes Amando de. LGPD: risco do negócio e dever de indenizar. São Paulo: Consultor Jurídico. Publicado em 27 mar. 2022. Disponível em https://www.conjur.com.br/2022-mar-27/laura-mendes-indenizacao-vazamento-dados. Acesso em 10 mai. 2023.

29. CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em 10 jan. 2023.

30. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 10 jan. 2023.

Código de Defesa do Consumidor[31] e menções que são efetuadas pela Constituição, conforme o artigo 5º, inciso XXXII, e o inciso V do artigo 170[32], ao determinar que o Estado promova a defesa do consumidor, reconhecendo a vulnerabilidade deste. No diploma legal, é reconhecida que a responsabilidade pelos danos causados em decorrência da relação de consumo independe de prova de culpa, salvo a responsabilidade dos profissionais liberais.

A responsabilidade objetiva, ao contrário da subjetiva, não exige a prova do erro do agente para reparar o dano. É o que entende Gonçalves[33] que a "[...] responsabilidade objetiva prescinde-se totalmente da prova da culpa. [...] Basta, assim, que haja relação de causalidade entre a ação e o dano".

No que tange a responsabilidade subjetiva, ela sim exige a análise da culpa[34]. A partir do exposto, conclui-se que o principal fundamento da responsabilidade subjetiva apenas surgirá quando o inadimplemento for causado por ato imputável ao devedor; daí a necessidade de se apreciar o comportamento do obrigado, a fim de se verificar, para a exata fixação de sua responsabilidade, se houve dolo, negligência, imperícia ou imprudência de sua parte, que resultou em prejuízo para o credor.

Definidos brevemente os conceitos da responsabilidade civil subjetiva e objetiva, parte-se para analisar qual o tipo de responsabilidade na LGPD no caso de vazamento de dados e a aplicação conforme o Código de Defesa do Consumidor a partir do plano teórico.

O tema de responsabilidade foi previsto na LGPD no Capítulo VI, Seção III, intitulado "Dos agentes de tratamento de dados pessoais". O artigo 42, caput, dispõe sobre o dever de reparação civil por dano patrimonial, moral, individual ou coletivo, que será imposto aos controladores e operadores, em casos em que o tratamento de dados apresente violação à referida lei[35].

A LGPD prevê princípios e fundamentos que visam à criação de um am-

---

31. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 10 jan. 2023.

32. BRASIL. Constituição Federal da República Federativa do Brasil de 1988. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 10 jan. 2023.

33. GONÇALVES, Carlos Roberto. Direito Civil Brasileiro – vol. 4: responsabilidade civil. 14. ed. São Paulo. Saraiva, 2019, p. 57.

34. TARTUCE, Flávio. Manual de Direito civil. 7 ed. São Paulo: Método, 2017.

35. BRASIL. Lei nº 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 10 jan. 2023.

biente de responsabilidade proativa. Isso significa que a prevenção será priorizada, levando em consideração o potencial risco de ocorrência de lesão na coleta e tratamento de dados pessoais. Além disso, o diploma legal propõe um sistema de responsabilização que propicia a efetiva tutela do titular de dados, e a integral reparação do dano[36].

O artigo 42 traz uma cláusula geral que afirma que 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, será obrigado a repará-lo. Combinando a atribuição da responsabilidade civil presente na LGPD, com o fato de serem dados pessoais vazados de usuários do e-commerce, logo, consumidores, analisa-se a aplicação do Código de Defesa do Consumidor e os incisos I e II, do parágrafo 1º, e o parágrafo 2º do artigo 42, que preveem a solidariedade dos agentes de tratamento que causarem lesão, bem como a possibilidade de o juiz inverter o ônus da prova, com o objetivo de mitigar a assimetria na relação entre os agentes de tratamento (controladores e operadores) e os titulares.

De acordo com Tasso[37], defensor da aplicação da responsabilidade civil subjetiva, o referido artigo 42 não prevê o elemento culpa, porém, também não o exclui expressamente. Conforme o autor: "ainda, traz como requisito da obrigação de reparar a circunstância de ter sido a operação de tratamento lesiva realizada em violação à legislação de proteção de dados"[38]. Importante mencionar que a regra geral trazida pelo artigo 42 da LGPD estabelece o dever de indenizar sempre que não observada fielmente a legislação atinente à proteção de dados, ou seja, inclui-se aqui todo o microssistema sobre o assunto (Código de Defesa do Consumidor, Código Civil, o Marco Civil da Internet, LGPD e a Lei do Cadastro Positivo).

Esse posicionamento também é encontrado em Guedes e Meireles[39] que informam que a LGPD de fato adotou claramente a teoria da responsabilidade

36. Idem.

37. TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 97-115, jan./mar. 2020, p. 104.

38. Idem.

39. GUEDES, Gisele Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2019.

civil subjetiva, devendo existir comprovação da conduta culposa do agente de tratamento de dados na ocasião de danos quando há o vazamento desses dados.

A partir disso, conclui-se que são utilizados dois critérios para fundamentar a responsabilidade civil da empresa que sofre o vazamento de dados dos consumidores, conforme bem denota a obra de Cruz[40]: (i) o exercício da atividade de tratamento de dados; e (ii) a violação da legislação de proteção de dados. Menciona-se, neste passo, o estudo de Oliveira[41] que traz o vazamento de dados pessoais e responsabilização civil com as compatibilidades e conflitos entre o Código de Defesa do Consumidor e a LGPD.

Ao se falar da responsabilidade objetiva ou subjetiva na LGPD, ressalta-se, como bem informa a problemática deste estudo e como dissertou Bruno[42] e Oliveira[43], que realmente há divergência doutrinária sobre qual seria a linha adotada pela referida legislação, afirmando-se que, em relação à aplicabilidade da responsabilidade objetiva ou subjetiva, a LGPD não é evidentemente clara.

O enunciado do artigo 42 da LGPD, ao utilizar a redação "em razão do exercício de atividade de tratamento de dados causar a outrem dano [...] é obrigado a repará-lo", não define com clareza suficiente qual o regime de responsabilidade adotado"[44]. Por conta disso, como mencionado, existem posicionamentos doutrinários opostos.

Os autores que adotam a posição de que a responsabilidade civil na LGPD seria de natureza objetiva defendem que a atividade de tratamento de dados apresentaria um risco intrínseco, uma vez que existiria um potencial risco significativo em caso de violação dos direitos dos titulares. Sendo assim, o trata-

40. CRUZ, Gisela Sampaio da. Responsabilidade civil da Lei de Proteção de Dados Pessoais. São Paulo: Congresso Internacional de Responsabilidade Civil do IBERC, 2019.

41. OLIVEIRA, Jordan Vinicíus de. Vazamento de dados pessoais e responsabilização civil: compatibilidades e conflitos entre o Código de Defesa do Consumidor e a lei geral de proteção de dados. São Paulo: Revista Brasileira de Direito Civil – RBDCivil, vol. 31, n. 01, 2022. Disponível em https://rbdcivil.emnuvens.com.br/rbdc/article/view/478. Acesso em 27 abr. 2023.

42. BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

43. OLIVEIRA, Jordan Vinicíus de. Vazamento de dados pessoais e responsabilização civil: compatibilidades e conflitos entre o Código de Defesa do Consumidor e a lei geral de proteção de dados. São Paulo: Revista Brasileira de Direito Civil – RBDCivil, vol. 31, n. 01, 2022. Disponível em https://rbdcivil.emnuvens.com.br/rbdc/article/view/478. Acesso em 27 abr. 2023.

44. CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 163-170, jan./mar. 2020, p. 165-167. Disponível em https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em 10 jan. 2023.

mento de dados pessoais seria considerado uma atividade de risco[45].

Retoma-se ao disposto no artigo 927, par. único, do Código Civil, que prevê que a responsabilização com ausência de culpa se dará de forma excepcional. E assim, para tal corrente, diversos artigos da LGPD justificariam o entendimento de que a atividade de tratamentos de dados é de risco. Exemplos são o artigo 5º, XVII, da Constituição Federal de 1988 e o artigo 48, caput: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares"[46].

Nesse sentido, defendem que, de forma implícita, o próprio artigo 42 da LGPD reconhece o risco da atividade na expressão "em razão do exercício de atividade de tratamento de dados pessoais"[47]. Adicionalmente, baseando-se na própria finalidade e nos princípios da lei, essa corrente doutrinária conclui que o legislador optou por um regime de responsabilidade objetiva, de forma a vincular o tratamento de dados pessoais a um risco inerente, que pode vir a causar danos aos titulares de dados.

No sentido oposto, há corrente doutrinária que defende que a LGPD adotou a responsabilidade civil subjetiva, sendo necessário provar a culpa do agente. A culpa, por sua vez, seria fundamentada na omissão na adoção de medidas de segurança para o tratamento adequado dos dados e no descumprimento das obrigações impostas na lei[48].

Um dos argumentos a favor dessa posição recai sobre os princípios e condutas a serem respeitados pelos controladores e operadores, relacionados à segurança, governança de dados, sigilo e boas práticas[49]. Além disso, analisando as excludentes de responsabilidade, dispostas no artigo 43 da LGPD, nota-se excludente que tipicamente se relaciona com a responsabilidade subjeti-

---

45. MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. Brasília: Revista de direito do consumidor, vol. 120, p. 469-483, nov./dez. 2018.

46. Grifo nosso. BRASIL. Lei nº 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 10 jan. 2023.

47. Idem.

48. TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 97-115, jan./mar. 2020.

49. ROSENVALD, Nelson (et al.). A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?. [S.l.]: Migalhas, Colunas. Publicado em 30 jun. 2020. Disponível em https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em 10 jan. 2023.

va, a seguir: os agentes de tratamento só não serão responsabilizados quando provarem que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados.

A partir do exposto, tem-se que o elemento subjetivo do dever de indenizar seria a violação da legislação, indicando o dever de indenizar[50]. Nesse sentido, alguns autores afirmam que não seria possível definir toda e qualquer atividade de tratamento de dados como de risco, considerando a ampla possibilidade de atividades, e que muitas delas apresentem baixo potencial de dano[51].

A responsabilidade civil na LGPD, então, seria baseada na culpa, para que, dessa forma, as empresas (operador ou controlador de dados) possam comprovar em juízo se cumpriam ou não com as condutas mencionadas acima, de segurança e boas práticas no tratamento de dados, de forma a se manterem em conformidade com a legislação.

De acordo com Tepedino, se a responsabilidade prevista na LGPD fosse objetiva, não caberia a discussão do cumprimento ou não de deveres jurídicos e a legislação apresentaria referência expressa ao risco como fundamento da responsabilidade. Neste mesmo sentido:

> A lógica da responsabilidade objetiva é outra: não cabe discutir cumprimento de deveres, porque a responsabilidade objetiva não decorre do descumprimento de qualquer dever jurídico. Quando se discute cumprimento de deveres, o que no fundo está sendo analisado é se o agente atuou ou não com culpa. Assim, apesar de a LGPD não ser explícita em relação à natureza da responsabilidade dos agentes de tratamento de dados, como é o Código de Defesa do Consumidor ao adotar a responsabilidade objetiva, a interpretação sistemática da LGPD leva à conclusão de que o regime adotado por este diploma foi mesmo o da responsabilidade subjetiva. O art. 42 da LGPD não faz referência expressa à culpa como elemento da responsabilidade civil, mas também não faz qualquer alusão ao risco como fundamento da responsabilidade objetiva[52].

50. GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019.

51. GUALDA, Diego; MATTA, Laura Aliende. Responsabilidade subjetiva na LGPD. [S.l.]: Inteligência Jurídica, Conteúdo Exclusivo Machado Meyer Advogados. Publicado em 04 dez. 2020. Disponível em https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/responsabilidade-subjetiva-na-lgpd. Acesso em 10 jan. 2023.

52. GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019, p. 236-252,

Diante dos argumentos apresentados, é notável o intenso debate doutrinário acerca da natureza jurídica da responsabilidade civil apresentada na LGPD. Antes de se abranger uma efetiva posição, entende-se ser essencial ter em mente o processo de elaboração da própria LGPD.

Durante os dez anos de debate, houve forte disputa a respeito da definição do modelo de regime de responsabilidade civil. Bioni[53] retoma que, tanto a primeira versão do anteprojeto da LGPD, como a proposta do Senado Federal, adotava o regime de responsabilidade civil objetiva. Havia previsão expressa ao tratamento de dados como atividade de risco e os agentes de tratamento poderiam ser responsabilizados independentemente da existência de culpa.

No entanto, a partir da segunda versão, tais expressões, que remetiam ao regime de responsabilidade objetiva, foram eliminadas, à medida que a opção pelo regime subjetivo se fortaleceu. Ademais, foi inserido o princípio da *accountability* (em inglês, responsabilização), acompanhado dos relatórios de impacto à proteção de dados pessoais.

O princípio da *accountability*, os relatórios de impacto, as boas práticas, a governança, entre outras condutas a serem cumpridas pelos agentes envolvidos na cadeia de tratamento de dados, desenham um cenário no qual a responsabilidade civil de natureza subjetiva é reforçada, mesmo de forma indireta. Bioni[54] retoma a refutação do regime de responsabilidade objetiva, indicando, ainda, que há outros dispositivos da LGPD que convergem para o entendimento de que a referida lei adota a responsabilidade subjetiva:

> Os trabalhos preparatórios da LGPD deixam claro que sua política legislativa refutou deliberadamente um regime de responsabilidade civil objetiva. Há outros elementos normativos que, direta ou indiretamente, convergem para que haja um juízo de valor em torno da culpa do lesante. Algo que não está apenas cristalizado no rol de excludentes de responsabilidade, mas também, na principiologia e em outras partes importantes e integrantes do texto da LGPD. É uma racionalidade inescapável e que está por trás da lógica do regime de responsabilidade civil em questão[55].

53. BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. [S.l.]: Revista Eletrônica de Direito Civil, vol. 9, n. 3, p. 1-23, 22 dez. 2020. Disponível em https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em 10 jan. 2023.

54. Idem.

55. Ibidem, p. 2.

Reconhecida a omissão do legislador acerca do tema e a preferência doutrinária para a interpretação da responsabilidade como subjetiva, Ferreira[56] complementa a argumentação ao dizer que, de forma geral, as atividades de tratamento de dados não apresentam graves riscos aos titulares. Entretanto, não descarta a possibilidade de atividades excepcionais que, de fato, apresentem riscos consideráveis. Sendo assim, a responsabilidade subjetiva como regra geral seria mais compatível com o cenário prático de tratamento de dados.

Com o objetivo de promover maior proteção possível para os titulares, entende-se que a LGPD propõe a criação de um sistema de proteção de dados que envolve colaboração entre os sujeitos, criando uma série de deveres, princípios e condutas que devem ser respeitados. Sendo assim, espera-se certo comportamento de tais agentes, o que colabora com o entendimento de que, a depender do cumprimento de tais deveres, isso influenciará nos parâmetros de responsabilização[57].

Portanto, considerando o exposto, a partir de uma interpretação sistemática e textual, entende-se que a LGPD elegeu o sistema de responsabilidade civil subjetiva como regra, sendo possível, porém, a responsabilização objetiva do agente em caso de comprovação de relação de consumo, conforme seu artigo 45, caso em que se aplicam as disposições previstas no Código de Defesa do Consumidor: “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”[58].

De acordo com o que foi abordado, entende-se pela aplicação da responsabilidade objetiva, com base no CDC e na proteção do consumidor vulnerável, quando ele for usuário de e-commerce e tiver seus dados vazados e expostos. Ele depende que as empresas se adaptem e assegurem que o tratamento de dados será com o máximo de segurança.

---

56. FERREIRA, Ramos Diogo. Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva? [S.l.]: Jota Info, 2019. Acesso em: https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019. Acesso em 10 jan. 2023.

57. CORRÊA, Leonardo; CHO, Tae. Responsabilidade civil na LGPD é subjetiva. [S.l.]: Consultor Jurídico. Publicado em 29 jan. 2021. Disponível em https://www.conjur.com.br/2021-jan-29/correa-cho-responsabilidade-civil-lgpd-subjetiva. Acesso em 06 abr. 2022.

58. BRASIL. Lei nº 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 10 jan. 2023.

3. Adequação das empresas e a regulamentação da coleta de dados do consumidor

Após a análise da responsabilidade das empresas que sofrem vazamentos de dados ou acessos indevidos de dados de seus usuários, é preciso considerar a necessidade de as empresas se adequarem perante a LGPD.

A partir da regulamentação e necessidade de proteção dos dados disponibilizados e lançados no meio eletrônico, mostra-se necessário que as empresas desenvolvam setores especializados, tanto para a tecnologia da informação quanto para o setor jurídico, compreendendo as formas em que esses dados serão tratados.

É preciso considerar que o Poder Judiciário já aborda a questão da vulnerabilidade do consumidor frente às compras no *e-commerce* e o vazamento de dados, como é o caso do Recurso Inominado nº 0510631-50.2014.8.19.0001, julgado em 2016[59]. Isso é ainda mais evidente no campo das relações de consumo (lembre-se que a existência de compensação financeira não é elemento essencial - como é a distribuição gratuita e "cortês" de amostras e serviços, por exemplo), desde que a Lei de Defesa do Consumidor dispôs sobre a responsabilidade objetiva (artigos 12 e 14 da Lei 8.078/90)[60].

Verifica-se a atribuição de responsabilidade objetiva na análise do vazamento de dados pelo Mercado Livre e Mercado Pago no Recurso Inominado nº 1011470-32.2019.8.26.0006 SP, pelo Tribunal de Justiça do Rio de Janeiro, em 2021[61].

A empresa recorrida, na relação jurídica, é totalmente dependente da segurança e disponibilidade da plataforma das recorrentes para conseguir vender seus produtos. Neste aspecto, cumpre observar que, nestes casos, consoante restou decidido na sentença atacada, tem-se aplicado a teoria finalista mitigada, que vem sendo adotada pelo STJ quando embora o contratante não seja o destinatário final dos produtos e/ou serviços for possível reconhecer a

59. BRASIL. Tribunal de Justiça do Rio de Janeiro (3ª Turma Recursal Especial Cível). Recurso Inominado nº 0510631-50.2014.8.19.0001. Rel. Luiz Cláudio Silva Jardim Marinho. Julgado em 1 set. 2016. Publicado em 05 set. 2016. Disponível em https://tj-rj.jusbrasil.com.br/jurisprudencia/380493531/recurso-inominado-ri-5106315020148190001-rio-de-janeiro-capital-xxi-jui-esp-civ. Acesso em 10 jan. 2023.

60. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 10 jan. 2023.

61. BRASIL. Tribunal de Justiça de São Paulo (2ª Turma Recursal Cível e Criminal). Recurso Inominado nº 1011470-32.2019.8.26.0006. Rel. Regiane dos Santos. Julgado em 26 nov. 2021. Publicado em 26 nov. 2021. Disponível em https://tj-sp.jusbrasil.com.br/jurisprudencia/1331477359/recurso-inominado-civel-ri-10114703220198260006-sp-1011470-3220198260006. Acesso em 10 jan. 2023.

vulnerabilidade, como se verifica na espécie, vez que o funcionamento do sistema das rés recorrentes EBazar e Mercado Pago é absolutamente desconhecido da contratante dos seus serviços. No que diz respeito ao mérito, restou incontroversa a troca de titularidade de chip em nome do recorrido. [...] Diante de tal contexto probatório, inegável a obrigação de indenizar ante a evidente falha na prestação do serviço por parte das recorrentes EBazar e Mercado Pago ante a desconformidade das transações com o perfil normal do consumidor, não as eximindo de responsabilidade o fato de que as transações impugnadas terem sido realizadas um dia antes de os recorridos lhes comunicarem a fraude. A teoria do risco e a responsabilidade objetiva das recorrentes foram bem esclarecidas na sentença recorrida[62].

O escritório de advocacia Opice Blum, Bruno e Vainzof Advogados realizou um estudo de jurimetria, com aproximadamente 160 (cento e sessenta) decisões[63]. Em sua análise, foi identificado que o tema incidente de segurança aparece em quase 70% das decisões, especialmente no mês de junho de 2021. Esse estudo demonstra, ainda, que o vazamento de dados, por si só, não vem gerando necessariamente o dever de indenização por dano moral, sendo necessário comprovar efetivamente o dano moral sofrido pelo titular de dados. Neste passo, comprova-se cada vez mais a necessidade de existirem profissionais preparados e especializados na área, tanto jurídica como tecnicamente, a fim de trabalharem em conjunto para formar novos formatos de proteção aos dados dos usuários.

Considerações finais

O presente trabalho buscou abordar a importância de se existir uma lei específica para a proteção de dados pessoais, para regular as atividades de tratamento de dados, buscando proteger os direitos fundamentais dos titulares de dados e considerar a vulnerabilidade do consumidor, enquanto aquele que utiliza programas e sites de e-commerce, por exemplo.

62. Idem.

63. OPICE BLUM. *Incidente de segurança é tema de 7 em cada 10 decisões judiciais relacionadas à LGPD, indica estudo do OPICE BLUM.* [S.l.]: Escritório Opice Blum. Publicado em 13 ago. 2021. Disponível em https://opiceblum.com.br/incidente-de-seguranca-e-tema-de-7-em-cada-10-decisoes-judiciais-relacionadas-a-lgpd-indica-estudo-do-opice-blum/. Acesso 10 jan. 2023; GOMES, Maria Cecília Oliveira. *Multas para vazamento de dados pessoais em limbo fiscalizatório.* São Paulo: Convergência Digital. Publicado em 19 dez. 2022. Disponível em https://www.convergenciadigital.com.br/Opiniao/Multas-para-vazamentos-de-dados-pessoais-em-limbo-fiscalizatorio-62197.html?UserActiveTemplate=site. Acesso em 25 mai. 2023; MONTEIRO, Thais Arza (et al.). *Vazamento de dados:* a necessidade de comprovação de danos. São Paulo: Consultor Jurídico. Publicado em 23 abr. 2023. Disponível em https://www.conjur.com.br/2023-abr-23/opiniao-vazamento-dados-comprovacao-danos. Acesso em 25 mai. 2023.

Para que tal lei específica possa ser efetiva e exercer seu papel de forma plena, é necessário que disponha de princípios e fundamentos, que sirvam como norteadores, estabelecendo um padrão de conduta e comportamento a serem observados por todos os agentes de tratamento de dados, provocando, assim, que as empresas se adequem à LGPD.

Adicionalmente, para garantir a efetividade da legislação, também é necessária a existência de um sistema justo de responsabilização civil, na hipótese de eventuais infrações à LGPD, cometidas por agentes de tratamento, podendo gerar danos imensuráveis aos titulares de dados. Para que tal mecanismo de responsabilização ocorra da melhor forma possível, sempre priorizando o titular, é importante definir se se trata da modalidade subjetiva ou objetiva de responsabilidade.

Sobre o risco em potencial das atividades de tratamento de dados pessoais, entende-se que, em sua grande maioria, não apresentam riscos graves o suficiente para justificar a responsabilidade objetiva como regra.

Neste sentido, reitera-se o posicionamento de que a interpretação que mais faz sentido do texto legal, que é propositalmente omisso, é a subjetiva. A partir da omissão legislativa, entende-se, também, que a intenção do legislador não foi definir uma forma de responsabilização absoluta, que não comportaria qualquer exceção, pois existem decisões no Brasil que mantém o posicionamento sobre uma atribuição de responsabilidade objetiva.

É importante ter em mente que há casos em que o tratamento de dados apresenta riscos imensuráveis para o titular, como tratar dados pessoais de crianças ou dados médicos (dados pessoais sensíveis) de pacientes, sobre os quais um eventual vazamento causaria imenso dano.

Adicionalmente, considerando a emergente terceira interpretação da responsabilidade civil na LGPD, denominada responsabilidade proativa, que busca fugir do conflito binário, é possível afirmar que a lei inovou ao criar um sistema de responsabilidade de prevenção, que busca promover um regime pautado nos deveres e condutas de segurança.

Referências

ANDREW, Scottie. ***Yahoo could pay you $358 for its massive data breach settlement. Here's how to claim it*.** Nova Iorque: CNN. Publicado em 15 out. 2019. Disponível em https://edition.cnn.com/2019/10/15/business/yahoo-data-breach-settlement-trnd/index.html. Acesso em 09 mai. 2023.

ASSOCIAÇÃO NACIONAL DOS PROFISIONAIS DE PRIVACIDADE DE DADOS (ANPPD). **Vazamento de dados pessoais continuam aumentando.** Brasília: ANPPD. Publicado em 30 mar. 2023. Disponível em https://anppd.org/noticia/vazamentos-de-dados-pessoais-continuam-aumentando-30-03-2023. Acesso em 27 abr. 2023.

BARAN, Guru. ***2.4 Million Blur Password Manager Users Data Exposed Online*.** [S.l.]: GBHackers on Security. Publicado em 3 jan. 2019. Disponível em https://gbhackers.com/2-4-million-blur-password/. Acesso em 09 mai. 2023.

BARROS, Laura Mendes Amando de. **LGPD: risco do negócio e dever de indenizar**. São Paulo: Consultor Jurídico. Publicado em 27 mar. 2022. Disponível em https://www.conjur.com.br/2022-mar-27/laura-mendes-indenizacao-vazamento-dados. Acesso em 10 mai. 2023.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. [S.l.]: Revista Eletrônica de Direito Civil, vol. 9, n. 3, p. 1-23, 22 dez. 2020. Disponível em https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em 10 jan. 2023.

BISSO, Rodrigo (et al.). **Vazamento de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados**. São Paulo: Revista Eletrônica Argentina-Brasil de Tecnologia da Informação e da Comunicação, vol. 3, n. 1, 2020. Disponível em https://revistas.setrem.com.br/index.php/reabtic/article/view/378. Acesso em 10 jan. 2023.

BRUNO, Marcos Gomes da Silva. **Dos agentes de tratamento de dados pessoais**. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em 10 jan. 2023.

CHACON, Guilherme. **Vazamento de dados pessoais: dano presumido ou expectativa não indenizável de dano**. São Paulo: Lapin.Org. Publicado em 13 set. 2021. Disponível em https://lapin.org.br/2021/09/13/vazamento-de-dados-pessoais-dano-presumido-ou-expectativa-nao-indenizavel-de-dano/. Acesso em 09 mai. 2023.

CORRÊA, Leonardo; CHO, Tae. **Responsabilidade civil na LGPD é subjetiva**. [S.l.]: Consultor Jurídico. Publicado em 29 jan. 2021. Disponível em https://www.conjur.com.br/2021-jan-29/correa-cho-responsabilidade-civil-lgpd-subjetiva. Acesso em 06 abr. 2022.

CRUZ, Gisela Sampaio da. **Responsabilidade civil da Lei de Proteção de Dados Pessoais**. São Paulo: Congresso Internacional de Responsabilidade Civil do IBERC, 2019.

DERMARTINI, Felipe. **Custos de vazamento de dados podem ultrapassar R$ 26 mi em 2023**. São Paulo: Canal Tech. Publicado em 04 jan. 2023. Disponível em https://canaltech.com.br/seguranca/custos-de-vazamento-de-dados-podem-ultrapassar-r-26-mi-em-2023-234616/. Acesso em 27 abr. 2023.

DESLANDES, Suely Ferreira (*et al.*). **Vazamento de nudes: da moralização e violência generificada ao empoderamento**. São Pau-

lo: Ciênc. Saúde Coletiva, vol. 27, n. 10, out. 2022. Disponível em https://www.scielo.br/j/csc/a/Fp9zrh6C64Y4DLpx5TdvL8b/abstract/?lang=pt. Acesso em 27 abr. 2023.

FERREIRA, Ramos Diogo. **Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva?** [S.l.]: Jota Info, 2019. Acesso em: https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019. Acesso em 10 jan. 2023.

FORGIONI, Paula. **Apontamentos sobre os aspectos jurídicos do e-commerce**. São Paulo: RAE – Revista de Administração de Empresas, vol. 40, n. 4, out./dez. 2000. Disponível em https://www.scielo.br/j/rae/a/b7jhPyWv6sbVfmpNDvzqKQs/?format=pdf&lang=pt. Acesso em 27 abr. 2023.

GODINHO, Adriano Marteleto (*et al.*). **A responsabilidade civil pela violação a dados pessoais**. São Paulo: Revista IBERC, vol. 3, n. 1, jan./abr. 2020. Disponível em https://revistaiberc.responsabilidadecivil.org/iberc/article/view/105/78. Acesso em 10 jan. 2023.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro – vol. 4: responsabilidade civil**. 14. ed. São Paulo. Saraiva, 2019.

GOGONI, Ronaldo. **Vazamento expôs dados de mais de 500 milhões de usuários do Yahoo!**. São Paulo: Meio Bit, 2018. Disponível em https://meiobit.com/352105/yahoo-vazamento-massivo-pode-ter-comprometido-centenas-de-milhoes-de-contas-de-usuarios/. Acesso em 27 abr. 2023.

GOMES, Anselmo Lacerda. **Mapeamento de incidentes com identidades digitais e estratégias de controle em ambientes virtuais**. Pernambuco: Universidade Federal de Pernambuco, Mestrado em Ciência da Computação, ago. 2015. Disponível em https://repositorio.ufpe.br/handle/123456789/16377. Acesso em 09 mai. 2023.

GOMES, Maria Cecília Oliveira. **Multas para vazamento de dados pessoais em limbo fiscalizatório**. São Paulo: Convergência Digital. Publicado em 19 dez. 2022. Disponível em https://www.convergenciadigital.com.br/Opiniao/Multas-para-vazamentos-de-dados-pessoais-em-limbo-fiscalizatorio-62197.html?UserActiveTemplate=site. Acesso em 25 mai. 2023.

GUALDA, Diego; MATTA, Laura Aliende. **Responsabilidade subjetiva na LGPD**. [S.l.]: Inteligência Jurídica, Conteúdo Exclusivo Machado Meyer Advogados. Publicado em 04 dez. 2020. Disponível em https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/responsabilidade-subjetiva-na-lgpd. Acesso em 10 jan. 2023.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, **Término do tratamento de dados**. In. TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019.

HÁRAN, Juan Manuel. **Marriott sofre novo vazamento de dados que afeta 5,2 milhões de hóspedes**. [S.l.]: We Live Security. Publicado em 2 abr. 2020. Disponível em https://www.welivesecurity.com/br/2020/04/02/marriott-sofre-novo-vazamento-de-dados-que-afeta-52-milhoes-de-hospedes/. Acesso em 06 abr. 2022.

KHANDELWAL, Swati. ***Hackers Stole Customers' Credit Cards from 103 Checkers and Rally's Restaurants***. [S.l.]: The Hacker News. Publicado em 31 mai. 2019. Disponível em https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html. Acesso em 09 mai. 2023.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova lei geral de proteção de dados**. Brasília: Revista de direito do consumidor, vol. 120, p. 469-483, nov./dez. 2018.

MONTEIRO, Thais Arza (et al.). **Vazamento de dados: a necessidade de comprovação de danos**. São Paulo: Consultor Jurídico. Publicado em 23 abr. 2023. Disponível em https://www.conjur.com.br/2023-abr-23/opiniao-vazamento-dados-comprovacao-danos. Acesso em 25 mai. 2023.

NEOTEL. **Global Privacy Control surge como a mais recente tentativa de permitir que os internautas escolham se querem ser rastreados online**. [S.l.]: Neotel Segurança Digital. Publicado em 12 out. 2020. Disponível em https://blog.neotel.com.br/2020/10/12/global-privacy-control-surge-como-a-mais-recente-tentativa-de-permitir-que-os-internautas-escolham-se-querem-ser-rastreados-online/. Acesso em 09 mai. 2023.

OLIVEIRA, Damião. **Dark Web vaza 2,1 millhões de cartões de crédito e débito**. São Paulo: Olhar Digital. Publicado em 30 mar. 2023. Disponível em https://www.linkedin.com/posts/dpodamiaooliveira_protectionday2024-somaxigroup-protecaodedados-activity-7046828578289651712-DzqY/?utm_source=share&utm_medium=member_android. Acesso em 09 mai. 2023.

OLIVEIRA, Jordan Vinicíus de. **Vazamento de dados pessoais e responsabilização civil: compatibilidades e conflitos entre o Código de Defesa do Consumidor e a lei geral de proteção de dados**. São Paulo: Revista Brasileira de Direito Civil – RBDCivil, vol. 31, n. 01, 2022. Disponível em https://rbdcivil.emnuvens.com.br/rbdc/article/view/478. Acesso em 27 abr. 2023.

OPICE BLUM. **Incidente de segurança é tema de 7 em cada 10 decisões judiciais relacionadas à LGPD, indica estudo do OPICE BLUM**. [S.l.]: Escritório Opice Blum. Publicado em 13 ago. 2021a. Disponível em https://opiceblum.com.br/incidente-de-seguranca-e-tema-de-7-em-cada-10-decisoes-judiciais-relacionadas-a-lgpd-indica-estudo-do-opice-blum/. Acesso 10 jan. 2023.

ROHR, Altieres. **Vazamento de dados do Snapchat expõe milhares de fotos na web**. São Paulo: G1. Publicado em 10 out. 2014. Disponível em https://g1.globo.com/tecnologia/noticia/2014/10/vazamento-de-dados-do-snapchat-expoe-milhares-de-fotos-na-web.html. Acesso em 10 jan. 2023.

ROHR, Altieres. **Vazamento de dados do Yahoo: veja o que você precisa saber**. São Paulo: G1. Publicado em 23 set. 2016. Disponível em https://g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-de-dados-do-yahoo-veja-o-que-voce-precisa-saber.html. Acesso em 10 jan. 2023.

ROSENVALD, Nelson (*et al.*). **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?**. [S.l.]: Migalhas, Colunas. Publicado em 30 jun. 2020. Disponível em https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em 10 jan. 2023.

SECURITY REPORT. **Vazamento de dados podem ultrapassar R$ 26 mi em 2023**. São Paulo: Security Report, Conteúdo Editorial. Publicado em 17 fev. 2023. Disponível em https://www.securityreport.com.br/overview/vazamento-de-dados-podem-ultrapassar-r-26-mi-em-2023/#.ZEqQLnbMLIU. Acesso em 27 abr. 2023.

SCHREIBER, Anderson. **Responsabilidade civil na Lei Geral de Proteção de dados pessoais**. In. BIONI, Bruno Ricardo (Org.). Tratado de Proteção de Dados Pessoais – vol. 1. Rio de Janeiro: Editora Forense, 2020.

SILVA, Walyf Lopes da (*et al.*). **Aspectos jurídicos da exposição de dados pessoais na internet e sua relação com o direito fundamental à privacidade**. São Paulo: Revista Ibero-Americana de Humanidades, Ciência e Educação, vol. 7, n. 10, 2021. Disponível em https://www.periodicorease.pro.br/rease/article/view/2906. Acesso em 09 mar. 2023.

TARTUCE, Flávio. **Manual de Direito civil**. 7 ed. São Paulo: Método, 2017.

TASSO, Fernando Antonio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. São Paulo: Cadernos Jurídicos, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TEPEDINO, Gustavo (coord.). **Lei Geral de Proteção de Dados Pessoais: e suas repercussões no Direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

ZANETTI, Dânton. **Proteção de Dados pessoais e publicidade processual: contrasenso?** [S.l.]: Consultor Jurídico. Publicado em 15 abr. 2021. Disponível em https://www.conjur.com.br/2021-abr-15/zanetti-protecao-dados-pessoais-publicidade-processual. Acesso em 10 jan. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

15

Acordo comercial internacional UE-MERCOSUL: uma oportunidade para a criação da maior zona de livre fluxo de dados do mundo?

JANAINA COSTA

JANAINA COSTA[1]

Sumário: Introdução. 1. A Decisão 15/20 do MERCOSUL e a retomada das negociações do acordo de livre comércio com a UE - uma oportunidade de negociar uma decisão de adequação mútua. 2. O Acordo de Livre Comércio MERCOSUL-UE - muitos dados correram sob a ponte desde o início das negociações. 3. Acordo de Livre Comércio MERCOSUL-UE - Momento ideal para avançar na agenda latino-americana de proteção de dados pessoais. 4. Decisão de Adequação da União Europeia. 5. Legislação do MERCOSUL sobre Status de Proteção de Dados - *Two down, two to go*. 6. Complicador na equação: o legado da decisão Schrems II. Considerações finais. Referências.

Introdução

A nova ordem econômica mundial está inexoravelmente ancorada na economia de dados. Estima-se que os fluxos de dados transfronteiriços agora exerçam um impacto maior no crescimento do produto interno bruto ("PIB") global do que os bens comerciais.[2]

Deve-se destacar que os dados pessoais são parte inerente de praticamente todas as transações comerciais e sua relevância vai além dos serviços digitais. Mesmo as transações comuns do dia a dia podem ser afetadas por questões de proteção de dados. Portanto, é importante fornecer uma estrutura legal que facilite o fluxo de dados pessoais em termos seguros e responsáveis.

A União Europeia ("UE") está na vanguarda nesta matéria. Desde 1995, a Diretiva 95/46/EC, posteriormente substituída pelo Regulamento Geral de Proteção de Dados ("GDPR"), previa um procedimento para garantir a proteção de dados em transações internacionais. A Comissão Europeia tem autoridade para determinar se um país fora da UE oferece um nível adequado de proteção de dados e deve se beneficiar de uma maneira simplificada mais acessível de transferir dados para o exterior - a chamada decisão de adequação.

Essas decisões complementam os acordos de livre comércio e impulsionam a cooperação entre a UE e os países contemplados com tal decisão.

---

1. Mestre em Desenvolvimento Econômico e Social pelo IEDES-Paris 1 Panthéon-Sorbonne. Pós-graduada em Direito Digital pela UERJ e ITS Rio. Graduada em Direito pela Universidade Federal do Estado de Minas Gerais (UFMG). Assistente Acadêmica na disciplina Inteligência Artificial e o futuro da tecnologia da Pós-Graduação em Direito Digital UERJ e ITS Rio .

2. Digital globalization: The new era of global flows | McKinsey, disponível em: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>. acesso em: 6 jun. 2023.

Tendo em vista os últimos acontecimentos, este breve artigo argumenta que uma oportunidade se apresenta para a criação da maior zona de fluxo livre de dados do mundo, incluindo Brasil e Paraguai como parte dos principais países de potências digitais. Nesse sentido, as decisões de adequação já concedidas ao Uruguai e à Argentina, bem como as últimas negociações e decisões da Comissão Europeia em relação ao Japão e à Coreia do Sul servirão de orientação para analisar os desafios e possíveis caminhos para que tal acordo seja concretizado.

1. A Decisão 15/20 do MERCOSUL e a retomada das negociações do acordo de livre comércio com a UE – uma oportunidade de negociar uma decisão de adequação mútua

O órgão máximo do Mercosul, Mercado Comum do Sul que envolve Brasil, Argentina, Uruguai e Paraguai, aprovou no dia 28 de janeiro de 2021 o Acordo de Comércio Eletrônico ("Decisão 15/20").[3]

A Decisão 15/20 e a retomada das negociações entre a UE e o Mercosul representam uma oportunidade para harmonizar as leis dos dois blocos econômicos e para que Brasil e Paraguai também negociem uma decisão de adequação mútua para que os países membros de ambos os blocos tenham livre fluxo de dados com base em padrões adequados de proteção.

Nesse instrumento, os membros do MERCOSUL reconhecem a importância de garantir a segurança dos usuários de comércio eletrônico e seu direito à proteção de dados pessoais. No artigo dedicado à proteção de dados pessoais (art. 6.º), as partes são instadas a adoptar ou manter um regime jurídico de protecção de dados pessoais, tendo em conta as normas internacionais existentes na matéria. Mas o que torna este parágrafo mais especial é o seguinte compromisso (Art. 6.7):

> As partes comprometem-se a aplicar aos dados pessoais que recebam de outra Parte um nível adequado de proteção por meio de regra geral ou regulamento autônomo específico ou por acordos mútuos, gerais ou específicos ou em instrumentos internacionais mais amplos, permitindo a execução de contratos ou auto-regulamentação para o setor privado.

3. SIM - Detalhes da Normativa, disponível em: <https://normas.mercosur.int/public/normativas/4018>. acesso em: 6 jun. 2023.

Adicionalmente, o artigo seguinte estabelece que a transferência transfronteiriça de dados está sujeita ao cumprimento do disposto no parágrafo acima transcrito.

Bem, quanto tempo você demorou para pensar no GDPR como um marco de instrumento internacional? É neste sentido que esta Decisão 15/20 dá um novo impulso ao mais recente acordo comercial entre a UE e o MERCOSUL.

Em 2019, a UE e o MERCOSUL concluíram as negociações de um acordo de livre comércio como parte das negociações mais amplas do Acordo de Associação da UE com o Mercosul.

O Acordo é bastante ambicioso e abrangente. Prevê também regras gerais para o comércio eletrônico que visam eliminar barreiras injustificadas, dar segurança jurídica às empresas e garantir um ambiente online seguro para os consumidores, cujos dados pessoais devem ser adequadamente protegidos - a exemplo do recém-assinado acordo intrabloco do MERCOSUL.

A comissária europeia para Justiça, Consumidores e Igualdade de Gênero, Vera Jourová, destacou à época do acordo que um dos efeitos positivos a seguir seriam melhorias nas políticas de proteção de dados para os dois blocos.[4]

Deve-se notar que uma decisão de adequação não é apenas um compromisso legal, mas também um compromisso econômico e político. Muitas vezes, os países solicitantes negociam a possibilidade de decisão com o Bloco, bem como possíveis acordos econômicos que podem ser negociados paralelamente.

De fato, os avanços na proteção de dados rumo a um marco regulatório comum dentro do bloco do MERCOSUL ainda são discretos, mas os últimos acordos constituem um importante avanço. Mais importante ainda, eles abrem caminho para um fluxo livre de zona de dados entre o MERCOSUL e a UE.

2. O Acordo de Livre Comércio MERCOSUL-UE - muitos dados correram sob a ponte desde o início das negociações

O acordo entre o MERCOSUL e a UE é de suma importância, pois juntas essas duas áreas respondem por um PIB de cerca de US $20 trilhões, aproximadamente 25% da economia mundial, e um mercado de aproximadamente

4. UE diz que acordo com o Mercosul aprimorará políticas de proteção de dados - 11/07/2019 - UOL Economia, disponível em: <https://economia.uol.com.br/noticias/efe/2019/07/11/ue-diz-que-acordo-com-o-mercosul-aprimorara-politicas-de-protecao-de-dados.htm>. acesso em: 6 jun. 2023.

780 milhões de pessoas.[5] O acordo, quando ratificado, constituirá uma das maiores áreas de livre comércio do mundo.

A tecnologia avançou significativamente desde o início das negociações, há 20 anos.[6] A digitalização da economia trouxe as informações pessoais para o centro das atenções. Os dados se tornaram um bem indispensável da nova ordem econômica. Estima-se que o peso económico do mercado de dados deve representar 5,4% do PIB da União Europeia até ao ano de 2025.[7] As transferências de dados são, assim, condição sine qua non para o crescimento desta base em termos de negócio transfronteiriço.

Nesse cenário, a proteção de dados pessoais vem sendo progressivamente pensada como um direito humano fundamental,[8] com governos em todo o mundo buscando ativamente a sua regulamentação com objetivo de melhor proteger seus cidadãos.[9]

Na União Europeia, desde 1995, a Diretiva 95/46/EC previa um procedimento para garantir a proteção de dados em termos de transações internacionais. Além disso, a privacidade e os dados pessoais dos cidadãos e residentes europeus são protegidos como direitos fundamentais pela Carta dos Direitos Fundamentais da UE (artigos 7º e 8º).

Já para o bloco do Sul, a Decisão 15/20 é um marco para a proteção de dados no MERCOSUL. É a primeira vez, desde a fundação do bloco, há mais de 30 anos, que uma norma aprovada em âmbito regional estabelece regras de proteção de dados obrigatórias para seus Estados Partes.

Portanto, a fim de possibilitar o avanço deste acordo para ambos os blocos e, sobretudo, para os países do MERCOSUL, é necessário que suas legislações se harmonizem com as disposições e princípios do Regulamento Geral de Proteção de Dados (“GDPR”), o que também representam um salto significativo

5. Ministério das Relações Exteriores, disponível em: <https://www.gov.br/mre/images/ed_acesso_info/auditorias_brasil/MERCOSUL/MERCOSUL-UE/2019_10_24_-_Resumo_Acordo_Mercosul_UE_CGNCE.pdf>. acesso em: 6 jun. 2023.

6. EU trade relations with Mercosur, disponível em: <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mercosur_en>. acesso em: 6 jun. 2023.

7. Commission’s guidance on free flow of non-personal data, European Commission - European Commission, disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_2749>. acesso em: 6 jun. 2023.

8. Data Privacy Is a Human Right | Human Rights Watch, disponível em: <https://www.hrw.org/news/2018/04/19/data-privacy-human-right>. acesso em: 6 jun. 2023.

9. Data Privacy As A Basic Human Right, disponível em: <https://www.forbes.com/sites/forbestechcouncil/2019/11/12/data-privacy-as-a-basic-human-right/?sh=459758f54cbf>. acesso em: 6 jun. 2023.

para o reconhecimento da proteção de dados pessoais como um direito humano fundamental.

3. Acordo de Livre Comércio MERCOSUL-UE - Momento ideal para avançar na agenda latino-americana de proteção de dados pessoais

O acordo comercial negociado já representa uma série de externalidades positivas na agenda interna do MERCOSUL. Esse impulso também deve ser aproveitado para avançar na agenda de proteção de dados intrabloco e na harmonização das legislações de seus Estados membros sobre o assunto.

O próximo Acordo Comercial será aplicado sem prejuízo da legislação de cada parte no campo da proteção de dados. No entanto, uma decisão de adequação mútua - estabelecendo que o MERCOSUL e a UE tenham um nível comparável de proteção de dados pessoais - facilitaria ainda mais as trocas comerciais, complementando e ampliando os benefícios potenciais do Acordo Comercial UE-Mercosul.

O recém assinado Acordo de Comércio Eletrônico é apenas o exemplo mais recente de uma importante produção normativa vivenciada pelo bloco ao longo de 2019 e também de 2020, apesar do impacto da pandemia de COVID-19,[10] que, ao menos em parte, pode ser atribuído à conclusão das negociações do acordo comercial com a União Européia e a consequente percepção da necessidade de avançar nos compromissos intrabloco.

Deve-se destacar que regras comuns de proteção de dados pessoais vinham sendo discutidas há anos no âmbito do MERCOSUL. Em 2005, a Argentina propôs um regulamento sobre proteção de dados que resultou em um documento aprovado pelos estados membros em 2010, mas que nunca foi endossado como um regulamento do bloco.

De acordo com a Nota Técnica 2052 do Banco Interamericano de Desenvolvimento ("BID"),[11] o Acordo com a União Europeia incorpora regulamentação em áreas onde existe um vácuo regulatório no bloco sul-americano. A Nota Técnica informa que isso poderia colocar em risco a relevância do MERCO-

10. Mercosul se manteve ativo em 2020 — Planalto, disponível em: <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2020/12/mercosul-se-manteve-ativo-em-2020>. acesso em: 6 jun. 2023.

11. MERCOSUL 2020: Sob a pressão da agenda externa disponível em: <https://publications.iadb.org/publications/portuguese/document/Informe-MERCOSUL-2020-Sob-a-pressao-da-agenda-externa.pdf>

SUL, principalmente porque em sua Cúpula de julho de 2019, os sócios definiram que o Acordo UE-MERCOSUL poderia entrar provisoriamente em vigência bilateral, após ratificação pelo Parlamento Europeu e pelos parlamentos de cada país do MERCOSUL, sem a necessidade de aguardar a conclusão do processo de ratificação por todos os países membros do bloco.

Deve-se destacar que regras comuns de proteção de dados pessoais vinham sendo discutidas há anos no âmbito do MERCOSUL. Em 2005, a Argentina propôs um regulamento sobre proteção de dados que resultou em um documento aprovado pelos estados membros em 2010, mas que nunca foi endossado como um regulamento do bloco.

Essa possibilidade vai contra um dos princípios orientadores que regeram as negociações birregionais durante grande parte dos vinte anos do processo de negociação. Havia o entendimento de que se tratava de um processo de integração entre as duas uniões aduaneiras e que o Acordo contribuiria para consolidar no MERCOSUL um modelo de integração inspirado no exemplo europeu.

Enquanto não houver decisão de adequação, os dados podem não fluir livremente. Salvaguardas adicionais são exigidas tanto pelo Brasil quanto pela UE. Tais requisitos representam custos adicionais para empresas que consideram fazer transações comerciais.[12]

Como 2 dos 4 membros ativos do MERCOSUL já têm uma decisão de adequação (quais sejam, Argentina e Uruguai), esta parece ser uma oportunidade que Brasil e Paraguai - mas também o bloco como um todo - não podem perder se quiserem se manter competitivos.

4. Decisão de Adequação da União Europeia

Na União Europeia, desde 1995, a Diretiva 95/46/EC previa um procedimento para garantir a proteção de dados em termos de transações internacionais. A Comissão Europeia tinha autoridade para avaliar e decidir se determinados países atingiram um nível adequado de proteção e deveriam se beneficiar de uma forma simplificada mais acessível de transferir dados para o exterior.

O Regulamento Geral de Proteção de Dados (“GDPR”) se baseou no regu-

12. Art. 46 GDPR – Transfers subject to appropriate safeguards, disponível em: <https://gdpr-info.eu/art-46-gdpr/>. acesso em: 6 jun. 2023.

lamento anterior. Manteve a lógica do regime, mas clarificou e reforçou determinados procedimentos. Um exemplo é que ao abrigo da GDPR agora deve haver uma avaliação contínua das normas de proteção de dados de cada país com uma decisão de adequação.

A UE só tem decisões de adequação em relação a 12 países no mundo. O mais recente, e o primeiro emitido sob o GDPR, foi para o Japão[13]. Esta decisão também é emblemática porque, pela primeira vez, a UE e um país terceiro concordaram com o reconhecimento recíproco do nível adequado de proteção. Esse acordo de adequação mútua criou a maior área mundial de transferências seguras de dados com base em um alto nível de proteção de dados pessoais. Nas palavras do Comissário da UE para Justiça[14], Consumidores e Igualdade de Gênero, espera-se que o acordo "promova padrões globais para proteção de dados e dê um exemplo para futuras parcerias nesta área-chave".[15]

Tal afirmação se revelaria particularmente verdadeira na hipótese em análise. Serve também como paradigma para se pensar em possíveis obstáculos e formas de superação para que Brasil e UE cheguem a uma decisão mútua de adequação.

Primeiro, o acordo e o Acordo de Parceria Econômica UE-Japão[16] ocorreram quase simultaneamente, ilustrando como na era digital o comércio e os fluxos de dados andam de mãos dadas.

Em segundo lugar, assim como no Brasil, a legislação japonesa sofreu adaptações e agora, em muitos aspectos, segue um caminho semelhante ao europeu, ou seja, o sistema é baseado em um rígido padrão de proteção de dados imposto tanto ao setor privado quanto ao público. Uma autoridade de proteção de dados tem o mandato de supervisionar a implementação dos padrões de proteção de dados e pode promover a conformidade, se necessário.

Os sistemas nacionais exigem também uma decisão de adequação para

13. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance).

14. International data flows: Commission launches the adoption of its adequacy decision on Japan, European Commission - European Commission, disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433>. acesso em: 9 jun. 2023.

15. Também o México, após a conclusão do novo acordo comercial com a UE em 2020, está em processo de obtenção de uma decisão de adequação. Veja mais em: Reconocen a México por protección de datos, disponível em: <https://www.eluniversal.com.mx/nacion/reconocen-mexico-por-proteccion-de-datos/?amp>. acesso em: 9 jun. 2023.

16. EU and Japan sign Economic Partnership Agreement, European Commission - European Commission, disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4526>. acesso em: 9 jun. 2023.

transferências internacionais em regime mais livre. No caso do Japão, portanto, também houve um processo semelhante para reconhecer o quadro de proteção de dados da UE como adequado. O Brasil seguiria um caminho semelhante.

Os procedimentos negociais que culminaram na decisão mútua de adequação entre o Japão e a UE incluíram avaliações não só do marco regulatório, mas também dos arranjos institucionais domésticos. A oportunidade estava lá, mas havia alguns desafios presentes. Só se pode esperar o mesmo para o Brasil.

A seguir, são abordados esses desafios, bem como a situação atual da proteção de dados em cada um dos países membros do MERCOSUL.

5. Legislação do MERCOSUL sobre Status de Proteção de Dados - Two down, two to go

Como dito anteriormente, não havia regulamentação de proteção de dados do MERCOSUL antes da Decisão 10/20. A Decisão abre espaço para a criação de uma zona de livre fluxo de dados no âmbito do Mercosul.

A Decisão 10/20 prevê a transferência transfronteiriça de informações por meios eletrônicos, quando esta atividade visar a atividade comercial de uma entidade de uma das partes signatárias, desde que seja aplicado um nível de proteção adequado (art. 7.2), conforme especificado no início deste artigo. Ou seja, ao atual livre fluxo de bens e serviços e no Mercosul agora pode ser adicionado o livre fluxo de dados mediante o cumprimento dos requisitos de proteção de dados. Seguindo a legislação país a país do MERCOSUL sobre proteção de dados.

5.1 Argentina

A Argentina conta com uma lei de proteção de dados pessoais desde 2000. A Lei 25.326[17] traz os princípios gerais e classificação relativos à proteção de dados e regula a transferência internacional de dados, direitos dos titulares de dados, recursos e ações que eles têm tanto administrativa quanto judicialmente para obter o eliminação, retificação, modificação, adição e retificação dos dados que se encontrem em ficheiros ou bases de dados, tanto públicos

17. Protección de datos personales | Argentina.gob.ar, disponível em: <https://www.argentina.gob.ar/aaip/datospersonales>. acesso em: 9 jun. 2023.

como privados, e as obrigações dos responsáveis pelos referidos ficheiros ou bases de dados na recolha e tratamento de dados pessoais.

Na Argentina, a autoridade de execução em matéria de Dados Pessoais e Acesso à Informação Pública é a Agência Nacional de Acesso à Informação Pública[18]. Dispõe de um secretariado - Direcção Nacional de Protecção de Dados Pessoais[19] - responsável pela regulamentação e fiscalização das matérias relacionadas com os dados pessoais e pelo cumprimento da Lei de Protecção de Dados Pessoais.

Em 2003, a Comissão Européia promulgou uma decisão posicionando a Argentina como um país com nível adequado de proteção de dados pessoais, em conformidade com os termos da Diretiva 95/46/EC.

5.2 Brasil

Até 2018, o Brasil não possuía uma regulamentação geral que sistematizasse o tratamento de dados pessoais[20]. A Lei nº 13.709/2018, a Lei Geral de Proteção de Dados ("LGPD"), mudou o cenário. Este diploma legislativo tem uma inspiração inegável no modelo europeu. Como entrou em vigor em setembro de 2020, estabeleceu um quadro legal juridicamente robusto para a proteção de dados pessoais.

Com relação às transferências internacionais de dados, a legislação brasileira estabelece procedimento semelhante à Diretiva e ao GDPR. Nos termos do art. 33 e seguintes a Autoridade Nacional de Proteção de Dados ("ANPD") tem o mandato de avaliar os registros de proteção de dados de outros países e decidir se eles atingem um nível adequado de proteção de dados.

Assim, o GDPR e a LGPD estabelecem regras robustas para proteger os dados pessoais e estabelecem um mecanismo de decisão baseado em adequação para facilitar as transferências internacionais. Cada um tem suas particularidades e exige o cumprimento de determinados requisitos que visam manter esses altos padrões de proteção mesmo em uma situação em que os dados possam cruzar suas fronteiras.

---

18. Protección de datos personales, Argentina.gob.ar, disponível em: <https://www.argentina.gob.ar/aaip/datospersonales>. acesso em: 6 jun. 2023.

19. Ibid.

20. No entanto, vale ressaltar que o Marco Civil da Internet de 2014 já delineava os direitos dos cidadãos brasileiros em relação à transferência internacional de dados pessoais.

A Autoridade Nacional de Proteção de Dados ("ANPD") entrou em vigor em outubro de 2020. De acordo com a LGPD, a Autoridade goza de autonomia técnica e decisória. No entanto, a Autarquia faz parte da administração pública federal (Presidência da República), sem personalidade jurídica ou dotação orçamentária própria.

Um dos requisitos do artigo 45, n.º 2, do GDPR é a existência de uma Autoridade de Proteção de Dados independente. Com base nas negociações recentemente concluídas entre a UE e a Coreia do Sul (30 de março de 2021)[21], o atual status legal da ANPD pode representar um desafio para o Brasil em relação a essa exigência. Na primeira rodada de negociações com a Coréia do Sul, a UE deixou clara sua expectativa de cumprimento do art. 45(2), art.

De acordo com a lei geral de proteção de dados da Coreia (PIPA), o DPA coreano satisfaz o requisito de independência, mas a aplicação sob o PIPA depende do Ministério do Interior e Segurança. Esta configuração é um fator limitante que impede o seu estado adequado.

No entanto, podemos comparar o quadro regulatório do Brasil com o do Uruguai para avaliar possíveis futuros brasileiros. O Uruguai, além de possuir o status de adequação, possui um DPA que é muito semelhante em estrutura à Autoridade de Proteção de Dados brasileira tal como está. Ambos são órgãos administrativos dotados de independência técnica, sem personalidade jurídica distinta. Isso não foi visto como um obstáculo intransponível para a UE reconhecer o DPA uruguaio como compatível com os princípios do regime europeu de proteção de dados e considerar o país adequado.

5.3 Paraguai

No Paraguai, a proteção de dados pessoais está prevista na Constituição do país, mas também se baseia na Lei nº 1.682/2001[22], "Que regula a informação privada" e sua posterior modificação pelas Leis nº 1.969/2002[23] e 5.542/2015[24].

---

21. Personal Information Protection, European Commission - European Commission, disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506>. acesso em: 6 jun. 2023.

22. Ley N 1682 de 2001, disponível em: <http://www.oas.org/es/sla/ddi/docs/PA6%20Ley%20N%201682%20de%202001.pdf>. acesso em: 9 jun. 2023.

23. Ley n 1969 de 2002, disponível em: <http://digesto.senado.gov.py/ups/leyes/10389.pdf>. acesso em: 9 jun. 2023.

24. Ley 5542 de 2015, disponível em: <https://www.bacn.gov.py/archivos/4524/20160224131953.pdf>. acesso em:

Este conjunto de leis regula, entre outras questões: o processamento e tratamento de dados pessoais contidos em arquivos, registros e bancos de dados públicos e privados. A recolha, tratamento e tratamento de dados pessoais só é permitido para fins científicos, econômicos, estatísticos ou de marketing.

No entanto, a referida Lei assume que o interesse da proteção recai sobre a pessoa afetada, mais próximo da doutrina norte-americana do que do padrão GDPR, deixando a aplicação do regulamento mais para as partes envolvidas do que para a intervenção do Estado, exceto no que diz respeito ao papel dos tribunais de justiça.

Note-se ainda que não existem definições legais sobre "dados pessoais", "tratamento de dados" e "titular dos dados". Também não faz distinção entre processadores e controladores. Também não estabelece qualquer obrigação de reportar violações de dados ou incidentes que ocorram com dados pessoais.

Outra discrepância com os padrões internacionais de proteção de dados é que a Lei também carece de garantias quanto à transferência e comunicação de dados a terceiros e não inclui disposições relativas à transferência internacional de dados. Da mesma forma, não existe nenhuma autoridade no Paraguai que regule os assuntos relativos à proteção de dados pessoais e ao cumprimento da lei.

Por fim, embora a lei nada estabeleça quanto à possibilidade de reclamação perante entidades administrativas ou judiciais por violação de Dados Pessoais, as penalidades são estabelecidas por outras normativas, que permitem àqueles cujos dados tenham sofrido alguma violação o direito de reclamar perante cíveis ou justiça criminal a busca de uma compensação.

5.4 Uruguai

No Uruguai, os dados pessoais são regidos pela Lei nº 18.331, Lei de Proteção de Dados. A lei uruguaia reconhece no artigo 1º a proteção de dados pessoais como um direito humano. O regulamento é muito abrangente e fornece um quadro muito robusto de direitos e obrigações na matéria, semelhante ao quadro europeu.

No Uruguai, a autoridade responsável pela proteção de dados pessoais é

---

9 jun. 2023.

a Unidade Reguladora e de Controle de Dados Pessoais[25]. O órgão criado pela Lei nº 18.331 de Proteção de Dados Pessoais e Ação de Habeas Data (LPDP), embora com ampla autonomia técnica, não possui personalidade jurídica própria e é parte integrante da Agência de Desenvolvimento do Governo Eletrônico Gestão e Sociedade da Informação e do Conhecimento (AGESIC).

Em 2012, a Comissão Europeia promulgou uma decisão[26] posicionando o Uruguai como um país com nível adequado de proteção de dados pessoais, em conformidade com os termos da Diretiva 95/46/CE.

6. Complicador na equação: o legado da decisão Schrems II

Retomando o exemplo do processo de adequação japonês-europeu, envolveu o fornecimento de 'Regras Suplementares' para superar várias diferenças entre os dois sistemas de proteção de dados. Entre eles regras claras de necessidade e proporcionalidade quanto ao acesso a dados importados da UE pelo governo do país asiático e também a previsão de mecanismos efetivos de oposição para titulares de dados europeus[27].

A decisão do caso Schrems II do Tribunal de Justiça da União Europeia (TJUE)[28], em 16 de julho de 2020, somou-se ao referido processo de adequação japonesa. A decisão do Tribunal invalidou a decisão de adequação anteriormente concedida pela Comissão aos Estados Unidos com base no acordo "Privacy Shield". A decisão do Tribunal foi amplamente baseada na capacidade das autoridades de segurança pública e nacionais de obrigar as entidades de controle e processamento de dados a fornecer dados pessoais.

Os casos mencionados indicam que a possibilidade de governos de países terceiros da UE acessarem dados de detentores europeus pode ser um fator importante levado em consideração para decisões de adequação ao GDPR.

---

25. *Unidad Reguladora y de Control de Datos Personales*, Unidad Reguladora y de Control de Datos Personales, disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/inicio>. acesso em: 9 jun. 2023.

26. 2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704) disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484>. acesso em: 6 jun. 2023..

27. European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, European Commission - European Commission, disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421>. acesso em: 6 jun. 2023.

28. CURIA - Documents, disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404>. acesso em: 9 jun. 2023.

Nesse sentido, o Projeto de Lei Brasileiro de Liberdade, Responsabilidade e Transparência na Internet, também conhecido como Projeto de Lei das Fake News (PL 2630/2020), se aprovado, poderá impactar o processo de adequação Brasil-UE. Seu Artigo 32 geralmente exige a entrega de dados mediante solicitação das autoridades brasileiras independentemente de transferência internacional ou não. Pode ser problemático, pois o projeto de lei, como está, não fornece um propósito claro - por exemplo, segurança nacional. Ressalta-se, porém, que a regra se aplica mediante decisão da autoridade judiciária brasileira, em que poderão ser questionados os princípios da proporcionalidade e da adequação da medida.

Considerações finais

A Comissão logo após a entrada em vigor do GDPR emitiu uma Comunicação sobre Troca e Proteção de Dados Pessoais em um Mundo Globalizado[29]. Neste documento, a Comissão esclarece os critérios que devem ser levados em consideração ao selecionar países terceiros para conduzir um diálogo sobre adequação:

> (i) a extensão das relações comerciais (efetivas ou potenciais) da UE com um determinado país terceiro, incluindo a existência de um acordo de comércio livre ou negociações em curso;
>
> (ii) a extensão dos fluxos de dados pessoais da UE, refletindo laços geográficos e/ou culturais;
>
> (iii) o pioneirismo do terceiro país no campo da privacidade e proteção de dados que pode servir de modelo para outros países de sua região; e
>
> (iv) a relação política global com o país terceiro em causa, nomeadamente no que diz respeito à promoção de valores comuns e objetivos partilhados a nível internacional.

Com base nessas considerações, a Comunicação indica maior agilidade no relacionamento com os principais parceiros comerciais da UE - mencionando expressamente os países da América Latina, em particular os membros do

29. Communication-from-the-commission-to-the-european-parliament-and-the-council. disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>. acesso em: 9 jun. 2023.

Mercosul. Para os membros do MERCOSUL, isso pode representar uma grande oportunidade: mergulhar de cabeça nas oportunidades do acordo e em sua legislação de proteção de dados à altura da ocasião. Queremos dizer negócios e direitos humanos.

Referências

European Commission's guidance on free flow of non-personal data. - European Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_2749>. Acesso em: 6 jun. 2023.

European Commission Communication from the commission to the European parliament and the council. Disponível em: <https://primarysources.brillonline.com/browse/human-rights-documents-online/communication-from-the-commission-to-the-european-parliament-and-the-council;hrdhrd46790058>. Acesso em: 6 jun. 2023.

CURIA - ***Documents***. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404>. Acesso em: 9 jun. 2023.

Data Privacy As A Basic Human Right. Disponível em: <https://www.forbes.com/sites/forbestechcouncil/2019/11/12/data-privacy-as-a-basic-human-right/?sh=459758f54cbf>. Acesso em: 6 jun. 2023.

Data Privacy Is a Human Right | Human Rights Watch. Disponível em: <https://www.hrw.org/news/2018/04/19/data-privacy-human-right>. Acesso em: 6 jun. 2023.

Digital globalization: The new era of global flows | McKinsey. Disponível em: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>. Acesso em: 6 jun. 2023.

EU and Japan sign Economic Partnership Agreement. European Commission - European Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4526>. Acesso em: 9 jun. 2023.

EU trade relations with Mercosur. Disponível em: <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mercosur_en>. Acesso em: 6 jun. 2023.

European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows. European Commission - European Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421>. Acesso em: 6 jun. 2023.

International data flows: Commission launches the adoption of its adequacy decision on Japan. European Commission - European Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433>. Acesso em: 9 jun. 2023.

Mercosul se manteve ativo em 2020 — Planalto. Disponível em: <https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2020/12/mercosul-se-manteve-ativo-em-2020>. Acesso em: 6 jun. 2023.

Ministério das Relações Exteriores. Disponível em: <https://www.gov.br/mre/images/ed_acesso_info/auditorias_brasil/MERCOSUL/MERCOSUL-UE/2019_10_24_-_Resumo_Acordo_Mercosul_UE_CGNCE.pdf>. Acesso em: 6 jun. 2023.

Ley N 1682 de 2001. Disponível em: <http://www.oas.org/es/sla/ddi/docs/PA6%20Ley%20N%201682%20de%202001.pdf>. Acesso em: 9 jun. 2023.

Personal Information Protection. European Commission - European Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506>. Acesso em: 9 jun. 2023.

Protección de datos personales | Argentina.gob.ar. Disponível em: <https://www.argentina.gob.ar/aaip/datospersonales>. Acesso em: 9 jun. 2023.

Reconocen a México por protección de datos. Disponível em: <https://www.eluniversal.com.mx/nacion/reconocen-mexico-por-proteccion-de-datos/?amp>. Acesso em: 9 jun. 2023.

SIM - Detalhes da Normativa. Disponível em: <https://normas.mercosur.int/public/normativas/4018>. Acesso em: 6 jun. 2023.

UE diz que acordo com o Mercosul aprimorará políticas de proteção de dados - 11/07/2019 - UOL Economia. Disponível em: <https://economia.uol.com.br/noticias/efe/2019/07/11/ue-diz-que-acordo-com-o-mercosul-aprimorara-politicas-de-protecao-de-dados.htm>. Acesso em: 6 jun. 2023.

Unidad Reguladora y de Control de Datos Personales. Unidad Reguladora y de Control de Datos Personales. Disponível em: <https://www.gub.uy/unidad-reguladora-control-datos-personales/inicio>. Acesso em: 9 jun. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

EIXO 3

Inteligência artificial e suas aplicações

AUTORES

Gabriel Lacerda Ferreira

Jeannine de Souza Hagnauer

Lucas Cabral de Souza Ramos

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

16

Sobre o uso de inteligências artificiais para gerência de direitos autorais na internet: funcionamento e legalidade dos filtros tecnológicos

GABRIEL LACERDA FERREIRA

GABRIEL LACERDA FERREIRA[1]

Sumário: Introdução. 1. Algoritmos de moderação por inteligência artificial: como funcionam os chamados "filtros tecnológicos". 2. Uso de inteligência artificial para gestão de direitos autorais no direito brasileiro. Considerações finais. Referências.

Introdução

Na aurora da internet, o compartilhamento de conteúdo era limitado por questões técnicas. Até carregar um arquivo de texto era uma tarefa árdua, quem dirá uma música ou um filme. Com o avanço da infraestrutura e a mudança de natureza da chamada "Web 2.0"[2], uma parcela crescente dos usuários desenvolveu o hábito de compartilhar textos, fotos, áudios e vídeos, muitos desses contendo materiais protegidos pelos direitos autorais. Como apresentado por Engstrom e Feamster:

> No nascer da era da Internet, ficou claro que uma de suas virtudes centrais – a capacidade de facilitar a distribuição quase instantânea de informação de todo tipo, inclusive material protegido por direitos autorais, para qualquer lugar conectado do globo – apresentava complicações para a legislação de direitos autorais vigente.[3]

Sejam tentativas de pirataria ou expressões criativas legítimas, desde a criação das plataformas de compartilhamento de conteúdo multimídia (YouTube, Facebook, Instagram, Twitter), o aumento dos conflitos entre usuários e detentores de direitos autorais é natural e lógico. As partes têm interesses antagônicos: os usuários querem ter a maior liberdade possível para criar e compartilhar suas criações, enquanto os entes econômicos das indústrias multimídia desejam proteger seus investimentos de pirataria e diluição. Assim sendo, fez-se necessária a criação de mecanismos para o controle de direitos

1. Advogado. Graduado pela Faculdade de Direito da Universidade Presbiteriana Mackenzie. Pós-graduado em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro).

2. O'REILLY, Tim. What Is Web 2.0: design patterns and business models for the next generation of software. Design Patterns and Business Models for the Next Generation of Software. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html. Acesso em: 12 jan. 2023.

3. ENGSTROM, Evan; FEAMSTER, Nick. The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools. Engine, março 2017. p 3. Tradução Livre. Disponível em: https://www.engine.is/the-limits-of-filtering. Acesso em: 12 jan. 2023.

autorais na internet e o combate à pirataria. Inicialmente tímidos e simples, na maioria das vezes simples formulários preenchidos manualmente, a demanda por soluções mais complexas cresceu juntamente da complexidade dos sites e plataformas onde esses embates foram travados. O mero volume de material adicionado à internet a todo o momento desafia a compreensão. Só no Brasil, 90% dos lares já têm acesso à internet[4]. Em números totais, são mais de 155 milhões de brasileiros utilizando a internet diariamente, constantemente realizando ações que podem violar direitos autorais e, portanto, devem ser monitoradas. É impossível para qualquer ser humano ou poder judiciário moderar esta quantidade de conteúdo utilizando o trabalho humano. Portanto, as plataformas conceberam e criaram sistemas, impulsionados por algoritmos e inteligências artificiais, para possibilitar algum nível de controle sobre os vastos materiais produzidos diariamente.

Como exemplo, a plataforma com talvez a situação mais complexa, por se tratar da maior plataforma de vídeo de acesso livre: YouTube. A cada minuto, cerca de 500 horas de vídeos são carregadas apenas ao YouTube[5]. Tendo isso em vista, é praticamente impossível que se modere esta quantidade de conteúdo utilizando o trabalho humano. Portanto, o YouTube conta com uma miríade de sistemas, que utilizam algoritmos, inteligências artificiais e ferramentas manuais, cada um com uma função diversa.

1. Algoritmos de moderação por inteligência artificial: como funcionam os chamados “filtros tecnológicos”

Os algoritmos de filtragem detêm funcionalidades diversas, mas em geral as inteligências artificiais são programadas para encontrar algum elemento identificador do arquivo ou material protegido por direitos autorais. Esse elemento pode ser metadados, um hash ou características da mídia usada[6]. Esses três elementos definem as três principais técnicas de filtragem, essas sendo:

---

4. BRASIL. MINISTÉRIO DAS COMUNICAÇÕES. 90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. 2022. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acessoem: 12 jan. 2023.

5. STATISA. Hours of video uploaded to YouTube every minute as of February 2020. 2021. Disponível em: https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/. Acessoem: Acesso em: 12 jan. 2023.

6. ENGSTROM, Evan; FEAMSTER, Nick. The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools. Engine, março 2017. p ii. Disponível em: https://www.engine.is/the-limits-of-filtering. Acesso em: 16 nov. 2021.

A mais antiga e mais simples das técnicas, a filtragem por metadados funciona através da catalogação dos metadados presentes em um arquivo. Estes metadados são alimentados a um algoritmo, que os cataloga e aponta sempre que um novo arquivo com os mesmos metadados é adicionado aos servidores de alguma aplicação[7]. Metadados são dados relativos a um arquivo, mas que não o integram. Por exemplo, no caso de uma música, os metadados seriam dados como os compositores, a duração, a capa do álbum etc. São "informação estruturada sobre um recurso de mídia"[8].

As vantagens desse tipo de ferramenta são o custo e a simplicidade. Metadados são facilmente pesquisáveis, até mesmo por um ser humano[9]. Além disso, já que apenas os metadados são utilizados, um algoritmo sequer precisa de acesso aos próprios arquivos[10]. Porém, pelos mesmos motivos, filtros calibrados para metadados podem ser facilmente enganados, bastando uma alteração nos mesmos. Um filme pode ser distribuído com outro nome, por exemplo. Uma música pode ser levemente acelerada ou encurtada para mudar a duração. Também existem casos de falsos positivos, situações em que dois arquivos possuem os mesmos metadados. Por exemplo, dois álbuns ou dois livros podem ter o mesmo título. Caso já exista um na base de dados, o segundo pode ser apontado como violando os direitos autorais do primeiro. Metadados também são facilmente apagados, seja por ferramentas específicas, seja pela conversão de formatos[11].

Como as deficiências da filtragem por metadados se devem ao fato de o elemento filtrado ser adjacente ao arquivo, e não o arquivo em si, a filtragem por *hash* é criada no sentido oposto. Um *hash* é "uma representação numérica de um arquivo que é significativamente menor que o arquivo original"[12]. Basicamente, uma função matemática é aplicada a um arquivo, gerando um *hash* específico àquele arquivo e àquele arquivo apenas, gerando um "identificador

7. Id. p. 11.

8. Ibid.

9. Ibid.

10. Id. p. 12.

11. Ibid.

12. Ibid.

efetivamente perfeito de um arquivo em particular"[13]. Este método também é especialmente conveniente para algoritmo, pois analisar um *hash* é muito mais fácil e rápido que um arquivo por completo, exigindo significativamente menos computação e espaço de arquivo, considerando que um *hash* tem cerca de um centésimo do tamanho de um arquivo equivalente de áudio[14]. Mas as forças da filtragem por *hash* são igualmente sua fraqueza. Como todo *hash* é um identificador perfeito e único de um arquivo específico, qualquer modificação a esse arquivo gera um *hash* diferente. Assim sendo, o filtro só é capaz de capturar cópias idênticas.

O comum a ambas essas técnicas é que a alteração dos arquivos seja capaz de enganar os algoritmos, o que se tornou sabedoria comum e permitiu que usuários burlassem facilmente tais filtros. Procurou-se, então, gerar um filtro que fosse capaz de detectar elementos das próprias obras e os encontrar em arquivos, mesmo que alterados. Com esse propósito foi criada a tecnologia de *fingerprinting*.

O *fingerprinting* funciona da seguinte maneira: um arquivo de áudio, imagem ou vídeo é submetido a processamento por um algoritmo, que analisa o maior número de características de uma obra para criar uma "impressão digital" daquela obra. No caso de uma música, por exemplo, podem ser analisadas as notas, as frequências de som, o volume, e as mudanças desses marcadores durante a faixa. Essa análise é muito mais robusta que a criação de um *hash*, e mais resistente a simples mudanças[15]. Além disso, uma mesma obra pode ter diversas impressões. Um filme, por exemplo, pode ter impressões relativas ao áudio, a imagem a ao vídeo, além de ter impressões de diversas cenas, devido a sua duração[16]. Essas impressões são armazenadas e um algoritmo diferente terá a função de procurar tais impressões em todos os arquivos no momento do *upload* ou procurar em todos os arquivos já presentes em uma base de dados.

Exemplos incluem o Content ID (YouTube), Audible Magic, PhotoDNS, Zefr e Echoprint. Importante que cada algoritmo é específico para um tipo de obra

13. Id. p 13.

14. Ibid.

15. Id. p. 13.

16. Id. p. 14.

específica[17]. O Echoprint, da Spotify, identifica apenas músicas, enquanto o PhotoDNS identifica apenas fotos. Cada tipo de mídia em um aplicativo exige uma solução de fingerprinting diferente. E, logicamente, uma solução de vídeo como o Content ID é a mais complexa possível, pois deve ser capaz de identificar tanto áudio e imagem individualmente quanto combinados.

Apesar de ser a técnica mais avançada e com melhor porcentagem de acerto, nem todo tipo de material pode ser detectado por essas IAs baseadas em *fingerprinting*. Diferente de técnicas baseadas em metadados ou *hashes*, não é aplicável a *softwares*, por exemplo. Também existe a necessidade de a inteligência artificial ter acesso total e irrestrito ao material a ser protegido para gerar as "digitais", o que impede o uso em arquivos encriptados e *torrents*[18].

Uma limitação que excede as questões técnicas é em relação ao preço dessas ferramentas. A grande maioria dos provedores de aplicações de internet não tem recursos para desenvolver sistemas efetivos de filtragem, especialmente aqueles baseados na tecnologia mais efetiva de *fingerprinting*, ou sequer contratar ou licenciar algo dessa natureza[19]. O YouTube, por exemplo, gastou pelo menos 100 milhões de dólares para o desenvolvimento da ferramenta Content ID até 2018, sem contar os gastos continuados para manutenção, operação e melhoramento da mesma[20]. Esse tipo de gasto fica completamente fora da realidade de qualquer operação que não seja de responsabilidade de uma *Big Tech*.

Como dito anteriormente, a relação entre os usuários e o controle de direitos autorais na plataforma não é inteiramente pacífica ou estritamente cordial. Muitos usuários não entendem os sistemas, sentem que frequentemente são injustamente afetados, ou acreditam que esse tipo de controle sequer deveria existir. Isso leva a uma série de fenômenos curiosos onde os usuários tentam enganar os algoritmos, ou manipulá-los de alguma maneira.

Mesmo tendo uma técnica mais avançada, o *fingerprinting* não é imune e

17. Id. p. 15

18. Id. p. 2

19. Ibid. p. ii.

20. MANARA, Cedric. Protecting what we love about the internet: our efforts to stop online piracy. 2018. Disponível em: https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/. Acessoem: 12 jan. 2023.

pode ser induzido a erros. Uma manifestação disso é o popularmente chamado "*Copyright Smuggling*"[21], ou "Contrabando de Direitos Autorais". Mídias protegidas por direitos autorais podem ser usadas em vídeos na plataforma sem ser detectadas pelo algoritmo de *fingerprinting* de diversas maneiras, em geral usando técnicas de edição de áudio e vídeo em uma tentativa de enganar o software de *fingerprinting*, como: serem usadas em baixíssima resolução; serem usadas no formato de "vídeos de reação"[22]; utilização de marcas d'água ou efeitos para obscurecer a imagem parcialmente; diminuir a imagem no quadro e utilizar outros elementos gráficos e sonoros no vídeo; espelhar a imagem; inserir cortes aleatórios, aumentar ou diminuir o tom ou velocidade do áudio. A ideia é gerar uma "poluição" sonora, visual ou textual suficiente para gerar uma impressão digital suficientemente diferente e enganar o algoritmo de filtragem. Essas técnicas, porém, não são garantidas e evoluem juntamente com o avanço da tecnologia de detecção da plataforma.

Outras soluções como uso de redes neurais e monitoramento comportamental dos espectadores[23] têm sido propostas pela academia e indústria, mas ainda estão em fase de estudo e implementação. Apesar de terem um maior potencial de acerto por usarem fatores externos às próprias obras (como, por exemplo, monitorar o chat de uma livestream ou ler os comentários de uma postagem para tentar relacionar com possíveis materiais protegidos), a maior complexidade aumenta ainda mais o custo de criação e operação. Além disso, são geradas novas preocupações legais em relação à privacidade e proteção de dados dos usuários.

Existem limitações que são universais ao funcionamento destes sistemas: sistemas automatizados de filtragem de conteúdo são incapazes de diferenciar conteúdos que usam obras de maneira lícita e ilícita, ou conforme os ter-

21. EMPLEMON. Copyright Smuggling | The YouTube Copyright Metagame pt. 2. Youtube, 21 nov. 2019. Disponível em: https://www.youtube.com/watch?v=VvFGumd_esg&ab_channel=EmpLemon. Acesso em: 16 nov. 2021.

22. Essa é uma modalidade de conteúdo onde o criador assiste um vídeo enquanto é gravado, com suas reações sendo mostradas conjuntamente com o vídeo assistido, geralmente em um quadro aplicado acima da imagem no canto inferior direito ou esquerdo. A adição de um novo quadro e o som da voz do criador podem ser o suficiente para "enganar" o algoritmo.

23. ZHANG, Daniel Yue; LI, Qi; TONG, Herman; BADILLA, Jose; ZHANG, Yang; WANG, Dong. Crowdsourcing-Based Copyright Infringement Detection in Live Video Streams. 2018 Ieee/Acm International Conference on Advances In Social Networks Analysis And Mining (Asonam), [S.L.], p. 367-374, ago. 2018. IEEE. http://dx.doi.org/10.1109/asonam.2018.8508523.

mos de uso da plataforma. Isto teria acarretado reiterados[24] casos[25] de remoção de conteúdos lícitos. Como notam Amaral e Boff:

> O Content ID não analisa a possibilidade de uso aceitável, ou limitações de direito autoral, apesar de isto estar descrito nas diretrizes de direitos autorais do site, uma vez que os algoritmos trabalham com soluções lógicas para problemas idênticos, o que se tem é a aplicação de uma solução única para todos os casos, isto é, o bloqueio do vídeo (ou até mesmo, a conta do usuário caso reivindicações de direitos autorais ocorram repetidamente) ou do áudio. Casos como citações, paráfrases e reproduções que não prejudiquem a obra ou o autor não podem ser objeto de veto, sob pena de obstar a liberdade de expressão. A própria LDA fez estas ressalvas criando institutos como as limitações ao direito de autor.[26].

Assim sendo, as ferramentas não levam em consideração qualquer tipo de nuance. Não é considerado se os detentores possuem direitos exclusivos sobre as obras alimentadas a algoritmos como Content ID, tampouco se há uso aceitável ou outro tipo de exceção legal para o uso da obra. As limitações essenciais dos filtros tecnológicos para gerência de direitos autorais são ainda mais exacerbadas para o monitoramento de transmissões ao vivo[27]. Como, pela própria natureza, transmissões ao vivo não podem ser revisadas antes de ficarem disponíveis para o consumo, existe um atraso insuperável entre a disponibilidade de um material possivelmente infringente e seu bloqueio. Aliado com o inconcebível volume de dados de livestreams, a técnica tradicional de *fingerprinting* tem índices muito baixos de efetividade nesses contextos, com estudos sugerindo que até 26% das transmissões ilegais demoram mais de trinta minutos para serem bloqueadas, e mais de 22% das transmissões apon-

24. VON LOHMANN, Fred. YouTube's Content ID (C)ensorship Problem Illustrated. 2010. Disponível em: https://www.eff.org/deeplinks/2010/03/youtubes-content-id-c-ensorship-problem: Acesso em: 12 jan. 2023.

25. TRENDACOSTA, Katharine. Unfiltered: How YouTube's Content ID Discourages Fair Use and Dictates What We See Online. 2020. Disponível em: https://www.eff.org/pt-br/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online. Acesso em: 12 jan. 2023.

26. AMARAL, Jordana Siteneski do; BOFF, Salete Oro. A FALIBILIDADE DO ALGORITMO CONTENT ID NA IDENTIFICAÇÃO DE VIOLAÇÕES DE DIREITO AUTORAL NOS VLOGS DO YOUTUBE: EMBATES SOBRE LIBERDADE DE EXPRESSÃO NA CULTURA PARTICIPATIVA. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, p. 59, Jul/Dez. 2018. Disponível em: https://indexlaw.org/index.php/revistadipic/article/view/4679. Acesso em: 12 jan. 2023.

27. WILLIAMS, Brett. YouTube has an illegal TV streaming problem: you can binge your favorite show on youtube, if you look hard enough. You can binge your favorite show on YouTube, if you look hard enough.2017. Disponível em: https://mashable.com/article/youtube-live-streaming-copyrights. Acesso em: 12 jan. 2023.

tadas como infringentes não contendo nenhum direito autoral de terceiro[28].

Um bom exemplo das limitações do funcionamento dos sistemas baseados em tecnologias *fingerprinting* pode ser visto em relação a artistas dentro do gênero de músicas clássicas. A grande maioria do catálogo desses artistas é composta de reproduções de obras originalmente compostas há muitos séculos e, por consequência, se encontram no domínio público, carecendo de proteção aos seus direitos autorais[29]. Porém, a informação de se uma gravação é baseada em obra em domínio público não consta nas bases de dados alimentadas aos softwares usados[30]. Toda regravação de obra no domínio público alimentada a uma dessas bases de dados é tratada como original, e não há nenhum mecanismo que impeça que haja reivindicações de direitos autorais para com outras regravações da mesma composição[31].

Aliado a isso está o fato de, devido ao conservadorismo musical presente em grande parte das gravações neste gênero, muitas das músicas soarem extremamente próximas, próximas demais para que o *fingerprinting* consiga diferenciar performances diferentes de diferentes artistas[32]. Importante ressaltar que, mesmo que os direitos autorais sobre a composição em si possam ter passado para o domínio público, os direitos sobre cada performance e gravação existente ainda persistem[33]. Durante o início da pandemia, com a transição dos concertos presenciais para os gravados e subidos em plataformas online, e as livestreams, estes problemas se exacerbaram. O número de reivindicações errôneas explodiu, e muitos artistas se viram impossibilitados de exercer sua profissão pelo mero volume de burocracia a ser lidada diariamente em disputar essas reivindicações[34]. Muitas performances sendo transmitidas ao vivo eram suspensas por reivindicações de mais de um detentor de direitos autorais simultaneamente[35].

---

28. BERKOWITZ, Adam. Classical Musicians v. Copyright Bots. Information Technology And Libraries, [S.L.], v. 41, n. 2, p. 1-9, 15 jun. 2022. p. 1-2. Boston College University Libraries. http://dx.doi.org/10.6017/ital.v41i2.14027. p. 2.

29. BERKOWITZ, Adam. Classical Musicians v. Copyright Bots. Information Technology And Libraries, [S.L.], v. 41, n. 2, p. 1-9, 15 jun. 2022. p. 1-2. Boston College University Libraries. http://dx.doi.org/10.6017/ital.v41i2.14027.

30. Ibid.

31. Ibid. p. 2.

32. Ibid.

33. Ibid.

34. Ibid. p. 3.

35. Ibid.

Outra deficiência presente é a falta de transparência empregada pelos provedores de aplicações de internet em relação aos algoritmos e critérios aplicados. Como notou a Fundação Libertis, através de seu Programa OBSERVACOM, em requerimento ao Ministério Público Federal:

> (...) não estão disponíveis dados sobre os critérios usados pelo YouTube para disponibilização do Content ID para determinados agentes, como já explicitado, e tampouco o número de usuários do sistema, bem como os dados sobre pedido de uso do recurso e autorização ou negativa. Tampouco estão disponíveis informações adequadas acerca das exigências do YouTube de uso dos detentores de direitos autorais autorizados a utilizar o Content ID em conformidade com as legislações locais para garantia da liberdade de expressão e acesso à informação, de forma a assegurar que seu uso não abra margem para abusos e má fé. Não há informação sobre possíveis sanções aplicáveis aos usuários do Content ID em caso de verificada má-fé na revisão nos reclamos de direitos autorais como, por exemplo, em caso de pedido de retirada de conteúdo utilizado de acordo com as limitações e exceções aos direitos de autor previstas nas normas internacionais e na legislação brasileira.[36]

2. Uso de inteligência artificial para gestão de direitos autorais no direito brasileiro

A situação jurídica deste sistema, segundo a doutrina, seria a seguinte: o sistema de gerenciamento de direitos autorais na internet, em geral, segue a lógica do *notice and takedown*: assim que o detentor de direitos notifica a plataforma de suposta violação de seus direitos, o conteúdo é retirado imediatamente e a legitimidade é discutida posteriormente. Este sistema é originário da lei DMCA estadunidense, que confere imunidade à plataforma no caso de remoção errônea,

Uma breve explicação: o "DMCA", ou *Digital Millennium Copyright Act* (Lei de Direitos Autorais do Milênio Digital), é uma lei federal estadunidense criada em 1998 com o propósito de viabilizar o mercado criativo na nascente inter-

36. OBSERVACOM. Requerimento ao Ministério Público Federal do Brasil. 2021. p, 19. Disponível em: https://intervozes.org.br/content-id-do-google-censura-e-requer-controle-publico-afirma-observacom-ao-mpf/. Acessoem: 12 jan. 2023.

net da época[37]. Parte dessa lei, especificamente o parágrafo 512, refere-se à limitação de responsabilidade dos provedores de aplicações de internet (ISPs, ou *Internet Service Providers*) sobre conteúdos de terceiros, conhecido como OCILLA (*Online Copyright Infringement Liability Limitation Act*, ou Lei de Limitação de Responsabilidade por Infração de Direito Autoral na Internet) ou como Safe Harbor ou "Porto Seguro", pois confere imunidade às ISPs que seguem os critérios da lei. Ou seja, os provedores se tornam imunes a responsabilização jurídica em relação ao armazenamento de conteúdos infringentes, desde que o provedor:

> (A)
>
> (i) não tenha conhecimento real de que o material ou uma atividade que usa o material no sistema ou rede seja infringente;
>
> (ii) na ausência de tal conhecimento real, não está ciente de fatos ou circunstâncias pelas quais a atividade infratora é aparente; ou
>
> (iii) ao obter tal conhecimento ou ciência, agir de forma célere para remover ou desabilitar o acesso ao material;
>
> (B) não receba benefício financeiro diretamente atribuível à atividade infratora, caso o provedor tenha o direito e a capacidade de controlar tal atividade; e
>
> (C) após a notificação da violação alegada, conforme descrito no parágrafo (3), responde rapidamente para remover ou desabilitar o acesso ao material que alegadamente infringiu ou foi objeto de atividade infratora.[38]

A OCILLA é, portanto, a base legal do sistema *notice and takedown* nos EUA. Por lá, os provedores de aplicações de internet têm uma obrigação legal de remover qualquer conteúdo que seja indicado pelos detentores de direitos autorais, sob a pena de serem responsabilizados legalmente caso seja detectada violação de fato. Essas mesmas regras eram aplicadas na prática e encontravam reciprocidade na jurisprudência. Anteriormente à promulgação

37. U.S. COPYRIGHT OFFICE (Estados Unidos). THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 U.S. Copyright Office Summary. 1998. Disponível em: https://www.copyright.gov/legislation/dmca.pdf. Acesso em: 12 jan. 2023.

38. 17 U.S. Code § 512 - Limitations on liability relating to material online. Tradução livre. Disponível em: https://www.law.cornell.edu/uscode/text/17/512. Acesso em: 12 jan. 2023.

do Marco Civil da Internet, no cenário de inexistência de uma lei específica versando sobre o tema, uma reprodução do sistema *notice and takedown* encontrava certo espaço na jurisprudência nacional, em especial em relação à atuação da Min. Nancy Andrighi[39]. Porém, com a promulgação do Marco Civil da Internet, o vazio não foi solucionado. A redação do *caput* dos artigos 18 e 19 estabelece que:

> Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> 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.[40]

Esta redação cria uma proibição geral a um sistema baseado no *notice and takedown*, condicionando a retirada de conteúdo gerado por terceiros a uma ordem judicial. Contudo, já no segundo parágrafo do artigo 19, cria-se uma exceção: "§2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal."[41]. Por questões políticas[42], tal legislação específica jamais se materializou, criando um vácuo legislativo em que, na falta de uma proibição expressa, o sistema *notice and takedown* e a sua extensão nos filtros

39. GOMES, Maria Cecília Oliveira. OS FILTROS TECNOLÓGICOS PODEM CONTRIBUIR PARA A PREVENÇÃO DAS VIOLAÇÕES DOS DIREITOS AUTORAIS NA INTERNET? Revista da ABPI, n. 153, p. 63, Mar/Abr 2018. Disponível em: https://www.academia.edu/37209106/Os_filtros_tecnol%C3%B3gicos_podem_contribuir_para_a_preven%C3%A7%C3%A3o_das_viola%C3%A7%C3%B5es_dos_direitos_autorais_na_internet. Acesso em: 12 jan. 2023.

40. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 2º, VII e VIII. Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2023.

41. Ibid

42. PARRA, Flávia; BRANCO, Sérgio; PADRÃO, Vinícius. Violações de direitos autorais de terceiros em plataformas de Internet no Brasil: uma análise a partir de decisões judiciais. 2021. p. 5. Disponível em: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/19466/1/%5bP%5d%5bW%5d%20Viola%c3%a7%c3%b5es%20de%20direitos%20autorais%20de%20terceiros%20em%20plataformas%20de%20internet%20no%20Brasil.pdf. Acesso em: 30 abr. 2023.

tecnológicos é autorizado, porém não obrigatório[43]. Explicitamente, no artigo 31 da referida lei, o estado de coisas é revertido ao anterior, até a promulgação de lei específica:

> No contexto descrito, a indefinição acerca de um regime de responsabilidade dos provedores no caso de violação de direitos de autor de terceiros abriu uma lacuna legal no assunto. Junto a isso, a jurisprudência ainda não está consolidada, o que resulta em uma tomada de decisões divergentes entre os tribunais no país. Assim, criou-se um espaço propício para os provedores regularem, no âmbito de suas políticas internas e relação contratual com os usuários, o ponto da violação de direitos autorais de terceiros e como ele seria endereçado na plataforma. Em razão disso, formaram-se ecossistemas privados, que variam a depender do provedor, com um objetivo de combater a violação retratada.[44]

Esse tipo de atuação está protegido pelo próprio Marco Civil, por exemplo, nos princípios da natureza participativa da rede e da liberdade dos modelos de negócios promovidos na internet[45]. Mas esses princípios não são absolutos e devem ser ponderados com outros como a liberdade de expressão, presunção de inocência e acesso à justiça. Socorre esse entendimento novamente a Min. Nancy Andrighi, ao decidir que:

> Esta Corte fixou entendimento de que "(i) não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso[46]

43. Id. p. 10

44. PARRA, Flávia; BRANCO, Sérgio; PADRÃO, Vinícius. Violações de direitos autorais de terceiros em plataformas de Internet no Brasil: uma análise a partir de decisões judiciais. 2021. p. 14. Disponível em: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/19466/1/%5bP%5d%5bW%5d%20Viola%c3%a7%c3%b5es%20de%20direitos%20autorais%20de%20terceiros%20em%20plataformas%20de%20internet%20no%20Brasil.pdf. Acesso em: 30 abr. 2023.

45. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art. 2º, VII e VIII. Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2023.

46. BRASIL. Supremo Tribunal Federal (Terceira Turma). Recurso Especial nº 1.642.560 (2016/0242777-4) - São Paulo. Civil e processual civil. Rede social. Responsabilidade civil do provedor de aplicação. Rede social. Facebook. [...]. Recor-

Como exposto anteriormente, o sistema de *notice and takedown* é mais restrito para a liberdade de expressão do que o praticado no Brasil, pois dá ao detentor de direitos autorais o poder de retirar o acesso ao conteúdo que acredita violar seus direitos praticamente imediatamente, com apenas uma notificação, sem necessidade de revisão judicial. E os filtros tecnológicos são um passo além disso. Ainda são um reflexo do sistema de *notice and takedown*, visto que quem decide dar início ao processo de remoção e decide quais materiais são protegidos são os detentores dos direitos autorais. Mas, como os provedores de aplicações de internet são quem desenvolvem e operam as inteligências artificiais, atraem para si também responsabilidade.

E, pela natureza automatizada dos filtros, muitas vezes essa aplicação mais restrita é feita sem a anuência ou sequer o conhecimento do detentor dos direitos autorais. Como ensina o Min. Barroso:

> Parece fora de dúvida que as redes sociais possam fazer prevalecer os seus Termos de Uso, evitando se tornarem vias de trânsito para conteúdo ilegal ou moralmente indesejável. (...) mas para que tal conduta seja legítima, não constituindo uma violação privada à liberdade de expressão, é imprescindível que seus critérios sejam públicos e transparentes, sem margem à arbitrariedade e à seletividade.[47]

O que se verifica na concretude é que existe uma liberdade garantida aos provedores de aplicação na moderação dos conteúdos gerados por terceiros em suas plataformas. E, dentro desta liberdade, a aplicação do critério legal estadunidense tende a ser a regra. Por exemplo, o instituto legal do "*fair use*", ou uso justo, presente em sistemas legais do *common law*, como os EUA, é próximo, porém não idêntico à "regra de três passos" da *civil law*, como no Brasil. Como ensinam os professores Marcos Wachowicz e Manoel J. Pereira dos Santos, a regra de três passos da Convenção de Berna foi recepcionada pelo direito brasileiro, especificamente no art. 46, VIII da lei nº 9.610/98 (Lei de Di-

---

rente: Google Brasil Internet LTDA. Recorrido: KF. Relatora: Min. Marco Aurélio Bellizze, 12 de setembro de 2017. Disponível em https://stj.jusbrasil.com.br/jurisprudencia/526809659/recursoespecial-resp-1642560-sp-2016-0242777-4/inteiro-teor-526809663. Acesso em 31 mar. 2023.

47. BARROSO, Luís Roberto. Da caverna à internet: evolução e desafios da liberdade de expressão. Revista Publicum, Rio de Janeiro, v. 6, n. 1, p. 1-12, 2020. Disponível em: https://www.e-publicacoes.uerj.br/index.php/publicum/article/view/57576. Acesso em: 12 jan. 2023. p. 10-11

reitos Autorais)[48]. A regra é uma exceção ao direito do autor, ditando critérios para julgar situações em que a liberdade de expressão do novo autor deve se sobrepor ao direito do autor de proteger sua obra. Continuando a explicação, Wachowicz e Santos explicam:

> A regra dos três passos basicamente consiste em dizer que: (i) a limitação cabe em certos casos especiais, (ii) desde que tal reprodução não prejudique a exploração normal da obra, e, (iii) nem cause um prejuízo injustificado aos legítimos interesses do autor.[49]

Já o sistema de Uso Justo, resumidamente, é um "teste de equilíbrio", baseado nas regras conforme o Art. 107 do *U.S. Copyright Act*[50]. Os Critérios são os seguintes: (i) A finalidade e a natureza do uso, incluindo se ele é de natureza comercial ou tem objetivos educativos que não visam o lucro; (ii) A natureza da obra protegida por direitos autorais; (iii) A quantidade e a importância da parcela usada em relação à obra protegida por direitos autorais como um todo; e (iv) O efeito do uso sobre um mercado em potencial ou sobre o valor da obra protegida por direitos autorais[51].

Pode se ver que a principal diferença é a consideração nos sistemas de uso justo da natureza do uso, especialmente se é de uso comercial ou educacional. Este tipo de critério não está presente na regra de três passos, mas está presente nas regras de uso justo. Porém, é aplicado de fato no Brasil pela maioria das plataformas. Está presente nos termos de uso do Instagram[52] e do Youtube[53], por exemplo. Dessa maneira, é aplicada uma interpretação mais restrita do direito autoral sem previsão legal, podendo colocar em xeque a liberdade de expressão dos criadores em sua plataforma.

Uma das maneiras em que isso se manifesta é em um possível *chilling ef-*

48. WACHOWICZ, Marcos; SANTOS, Manoel J. Pereira dos. ESTUDOS DE DIREITO DE AUTOR A Revisão da Lei de Direitos Autorais: Anais do III congresso de direito de autor e interesse público. p. 92. Florianópolis: Editora Boiteux, 2010.

49. Ibid.

50. CREWS, Kenneth D. Fair Use. Disponível em: https://copyright.columbia.edu/basics/fair-use.html. Acesso em: 12 jan. 2023.

51. Ibid.

52. INSTAGRAM. Termos e Políticas - Direitos autorais. Disponível em: https://www.facebook.com/help/instagram/126382350847838. Acesso em: 12 jan. 2023.

53. YOUTUBE. Uso aceitável no YouTube. 2021. Disponível em: https://support.google.com/youtube/answer/9783148?hl=pt-BR&ref_topic=2778546#zippy=. Acesso em: 12 jan. 2023.

fect, ou efeito silenciador da liberdade de expressão. Como definido por André Farah Alves:

> (...) é possível conceber o efeito silenciador como aquele no qual o indivíduo sente-se dissuadido, autocensurando-se, em razão de sentir medo de praticar uma conduta lícita, por conta de um ato estatal ou particular, que indireta ou diretamente, afeta-o com dano ou ameaça de dano à sua liberdade de expressão.[54]

Ou seja, são situações em que os interlocutores, prevendo sanção ou consequência injusta, decidem sequer exercer seu direito de liberdade de expressão, "esfriando" o mercado de ideias e empobrecendo o debate público. Considerando o que foi explicado até o momento, não é inconcebível que certos usuários, tendo tido experiências negativas com o sistema de gestão de direitos autorais na internet, decidam não mais criar conteúdo para a plataforma ou mudarem significativamente a natureza do seu trabalho com o propósito de evitar remoções.

Conforme exemplifica novamente Alves: "O provedor de serviços na Internet que, sempre que recebe notificações extrajudiciais, contemplando supostas difamações, provenientes de reclamação da classe política, derruba as postagens alvo do ataque, sem sombra de dúvida resfria o debate democrático"[55]. Não resfriaria também o provedor que faz o mesmo em relação a notificações extrajudiciais de direitos autorais ou, mais ainda, remoções automatizadas operadas por algoritmos?

Por esses motivos, existem processos[56] judiciais[57] no Brasil em que a própria utilização de filtros para controle de violações de direitos autorais é considerada censura prévia e manifestamente ilegal. Porém, inexiste decisão transitada em julgado que proíba em geral o uso de filtros tecnológicos, e as tecnologias continuam a ser usadas em território nacional.

---

54. ALVES, André Farah. Liberdade de expressão e remoção de conteúdo da Internet: anonimato, URL, árbitro e interação em portal de notícias. 2018. 245 f. p. 83. Dissertação (Mestrado) - Curso de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

55. Id. p. 79.

56. BRASIL. Tribunal de Justiça de São Paulo. Embargos de Declaração nº 1036141-31.2019.8.26.0100/50000. Embargante: Google Brasil Internet Ltda. Embargados: Intervozes Coletivo Brasil de Comunicação Social. Relator: JOSÉ CARLOS FERREIRA ALVES. São Paulo, SP, 14 de abril de 2021. ESAJ-TJSP. São Paulo.

57. BRASIL. Tribunal de Justiça de Santa Catarina. Apelação Cível nº 0000447-46.2016.8.24.0175. Apelante(s) Onerpm Comércio e Serviços de Mídia Digital Ltda e outro e Apelado(s) Daniel Candido dos Santos. Relator: Desembargador Saul Steil. Florianópolis, SC, 06 de fevereiro de 2018. ESAJ-TJSC. Florianópolis.

Considerações finais

Conforme apontado no artigo, inexiste proibição genérica para a utilização de filtros tecnológicos para a gestão de direitos autorais na legislação brasileira. Inexiste igualmente garantia de sua legalidade e não há, como exposto, obrigação para que os provedores de aplicações de internet disponibilizem ferramentas dessa natureza para os detentores de direitos autorais. Além disso, na falta de algum equivalente a algum "*safe harbor*" na legislação nacional, tanto detentores quanto provedores podem ser responsabilizados por eventuais excessos na moderação.

Na prática, estes filtros são duramente criticados, tanto por questões técnicas quanto sociais. São incontornáveis discussões sobre a precisão destas ferramentas, seu custo e a transparência em suas implementações. Porém os números são inevitáveis. Uma internet sem filtro seria efetivamente uma terra sem lei, o volume de dados desafia até a concepção da mente humana, quem dirá algum tipo de moderação manual. No caso específico dos direitos autorais, sem dúvidas a pirataria seria completamente incontrolável.

Urge então uma solução mediada, baseada em uma visão moderna e pluralista da liberdade de expressão, como a descrita pelo professor Jack M. Balkin em seu "triângulo da liberdade de expressão"[58]: levando em consideração os interesses e direitos tanto da sociedade civil, dos Estados-nações e dos entes privados (neste caso os provedores de aplicações de internet e os detentores de direitos autorais). São necessários desenhos novos e ousados de colaboração, e não o antagonismo do passado, para adequadamente servir a todos os interesses.

---

58. BALKIN, Jack M. FREE SPEECH IS A TRIANGLE. Columbia Law Review, New York, v. 118, n. 7, 2018. Disponível em: https://columbialawreview.org/content/free-speech-is-a-triangle/. Acesso em: 12 jan. 2023.

Referências

17 U.S. ***Code § 512 - Limitations On Liability Relating To material online***. Tradução livre. Disponível em: https://www.law.cornell.edu/uscode/text/17/512. Acesso em: 12 jan. 2023.

ALVES, André Farah. **Liberdade de expressão e remoção de conteúdo da Internet:anonimato, URL, árbitro e interação em portal de notícias**. 2018. 245 f. Dissertação (Mestrado) - Curso de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2018.

AMARAL, Jordana Siteneski do; BOFF, Salete Oro. **A FALIBILIDADE DO ALGORITMO CONTENT ID NA IDENTIFICAÇÃO DE VIOLAÇÕES DE DIREITO AUTORAL NOS VLOGS DO YOUTUBE: EMBATES SOBRE LIBERDADE DE EXPRESSÃO NA CULTURA PARTICIPATIVA**. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, p. 43-62, Jul/Dez. 2018. Disponível em: https://indexlaw.org/index.php/revistadipic/article/view/4679. Acesso em: 12 jan. 2023.

BALKIN, Jack M. **FREE SPEECH IS A TRIANGLE**. Columbia Law Review, New York, v. 118, n. 7, 2018. Disponível em: https://columbialawreview.org/content/free-speech-is-a-triangle/. Acesso em: 12 jan. 2023.

BARROSO, Luís Roberto. **Da caverna à internet: evolução e desafios da liberdade de expressão**. Revista Publicum, Rio de Janeiro, v. 6, n. 1, p. 1-12, 2020. Disponível em: https://www.e-publicacoes.uerj.br/index.php/publicum/article/view/57576. Acesso em: 12 jan. 2023.

BERKOWITZ, Adam. ***ClassicalMusicians v. Copyright Bots. Information Technology AndLibraries***, [S.L.], v. 41, n. 2, p. 1-9, 15 jun. 2022. p. 1-2. Boston CollegeUniversityLibraries. http://dx.doi.org/10.6017/ital.v41i2.14027.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 jan. 2023.

BRASIL. MINISTÉRIO DAS COMUNICAÇÕES. **90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa. 2022**. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em: 12 jan. 2023.

BRASIL. Supremo Tribunal Federal (Terceira Turma). **Recurso Especial nº 1.642.560 (2016/0242777-4)** - São Paulo. Civil e processual civil. Rede social. Responsabilidade civil do provedor de aplicação. Rede social. Facebook. [...]. Recorrente: Google Brasil Internet LTDA. Recorrido: KF. Relatora: Min. Marco Aurélio Bellizze, 12 de setembro de 2017. Disponível em https://stj.jusbrasil.com.br/jurisprudencia/526809659/recursoespecial-resp-1642560-sp-2016-0242777-4/inteiro-teor-526809663. Acesso em 31 mar. 2023.

BRASIL. Tribunal de Justiça de Santa Catarina. **Apelação Cível nº 0000447-46.2016.8.24.0175**. Apelante(s) Onerpm Comércio e Serviços de Mídia Digital Ltda e outro e Apelado(s) Daniel Candido dos Santos. Relator: Desembargador Saul Steil. Florianópolis, SC, 06 de fevereiro de 2018. ESAJ-TJSC. Florianópolis.

BRASIL. Tribunal de Justiça de São Paulo. **Embargos de Declaração nº 1036141-31.2019.8.26.0100/50000**. Embargante: Google Brasil Internet Ltda. Embargados: Intervozes Coletivo Brasil de Comunicação Social. Relator: JOSÉ CARLOS FERREIRA ALVES. São Paulo, SP, 14 de abril de 2021. ESAJ-TJSP. São Paulo.

CREWS, Kenneth D. ***Fair Use***. Disponível em: https://copyright.columbia.edu/basics/fair-use.html. Acesso em: 07 jan. 2022.

EMPLEMON. ***Copyright Smuggling*** | The YouTube Copyright Metagame pt. 2.Youtube, 21 nov. 2019. Disponível em: https://www.youtube.com/

watch?v=VvFGumd_esg&ab_channel=EmpLemon. Acesso em: Acessoem: 12 jan. 2023.

ENGSTROM, Evan; FEAMSTER, Nick. ***The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools***. Engine, março 2017. Disponível em: https://www.engine.is/the-limits-of-filtering. Acesso em: Acesso em: 12 jan. 2023.

GOMES, Maria Cecília Oliveira. **OS FILTROS TECNOLÓGICOS PODEM CONTRIBUIR PARA A PREVENÇÃO DAS VIOLAÇÕES DOS DIREITOS AUTORAIS NA INTERNET?** Revista da ABPI, n. 153, p. 57-71, Mar/Abr 2018. Disponível em: https://www.academia.edu/37209106/Os_filtros_tecnol%C3%B3gicos_podem_contribuir_para_a_preven%C3%A7%C3%A3o_das_viola%C3%A7%C3%B5es_dos_direitos_autorais_na_internet. Acesso em: 12 jan. 2023.

INSTAGRAM. **Termos e Políticas - Direitos autorais**. Disponível em: https://www.facebook.com/help/instagram/126382350847838. Acesso em: 12 jan. 2023.

MANARA, Cedric. ***Protecting what we love about the internet: our efforts to stop online piracy***. 2018. Disponível em: https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/. Acesso em: 12 jan. 2023.

OBSERVACOM. **Requerimento ao Ministério Público Federal do Brasil**. 2021. Disponível em: https://intervozes.org.br/content-id-do-google-censura-e-requer-controle-publico-afirma-observacom-ao-mpf/. Acesso em: 12 jan. 2023.

O'REILLY, Tim. ***WhatIs Web 2.0: design patterns and business models for the next generation of software***. Design Patterns And Business Models for the Next Generation of Software. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html. Acesso em: 12 jan. 2023.

PARRA, Flávia; BRANCO, Sérgio; PADRÃO, Vinícius. **Violações de direitos autorais de terceiros em plataformas de Internet no Brasil: uma análise a partir de decisões judiciais**. 2021. Disponível em: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/19466/1/%5bP%5d%5bW%5d%20Viola%c3%a7%c3%b5es%20de%20direitos%20autorais%20de%20terceiros%20em%20plataformas%20de%20internet%20no%20Brasil.pdf. Acesso em: 30 abr. 2023.

STATISA. ***Hours of video uploaded to YouTube every minute as of February 2020***. 2021. Disponível em: https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/. Acessoem: Acesso em: 12 jan. 2023.

TRENDACOSTA, Katharine. ***Unfiltered: How YouTube's Content ID Discourages Fair Use and Dictates What We See Online***. 2020. Disponível em: https://www.eff.org/pt-br/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online. Acesso em: 12 jan. 2023.

U.S. COPYRIGHT OFFICE (Estados Unidos). ***THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 U.S***. Copyright Office Summary. 1998. Disponível em: https://www.copyright.gov/legislation/dmca.pdf. Acesso em: 12 jan. 2023.

VON LOHMANN, Fred. ***YouTube's Content ID (C) ensorship Problem Illustrated***. 2010. Disponível em: https://www.eff.org/deeplinks/2010/03/youtubes-content-id-c-ensorship-problem. Acesso em: 12 jan. 2023.

WACHOWICZ, Marcos; SANTOS, Manoel J. Pereira dos. **ESTUDOS DE DIREITO DE AUTOR A Revisão da Lei de Direitos Autorais: Anais do III congresso de direito de autor e interesse público**. Florianópolis: Editora Boiteux, 2010. p. 73-105. Disponível em: https://www.gedai.com.br/wp-content/uploads/2014/07/LIVRO-ESTUDOS-SOBRE-DIREITO-DE-AUTOR-FINAL1.pdf. Acesso em: 12 jan. 2023.

WILLIAMS, Brett. ***YouTube hasanillegal TV streaming problem: you can binge your favorite show on youtube, if you look hard enough***. You can binge your favorite show on YouTube, if you look hard enough.. 2017. Disponível em: https://mashable.com/article/youtube-live-streaming-copyrights. Acesso em: 12 jan. 2023.

YOUTUBE. **Uso aceitável no YouTube**. 2021. Disponível em: https://support.google.com/youtube/answer/9783148?hl=pt-BR&ref_topic=2778546#zippy=. Acesso em: 12 jan. 2023.

_____. **Termos de Serviço**. 2021. Disponível em: https://www.youtube.com/static?gl=BR&template=terms&hl=pt. Acesso em: 12 jan. 2023.

ZHANG, Daniel Yue; LI, Qi; TONG, Herman; BADILLA, Jose; ZHANG, Yang; WANG, Dong. ***Crowdsourcing-Based Copyright Infringement Detection in Live Video Streams***. 2018 Ieee/AcmInternationalConferenceOnAdvances In Social Networks AnalysisAnd Mining (Asonam), [S.L.], p. 367-374, ago. 2018. IEEE. http://dx.doi.org/10.1109/asonam.2018.8508523.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

17

Inteligência Artificial e Direitos Autorais

JEANNINE DE SOUZA HAGNAUER

Introdução

Em um passado distante, já se considerou a existência de robôs no cotidiano como sendo "coisa de cinema", mas atualmente este fato está cada vez mais presente no convívio em sociedade, muitas vezes sem sequer nos darmos conta de sua presença. Assim como entendeu Federico Pistono:

> (...) a revolução propiciada pela IA provocará mudanças nas estruturas sociais e de poder, bem como que será a grande chance que a humanidade terá de repactuar o convívio em sociedade, tornando efetivo o termo colaboração, mudando também sua relação com o próprio Estado.[2]

Desse modo, é evidente que "não há como o Direito ficar alheio às transformações"[3], devendo inclusive norteá-las quando necessário.

Especificamente na esfera dos Direitos Autorais, o uso da Inteligência Artificial no desenvolvimento de obras vem fomentando inúmeros debates, em virtude de esta vir sendo cada vez mais utilizada e, na medida que melhorias estão sendo implementadas, podem até vir a substituir o ser humano.

Na realidade, a Inteligência Artificial (IA) já vem sendo utilizada na criação de obras desde 1970, com estruturas criativas e originais e, a cada ano, as técnicas estão sendo aprimoradas[4].

---

1. Advogada. Graduada pela Universidade Federal do Rio de Janeiro. Pós-graduada em Propriedade Intelectual pela Pontifícia Universidade Católica do Rio de Janeiro e especialista em Direito do Entretenimento pela Universidade do Estado do Rio de Janeiro. Pós-graduada em Direito Digital pelo ITS Rio (Instituto de Tecnologia e Sociedade do Rio) em parceria com o CEPED/UERJ (Universidade do Estado do Rio de Janeiro).

2. PISTONO, Federico. Os robôs vão roubar o seu trabalho, mas tudo bem. Tradução de Pedro Soares. São Paulo. Portfolio Pinguin, 2017 apud CANTALI, F. B. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

3. HOHENDORFF, Raquel Von ; CANTALI, Fernanda Borghetti ; D'ÁVILA, Fernanda Felitti da S. Inteligência artificial e direitos autorais: desafios e possibilidades no cenário jurídico brasileiro e internacional, PragMATIZES – Revista Latino-Americana de Estudos em Cultura, Niterói/RJ, Ano 10, n. 19, set. 2020. Disponível em https://doi.org/10.22409/pragmatizes.v10i19.41210. Acesso em: 4 mai. 2023.

4. CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez.

Tem-se como recentíssimo exemplo a canção "*Heart on my sleeve*" disponibilizada inicialmente na plataforma *TikTok* e após difundida em todos os tocadores de música online. A referida obra foi produzida por um indivíduo que se intitulou *Ghostwrite*r e utilizou IA para emular a voz dos rappers Drake e The Weekend[5].

Ainda, é importante mencionar a ferramenta mais comentada do momento: o Chat GPT. Trata-se de uma assistente virtual que funciona por meio de IA. É capaz de elaborar textos, artigos informativos, redações informais, receitas de bolo, dentre outros e já conquistou mais de 100 milhões de usuários em todo o mundo[6].

A polêmica envolvendo a referida aplicação se dá justamente porque, considerando que esta IA é alimentada por uma série de dados e obras de autoria de terceiros, deveriam as suas produções ter proteção autoral? Ou melhor, como se daria a proteção autoral nesses casos?

Nesse sentido, as discussões são das mais variadas e versam principalmente sobre: a tutela destes direitos, a titularidade das obras desenvolvidas por ou com o uso de IA e todos os seus reflexos, como o proveito econômico destas, a responsabilização em caso de violação de obras de outros, responsabilização civil e o interesse público na exploração destas obras.

Assim, inicialmente, no presente trabalho será feita uma breve exposição sobre conceitos básicos dentro dos Direitos Autorais e após a exposição dos diferentes posicionamentos doutrinários que discutem a tutela dos direitos autorais no âmbito das obras produzidas por e com IA.

1. Direitos Autorais

Os Direitos Autorais são parte importante da propriedade Intelectual e são fruto de uma vertente tecnológica, que em razão do surgimento de máquinas facilitou a reprodução em escala de obras intelectuais e a ideológica e atingiu

---

2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

5. Inteligência Artificial coloca voz de Drake em música que ele nunca cantou. Disponível em: https://www.portalt5.com.br/noticias/single/nid/inteligencia-artificial-coloca-voz-de-drake-em-musica-que-ele-nunca-cantou/. Acesso em: 04 Mai. 2023.

6. NEVES, Ricardo. O que faremos com o ChatGPT? Disponível em: https://www.updateordie.com/2023/02/27/o-que-faremos-com-o-chatgpt/. Acesso em: 12 mai 2023.

maior força com a globalização[7].

No Brasil, sua principal regulação é encontrada na Lei nº 9.610/98 e internacionalmente nas Convenções Internacionais de Berna e Viena. A doutrina pátria os define como sendo o conjunto de prerrogativas morais e patrimoniais pertencentes ao autor de uma obra literária, artística ou científica, por exemplo.[8] As prerrogativas morais seriam aquelas que pertencem exclusivamente ao autor da obra, assumindo um caráter personalíssimo, e as patrimoniais as prerrogativas que podem ser exploradas economicamente.

Nas palavras do doutrinador Carlos Alberto Bittar: "(...) o Direito Autoral é o ramo do Direito Privado que regula as relações jurídicas, advindas da criação e da utilização econômica de obras intelectuais estéticas e compreendidas na literatura, nas artes e na ciência."[9]

Os Direitos Autorais passaram a ser tutelados internacionalmente com a criação da Convenção da União de Berna – CUB em 1866, que tinha como principal intuito a proteção de obras literárias e artísticas[10]. Contudo, já existiam diversas criações provenientes do intelecto humano, de acordo com registros de obras de artistas que se tem conhecimento que datam de 650 a.C.

Entretanto, foi a invenção da imprensa por Johannes Gutenberg em meados de 1450 que revolucionou o Direito Autoral. A partir desta invenção foi possível difundir conhecimento de uma forma mais ampla, o que contribuiu significativamente com o avanço no campo das ciências e das artes.[11]

Além da referida mudança no comportamento da sociedade, pelo fato de anteriormente a essa invenção a leitura ser um momento coletivo pela dificuldade de locomoção e leitura dos manuscritos e outras obras, esta também contribuiu com o surgimento da percepção de privacidade pessoal. Isso porque, a leitura passou a ser um momento individual.[12] Segundo Guilherme Car-

---

7. ABRAAO, Eliane. Y. Direitos de Autor e Direitos Conexos, São Paulo: Editora Brasil, 2002. 15 p.

8. ABRAAO, Eliane Y. Direitos de Autor e Direitos Conexos. São Paulo: Editora Brasil, 2002. 16 p.

9. BITTAR, Carlos Alberto. Direito de Autor. São Paulo: Forense Universitária. 8 p.

10. ZANINI. Leonardo Estevam de Assis. Direito de autor em perspectiva histórica: da idade média ao reconhecimento dos direitos da personalidade do autor. 224 p. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/532-2425-1-pb.pdf. Acesso em: 04 dez. 2022.

11. LEIRA, Thales Boechat Nunes. Os desdobramentos do Direito Autoral na Era Digital. Disponível em: https://www.gedai.com.br/wp-content/uploads/2019/05/023-OS-DESDOBRAMENTOS-DO-DIREITO.pdf. Acesso em: 04 de dez. 2022.

12. Ibid. Acesso em: 04 dez. 2022.

boni, passou também a ser individualizada, imutável em seu conteúdo e passou a ser possível identificar o autor.[13]

Contudo, mesmo com tantas mudanças proporcionadas pela invenção, os autores ainda não eram valorizados pelo seu trabalho como deveriam e os editores eram quem dominavam o mercado. Assim, diante da ausência de regras claras sobre o tema, a Rainha Ana promulgou o Copyright Act. em 1710, que viria a ser a primeira lei sobre Direito Autoral.[14]

A professora americana Martha Woodmansee entendia que no período do Renascimento e no Neoclássico, o autor era sempre compreendido como um veículo ou um instrumento, pois na primeira interpretação, como um artesão, ele manipulava estratégias predefinidas visando atingir objetivos ditados por seu público e na segunda, o escritor seria um instrumento de uma força externa ou divina[15].

A partir desses dois conceitos, teóricos do séc. XVIII criaram um novo no qual o elemento inspiração foi enaltecido, não sendo ele mais proveniente de elementos externos ou poder superior, mas sim diretamente do autor. A obra passou a ser compreendida como produto único e exclusivo do autor, que passou a ser visto segundo Woodmansee como o "*original genius*" ou o gênio original[16].

Como será melhor abordado adiante, o conceito do "gênio original" e a individualidade do autor, bem como outros conceitos outrora sedimentados, vêm sendo relativizados em virtude de toda conectividade e interação da sociedade atual.

Nessa mesma esteira, o filósofo Johann Gottlieb Fichte concluiu que o livro seria dividido entre os aspectos físicos e intelectuais, visto que a obra funcionaria como uma espécie de emanação verbal do autor. Esse segundo aspecto, por sua vez, poderia ser dividido em dois segmentos, um seria o conteúdo e o

13. CARBONI, Guilherme. Direito Autoral e Autoria Colaborativa na Economia da Informação em Rede. São Paulo: Quartier Latin, 2010.

14. CARBONI, Guilherme. Direito Autoral e Autoria Colaborativa na Economia da Informação em Rede. São Paulo: Quartier Latin, 2010.

15. WOODMANSEE, Martha. The genius and the copyright: economic and legal conditions of the emergence of the "author". EighteenthCentury Studies, v. 17, Issue 4, Summer, 1984. 427 p.

16. LEIRA, Thales Boechat Nunes. Os desdobramentos do Direito Autoral na Era Digital. Disponível em: https://www.gedai.com.br/wp-content/uploads/2019/05/023-OS-DESDOBRAMENTOS-DO-DIREITO.pdf. Acesso em: 04 dez. 2022.

outro, a forma como são exteriorizadas. [17]

Assim, segundo Fichte a forma seria sempre propriedade do autor, enquanto o conteúdo e ideias ali dispostos seriam propriedade conjunta entre o leitor e o autor.

O referido conceito é de suma importância na história do Direito Autoral, visto que balizou a lei sobre o tema, bem como orienta entendimentos doutrinários e jurisprudenciais até os dias atuais.

Nesse mesmo sentido, de que no século XX a obra dependia do suporte, é o entendimento de Sérgio Branco. Contudo, a partir do século XXI, com a influência da Internet e das inúmeras plataformas de distribuição de vídeos, músicas e imagens tal elemento foi dispensado. Ainda, a facilidade de transmissão de arquivos e modificação por qualquer usuário da rede mundial de computadores exigiu a reconfiguração do regramento sobre Direitos Autorais muito antes do advento da IA[18].

Contudo, o direito autoral não visa somente proteger o autor e sua obra, nas palavras de José Carlos Costa Netto:

> (...) o direito de propriedade evolui à medida que possa ser exercido não somente para conceder segurança e conforto ao seu titular e ao fechado círculo de seus parentes, amigos e protegidos, mas, sim, que seja exercido em condições tais que, além de possibilitar a justa recompensa individual, exerça uma função construtiva na melhoria das condições de vida do conjunto social.

Assim, ressalta-se que a proteção conferida pelo Direito Autoral não deve ser tutelada apenas para resguardar os interesses do autor, mas também para promover o interesse social e desenvolvimento da cultura. Contudo, esta deve se moldar e conviver com os demais regramentos observando sempre os ditames da Constituição Federal.

Nesse mesmo sentido, os juristas Diego Brainer de Souza e Cássio Monteiro Rodrigues, abordaram o tema da seguinte forma:

> A hermenêutica civil-constitucional deve atuar sempre no senti-

17. Ibid.

18. CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 05 mai. 2023.

> do de identificar a rigidez ou incompatibilidade de uma disposição normativa de direito autoral que, analisada in concreto, limite excessivamente ou não promova a disseminação da cultura ou informação, para, então, flexibilizar a tutela excludente autoral e garantir o acesso à obra aos demais interessados.[19]

No Brasil, os Direitos Autorais constam na Constituição Federal desde a primeira edição e podem ser encontrados em dois incisos do art. 5º[20]. No inciso XXVII estão previstos os direitos do autor de utilizar, publicar e reproduzir suas obras, sendo esses transmissíveis aos seus herdeiros pelo tempo previsto em lei. [21] Neste dispositivo definem-se os direitos patrimoniais do autor.

No referido inciso, o legislador fala em "direito exclusivo", este segundo termo empregado refere-se justamente à noção de patrimônio ou de propriedade[22].

Por sua vez, no inc. XXVIII do mesmo artigo da Carta Magna estão resguardados os direitos de participação individual em obras coletivas, de reprodução da imagem e voz humana, de fiscalização do aproveitamento econômico de obras que criaram ou participaram os criadores, os intérpretes e as suas representações sindicais e associativas[23].

Os direitos morais estão tutelados também em outros dispositivos da Constituição, como nos gerais de tutela da expressão, como o IX e o X[24] e em tratados internacionais, como será abordado mais à frente.

Assim, os itens a seguir abordarão os dois grupos que se dividem os Direitos Autorais são divididos em dois grupos: os morais e os patrimoniais.

1.1 Direitos Morais

19. SOUZA, Diego Brainer de; RODRIGUES, Cássio Monteiro. Memes e direito autoral: da superação da lógica proprietária à tutela do elemento cultural apud SCHREIBER, Anderson; Terra de Moraes, Bruno; Spadaccini de Teffé, Chiara. (Org.). Direito e Mídia: tecnologia e liberdade de expressão. 1 ed. São Paulo: Editora Foco.

20. BARBOSA, Denis Borges. Uma introdução à propriedade intelectual. Segunda Edição Revista e Atualizada. 88 p. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 04 dez. 2022.

21. BRASIL. Constituição Federal. Art. 5º, inc. XXVII

22. BARBOSA, Denis Borges. Uma introdução à propriedade intelectual. Segunda Edição Revista e Atualizada. 126 p. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 04 dez. 2022.

23. BRASIL. Constituição Federal. Art. 5º, inc. XXVIII

24. "Art. 5º(...)IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;(...)" BRASIL. Constituição Federal.

Os Direitos Morais estão dispostos na lei de Direitos Autorais ("LDA" - Lei 9.610/98) nos artigos 24 a 27[25]. São eles: o direito de paternidade, o direito de inédito, direito à integridade da obra, direito de modificar a obra, direito de retirar a obra de circulação e direito de o autor ter acesso a exemplar único e raro de obra sua.

Quando se fala em paternidade significa que estes direitos têm o condão de possibilitar aos autores a reivindicar a proteção deste em favor de seus legítimos interesses de ordem não patrimonial[26].

> Ainda, importa comentar que existem discussões entre os doutrinadores sobre se os direitos morais seriam um direito de personalidade. Contudo, como afirmou o jurista Adriano de Cupis:
> [o] direito moral de autor, (...), não é um direito inato. De fato, só surge em seguida a um ato de criação intelectual. Quer dizer, não corresponde a todo aquele que seja munido de personalidade, mas àquele que, além de ter personalidade, se qualifique ulteriormente como 'auto'[27]
> Ademais, cumpre esclarecer que os demais direitos que compõem os direitos de personalidade, tal qual a imagem, privacidade, honra, nome, etc. são elementos indissociáveis de seu titular, enquanto os direitos morais dependem que a obra seja externalizada para

---

25. Lei de Direitos Autorais, n.°9.610/98. "Art. 24. São direitos morais do autor:
I - o de reivindicar, a qualquer tempo, a autoria da obra;
II - o de ter seu nome, pseudônimo ou sinal convencional indicado ou anunciado, como sendo o do autor, na utilização de sua obra;
III - o de conservar a obra inédita;
IV - o de assegurar a integridade da obra, opondo-se a quaisquer modificações ou à prática de atos que, de qualquer forma, possam prejudicá-la ou atingi-lo, como autor, em sua reputação ou honra;
V - o de modificar a obra, antes ou depois de utilizada;
VI - o de retirar de circulação a obra ou de suspender qualquer forma de utilização já autorizada, quando a circulação ou utilização implicarem afronta à sua reputação e imagem;
VII - o de ter acesso a exemplar único e raro da obra, quando se encontre legitimamente em poder de outrem, para o fim de, por meio de processo fotográfico ou assemelhado, ou audiovisual, preservar sua memória, de forma que cause o menor inconveniente possível a seu detentor, que, em todo caso, será indenizado de qualquer dano ou prejuízo que lhe seja causado.
§ 1º Por morte do autor, transmitem-se a seus sucessores os direitos a que se referem os incisos I a IV.
§ 2º Compete ao Estado a defesa da integridade e autoria da obra caída em domínio público.
§ 3º Nos casos dos incisos V e VI, ressalvam-se as prévias indenizações a terceiros, quando couberem.
Art. 25. Cabe exclusivamente ao diretor o exercício dos direitos morais sobre a obra audiovisual.
Art. 26. O autor poderá repudiar a autoria de projeto arquitetônico alterado sem o seu consentimento durante a execução ou após a conclusão da construção.
Parágrafo único. O proprietário da construção responde pelos danos que causar ao autor sempre que, após o repúdio, der como sendo daquele a autoria do projeto repudiado.
Art. 27. Os direitos morais do autor são inalienáveis e irrenunciáveis."

26. MENEZES, Elisângela Dias. Curso de Direito Autoral. Belo Horizonte: Del Rey, 2007. 67 p.

27. CUPIS, Adriano de. Os Direitos da Personalidade. cit., p. 337 apud BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em: 17 dez. 2022.

que seja considerada sua existência. [28]
Além disso, cumpre ressaltar que os direitos morais também se encontram previstos no artigo 6 bis da Convenção de Berna (CUB).[29]

1.2 Direitos Patrimoniais

Os Direitos patrimoniais são aqueles que garantem ao titular aproveitar economicamente a obra protegida e suas hipóteses encontram-se na lista exemplificativa apresentada no art. 29 da LDA. [30]

Os direitos patrimoniais, de acordo com a legislação, apresentam um prazo para sua proteção de 70 anos a contar de 1º de janeiro do ano subsequente ao falecimento do autor[31]. Após esse período, a obra cai em domínio público e

28. BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em 17 dez. 2022.

29. CUB: "Artigo 6 bis. 1) Independentemente dos direitos patrimoniais de autor, e mesmo depois da cessão dos citados direitos, o autor conserva o direito de reivindicar a paternidade da obra e de se opor a toda deformação, mutilação ou a qualquer dano à mesma obra, prejudiciais à sua honra ou à sua reputação. 2) Os direitos reconhecidos ao autor por força do parágrafo 1) antecedente mantêm se, depois de sua morte, pelo menos até à extinção dos direitos patrimoniais e são exercidos pelas pessoas físicas ou jurídicas a que a citada legislação reconhece qualidade para isso. Entretanto, os países cuja legislação, em vigor no momento da ratificação do presente Ato ou da adesão a ele, não contenha disposições assegurando a proteção depois da morte do autor, de todos os direitos reconhecidos por força do parágrafo 1) acima, reservam-se a faculdade de estipular que alguns desses direitos não serão mantidos depois da morte do autor. 3) Os meios processuais destinados a salvaguardar os direitos reconhecidos no presente artigo regulam-se pela legislação do país onde é reclamada a proteção."

30. Lei de Direitos Autorais, n.°9.610/98. "Art. 29. Depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, tais como:
I - a reprodução parcial ou integral;
II - a edição;
III - a adaptação, o arranjo musical e quaisquer outras transformações;
IV - a tradução para qualquer idioma;
V - a inclusão em fonograma ou produção audiovisual;
VI - a distribuição, quando não intrínseca ao contrato firmado pelo autor com terceiros para uso ou exploração da obra;
VII - a distribuição para oferta de obras ou produções mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para percebê-la em um tempo e lugar previamente determinados por quem formula a demanda, e nos casos em que o acesso às obras ou produções se faça por qualquer sistema que importe em pagamento pelo usuário;
VIII - a utilização, direta ou indireta, da obra literária, artística ou científica, mediante:
a) representação, recitação ou declamação;
b) execução musical;
c) emprego de alto-falante ou de sistemas análogos;
d) radiodifusão sonora ou televisiva;
e) captação de transmissão de radiodifusão em locais de frequência coletiva;
f) sonorização ambiental;
g) a exibição audiovisual, cinematográfica ou por processo assemelhado;
h) emprego de satélites artificiais;
i) emprego de sistemas óticos, fios telefônicos ou não, cabos de qualquer tipo e meios de comunicação similares que venham a ser adotados;
j) exposição de obras de artes plásticas e figurativas;
IX - a inclusão em base de dados, o armazenamento em computador, a microfilmagem e as demais formas de arquivamento do gênero;
X - quaisquer outras modalidades de utilização existentes ou que venham a ser inventadas.

31. Lei de Direitos Autorais, n.°9.610/98. "Art. 41. Os direitos patrimoniais do autor perduram por setenta anos contados de 1° de janeiro do ano subseqüente ao de seu falecimento, obedecida a ordem sucessória da lei civil.
Parágrafo único. Aplica-se às obras póstumas o prazo de proteção a que alude o caput deste artigo."

persistem apenas os direitos morais.

Importa esclarecer que a lei prevê limitações aos Direitos Autorais, os quais se encontram a partir do art. 46 do respectivo regramento. Essas tratam de hipóteses especiais, tais como o uso de pequenos trechos ou a realização de cópias de algumas páginas para estudo, por exemplo.

José Ascenção entendia que os Direitos Autorais poderiam ser classificados dentro dos direitos de exclusivo. Essa crença difere da de diversos doutrinadores, que enquadravam os direitos patrimoniais como sendo direito de propriedade[32]. Tal questão ainda não é pacífica e merece um breve esclarecimento, pois contribui com o tema central deste trabalho. O ponto polêmico entre os doutrinadores é a distinção sobre a propriedade material e imaterial. Alguns entendem que é proprietário de um livro, aquele que o adquiriu, outros defendem, assim como Ascensão que:

> [p]or natureza, a obra literária ou artística não é susceptível de apropriação exclusiva, não podendo, portanto, originar uma propriedade. Uma vez divulgada, a obra literária ou artística comunica-se a todos os que dela participarem. Não pode estar submetida ao domínio exclusivo de um só [33]

Ascensão ao inserir os Direitos Autorais na categoria de direitos de exclusivo, esclarece a natureza dos direitos morais do autor afastando dos direitos de personalidade, visto que os primeiros não são inatos, enquanto os segundos são atributos da pessoa e supostamente ligariam a obra ao autor. Contudo, os doutrinadores que defendem esse argumento se esquecem das obras publicadas por ghostwriter, por exemplo.[34]

2. O que é Inteligência Artificial (“IA”)?

Definir Inteligência Artificial não é das mais fáceis tarefas. Isso porque, desde o primeiro trabalho sobre o tema, este foi muito explorado e, portanto, já existem diversas definições para o termo.

---

32. BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com.Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. P.20. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em 17 dez. 2022.

33. ASCENSÃO, José de Oliveira. Direito Autoral. cit.; 604p. apud BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com.Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. P.20. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em: 17 dez. 2022.

34. Ibid.

Tal expressão pode remeter a robôs e humanoides, como já foi apresentado em dezenas de filmes de ficção científica, mas a IA não se limita a isso. Como se verá ao longo desse estudo, esta pode ser encontrada em mecanismos de Internet e até mesmo em objetos domésticos.

O primeiro estudioso a pensar essa tecnologia foi Alan Turing, em 1950 em seu artigo "*Computing Machinery and Inteligency*". Neste importante documento, que serve até hoje como base para trabalhos que vieram na sequência, Turing buscou entender se eventualmente no futuro as máquinas poderiam pensar como os seres humanos.[35]

Luckas Ruthes Gonçalves compreende a Inteligência Artificial como "a área de estudo focada em desenvolver aplicações que possam emular a capacidade de raciocínio humano para resolver diversos problemas."[36]

Já o cientista da computação John McCarthy cunhou a IA como sendo "a ciência e engenharia de produzir máquinas inteligentes"[37].

A Resolução Europeia 2021/C 404/05 de 20/10/2020[38] define o sistema de IA como segue:

> um sistema baseado em software ou integrado em dispositivos físicos e que apresenta um comportamento que simula inteligência, nomeadamente recolhendo e tratando dados, analisando e interpretando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos;(...)

No entendimento dos doutrinadores Zaffari e Espindola:

> uma parte da ciência da computação que tem como foco o desen-

35. VON HOHENDORFF, Raquel; CANTALI, F. B.; D'AVILA, F. F. da S.. "Inteligência Artificial e Direitos Autorais: Desafios e Possibilidades no Cenário Jurídico Brasileiro e Internacional". 254 p. Disponível em: https://periodicos.uff.br/pragmatizes/article/view/41210/24697. Acesso em 18 dez. 2022.

36. GONÇALVES, Lukas Ruthes. A tutela jurídica de trabalhos criativos feitos por aplicações de inteligência artificial no Brasil. Dissertação apresentada ao Programa de Pós-Graduação em Direito, Faculdade de Direito, Setor de Ciências Jurídicas, da Universidade Federal do Paraná como requisito parcial para obtenção do título de Mestre em Direito. Orientador: Prof. Dr. Marcos Wachowicz. Curitiba. 2019. Disponível em: https://www.gedai.com.br/wpcontent/uploads/2019/10/DISSERTA%C3%87%C3%83O-Lukas-Ruthes_Direitoe-Inteligencia-Artificial.pdf. Acesso em: 18 dez. 2022.

37. RAJARAMAN, V. John McCarthy – Father of Artificial Intelligence. Asia Pacific Mathematics Newsletter. Jul. 2014, v. 4, nº 3, p. 15-20. Disponível em: http://www.asiapacific-mathnews.com/04/0403/0015_0020.pdf, apud CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 05 mai. 2023.

38. Resolução do Parlamento Europeu, de 20 de outubro de 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020IP0276&from=PT. Acesso em: 24 abr. 2023.

> volvimento de máquinas ou sistemas que possam resolver problemas que requerem inteligência humana. Inteligência Artificial combina os conhecimentos de ciência da computação, física e filosofia. A ideia geral que permeia a inteligência artificial é a de se criar uma máquina artificialmente pela incorporação de programas e equipamentos que fossem capazes de tomar decisões à sua própria maneira quando deparados com problemas de um domínio particular para o qual o sistema foi feito(...).[39]

Em resumo, a IA busca se igualar à capacidade do cérebro humano, não sendo necessariamente de um corpo físico igual ao de um humano, bastando um computador como suporte. É importante destacar que, apesar de toda capacidade intelectual, tal tecnologia não dispõe – ainda - de consciência.[40]

Assim, a velocidade que algumas máquinas dotadas de IA desempenham determinadas funções representa um grande ganho de produtividade, sem haver a substituição de humanos, dado que estas não dispõem de consciência.

Nesse sentido, importa mencionar outra definição relevante sobre o tema, que é a divisão entre as IA Fraca e IA Forte. Segundo Sergio García:

> (...)IA fraca seria a ciência que permitiria o projeto e a programação de computadores capazes de realizar tarefas de forma inteligente, enquanto a IA forte seria a ciência que permitiria a replicação da inteligência humana em máquinas. Em outras palavras, IA fraca permitiria o desenvolvimento sistemas com inteligência especializada - computadores que jogam xadrez, diagnosticam doenças ou resolver teoremas matemáticos - enquanto uma IA forte permitiria desenvolver computadores e máquinas dotadas de inteligência geral.[41]

Em outros termos, a fraca seria aquela que vemos nos dias atuais, com as quais as tecnologias desempenham atividades facilmente desempenhadas por humanos, porém de forma mais ágil e com aplicação comercial. A forte,

---

39. ZAFFARI, Felipe Pozueco; ESPÍNDOLA, Jean Carlo de Borba. “Conceitos o que é inteligência artificial” apud BARONE, Dante Augusto; Couto; BOESING, Ivan Jorge (org.). Inteligência artificial: diálogos entre mentes e máquinas. Porto Alegre: AGE/Evangraf, 2015.

40. HOHENDORFF, Raquel Von; CANTALI, Fernanda Borghetti; D’ÁVILA, Fernanda Felitti da S., Inteligência artificial e direitos autorais: desafios e possibilidades no cenário jurídico brasileiro e internacional. PragMATIZES – Revista Latino-Americana de Estudos em Cultura, Niterói/RJ. Ano 10, n.19, p.255, set. 2020.

41. GARCÍA, Sergio Marín. Ética e inteligência artificial. 19 p. Disponível em: https://dx.doi.org/10.15581/018.ST-522. Acesso em: 08 mai. 2023. Tradução livre.

que atualmente suscita inúmeros debates, se assemelha a inteligência humana ou até uma superinteligência, seria baseada em tecnologias que ainda não existem e poderiam vir até a substituir um ser humano.[42]

Embora ainda não haja conceito definido de forma exata sobre IA, das definições anteriormente trazidas se extrai resumidamente que consiste na capacidade, de forma artificial, de capacitar um objeto a realizar atividades normalmente desempenhadas por seres humanos, através de uma inteligência que simula o cérebro humano.

Assim, dessa premissa se parte para, na sequência, analisar a relação entre as obras desenvolvidas por essa tecnologia e os direitos autorais relacionados.

3. A Titularidade dos Direitos Autorais Patrimoniais de obras criadas por IA

Quando Turing, em seu artigo "*Computing Machinery and Intelligence*" publicado em 1950, buscou respostas para entender se algum dia as máquinas seriam capazes de pensar, ele propôs um jogo da imitação. O teste verificaria se a máquina conseguiria responder as perguntas tal qual um ser humano e estas passariam no teste se alcançassem quatro requisitos: utilização da linguagem natural, permitindo a comunicação em inglês; conhecimento para armazenar o que já sabe e ouve; raciocínio automatizado e *machine learning*.[43]

Trinta anos após a divulgação do Teste de Turing ("TT"), em 1980, um dos principais críticos da IA forte, o filósofo John Searle, publicou um estudo no qual defende que uma máquina é capaz de compreender genuinamente as informações que lhe foram transmitidas e não somente imitar o comportamento humano. Para elaborar este artigo, o estudioso realizou um teste o qual o objetivo era demonstrar que mesmo sem compreender o que está escrito, a máquina conseguiria responder corretamente. Seu objetivo era demonstrar que não é necessária consciência para que haja inteligência.[44]

---

42. SCHIRRU, Luca. A inteligência artificial e o Big Data no setor da saúde. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/6748173.pdf>. Acesso em 18 de Dez. 2022.

43. RUSSEL, Stuart; NORVIG, Peter. Artificial Intelligence: A Modern Approach. New Jersey: Prentice Hall, 2009 (3º Ed. apud Inteligência Artificial: questões éticas a serem enfrentadas. KAUFMAN, Dora. Disponível em:https://abciber.org.br/anaiseletronicos/wpcontent/uploads/2016/trabalhos/inteligencia_artificial_questoes_eticas_a_serem_enfrentadas_dora_kaufman.pdf. Acesso em: 19 de Dez. 2022.

44. FILHO, Maxwell Morais de Lima. O Experimento de Pensamento do Quarto Chinês: a Crítica de John Searle à Inteligência Artificial Forte Argumentos, Ano 2, N°. 3 – 2010. Disponível em https://repositorio.ufc.br/bitstream/riufc/3566/1/2010_

Nessa esteira, e adentrando o tema do presente tópico deste trabalho, o ordenamento jurídico é claro ao dispor no artigo 11 da LDA que o "autor é a pessoa física criadora da obra literária, artística ou científica". Ressalta-se da referida disposição, o critério de que necessariamente o autor deve ser uma pessoa física. E, no que tange a esse último ponto em relação ao uso de IA, a doutrina dominante se posiciona contra a possibilidade de se considerar como autor um agente não-humano.[45]

Outro pré-requisito que merece ser destacado é o apresentado no caput do art. 7º da mesma lei – que dispõe que "são obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, (...)" - as "criações de espírito". Em outros termos, tal expressão estabelece que não basta apenas que a obra seja concebida por alguém dotado de inteligência, mas essa deveria ser uma "criação de espírito" do mesmo - segundo a doutrina, não no sentido metafísico ou espiritual, mas significando "intuito".

Ainda, cumpre definir o conceito de "domínio publico". Utilizando as palavras de Eliane Abraão: "Pertencem, originariamente, ao domínio público as peças ou obras de autor desconhecido, incluindo as folclóricas, ressalvadas quanto a estas (inciso III do art. 45) a proteção legal aos conhecimentos étnicos e tradicionais."[46]

Além dessas hipóteses, o art. 45 da LDA dispõe que a obra estaria em domínio público quando o seu autor faleceu sem deixar sucessores e quando estiver expirado o prazo de proteção garantido pela legislação autoral, conforme constante no art. 41 da LDA.

Cumpre elucidar, que a entrada em domínio público de uma obra viabiliza, conforme apresentado no art. 14 da LDA[47], que esta seja traduzida, adaptada, arranjada ou orquestrada. Alerta-se que, ainda diante destas possibilidades, devem ser respeitados os direitos morais, o que também não obsta a liberdade de utilização por qualquer interessado. Nas palavras de Denis Barbosa: "O real

---

Art_MMLFilho.pdf. Acesso em: 29 dez. 2022.

45. SCHIRRU, Luca. A inteligência artificial e o direito autoral: o domínio publico em perspectiva. Disponível em: https://its-rio.org/wp-content/uploads/2019/04/Luca-Schirru-rev2-1.pdf. Acesso em: 09 jan. 2023.

46. ABRAAO, Eliane Y. Direitos de Autor e Direitos Conexos, São Paulo, Editora Brasil: 2002.

47. Lei de Direitos Autorais, n.°9.610/98. "Art. 14. É titular de direitos de autor quem adapta, traduz, arranja ou orquestra obra caída no domínio público, não podendo opor-se a outra adaptação, arranjo, orquestração ou tradução, salvo se for cópia da sua."

efeito do domínio público é a liberdade de utilização da obra intelectual pelo término da exclusividade legal, de maneira que o exercício do direito pessoal jamais poderia obstaculizar esse efeito." [48]

Dessa forma, dentre os questionamentos que surgem sobre o tema e principalmente sobre a titularidade da obra, indaga-se se seria possível concluir que assim que criadas as obras desenvolvidas por inteligência artificial pertenceriam ao domínio público. No mesmo sentido, existem muitas dúvidas sobre a possibilidade de se considerar um sistema de IA como autor, ou até mesmo titular de direitos exclusivos, visto que envolvem discussões não só dentro da esfera do direito autoral, como também sobre direito de personalidade.

Esse último debate passa pela possibilidade de atribuir a esses sistemas, algum tipo de personalidade, seja os comparando a pessoas físicas, jurídicas ou até mesmo com a criação de uma nova figura jurídica, de modo a tutelar tais situações.

Isso tudo, porque atualmente há um movimento muito forte de surgimento de produtos que apresentam mecanismos capazes de desenvolver obras artísticas, literárias e musicais através de sistemas de inteligência artificial. E daí advém os questionamentos: esses itens deveriam ter alguma tutela jurídica? Caso positivo, qual seria o ramo do direito responsável? Caso negativo e essas obras caíssem em domínio público, não poderia configurar o desestímulo a investimentos importantes e salutares no campo das inovações?

Como exemplos, tem-se os roteiros cinematográficos da obra audiovisual *Sunspring*[49], o projeto *Lost Tapes of the 27 Club* que criou diversas músicas com o intuito de homenagear artistas como Amy Winehouse Jimi Hendrix[50] e a obra de arte denominada "The Next"[51].

Nesse último, um dos casos mais emblemáticos, o diretor responsável pelo projeto afirma que dados e tecnologia foram utilizados assim como o artista renascentista se utilizou de pintura e pincéis para criar algo gigante. Para

48. BARBOSA, Denis. Borges. Domínio Público e Patrimônio Cultural. In: O Domínio do Público. Revista Eletrônica do IBPI. N. 6. 2012. 172 p.

49. Sunspring | A Sci-Fi Short Film Starring Thomas Middleditch, 2016. Disponível em: https://www.youtube.com/watch?-v=LY7x2Ihqjmc. Acesso em: 05 jan. 2023.

50. Inteligência artificial cria música inédita do Nirvana. CNN Brasil, 2021. Disponível em: <https://www.cnnbrasil.com.br/entretenimento/inteligencia-artificial-cria-musica-inedita-donirvana/>.
Acesso em: 07 jan. 2023.

51. FRANKEN, Morris; HAANSTRA, Bem. Disponível em: <https://www.nextrembrandt.com/> . Acesso em: 05 jan. 2023.

seu desenvolvimento foram coletados dados de diversos trabalhos do pintor e dessa forma foi definido o tema da obra a ser elaborada (um exemplo de *machine learning*). Na sequência, os especialistas verificaram se os resultados estavam de acordo com as características das obras já confeccionadas pelo pintor, e finalmente, esta foi impressa em material que mais se aproximasse a textura de uma pintura. O resultado foi um quadro que poderia facilmente confundir o maior *expert* dentre os grandes colecionadores.

Este feito só foi alcançado através da coleta de dados que foram imputados no sistema de IA, que conseguiu captar o padrão das obras geradas anteriormente pelo artista, e através dos algoritmos produziu uma nova pintura. A partir da compreensão deste processo, tem-se outro motivo para debates, qual seja: qual seria o limite de utilização de uma obra anterior protegida por direitos autorais para o desenvolvimento de uma nova?

Além disso, no Brasil o artigo 46, VIII da LDA[52] autoriza a utilização de trechos de obras preexistentes ou de sua integralidade - em caso de artes plásticas - quando não há intuito de reprodução da obra anterior na nova. Contudo, quando em obras desenvolvidas por IA o limite é ultrapassado, quem deveria ser responsabilizado pela violação dos direitos?

Ressalta-se que a discussão envolvendo obras criadas com Inteligência Artificial como ferramenta ou meio sendo operada por um humano já foi ultrapassada. É evidente que se atribuam os direitos autorais ao autor. Os debates ocorrem quando o desenvolvimento e fixação da obra se dão sem qualquer

---

52. Lei de Direitos Autorais, n.°9.610/98. "Art. 46. Não constitui ofensa aos direitos autorais:
I - a reprodução:
a) na imprensa diária ou periódica, de notícia ou de artigo informativo, publicado em diários ou periódicos, com a menção do nome do autor, se assinados, e da publicação de onde foram transcritos;
b) em diários ou periódicos, de discursos pronunciados em reuniões públicas de qualquer natureza;
c) de retratos, ou de outra forma de representação da imagem, feitos sob encomenda, quando realizada pelo proprietário do objeto encomendado, não havendo a oposição da pessoa neles representada ou de seus herdeiros;
d) de obras literárias, artísticas ou científicas, para uso exclusivo de deficientes visuais, sempre que a reprodução, sem fins comerciais, seja feita mediante o sistema Braille ou outro procedimento em qualquer suporte para esses destinatários;
II - a reprodução, em um só exemplar de pequenos trechos, para uso privado do copista, desde que feita por este, sem intuito de lucro;
III - a citação em livros, jornais, revistas ou qualquer outro meio de comunicação, de passagens de qualquer obra, para fins de estudo, crítica ou polêmica, na medida justificada para o fim a atingir, indicando-se o nome do autor e a origem da obra;
IV - o apanhado de lições em estabelecimentos de ensino por aqueles a quem elas se dirigem, vedada sua publicação, integral ou parcial, sem autorização prévia e expressa de quem as ministrou;
V - a utilização de obras literárias, artísticas ou científicas, fonogramas e transmissão de rádio e televisão em estabelecimentos comerciais, exclusivamente para demonstração à clientela, desde que esses estabelecimentos comercializem os suportes ou equipamentos que permitam a sua utilização;
VI - a representação teatral e a execução musical, quando realizadas no recesso familiar ou, para fins exclusivamente didáticos, nos estabelecimentos de ensino, não havendo em qualquer caso intuito de lucro;
VII - a utilização de obras literárias, artísticas ou científicas para produzir prova judiciária ou administrativa;
VIII - a reprodução, em quaisquer obras, de pequenos trechos de obras preexistentes, de qualquer natureza, ou de obra integral, quando de artes plásticas, sempre que a reprodução em si não seja o objetivo principal da obra nova e que não prejudique a exploração normal da obra reproduzida nem cause um prejuízo injustificado aos legítimos interesses dos autores.

intervenção humana.

Considerando o já elucidado anteriormente, poderia a máquina ao desenvolver uma obra artística ou intelectual, não sendo uma pessoa física e não sendo capaz de realizar uma "criação do espirito", ter garantido os direitos autorais desta? Essas obras já nasceriam em domínio publico? Ou ainda, a ausência de proteção desse tipo de obra não poderia causar um desestímulo em desenvolvedores e programadores de IA e travar processos evolutivos nesse sentido?

As correntes doutrinárias sobre o tema se dividem. O jurista Ryan Abbott entende que é importante que a autoria seja atribuída com precisão, de forma a otimizar o uso dos direitos autorais e de patentes como incentivo econômico, e ainda preservar os direitos morais da pessoa natural. Isso porque, muitas vezes a obra produzida por IA cai em domínio público por não ter sua autoria reconhecida assim que desenvolvida, o que faz com que usuários se identifiquem como seus autores. [53]

Há outra corrente que defende que, considerando a imprevisibilidade do resultado do trabalho desses mecanismos e por não haver, de forma clara, um autor pessoa física nesses casos, não haveria a possibilidade de se proteger os direitos autorais de obras criadas por AI.

Segundo o doutrinador Pedro Lana, o melhor caminho a ser adotado seria o da ausência de proteção para obras autonomamente geradas por IA – o domínio público. Ele ainda ressalta a necessidade de fugir da ideia de que os direitos de propriedade intelectual garantem maior estímulo à criatividade, além de destacar o benefício desta solução para a economia cultural, bem como sendo uma forma de balancear os avanços acelerados decorrentes do uso de IA. [54]

Importante mencionar também os estudos de Gunther Teubner, através dos quais o autor concluiu que seria "(...) necessário sedimentar a ideia de uma Constituição e um constitucionalismo que se encontra, também, além do Estado" com a criação de uma Constituição Digital, que seria a única capaz de

53. ABBOTT, Ryan Benjamin. Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom (November 2, 2017). Research Handbook on Intellectual Property and Digital Technologies (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming. Disponível em: https://ssrn.com/abstract=3064213. Acesso em: 10 jan. 2023

54. LANA, Pedro de Perdigão. Inteligência artificial e autoria: questões de direito de autor e domínio público. Curitiba: IODA, 2021. P. 173 – 174. Disponível em: https://ioda.org.br/wp-content/uploads/2021/12/1_A-autoria-das-obras_Pedro-de-Perdigao-Lana.pdf. Acesso em: 10 jan. 2023.

cuidar das questões no ambiente digital de forma globalizada e descentralizada[55].

Assim, entende-se que ainda que sobre a tutela de obras desenvolvidas com IA como ferramenta já se tenha um entendimento pacificado, ainda há um longo caminho para que haja um consenso sobre a tutela de obras produzidas por inteligência artificial de forma autônoma.

Contudo, trata-se de assunto latente e de bastante relevância, por se encontrar em constante mudança e possibilitar inúmeras melhorias e evolução à sociedade. Por este mesmo motivo, o Direito Autoral deve se atualizar, pois, caso contrário, e como acredita Ronaldo Lemos, "(...) vai se tornar uma criação obsoleta como um dirigível do início do século 20."[56]

Considerações finais

A partir do que foi apresentado, verifica-se que a Inteligência Artificial pode ser utilizada também na elaboração de obras artísticas, literárias e intelectuais devendo estas ter seus direitos autorais também resguardados. Contudo, notam-se grandes questionamentos acerca desses, que decorrem muito da autonomia cada vez maior que as tecnologias de IA adquirem.

Concluiu-se, ainda, que a respeito das obras desenvolvidas por seres humanos com o uso de IA, já resta pacífico que os usuários/operadores/desenvolvedores dessa tecnologia seriam os detentores dos Direitos Autorais.

Assim, a grande discussão atual reside na questão das obras que são produzidas por estas sem a intervenção humana, isso porque atualmente já existem IAs que foram alimentadas de tal forma que são capazes de desenvolver obras idênticas às produzidas por seres humanos.

Diante do exposto, considerando as mudanças que vêm ocorrendo no âmbito tecnológico e a insegurança jurídica proporcionada por estas, mostra-se imperioso que se busquem definições e delimitações sobre o tema, de forma a garantir a observância e respeito aos direitos de propriedade intelectual a quem couber, sejam as pessoas naturais que se utilizam de IA, os desenvolve-

55. TEUBNER, Gunther. Fragmentos constitucionais: constitucionalismo social na globalização. São Paulo: Saraiva, 2016 apud CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

56. LEMOS, Ronaldo. Inteligência Artificial vai acabar com o direito autoral? Disponível em: https://itsrio.org/pt/artigos/inteligencia-artificial-vai-acabar-com-o-direito-autoral/. Acesso em: 04 mai. 2023.

dores ou seus usuários.

A tecnologia e evoluções digitais devem ser utilizadas como aliadas do progresso, visando sempre ao melhor interesse da sociedade, não podendo as incertezas jurídicas servir como entraves a este processo.

Referências

ABBOTT, Ryan Benjamin. ***Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom (November 2, 2017)***. Research Handbook on Intellectual Property and Digital Technologies (Tanya Aplin, ed), Edward Elgar Publishing Ltd, Forthcoming. Disponível em: https://ssrn.com/abstract=3064213. Acesso em: 10 jan. 2023

ABRAAO, Eliane.Y. **Direitos de Autor e Direitos Conexos**, São Paulo, Editora Brasil: 2002. Acesso em: 07 jan. 2023.

ASCENSÃO, José de Oliveira. **Direito Autoral**. apud BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com.Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. P.20. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em: 17 dez. 2022.

BARBOSA, Denis Borges. **Uma introdução à propriedade intelectual**. Segunda Edição Revista e Atualizada. 88 p. Disponível em: https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf. Acesso em: 04 dez. 2022.

BARBOSA, Denis. Borges. **Domínio Público e Patrimônio Cultural**. In: O Domínio do Público. Revista Eletrônica do IBPI. N. 6. 2012. 172 p.

BITTAR, Carlos Alberto. **Direito de Autor**. São Paulo: Forense Universitária. 8 p.

BRANCO, Sérgio. **A natureza jurídica dos direitos autorais**. Civilistica.com. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em 17 dez. 2022.

CANTALI, Fernanda Borghetti. I**nteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas**. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

CANTALI, Fernanda Borghetti. **Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas**. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 05 mai. 2023.

CARBONI, Guilherme. **Direito Autoral e Autoria Colaborativa na Economia da Informação em Rede**. São Paulo: Quartier Latin, 2010.

CUPIS, Adriano de. **Os Direitos da Personalidade**. cit., p. 337 apud BRANCO, Sérgio. A natureza jurídica dos direitos autorais. Civilistica.com. Rio de Janeiro, a. 2, n. 2, abr.-jun./2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/91/61. Acesso em: 17 dez. 2022.

FILHO, Maxwell Morais de Lima. **O Experimento de Pensamento do Quarto Chinês: a Crítica de John Searle à Inteligência Artificial Forte Argumentos**, Ano 2, N°. 3 – 2010. Disponível em https://repositorio.ufc.br/bitstream/riufc/3566/1/2010_Art_MMLFilho.pdf. Acesso em: 29 dez. 2022.

FRANKEN, Morris; HAANSTRA, **Bem**. Disponível em: <https://www.nextrembrandt.com/> . Acesso em: 05 jan. 2023.

GARCÍA, Sergio Marín. **Ética e inteligência artificial**. 19 p. Disponível em: https://dx.doi.org/10.15581/018.ST-522. Acesso em: 08 mai. 2023. Tradução livre.

GONÇALVES, Lukas Ruthes. **A tutela jurídica de trabalhos criativos feitos pro aplicações de inteligência artificial no Brasil**. Dissertação apresentada ao Programa de Pós-Graduação em Direito, Faculdade de Direito, Setor de Ciências Jurídicas, da Universidade Federal do Paraná como requisito parcial para obtenção do título de Mestre em Direito. Orientador: Prof. Dr. Marcos Wachowicz. Curitiba. 2019.

Disponível em: https://www.gedai.com.br/wpcontent/uploads/2019/10/DISSERTA%C3%87%C3%83O-Lukas-Ruthes_Direitoe-Inteligencia-Artificial.pdf. Acesso em: 18 dez. 2022.

HOHENDORFF, Raquel Von ; CANTALI, Fernanda Borghetti ; D'ÁVILA, Fernanda Felitti da S. **Inteligência artificial e direitos autorais: desafios e possibilidades no cenário jurídico brasileiro e internacional**, PragMATIZES – Revista Latino-Americana de Estudos em Cultura, Niterói/RJ, Ano 10, n. 19, set. 2020. Disponível em https://doi.org/10.22409/pragmatizes.v10i19.41210. Acesso em: 4 mai. 2023.

LANA, Pedro de Perdigão. **Inteligência artificial e autoria: questões de direito de autor e domínio público**. Curitiba: IODA, 2021.
P. 173 – 174. Disponível em: https://ioda.org.br/wp-content/uploads/2021/12/1_A-autoria-das-obras_Pedro-de-Perdigao-Lana.pdf. Acesso em: 10 jan. 2023.

LEIRA, Thales Boechat Nunes. **Os desdobramentos do Direito Autoral na Era Digital**. Disponível em: https://www.gedai.com.br/wp-content/uploads/2019/05/023-OS-DESDOBRAMENTOS-DO-DIREITO.pdf. Acesso em: 04 de dez. 2022.

LEMOS, Ronaldo. **Inteligência Artificial vai acabar com o direito autoral?** Disponível em: https://itsrio.org/pt/artigos/inteligencia-artificial-vai-acabar-com-o-direito-autoral/. Acesso em: 04 mai. 2023.

MENEZES, Elisângela Dias. **Curso de Direito Autoral**. Belo Horizonte: Del Rey, 2007. 67 p.

NEVES, Ricardo. **O que faremos com o ChatGPT?** Disponível em: https://www.updateordie.com/2023/02/27/o-que-faremos-com-o-chatgpt/. Acesso em: 12 mai 2023.

PISTONO, Federico. Os robôs vão roubar o seu trabalho, mas tudo bem. Tradução de Pedro Soares. São Paulo. Portfolio Pinguin, 2017 apud CANTALI, F. B. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

RAJARAMAN, V. John McCarthy – **Father of Artificial Intelligence**. Asia Pacific Mathematics Newsletter. Jul. 2014, v. 4, nº 3, p. 15-20. Disponível em: http://www.asiapacific-mathnews.com/04/0403/0015_0020.pdf, apud CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 05 mai. 2023.

RUSSEL, Stuart; NORVIG, Peter. ***Artificial Intelligence: A Modern Approach***. New Jersey: Prentice Hall, 2009 (3º Ed. apud Inteligência Artificial: questões éticas a serem enfrentadas. KAUFMAN, Dora. Disponível em: https://abciber.org.br/anaiseletronicos/wpcontent/uploads/2016/trabalhos/inteligencia_artificial_questoes_eticas_a_serem_enfrentadas_dora _kaufman.pdf. Acesso em: 19 de Dez. 2022.

SCHIRRU, Luca. **A inteligência artificial e o Big Data no setor da saúde**. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/6748173.pdf>. Acesso em 18 de Dez. 2022.

SCHIRRU, Luca. **A inteligência artificial e o direito autoral: o domínio publico em perspectiva**. Disponível em: https://itsrio.org/wp-content/uploads/2019/04/Luca-Schirru-rev2-1.pdf. Acesso em: 09 jan. 2023.

SOUZA, Diego Brainer de; RODRIGUES, Cássio Monteiro. **Memes e direito autoral: da superação da lógica proprietária à tutela do elemento cultural apud SCHREIBER**, Anderson; Terra de Moraes, Bruno; Spadaccini de Teffé, Chiara. (Org.). Direito e Mídia: tecnologia e liberdade de expressão. 1 ed. São Paulo: Editora Foco.

TEUBNER, Gunther. **Fragmentos constitucionais: constitucionalismo social na globalização**. São Paulo: Saraiva, 2016 apud CANTALI, Fernanda Borghetti. Inteligência Artificial e Direito de Autor: Tecnologia Disruptiva Exigindo Reconfiguração de Categorias Jurídicas. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, Porto Alegre, v. 4, n. 2, jun.-dez. 2018. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0014/2018.v4i2.4667. Acesso em: 04 mai. 2023.

VON HOHENDORFF, Raquel; CANTALI, F. B.; D'AVILA, F. F. da S.. "**Inteligência Artificial e Direitos Autorais: Desafios e Possibilidades no Cenário Jurídico Brasileiro e Internacional**". 254 p. Disponível em: https://periodicos.uff.br/pragmatizes/article/view/41210/24697. Acesso em 18 dez. 2022.

WOODMANSEE, Martha. ***The genius and the copyright: economic and legal conditions of the emergence of the "author"***. Eighteenth-Century Studies, v. 17, Issue 4, Summer, 1984. 427 p.

ZAFFARI, Felipe Pozueco; ESPÍNDOLA, Jean Carlo de Borba. "**Conceitos o que é inteligência artificia**l" apud BARONE, Dante Augusto; Couto; BOESING, Ivan Jorge (org.). Inteligência artificial: diálogos entre mentes e máquinas. Porto Alegre: AGE/Evangraf, 2015.

ZANINI. Leonardo Estevam de Assis. **Direito de autor em perspectiva histórica: da idade média ao reconhecimento dos direitos da personalidade do autor**. 224 p. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/532-2425-1-pb.pdf. Acesso em: 04 dez. 2022.

BRASIL. Lei nº 9.610 de /98. **Regula direitos e obrigações relativos à Direitos Autorais**. Brasília, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d75699.htm.

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

SUIÇA. **Convenção de Berna**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d75699.htm.

Inteligência Artificial coloca voz de Drake em música que ele nunca cantou. Disponível em: https://www.portalt5.com.br/noticias/single/nid/inteligencia-artificial-coloca-voz-de-drake-em-musica-que-ele-nunca-cantou/. Acesso em: 04 mai. 2023.

Inteligência artificial cria música inédita do Nirvana. CNN Brasil, 2021. Disponível em: <https://www.cnnbrasil.com.br/entretenimento/inteligencia-artificial-cria-musica-inedita-do-nirvana/>.

Sunspring | A Sci-Fi Short Film Starring Thomas Middleditch, 2016. Disponível em: https://www.youtube.com/watch?v=LY7x2Ihqjmc. Acesso em: 05 jan. 2023.

DIÁLOGOS DA
PÓS-GRADUAÇÃO
EM DIREITO DIGITAL

18

Análise de dados e sua aplicação em processos judiciais: exemplos práticos, desafios e perspectivas futuras

LUCAS CABRAL DE SOUZA RAMOS

LUCAS CABRAL DE SOUZA RAMOS[1]

Introdução: contextualização do uso da análise de dados no sistema judicial

A prática de realizar análise de dados, principalmente visando a tomada de decisões, tornou-se uma ferramenta cada vez mais relevante e poderosa em diversos setores, e o sistema judicial não é exceção. No contexto jurídico, tem despertado o interesse de acadêmicos e profissionais do Direito, que buscam compreender como essa abordagem pode aprimorar a eficiência, precisão e imparcialidade das decisões judiciais.

De acordo com Raphael Arévalos[2], a análise de dados no sistema judicial pode proporcionar insights valiosos sobre o comportamento dos tribunais, a eficácia de leis e políticas públicas, bem como identificar tendências e padrões nas decisões judiciais. Essa abordagem baseada em dados permite aos juristas uma compreensão mais aprofundada dos casos em questão, contribuindo para uma análise mais objetiva e fundamentada.

No entanto, é importante ressaltar que a análise de dados no sistema judicial também traz desafios éticos e de privacidade. A utilização de informações sensíveis requer cuidados e garantias para preservar a confidencialidade e a integridade dos dados, além de assegurar a imparcialidade nas análises. Nesse sentido, a adequação da legislação e a implementação de protocolos de segurança são fundamentais para assegurar a confiabilidade e a legitimidade do uso da análise de dados no contexto jurídico.

1. Cursando MBA em Business Intelligence (BI) pela Innovation & Entrepreneurship Business School (IEBS). Graduado em análise e desenvolvimento de sistemas pela Faculdade de Educação Tecnológica do Estado Rio de Janeiro (FAETERJ-Rio). Programador e analista de dados. Atuou como pesquisador em educação e tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Atualmente, é analista de BI dentro do aplicativo Cíngulo e Product Owner da equipe de dados na Play9. Assistente acadêmico na disciplina Machine Learning e Programação para Advogados na pós-graduação em direito digital ITS/UERJ.

2. ARÉVALOS, Raphael. USO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO: eficácia dos princípios da celeridade processual e razoável duração do processo. Florianópolis, 2021. 81 p.

Objetivo do artigo

Explicar quais são os fundamentos, conceitos e métodos para se realizar uma análise de dados; Demonstrar as principais aplicações da análise de dados que podem ser utilizadas em processos judiciais; Identificar quais são os desafios e considerações éticas na análise de dados em processos judiciais; Apresentar os benefícios que a análise de dados pode promover para o sistema judicial, identificando os seus possíveis impactos; e Traçar as perspectivas futuras da análise de dados dentro do contexto judicial.

1. Fundamentos da análise de dados

1.1. Definição e conceitos básicos da análise de dados

A análise de dados é um campo fundamental no atual cenário digital, impulsionado pelo crescente volume de informações disponíveis. Para compreender melhor a definição e conceitos básicos da análise de dados é necessário explorar estudos sobre estatística e fundamentos matemáticos. De acordo com Márcio Schwaab e José Carlos Pinto[3], a análise de dados refere-se ao processo de examinar, limpar, transformar e modelar informações para obter *insights* e tomar decisões embasadas.

Tendo em vista que no cenário atual contamos com técnicas estatísticas, algoritmos de aprendizado de máquina e linguagens de programação desenvolvidas para visualização de dados, é importante entender que a base fundamental de uma boa análise envolve definir objetivos claros, coletar dados relevantes e ter pensamentos críticos para interpretar os resultados de forma significativa. Além disso, Schwaab e Pinto[3] também exploram as implicações éticas e as considerações de privacidade associadas à análise de dados, ressaltando a importância de garantir a segurança e a confidencialidade das informações.

1.2. Técnicas e métodos utilizados na análise de dados

No âmbito da análise de dados, existem diversas técnicas e métodos que podem ser empregados para extrair percepções valiosas a partir das informa-

3. SHWAAB, Marcio; PINTO, José Carlos. ANÁLISE DE DADOS EXPERIMENTAIS I: fundamentos de estatística e estimação de parâmetros. Rio de Janeiro, 2007. 462 p.

ções disponíveis. De acordo com Djalma Pessoa e Pedro Nascimento Silva[4], no estudo para o departamento de Metodologia do IBGE, existem duas etapas para a realização de uma boa análise, a fase exploratória e a descritiva.

A análise exploratória é uma etapa fundamental dentro de todo processo, envolvendo a aplicação de técnicas estatísticas e visualizações para compreender a estrutura e as características dos dados. Já a fase descritiva, são métodos que permitem resumir e descrever os dados de forma clara e concisa, como a utilização de medidas de tendência central e dispersão.

O estudo de Pessoa e Silva[5] também aborda técnicas de análise preditiva, que visam fazer previsões e estimativas com base nos dados disponíveis. Entre essas técnicas, destacam-se a regressão linear, análise de séries temporais e algoritmos de aprendizado de máquina. Essas abordagens permitem identificar padrões e tendências nos dados, auxiliando na tomada de decisões futuras. Dominando essas técnicas e métodos que são utilizados na análise de dados, é possível construir uma base sólida para explorar esse campo da tecnologia que está em constante evolução.

1.3. Importância da qualidade e integridade dos dados

A qualidade e integridade dos dados que serão levados em consideração dentro de uma análise são elementos essenciais para qualquer experimento. Sendo fundamental entender que quaisquer interferências na integridade dos dados analisados podem gerar impactos significativos na confiabilidade das informações, afetando assim as tomadas de decisões que serão baseadas no experimento.

De acordo com Thais Correia, José Quintanilha, Alessandra Corsi e Lucas Sandre[6], a qualidade dos dados é fundamental para garantir a precisão e a representatividade das análises realizadas. Dados incorretos ou incompletos podem levar a conclusões equivocadas e decisões inadequadas, prejudicando a eficiência da análise.

Além disso, a integridade dos dados é um fator crítico para assegurar a

4. PESSOA, Djalma; SILVA, Pedro Nascimento. ANÁLISE DE DADOS AMOSTRAIS COMPLEXOS. São Paulo: Departamento de Metodologia do IBGE, 2018. 148 p

5. PESSOA, Djalma; SILVA, Pedro Nascimento. ANÁLISE DE DADOS AMOSTRAIS COMPLEXOS. São Paulo: Departamento de Metodologia do IBGE, 2018. 148 p

6. CORREIA, Thaís; QUINTANILHA, José; CORSI, Alessandra; SANDRE, Lucas. DO SIG AO BIG DATA: estruturação dos dados espaciais do entorno das estações ferroviárias caieiras e Francisco Morato. São Paulo, 2020. 5 p.

confiabilidade das análises e a transparência das informações. A veracidade e a consistência dos dados coletados e utilizados são fundamentais para evitar distorções e vieses nas análises, bem como para garantir a confiança do público e dos tomadores de decisão. Portanto, investir em procedimentos e práticas que promovam a qualidade e integridade dos dados é essencial para obter resultados robustos e embasar ações efetivas em qualquer análise de dados.

2. Aplicação da análise de dados em processos judiciais

2.1. Apoio na tomada de decisões judiciais

O uso de ferramentas para análise de dados, cálculos estatísticos e aplicação de Inteligência Artificial (IA) para tomada de decisões judiciais tem se tornado um tema de grande relevância no âmbito do sistema judiciário. Tendo isto em vista, é de suma importância entender os benefícios que o uso destes sistemas de apoio pode gerar no quesito das tomadas de decisão dentro do contexto jurídico.

O apoio na tomada de decisões judiciais através de sistemas computacionais pode proporcionar um auxílio valioso aos magistrados. Segundo André Vasconcelos Roque e Lucas Braz Rodrigues dos Santos[7] , é possível oferecer informações relevantes e embasadas para fundamentar suas decisões. Essas ferramentas podem fornecer acesso rápido a jurisprudências, leis, doutrinas e outros dados legais, permitindo uma análise mais completa e consistente dos casos em questão.

Além disso, o uso de sistemas de apoio à decisão judicial pode contribuir para aumentar a imparcialidade e a consistência nas decisões, reduzindo a subjetividade e o viés individual. Isto porque essas ferramentas auxiliam na identificação de precedentes e padrões em casos similares, facilitando a aplicação da lei de forma mais uniforme e coerente. No entanto, é importante ressaltar que o uso desses sistemas não deve substituir a expertise e o discernimento dos magistrados, mas sim servir como uma ferramenta complementar que amplia a base de conhecimento disponível para uma tomada de decisão mais informada e justa.

7. ROQUE, André Vasconcelos; SANTOS, Lucas Braz Rodrigues dos. INTELIGÊNCIA ARTIFICIAL NA TOMADA DE DECISÕES JUDICIAIS: três premissas básicas. Rio de Janeiro, 2020. 21 p.

2.2. Uso de modelos preditivos e estatísticos

A maior aplicação da análise de dados para processos judiciais é a utilização de modelos preditivos e estatísticos nas decisões. Este tipo de ferramenta é capaz de gerar uma previsão de resultados, calcular o intervalo de confiança estatístico para uma decisão e organizar todas as variáveis que um processo judicial possui, mas para isto acontecer é necessária uma base de dados previamente alimentada com os devidos dados relevantes para o caso específico. Este banco de dados pode conter, por exemplo, artigos da legislação local, decisões jurídicas similares ao caso, dados pessoais das partes envolvidas no processo ou qualquer informação relevante para a ação em andamento. Este tema tem despertado um intenso debate sobre sua eficácia e ética, que visam auxiliar e agilizar todos os processos no contexto jurídico.

Conforme Cinthia Obladen Freitas e Jean Paul Barddal[8], o uso de modelos preditivos e estatísticos podem trazer benefícios no sistema judicial, proporcionando *insights* valiosos sobre tendências, comportamentos e riscos relacionados a casos judiciais. Essas ferramentas podem auxiliar os magistrados na identificação de padrões e na avaliação de probabilidades, contribuindo para uma tomada de decisão mais embasada. No entanto, também é fundamental entender os desafios e as preocupações éticas associadas ao uso desses modelos na esfera jurídica. A transparência, a interpretação e a proteção de direitos fundamentais são questões cruciais a serem consideradas. Além disso, é necessário garantir que os modelos preditivos e estatísticos sejam utilizados como uma ferramenta de apoio, sem substituir o julgamento humano e o devido processo legal. Portanto, é essencial estabelecer diretrizes claras e promover um diálogo aberto e crítico sobre o uso dessas técnicas, visando alcançar um equilíbrio adequado entre a eficiência e a justiça nas decisões judiciais.

3. Exemplos práticos de aplicação da análise de dados em processos judiciais

3.1.Análise forense de dados digitais e recuperação de informações apagadas

8. FREITAS, Cinthia Obladen de Almendra; BARDDAL, Jean Paul. ANÁLISE PREDITIVA E DECISÕES JUDICIAIS: controvérsia ou realidade? Florianópolis, 2019. 20 p

Um exemplo prático do uso de análise de dados dentro de um processo judicial é a coleta e preservação de evidências com base em análise forense de dados digitais e a recuperação de informações apagadas, se necessário. Estes são processos cruciais no campo da investigação e da segurança cibernética sendo possível ser realizada somente com um grande conhecimento técnico, porém a compreensão jurídica desses dados é fundamental para sua utilização dentro de uma ação judicial.

A análise forense de dados digitais refere-se ao processo de coleta, preservação, recuperação e análise de evidências digitais presentes em dispositivos de armazenamento. Segundo Jéssica Silva e Henrique Pachioni Martins[9] , essa técnica permite identificar e reconstruir atividades realizadas em meios eletrônicos, auxiliando em investigações criminais e disputas legais.

Hoje em dia, na era digital, é muito comum em processos de investigação judicial existirem tentativas de destruição ou ocultamento de provas que estavam armazenadas em nuvem ou em dispositivos físicos. A recuperação de informações apagadas é um aspecto crucial na análise forense de dados. Através de métodos e ferramentas especializadas, é possível recuperar arquivos e dados excluídos intencionalmente ou acidentalmente. Essa prática é de extrema importância para obter evidências completas e confiáveis, uma vez que dados apagados podem conter informações relevantes para investigações.

Em suma, a análise forense de dados digitais e a recuperação de informações apagadas desempenham um papel fundamental na busca pela verdade e na segurança cibernética. Com o avanço contínuo da tecnologia, é essencial que os profissionais envolvidos nesse campo estejam atualizados com as melhores práticas e ferramentas disponíveis para garantir a integridade das investigações e a proteção dos dados.

3.2. Utilização de algoritmos de aprendizado de máquina para prever resultados de casos

A técnica de aprendizado de máquina se baseia no desenvolvimento de um algoritmo, que é um sistema inteligente que realiza instruções previamente definidas pelo desenvolvedor, e de um banco de dados alimentado com informações relevantes para a execução da tarefa proposta. Para exemplificar o

9. SILVA, Jéssica; MARTINS, Henrique Pachioni. ANÁLISE E RECUPERAÇÃO DE ARQUIVOS EM DISPOSITIVOS DE ARMAZENAMENTO, UTILIZANDO TÉCNICAS DE PERÍCIA FORENSE. São Paulo, 2021. 13 p.

uso desta ferramenta pode-se pensar no algoritmo que joga xadrez, onde é inserido em seu banco de dados todas as regras do jogo e, com base nessas informações, o algoritmo é capaz de aprender a realizar jogadas complexas. Tendo em vista essas definições, é possível pensar em diversas utilizações dos algoritmos de aprendizado de máquina para o âmbito jurídico, prevendo resultados de casos, elaborando contratos e auxiliando os juristas em tarefas repetitivas. Este cenário tem se mostrado promissor no campo judicial fazendo-se fundamental explorar essa aplicação e seus potenciais benefícios.

De acordo com Daniel Henrique Arruda Boeing[10] , os algoritmos de aprendizado de máquina têm o objetivo de ensinar um sistema a reconhecer padrões e relações em grandes volumes de dados jurídicos. Esses modelos são treinados com base em decisões judiciais passadas, considerando variáveis relevantes para o resultado do caso, como jurisprudência, leis e argumentos apresentados. A utilização desses algoritmos na previsão de resultados de casos pode trazer vantagens, como a agilidade na análise de processos e a identificação de tendências e padrões ocultos. No entanto, é importante considerar as limitações e desafios éticos associados a essa abordagem. A interpretação dos modelos e a necessidade de evitar vieses algorítmicos são questões cruciais a serem abordadas para garantir a confiabilidade e a justiça nas decisões judiciais. Portanto, a utilização de algoritmos de aprendizado de máquina como ferramentas de apoio na previsão de resultados de casos requer uma análise crítica e cuidadosa para garantir a transparência e a imparcialidade no sistema judiciário.

4. Desafios e considerações éticas na análise de dados em processos judiciais

4.1. Viés e equidade na análise de dados

A questão do viés e da equidade na análise de dados em decisões judiciais é um tema de extrema relevância e complexidade. Isto porque, normalmente, essas análises preditivas são realizadas utilizando algoritmos de IA e baseadas em informações previamente inseridas em bancos de dados. Neste con-

10. BOEING, Daniel Henrique Arruda. ENSINANDO UM ROBÔ A JULGAR: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no judiciário. Florianópolis, 2019. 84 p.

texto, caso o desenvolvimento dessa inteligência for feito de forma enviesada ou tendenciosa, pode-se gerar uma análise equivocada, errada e até mesmo preconceituosa. Observando esse cenário, torna-se necessário explorar a influência dos vieses nos resultados das análises de dados e a importância de promover a equidade no sistema judiciário.

Para Adalberto Simão Filho e Cintia Rosa Pereira de Lima[11], é fundamental compreender que os dados utilizados na análise podem refletir vieses existentes na sociedade, como preconceitos, estereótipos e desigualdades sistêmicas. A aplicação de algoritmos e modelos de análise de dados sem uma avaliação cuidadosa pode resultar na perpetuação desses vieses, gerando decisões judiciais injustas e discriminatórias. Portanto, é imprescindível adotar medidas para mitigar e corrigir esses vieses, garantindo a equidade na análise de dados em decisões judiciais. Isso envolve a identificação e o monitoramento constante dos potenciais vieses presentes nos algoritmos e nos conjuntos de dados utilizados. Além disso, é necessário o desenvolvimento de técnicas e abordagens que promovam a equidade, como a implementação de ajustes e contramedidas para corrigir desequilíbrios e assegurar que as decisões sejam justas e imparciais.

4.2. Confidencialidade e segurança das informações

Visando preservar a integridade do sistema jurídico e proteger os direitos das partes envolvidas dentro de um processo, a confidencialidade e a segurança das informações em decisões judiciais são aspectos críticos. O grande desafio atualmente é lidar constantemente com um volume imenso de dados pessoais que são necessários para realizar as análises de processos judiciais. Sendo importante então entender os princípios da privacidade e da proteção de dados e quais são as medidas necessárias para garantir sua efetividade.

A confidencialidade das informações em decisões judiciais envolve a restrição do acesso não autorizado a dados sensíveis e protegidos por sigilo, como informações pessoais, financeiras e estratégicas. Essa proteção é essencial para preservar a privacidade das partes envolvidas e evitar possíveis danos decorrentes de divulgações indevidas. Além disso, para Guilherme Damásio

11. SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de. A(IN)DECISÃO JUDICIAL E OS ALGORITMOS TÓXICOS: pelo direito de revisão de decisões automatizadas. São Paulo, 2021. 4 p.

Goulart[12] a segurança das informações também é fundamental para impedir acessos não autorizados, manipulação ou corrupção dos dados presentes nas decisões judiciais. Isso requer a implementação de medidas técnicas e organizacionais, como a criptografia, o controle de acesso, a auditoria e a proteção contra ameaças cibernéticas. A adoção de práticas de segurança adequadas é essencial para garantir a integridade do sistema judicial e a confiança da sociedade nas decisões proferidas.

Em suma, a confidencialidade e a segurança das informações em decisões judiciais são pilares fundamentais do sistema jurídico. O cumprimento desses princípios requer a implementação de políticas e medidas robustas para garantir a privacidade das partes envolvidas e proteger os dados sensíveis contra acessos não autorizados, contribuindo para a justiça e a credibilidade do sistema jurídico.

5. Benefícios e impactos da análise de dados no sistema judicial

5.1. Aceleração de processos e redução de custos

A aceleração de processos e a redução de custos em decisões judiciais são objetivos essenciais para a eficiência e a efetividade do sistema jurídico. Para isto, é necessário desenvolver estratégias e práticas que visam agilizar os trâmites processuais e otimizar a alocação de recursos.

No âmbito judicial existe uma necessidade premente para uma aceleração nos processos judiciais. A implementação de ferramentas e tecnologias, como sistemas de processo eletrônico, inteligência artificial e automação de tarefas, pode agilizar a tramitação dos casos, reduzir a burocracia e eliminar atividades desnecessárias, permitindo uma resposta mais rápida às demandas judiciais.

Segundo Dirceu Pereira Siqueira e Matheus Ribeiro de Oliveira Wolowski[13] , a redução de custos é um aspecto crucial para a sustentabilidade do siste-

12. GOULART, Guilherme Damásio. SEGURANÇA DA INFORMAÇÃO E A PROTEÇÃO CONTRA A VIOLAÇÃO DE DADOS PESSOAIS: a confidencialidade no direito do consumidor. Porto Alegre, 2012. 215 p.

13. SIQUEIRA, Dirceu Pereira; WOLOWSKI, Matheus Ribeiro de Oliveira. INTELIGÊNCIA ARTIFICIAL E O POSITIVISMO JURÍDICO: benefícios e obstáculos para efetivação da justiça. Rio Grande do Sul, 2022. 18 p.

ma judiciário. A busca por soluções que otimizem a alocação de recursos financeiros, humanos e tecnológicos é fundamental para garantir a eficiência e a economicidade nas decisões judiciais. Medidas como a racionalização de procedimentos, a adoção de métodos alternativos de solução de conflitos e a gestão eficiente dos processos são estratégias que podem contribuir para a redução de custos sem comprometer a qualidade e a justiça das decisões.

Em resumo, a aceleração de processos e a redução de custos em decisões judiciais são metas que visam aprimorar o sistema jurídico. A utilização de tecnologias e a implementação de práticas eficientes são essenciais para agilizar os trâmites processuais, reduzir a burocracia e otimizar a alocação de recursos, resultando em decisões mais rápidas, econômicas e efetivas.

5.2. Melhoria da eficiência e qualidade das decisões judiciais

Visando promover a justiça e a efetividade do sistema jurídico, é fundamental realizar melhorias na eficiência e qualidade das decisões judiciais. De acordo com Antônio Donizete Ferreira da Silva[14] a eficácia nas decisões judiciais pode ser alcançada por meio de uma gestão produtiva do fluxo de trabalho no poder judiciário. A adoção de métodos e tecnologias que otimizem os processos, como sistemas de processo eletrônico, automação de tarefas e gestão de dados, pode agilizar a tramitação dos casos, reduzir a burocracia e aumentar a produtividade dos profissionais envolvidos.

Além disso, a qualidade das decisões judiciais é um aspecto crucial para garantir a confiança e a legitimidade do sistema jurídico. A valorização da imparcialidade, fundamentação adequada, consistência na aplicação do direito e acesso a informações relevantes são fatores que contribuem para aprimorar a qualidade das decisões. A capacitação contínua dos profissionais do direito, a promoção do debate jurídico e a utilização de dados e estudos empíricos também podem fornecer subsídios para decisões mais embasadas e consistentes.

Portanto, a melhoria da eficiência e qualidade das decisões judiciais é um desafio importante para o sistema jurídico. A implementação de práticas de gestão eficiente, o uso de tecnologias adequadas e o fomento de um ambiente

14. SILVA, Antônio Donizete Ferreira da. PROCESSO JUDICIAL ELETRÔNICO E A INFORMÁTICA JURÍDICA: um olhar para o uso da inteligência artificial como ferramenta de eficiência na prestação jurisdicional. São Paulo, 2017. 138 p.

jurídico embasado e transparente são medidas essenciais para alcançar decisões mais rápidas, eficientes e de qualidade, contribuindo para a justiça e a confiança no sistema jurídico.

Conclusão

No presente artigo, foi discutido o uso da análise de dados no contexto jurídico, com o objetivo de aprimorar a eficiência, precisão e imparcialidade das decisões judiciais. Foi destacado que a análise de dados no sistema judicial proporciona *insights* valiosos sobre o comportamento dos tribunais, a eficácia das leis e políticas públicas, bem como a identificação de tendências e padrões nas decisões. No entanto, foram mencionados também os desafios éticos e de privacidade associados ao uso de informações sensíveis, sendo ressaltada a importância de uma legislação adequada e da implementação de protocolos de segurança, para garantir a confiabilidade e a legitimidade da análise de dados no contexto jurídico.

Foram abordados os fundamentos da análise de dados, incluindo sua definição e conceitos básicos, bem como as técnicas e métodos utilizados para extrair percepções valiosas das informações disponíveis. Também foi destacada a importância da qualidade e integridade dos dados, enfatizando que dados incorretos ou incompletos podem levar a conclusões equivocadas e decisões inadequadas.

No contexto específico dos processos judiciais, foram exploradas as aplicações da análise de dados, como o apoio na tomada de decisões judiciais, o uso de modelos preditivos e estatísticos e a análise forense de dados digitais. Foi ressaltado que o uso de ferramentas de análise de dados pode auxiliar os magistrados na fundamentação de suas decisões, aumentando a imparcialidade e consistência. Além disso, foi discutido o potencial dos modelos preditivos e estatísticos para identificar tendências, comportamentos e riscos relacionados a casos judiciais.

Foi explorado também como a análise de dados pode ser utilizada para aprimorar a gestão do sistema judicial, melhorando a eficiência dos tribunais, a distribuição de recursos e o planejamento estratégico.

Ao longo do artigo, foram ressaltados os benefícios potenciais da análise de dados no contexto judicial, como a redução de erros, a economia de tempo e recursos, a maior transparência e o acesso à justiça. No entanto, também abordamos as preocupações éticas e os desafios associados à análise de dados, incluindo a privacidade, a equidade e a interpretação correta dos resulta-

dos.

Em resumo, a análise de dados está se tornando uma ferramenta cada vez mais importante no campo jurídico, com o potencial de aprimorar a eficiência, a transparência e a justiça do sistema judicial. No entanto, é essencial abordar os desafios éticos e promover uma aplicação responsável da análise de dados para garantir resultados equitativos e proteção dos direitos individuais.

Olhando para o futuro, a análise de dados tem o potencial de transformar ainda mais o sistema judicial. Com avanços contínuos em técnicas estatísticas, algoritmos de aprendizado de máquina e inteligência artificial, é possível prever resultados de casos com maior precisão, elaborar contratos de forma mais eficiente e auxiliar os juristas em tarefas repetitivas. Essas perspectivas trazem benefícios como economia de tempo, redução de erros e maior acesso à justiça.

Uma das áreas promissoras é o uso de modelos preditivos para auxiliar juízes na determinação de sentenças e na avaliação de riscos. Com base em dados históricos e padrões identificados, esses modelos podem fornecer insights valiosos sobre a probabilidade de um caso ser favorável a uma determinada parte. No entanto, é importante notar que a utilização de modelos preditivos deve ser feita com cautela, pois eles podem refletir vieses históricos e sociais presentes nos dados de treinamento.

Além disso, a análise de dados pode ser aplicada no desenvolvimento de sistemas de resolução de disputas online, oferecendo uma alternativa eficiente e acessível ao processo judicial tradicional. Esses sistemas podem ser projetados para analisar dados de casos semelhantes, identificar padrões e propor soluções justas e equitativas. Isso poderia acelerar a resolução de disputas e aliviar a carga sobre os tribunais.

Outra perspectiva é a aplicação da análise de dados na identificação de fraudes e atividades ilegais. A análise forense de dados digitais pode desempenhar um papel fundamental na investigação de crimes cibernéticos, recuperação de evidências e identificação de padrões suspeitos. Com o aumento do uso de tecnologias digitais e da internet, a análise de dados torna-se essencial para a investigação eficaz de crimes e a garantia da segurança jurídica.

No entanto, é importante abordar os desafios éticos e de privacidade associados à análise de dados no contexto judicial. É necessário garantir a proteção adequada dos dados pessoais e a transparência na utilização de algoritmos e modelos de aprendizado de máquina. Também é essencial que os profissionais do direito estejam preparados para compreender e interpretar corretamente

os resultados da análise de dados, evitando conclusões simplistas ou injustas.

Para que a análise de dados continue a evoluir no contexto judicial, é necessário promover a atualização constante dos profissionais envolvidos nessa área, bem como estabelecer diretrizes claras para seu uso. O diálogo aberto entre juristas, especialistas em tecnologia e a sociedade em geral é fundamental para encontrar um equilíbrio adequado entre eficiência e justiça nas decisões judiciais. Dessa forma, a análise de dados pode contribuir para um sistema judicial mais eficiente, transparente e acessível a todos.

Referências bibliográficas

ARÉVALOS, Raphael. **USO DA INTELIGÊNCIA ARTIFICIAL NO PODER JUDICIÁRIO: eficácia dos princípios da celeridade processual e razoável duração do processo**. Florianópolis, 2021. 81 p.

BOEING, Daniel Henrique Arruda. **ENSINANDO UM ROBÔ A JULGAR: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no judiciário**. Florianópolis, 2019. 84 p.

CORREIA, Thaís; QUINTANILHA, José; CORSI, Alessandra; SANDRE, Lucas. **DO SIG AO BIG DATA: estruturação dos dados espaciais do entorno das estações ferroviárias caieiras e Francisco Morato**. São Paulo, 2020. 5 p.

FREITAS, Cinthia Obladen de Almendra; BARDDAL, Jean Paul. **ANÁLISE PREDITIVA E DECISÕES JUDICIAIS: controvérsia ou realidade?** Florianópolis, 2019. 20 p

GOULART, Guilherme Damásio. **SEGURANÇA DA INFORMAÇÃO E A PROTEÇÃO CONTRA A VIOLAÇÃO DE DADOS PESSOAIS: a confidencialidade no direito do consumidor**. Porto Alegre, 2012. 215 p.

PESSOA, Djalma; SILVA, Pedro Nascimento. **ANÁLISE DE DADOS AMOSTRAIS COMPLEXOS**. São Paulo: Departamento de Metodologia do IBGE, 2018. 148 p

ROQUE, André Vasconcelos; SANTOS, Lucas Braz Rodrigues dos. **INTELIGÊNCIA ARTIFICIAL NA TOMADA DE DECISÕES JUDICIAIS: TRÊS PREMISSAS BÁSICAS**1. Rio de Janeiro, 2020. 21 p.

SHWAAB, Marcio; PINTO, José Carlos. **ANÁLISE DE DADOS EXPERIMENTAIS I: fundamentos de estatística e estimação de parâmetros**. Rio de Janeiro, 2007. 462 p.

SILVA, Antônio Donizete Ferreira da. **PROCESSO JUDICIAL ELETRÔNICO E A INFORMÁTICA JURÍDICA: um olhar para o uso da inteligência artificial como ferramenta de eficiência na prestação jurisdicional**. São Paulo, 2017. 138 p.

SILVA, Jéssica; MARTINS, Henrique Pachioni. **ANÁLISE E RECUPERAÇÃO DE ARQUIVOS EM DISPOSITIVOS DE ARMAZENAMENTO, UTILIZANDO TÉCNICAS DE PERÍCIA FORENSE**. São Paulo, 2021. 13 p.

SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de. **A(IN)DECISÃO JUDICIAL E OS ALGORITMOS TÓXICOS: pelo direito de revisão de decisões automatizadas**. São Paulo, 2021. 4 p.

SIQUEIRA, Dirceu Pereira; WOLOWSKI, Matheus Ribeiro de Oliveira. **INTELIGÊNCIA ARTIFICIAL E O POSITIVISMO JURÍDICO: benefícios e obstáculos para efetivação da justiça**. Rio Grande do Sul, 2022. 18 p.

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 setembro de 2023.