COORDENADORES
SÉRGIO BRANCO
CHIARA DE TEFFÉ

PUBLICAÇÕES 2022

PROTEÇÃO DE DADOS E TECNOLOGIA

Estudos da Pós-Graduação em Direito Digital

CEPED Online
Centro de Estudos e Pesquisas no Ensino do Direito da UERJ
UERJ Universidade do Estado do Rio de Janeiro
ITS

LISTA DE AUTORES

- Amanda Perli Golombiewski
- Ana Paula Vasconcellos da Silva
- Andressa Delmondes Gomes
- Barbara Schelble
- Bruna Veríssimo Lima Santos
- Fábio Pimentel de Carvalho
- Fernanda Alves Corrêa
- Giovanna Bonach Pires Ribeiro
- Júlia de Paula Cople
- Larissa Chen Yi Qian
- Marcelo Batista Gomes da Cruz
- Marcos Vinícius Palomo Pessin
- Rafaela Monteiro Montenegro
- Rafaella Fernandes dos Santos
- Ramon Silva Costa
- Silvia Helena Von Calmbach
- Victor Hugo Lameira da Silva

COORDENADORES:
SÉRGIO BRANCO
CHIARA DE TEFFÉ

PUBLICAÇÕES 2022

PROTEÇÃO DE DADOS E TECNOLOGIA:
Estudos da Pós-Graduação em Direito Digital

Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital

CC Atribuição-NãoComercial-SemDerivações 4.0 Brasil (CC BYNC- ND 4.0 BR)

Texto revisto pelo Acordo Ortográfico de 1990.

Produção editorial
Obliq Livros

Preparação dos originais
ITS Rio

Capa
Obliq Livros

eISBN: 978-85-65404-38-9

Obliq Edição e Produção Ltda.
E-mail: comercial@obliq.com.br
http://obliq.com.br

Para citação:
TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.).
Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq, 2022.

SUMÁRIO

APRESENTAÇÃO

O ano de 2022 trouxe o início de novos projetos e pesquisas, assim como a formação da primeira turma da Pós-Graduação em Direito Digital, conduzida pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) em parceria com a Universidade do Estado do Rio de Janeiro (UERJ). A pluralidade de pensamentos e a diversidade de pessoas envolvidas vêm trazendo reflexões e textos de elevada qualidade acadêmica, o que nos motiva a coordenar iniciativas e publicações com nossos queridos alunos, assistentes acadêmicos e professores.

Na presente obra, foram selecionados 17 artigos de integrantes do programa de Pós-Graduação, os quais abordam diversas questões jurídicas em que a tecnologia e as relações digitais se mostram atuantes. Proteção de dados pessoais, novos modelos de negócios, liberdade de expressão, moderação de conteúdo em plataformas digitais, desinformação, teletrabalho e herança digital são alguns dos interessantes temas tratados na coletânea.

Ainda que o conteúdo aqui exposto não reflita necessariamente a opinião institucional do ITS, ou de seus membros, entendemos ser fundamental oferecer, de forma aberta e livre, trabalhos acadêmicos novos e relevantes ao debate público. Para 2022, esperamos ampliar parcerias e desenvolver mais ações que impactem a sociedade e promovam a educação digital.

Agradecemos a todos que contribuíram e se interessaram por esse projeto.

Rio de Janeiro, 08 de dezembro de 2021.

Os coordenadores[1][2]

[1] Sérgio Branco é cofundador e diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (Uerj). Professor do Ibmec. Professor convidado da Universidade de Montreal. Especialista em propriedade intelectual pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Pós-graduado em cinema documentário pela FGV. Advogado.

[2] Chiara Spadaccini de Teffé é 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), quando foi bolsista de iniciação científica do CNPq e da FAPERJ. Atualmente, é coordenadora de pesquisa e publicações da pós-graduação em Direito Digital do ITS Rio em parceria com a UERJ. Professora de Direito Civil e Direito Digital na Faculdade de Direito do IBMEC-Rio. Leciona em cursos de pós-graduação do CEPED-UERJ, na Pós-graduação da PUC-Rio, na Pós-graduação do Instituto New Law e na Pós-graduação em Advocacia Contratual e Responsabilidade Civil da EBRADI. É também professora da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ) e do Instituto de Tecnologia e Sociedade do Rio (ITS Rio). Membro da Comissão de Proteção de Dados e Privacidade da OABRJ. Membro do Fórum Permanente de Liberdade de Expressão, Liberdades Fundamentais e Democracia 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.

O CONSENTIMENTO DIANTE DAS INTERFACES MALICIOSAS BASEADAS EM VIESES COGNITIVOS

Andressa Delmondes Gomes[3]

INTRODUÇÃO

As últimas décadas foram marcadas por uma intensa alteração no arranjo social, econômico, político e cultural, dando início ao que ficou conhecido como Sociedade da Informação[4]. Nela, os dados passaram a ser um dos principais insumos para as tecnologias, estabelecendo uma verdadeira economia de dados. Se antes o normal era usar a informação no desenvolvimento de novos mecanismos, a lógica nesse novo cenário se inverte: as tecnologias servem como um instrumento para manipular e utilizar a informação.

No contexto do ambiente virtual, muito se fala sobre o excesso de informações e a constante exposição a notícias, publicidades e os mais diversos conteúdos, com o uso de várias estratégias para chamar a atenção dos usuários da internet. Contudo, existe também uma outra realidade que se contrapõe

[3] Consultora em Governança, Risco e Compliance, com ênfase em Privacidade e Proteção de Dados Pessoais. Pós-graduanda em Direito Digital pela Universidade Estadual do Rio de Janeiro (UERJ) em parceria com o Instituto de Tecnologia e Sociedade (ITS Rio). Graduada em Direito pela Universidade de São Paulo (USP).

[4] Sobre isso, ver definição de Manuel Matos: "*A sociedade da informação é uma expressão comumente usada para designar uma forma de organização social, económica e cultural que tem como base, tanto material, quanto simbólica, a informação. Esta sociedade assim organizada seria aquela em que vivemos e, nos termos desta definição, que é de resto inspirada em Castells (1999 para versão francesa, 1998 para o original inglês), a sociedade da informação representa verdadeiramente uma nova sociedade*" (MATOS, Manuel. O que é a sociedade da informação*? Educação, Sociedade & Culturas*, Porto, n. 18, p.7-23, 2002. Disponível em: <https://www.fpce.up.pt/ciie/revistaesc/ESC18/18-1.pdfv>. Acesso em: 21 de nov. 2021, p. 12-13).

a esse movimento, na qual o objetivo é justamente desviar a atenção das pessoas em relação a certos aspectos. Combinada com elementos de *design*, essa outra tendência guia os usuários a tomarem decisões inconscientes ou até mesmo contrárias ao desejado. Isso é conhecido como *dark patterns*, chamadas de interfaces maliciosas no presente artigo[5].

Não é difícil imaginar que muitas dessas manobras utilizadas para influenciar a tomada de decisão dos indivíduos afetam a privacidade e a proteção de dados pessoais, contrariando muitos aspectos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), especialmente no que diz respeito à obtenção do consentimento dos titulares. O uso de interfaces maliciosas pode prejudicar essa autorização em relação ao uso dos dados pessoais, a qual não necessariamente será livre, informada e inequívoca, como a LGPD estabelece que deve ser.

Assim, este artigo tem a pretensão de examinar a questão das interfaces maliciosas perante dois recortes: o uso de vieses cognitivos e a manipulação do consentimento dos titulares de dados. O objetivo é verificar como o paradigma do consentimento é afetado pelas interfaces maliciosas que se utilizam de vieses cognitivos para influenciar as escolhas dos titulares sobre os seus dados pessoais, gerando, na verdade, um paradoxo quanto à essa base legal.

[5] O termo mais comum para o objeto de análise deste artigo é *dark pattern*, o que, em tradução literal, significa padrão escuro. Entretanto, a fim de facilitar a compreensão, optou-se pelo uso da expressão "interfaces maliciosas", tradução proposta por André Lemos e Daniel Marques (Interfaces Maliciosas: estratégias de coleta de dados pessoais em aplicativos. V!RUS, São Carlos, n. 19, 2019. Disponível em: <http://www.nomads.usp.br/virus/virus19/?sec=4&item=2&lang=pt>. Acesso em: 21 de nov. 2021).

Para tanto, em um primeiro momento, será analisado o que é entendido como consentimento válido, dispondo de conceituações trazidas pela própria LGPD, mas também aproveitando análises de como isso é interpretado na Europa, especificamente pelo *European Data Protection Board* (EDPB), que disponibilizou em 2020 diretrizes a respeito da base legal do consentimento para tratamento de dados, em atenção ao Regulamento Geral sobre a Proteção de Dados (RGPD)[6]. Em seguida, será verificado o que e quais são os vieses cognitivos mais comuns de serem usados na internet para manipular as decisões dos usuários. Diante desses elementos, serão mostradas algumas interfaces maliciosas com o uso de vieses cognitivos. E, por fim, serão apresentadas algumas iniciativas que buscam lidar com esse problema.

1. O PARADIGMA E O PARADOXO DO CONSENTIMENTO

Laura Schertel Mendes e Gabriel Campos Soares da Fonseca explicam que o consentimento é muitas vezes entendido como um paradigma quando o assunto é proteção de dados, pois se trata de uma forma de possibilitar maior autonomia ao titular, colocando-o no centro do processo decisório sobre como seus dados serão utilizados. Isso conversa diretamente com o direito fundamental à autodeterminação informativa, segundo o qual o titular tem direito de decidir o que será feito com seus dados[7].

---

[6] EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Versão 1.1. 4 de maio de 2020. Disponível em: < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>. Acesso em: 21 de nov. 2021.

[7] MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de ma-

Por outro lado, os próprios autores mencionam existir diversas limitações para o uso do consentimento[8]. Nesse sentido, há quem entenda que o consentimento válido é de difícil comprovação e fácil de ser manipulado. Isso porque possibilitar um controle muito grande pelo titular pode gerar um paradoxo, como bem observam Régis Chatellier et al em relatório técnico formulado para a autoridade de proteção de dados francesa, *Commission Nationale de l'Informatique et des Libertés* (CNIL)[9], uma vez que o excesso de controle e de possibilidades de escolha pode sobrecarregar os indivíduos, causando o efeito contrário, momento no qual eles não serão capazes de gerenciar suas decisões quanto aos seus dados de maneira complementarmente esclarecida e livre.

Sobre esse tema, a EDPB destaca o seguinte ponto:

> 87. No contexto digital, muitos serviços necessitam de dados pessoais para funcionar, daí que os titulares dos dados recebam diariamente vários pedidos de consentimento que exigem respostas através de cliques ou do deslizar do dedo. Esta situação pode resultar num certo «cansaço» em relação aos cliques: quando aparecem demasiadas vezes, o

terialização. In: MENDES, Laura Schertel; et. al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, p. 73-95, 2021, p. 78.

[8] MENDES; DA FONSECA, op. cit., p. 78-84.

[9] CHATELLIER, Régis et al. Shaping choices in the digital world. From dark patterns to data protection: the influence of UX/UI design on user empowerment. In: Technical Report. CNIL, 2019. Disponível em: < https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdfv>. Acesso em: 21 de nov. 2021, p. 30.

> efeito de alerta dos mecanismos de consentimento começa a diminuir.
>
> 88. Resulta daqui que as questões ligadas ao consentimento começam a deixar de ser lidas. Esta situação constitui um risco particular para os titulares dos dados, uma vez que, tipicamente, o consentimento é solicitado para ações que, em princípio, são ilícitas sem o seu consentimento. O RGPD imputa aos responsáveis pelo tratamento o dever de desenvolver formas de dar resposta a esta questão[10].

O consentimento não pode ser usado como um mecanismo de imputação da responsabilidade inteiramente sobre os titulares, de modo a ocorrer quase que uma renúncia dos agentes de tratamento sobre suas responsabilidades no sentido de garantir a proteção de dados pessoais.

Analisando a situação por essa perspectiva, Bruno Ricardo Bioni e Maria Luciano[11] apresentam a ideia de consentimento como processo. Não se limitando ao mero ato de consentir, o consentimento seria um processo inteiro, cujas fases são representadas pelos adjetivos que servem como requisitos para a sua validade na LGPD: informado, livre e manifesto[12].

---

[10] EUROPEAN DATA PROTECTION BOARD, op. cit., p. 22.

[11] BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; et. al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, p. 149-161, 2021, p. 152-155.

[12] Este artigo não tem como objetivo analisar especificamente a questão da obtenção do consentimento para tratamento de dados sensíveis, tema que poderá ser analisado em estudo posterior.

Tal processo começa com o dever de informação, pois apenas ciente do contexto e condições relativas ao tratamento de seus dados é que o titular consegue dar início à tomada de decisão. Assim, junto à solicitação de consentimento, deve estar explícito o motivo pelo qual os dados estão sendo solicitados, para que eles serão utilizados e quais eventuais consequências surgirão da ausência do consentimento. Todas essas informações compõem os direitos dos titulares e conversam diretamente com o princípio da transparência.

É fundamental fornecer informações aos titulares dos dados antes da obtenção do consentimento para que estes possam tomar decisões informadas, compreendendo com o que estão a concordar e, por exemplo, exercer o direito de retirar o consentimento dado. Se o responsável pelo tratamento não fornecer informações acessíveis, o controlo do utilizador torna-se ilusório e o consentimento será um fundamento inválido para o tratamento[13].

Dando continuidade ao processo, é importante garantir que o consentimento será livre, isto é, o usuário deve poder tomar a decisão de disponibilizar ou não seus dados sem sofrer qualquer retaliação. Aqui entra a discussão se impedir o acesso do usuário a determinado serviço diante da falta de consentimento seria uma violação. Nesse caso, o que deve ser analisado é se os dados solicitados são estritamente necessários para a prestação do serviço. Apenas nessa situação negar o acesso não é uma ofensa à LGPD.

E para finalizar o processo de obtenção válida do consentimento, ele deve se apresentar de maneira inequívoca.

[13] EUROPEAN DATA PROTECTION BOARD, op. cit., p. 17.

Nesta fase, o agente de tratamento precisa demonstrar que houve manifestação de vontade por parte do titular para consentir com o tratamento de seus dados para uma finalidade específica, a qual deve ter sido previamente informada para a tomada de uma decisão verdadeiramente livre. Passadas essas três, só então o aceite do titular pode ser apresentado sem qualquer vício.

Seguindo este formato, há uma valorização da função dos agentes de tratamento, os quais são responsáveis por garantir que cada fase ocorra dentro do esperado para conseguir um aceite válido ao final do processo. E um dos meios de assegurar o sucesso desse processo de obtenção do consentimento é justamente através do *design*.

No entanto, não há como ignorar que da mesma forma que o *design* pode ser usado como uma forma de reforçar os direitos dos titulares de dados, ele também pode servir como um meio de enganá-los:

Design and consent are tied, either positively, when design practices are aimed at improving the ability of individuals to make choices consciously or negatively, when they seek to deceive by abusive or misleading design practices.[14]

Diante desse cenário, a CNIL disponibilizou um estudo relacionando *design* e proteção de dados. No documento a autoridade francesa destaca uma grande preocupação com a transparência e a validade do consentimento dado pelo titular,

[14] Tradução livre: "*Design e consentimento estão relacionados seja de maneira positiva, quando as práticas de design são utilizadas para melhorar a capacidade das pessoas tomarem decisões conscientes, seja negativamente, quando busca-se enganar as pessoas por meio de práticas de design abusivas ou errôneas*". CHATELLIER, op. cit., p. 41.

tendo em vista alguns usos questionáveis do *design*[15]. E um dos pontos levantados é o uso de vieses cognitivos.

2. VIESES COGNITIVOS E SUA INFLUÊNCIA NA TOMADA DE DECISÕES

Alessandro Acquisti et al conceituam vieses cognitivos como erros sistemáticos de julgamento que afetam o modo como uma pessoa realiza decisões racionais, independentemente da complexidade de tal decisão[16]. É certo que nem todos os vieses cognitivos afetam as pessoas de maneira igual, mas ainda assim grande parte das pessoas são influenciadas por esses mecanismos ao usar a internet. Por que essa incidência é tão alta?[17]

Para compreender melhor essa questão, é necessário adentrar no campo da Economia Comportamental que estuda o modo como as informações são processadas nas mentes das pessoas e como isso influencia na tomada de decisões. Uma das vertentes mais famosas é de "heurísticas e vieses", a qual tem como expoentes os autores Amos Tversky e Daniel Kahneman. De acordo com essa vertente, heurísticas são atalhos

[15] CHATELLIER, op. cit., p. 39-41.

[16] ACQUISTI, Alessandro et al. Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), v. 50, n. 3, p. 1-41, 2017. Disponível em: <https://dl.acm.org/doi/10.1145/3054926>. Acesso em: 21 de nov. 2021, p. 6.

[17] BÖSCH, Christoph et al. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proc. Priv. Enhancing Technol., v. 2016, n. 4, p. 237-254, 2016. Disponível em: < https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 21 de nov. 2021. p. 244-245.

cognitivos utilizados para solucionar problemas, contudo, elas podem ser influenciadas por vieses cognitivos[18].

Como Kahneman explica, nosso cérebro atua de duas formas diferentes: (i) uma automática e rápida, tomando decisões intuitivamente, sem controle voluntário daquilo que está sendo definido (Sistema 1), e (ii) outra lenta, usada na tomada de decisões de maneira consciente para atividades mentais que exigem maior esforço, escolha e concentração (Sistema 2)[19]. O processamento de informações por meio do Sistema 1 permite que muitas pessoas sejam enganadas e façam escolhas inconscientes no ambiente virtual.

Dessa forma, o que explica a eficiência dessas estratégias é o fato de que, além de ser automático, o Sistema 1 é usado em situações nas quais as pessoas não possuem motivação suficiente para pensar de forma consciente ou quando não conseguem pensar de maneira consciente e esforçada, por meio do Sistema 2, pois não possuem conhecimento suficiente para tanto[20].

A tabela abaixo contém uma amostragem com alguns vieses cognitivos identificados em pesquisas bibliográficas sobre o tema:

[18] HORTA, Ricardo Lins. Por que existem vieses cognitivos na Tomada de Decisão Judicial? A contribuição da Psicologia e das Neurociências para o debate jurídico. Revista Brasileira de Políticas Públicas, Brasília, v. 9, n. 3 p.83-122, 2019. Disponível em: < https://www.publicacoes.uniceub.br/RBPP/article/view/6089v>. Acesso em: 21 de nov. 2021. p. 93

[19] KAHNEMAN, Daniel. Rápido e devagar: duas formas de pensar. Tradução: Cássio de Arantes Leite. 1ª Ed. Rio de Janeiro: Objetiva, 2012, p. 29.

[20] BÖSCH, op. cit., p. 244-245.

Viés Cognitivo	Definição
Ancoragem	Trata-se da prática de apresentar referenciais ao usuário que, apesar de não necessariamente possuírem alguma relevância no processo, acabam por tendenciar a escolha final.
Enquadramento	Ocorre quando algo é previamente apresentado como bom ou ruim, sem que o usuário possa fazer o seu próprio julgamento e, dessa forma, leva-o a aceitar aquela afirmação sem partir de uma reflexão mais profunda sobre o tema.
Efeito padrão	Tendência do usuário em manter uma opção previamente apresentada a ele, permanecendo na inércia.
Desconto hiperbólico	É dada maior ênfase no benefício imediato que o usuário pode vir a ter ao compartilhar seus dados, sem apresentar ou dar indícios dos potenciais malefícios de médio ou longo prazo.
Excesso de opções	Maneira quantitativa de manipular a percepção do usuário. Ao dar muitas opções de escolhas, o usuário se cansa de refletir sobre elas e acaba decidindo pela opção mais fácil.
Processos metacognitivos	Assemelham-se ao excesso de opções, com a diferença que neste caso a dificuldade não é quantitativa e sim qualitativa: o usuário se vê diante de uma decisão difícil, que necessitaria de uma maior reflexão, mas devido à essa dificuldade ele é levado a escolher uma opção mais fácil e irrefletida.
Viés da escassez	Por meio dele, o usuário tende a fazer uma escolha por acreditar que está perante algo escasso e que está prestes a acabar.

Fonte: Elaborada pela Autora com base em pesquisas bibliográficas[21][22]

[21] WALDMAN, Ari Ezra. Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology, v. 31, p. 105-109, 2020, Disponível em: < https://www.sciencedirect.com/science/article/pii/S2352250X19301484>. Acesso em : 21 de nov. 2021. p. 106-107.

[22] MATHUR, Arunesh et al. Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer

O uso desses vieses de maneira proposital e combinados com técnicas de *design* caracteriza as interfaces maliciosas que são objeto de estudo deste artigo. O capítulo seguinte apresentará o seu conceito e alguns exemplos de como esses elementos juntos representam ofensas à legislação sobre dados pessoais.

3 O USO DAS INTERFACES MALICIOSAS

As interfaces maliciosas foram conceituadas pela primeira vez em 2010 por Harry Brignull, especialista em experiência do usuário e doutor em ciência cognitiva[23]. Elas usam do *design* para influenciar a tomada de decisão das pessoas, muitas vezes contando com outros elementos, como os vieses cognitivos, para tanto. Elas não podem ser confundidas com meros *designs* malfeitos, pois um elemento essencial da sua definição é a intenção de manipular a percepção e, consequentemente, a atuação do usuário.

Christoph Bösch et al[24] fazem um interessante paralelo entre padrões de privacidade, ou seja, padrões que guiam para a máxima proteção aos dados dos titulares, com as características

Interaction, v. 3, n. CSCW, p. 1-32, 2019. Disponnível em: <https://dl.acm.org/doi/abs/10.1145/3359183>. Acesso em: 21 de nov. 2021, p. 6.

[23] Brignull mantém um site sobre o tema qual são listados os doze principais tipos de interfaces maliciosas mais comuns (os quais ele chama de *trick questions*, *sneak into basket*, *roach motel*, *privacy zuckering*, *price comparison prevention*, *misdirection*, *hidden costs*, *bait and switch*, *confirmshaming*, *disguised ads*, *forced continuity* e *friend spam*) e um "mural da vergonha", contendo exemplos de interfaces maliciosas publicadas por usuários do Twitter. Sobre o tema, ver: <https://www.darkpatterns.orgv>. Acesso em: 21 de nov. 2021.

[24] BÖSCH, op. cit., p. 241-243.

das interfaces maliciosas. Segundo os autores, os padrões de privacidade se atentam a oito estratégias: minimizar, esconder, separar, agregar, informar, controlar, impor e demonstrar. Em contraste a essas oito boas práticas, existem oito atributos típicos das interfaces maliciosas: maximizar, publicar, centralizar, preservar, obscurecer, negar, violar e fingir.

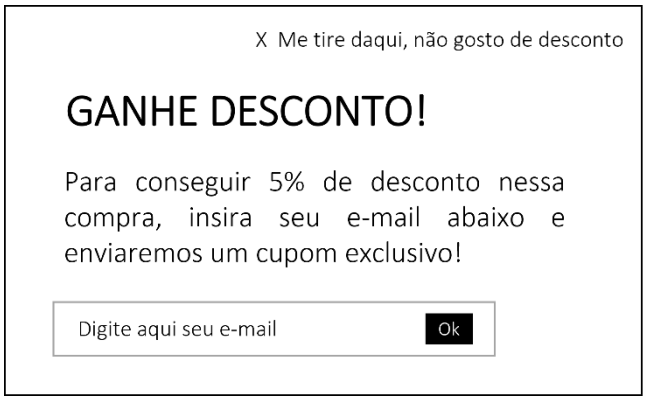
Como será visto, com o intuito principalmente de maximizar a coleta de dados e de preservar aqueles já obtidos, os agentes de tratamento podem tornar o processo de obtenção de consentimento menos transparente, utilizando da negação e do fingimento para atingir seus objetivos. Diante da evidente violação aos direitos dos titulares que motiva esses agentes, eles se valem desses esforços para obscurecer o processo.

A seguir, algumas dessas interfaces serão apresentadas e como elas se relacionam com os conceitos vistos até o momento.

3.1. CONFIRME A VERGONHA (*CONFIRMSHAMING*)[25]

Trata-se de um padrão de interface que tenta manipular a escolha do usuário por meio do uso de linguagem cuja finalidade é depreciar determinada escolha, de modo a dissuadi-lo a tomar uma decisão que, muitas vezes, seria mais protetiva de seus dados.

[25] MATHUR, op. cit., p. 16-17.



Fonte: Autora[26]

No exemplo acima, para não compartilhar seu e-mail, o usuário precisa fechar a janela que vem acompanhada da mensagem "Me tire daqui, não gosto de desconto". Como é possível observar, o Confirme a Vergonha se utiliza do viés cognitivo do enquadramento, ou seja, cria um juízo de valor sobre uma possível escolha do indivíduo de modo a influenciar a sua decisão sobre compartilhar ou não os dados.

3.2. INTERFERÊNCIA VISUAL (*VISUAL INTERFERENCE*)[27]

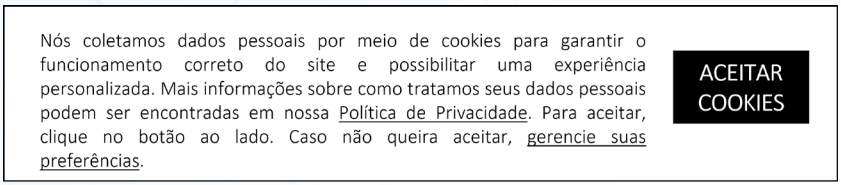
Quando há o uso de elementos visuais para direcionar a escolha do usuário. Isso pode ocorrer por meio do destaque dos botões que o agente de tratamento quer que o titular clique e o mascaramento de botões que levam o usuário a fazer uma escolha distinta. Há nessa situação a manipulação

[26] Todas as figuras deste artigo foram criadas pela Autora, mas baseadas em interfaces maliciosas reais observadas em diferentes sites.

[27] MATHUR, op. cit., p. 17.

por meio de cores, formas, fontes, dentre outros elementos visuais.

Tal prática é bastante comum em barras de *cookies*, por exemplo. Mesmo quando elas apresentam uma opção de personalizar ou não aceitar os *cookies*, isso costuma vir disfarçado, enquanto há um maior destaque para a opção de aceitá-los:



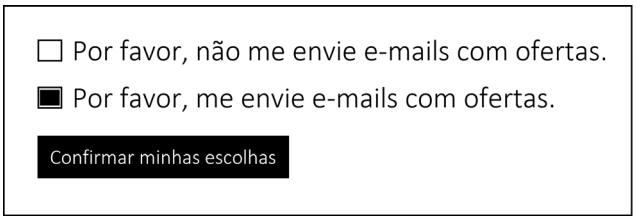
Fonte: Autora

Esse tipo de interface pode se utilizar de dois vieses cognitivos: (i) a ancoragem, pois apresenta ao usuário com mais destaque a opção que quer ser escolhida, e (ii) o enquadramento, pois pode dar uma conotação positiva àquilo que deseja ser aceito pelo titular.

3.3. PERGUNTAS CONFUSAS (*TRICK QUESTIONS*)[28]

São questões formuladas de modo ambíguo ou complicado a fim de direcionar o usuário a fazer uma escolha que provavelmente não faria se não houvesse sem essa interferência. São usadas estratégias linguísticas de modo a dificultar a completa compreensão do titular como, por exemplo, duplos negativos, uso de termos técnicos de difícil compreensão por pessoas não especializadas no assunto, dentre outros.

[28] MATHUR, op. cit., p. 17.



Fonte: Autora

Nesse caso, os principais vieses cognitivos são o efeito padrão, quando a opção mais onerosa no que tange ao compartilhamento de dados vem pré-selecionada, e o excesso de opções, já que mais de uma frase é apresentada para a mesma finalidade: aceitar ou não o recebimento de e-mails com ofertas.

***

Esse tipo de *design* que busca manipular os usuários por meio de vieses cognitivos é abusivo[29]. Entretanto, para além da abusividade, ao macularem o processo de obtenção de consentimento do titular impedindo que ele seja informado, livre e manifesto, o uso dessas interfaces torna o tratamento de dados ilícito e, consequentemente, inválido.

Isso vai de acordo com o entendimento do EDPB:

(...) qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.[30]

[29] CHATELLIER, op. cit., p. 27.

[30] EUROPEAN DATA PROTECTION BOARD, op. cit., p. 8.

Dessa forma, não restam dúvidas de que as interfaces maliciosas, valendo-se de vieses cognitivos, têm um potencial de prejudicar o consentimento válido por parte do titular dos dados e este é um problema que precisa ser endereçado quando o assunto é a privacidade e a proteção de dados.

A seguir serão descritas algumas iniciativas no sentido de resolver esse problema.

4. ALGUMAS POSSÍVEIS ABORDAGENS DA PROBLEMÁTICA

O tema das interfaces maliciosas não é novidade e já possui algumas discussões a seu respeito tanto no setor público quanto no privado, especialmente em países que já se encontram mais avançados quando o assunto é privacidade e proteção de dados.

Uma das formas de lidar com a problemática do uso de interfaces maliciosas é por meio da regulamentação. Em março de 2021, o tema recebeu atenção na Califórnia e as interfaces maliciosas foram banidas. Na regulamentação, foram apresentados exemplos de situações proibidas que se utilizam dessa prática: (i) usar linguagem confusa, como os duplo-negativos, (ii) apresentar ao usuário uma série de razões pelas quais ele não deve se descadastrar de um processo, antes de, de fato, oferecer a opção de descadastro, (iii) obrigar o usuário a acessar uma política de privacidade para encontrar a opção de se descadastrar, (iv) estabelecer para o descadastro uma quantidade de cliques muito superior em relação à quantidade de cliques para se cadastrar, (v) exigir

que o titular dê mais dados pessoais a fim de possibilitar o descadastro[31] [32].

Nesse sentido, a *Federal Trade Commission* (FTC) – agência governamental dos Estados Unidos que tem como objetivo proteger os consumidores e a concorrência – divulgou em outubro de 2021 uma política a respeito do uso de interfaces maliciosas que visam enganar os consumidores a se inscreverem ou continuarem inscritos em serviços de assinatura. Segundo a agência, para agir adequadamente as empresas devem se atentar a três pontos: (i) fornecer informações claras e visíveis sobre as assinaturas, (ii) obter o consentimento expresso e informado do consumidor, e (iii) possibilitar cancelamento facilitado dos serviços[33].

A CNIL, por sua vez, destaca a necessidade de uma regulamentação de uma perspectiva não apenas jurídica de como o *design* deve ser usado, mas que envolva também aspectos técnicos, com a participação de *designers* e especialistas em psicologia nesse debate, entendendo que eles atuam como

[31] VICENT, James. California bans 'dark patterns' that trick users into giving away their personal data. The Verge, 16 de mar. de 2021. Disponível em: <https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data>. Acesso em: 21 de nov. de 2021.

[32] MERKEL, Jeremy. Dark Patterns Come to Light in California Data Privacy Laws. The National Law Review, vol. XI, n. 183, 02 de jul. de 2021. Disponível em: < https://www.natlawreview.com/article/dark-patterns-come-to-light-california-data-privacy-laws>. Acesso em: 21 de nov. de 2021.

[33] FEDERAL TRADE COMMISSION. FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions. 28 de out. 2021. Disponível em: < https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap>. Acesso em: 22 de nov. 2021.

"arquitetos de escolhas" nesse contexto e reconhecendo que são capazes de determinar como o indivíduo poderá exercer seu poder de decisão[34]:

Regulators and legislators therefore need to immediately build a rigorous analysis grid of architectures of choice and of their consequences on individuals and on society, in an ethical and political approach that goes beyond both a purely legal and a simply instrumental approach to design[35].

Outra opção de como lidar com essa questão é por meio da conscientização e do estímulo à discussão por parte da sociedade, pois, uma vez que as pessoas tenham consciência do uso desses mecanismos para influenciar suas decisões, mais atentas ficarão quando se depararem com situações como essas[36].

Por fim, é possível uma atuação de iniciativa por parte dos próprios *designers*. Da mesma forma que existe um leque de interfaces maliciosas as quais podem ser – e são – replicadas em diversos ambientes virtuais, seria interessante uma iniciativa de profissionais que atuam na área para apresentar recomendações com padrões de boas interfaces, uma vez que há uma infinidade de possibilidades quando o assunto

[34] CHATELLIER, op. cit., p. 41-42.

[35] Tradução livre: "*Os reguladores e legisladores, portanto, precisam construir imediatamente uma grade de análise rigorosa das arquiteturas de escolha e de suas consequências para os indivíduos e para a sociedade, em uma abordagem ética e política que vai além de uma abordagem puramente legal e simplesmente instrumental do design*". CHATELLIER, op. cit., p. 41.

[36] CHATELLIER, op. cit., p. 45.

é usar elementos gráficos e cognitivos para atender o melhor interesse dos titulares de dados e sua privacidade.

CONCLUSÃO

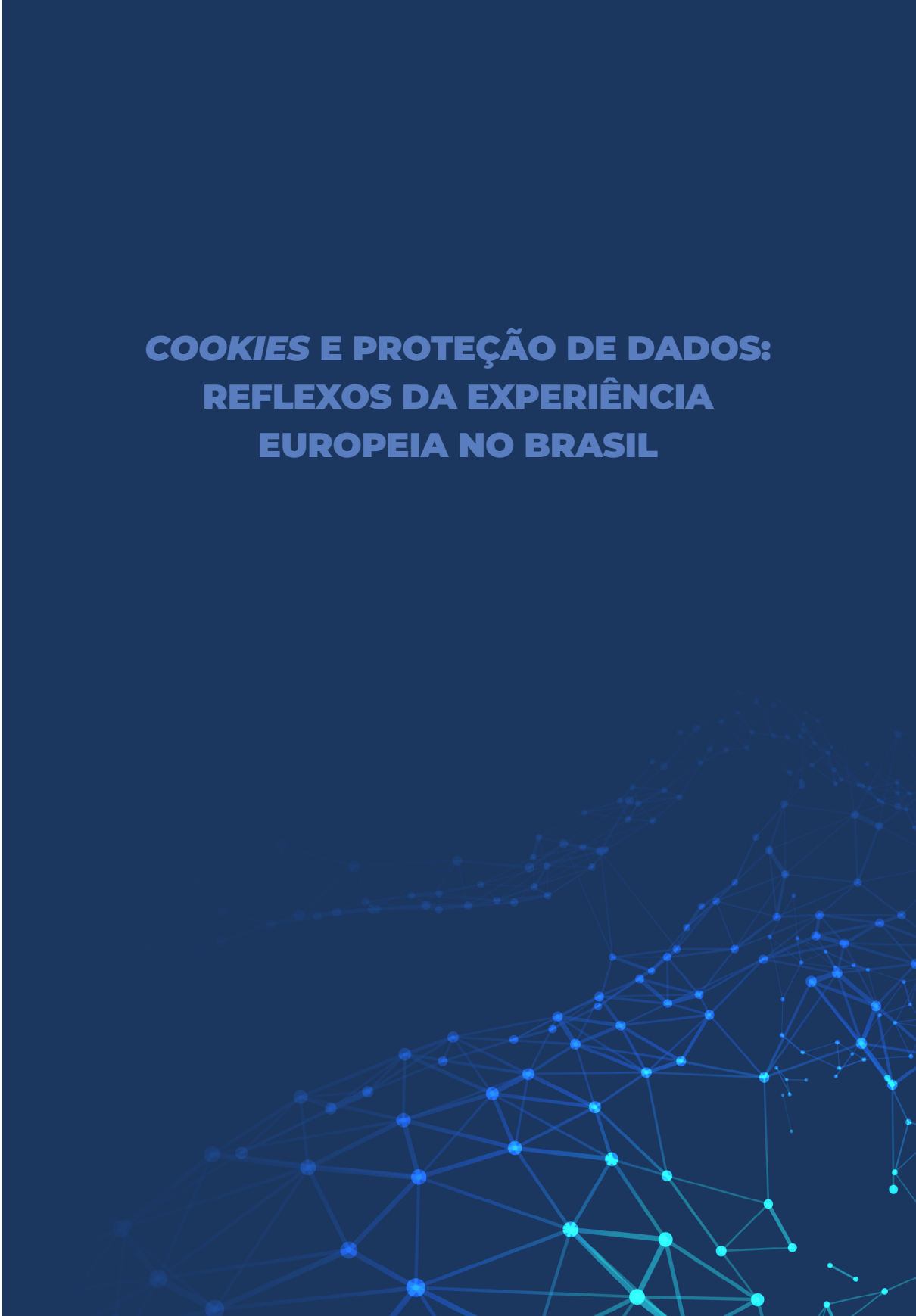
O presente artigo buscou analisar o uso de interfaces maliciosas que, por meio de vieses cognitivos, manipulam a tomada de decisão por parte dos titulares de dados de modo a possibilitar a obtenção do consentimento.

É importante destacar que, tratando-se de uma seara que ainda pode ser muito explorada, os elementos aqui trazidos não foram exaustivos sobre o tema, mas sim exemplificativos. As interfaces maliciosas aqui mencionadas foram identificadas por meio de pesquisa bibliográfica e não foi realizada qualquer pesquisa quantitativa para entender qual o grau de predominância que cada uma delas representa nos ambientes virtuais, de modo que não traduzem a totalidade de interfaces possíveis.

Como demonstrado, esse tipo de prática não se atenta aos requisitos estabelecidos pela LGPD para garantir a validade do consentimento. Assim, além de ser considerada abusiva, ela torna o tratamento dos dados ilícito. Esse é um problema bastante atual e recorrente, e já existem algumas iniciativas – principalmente internacionais – para atenuá-lo, seja por meio do Poder Público, com a regulamentação, ou até mesmo iniciativas da sociedade civil e do setor privado, com a conscientização sobre o tema valorizando o direito fundamental de autodeterminação informativa do titular.

O fato é que há uma intrínseca relação entre *design* e consentimento, mas ela não deve ser observada apenas por um prisma negativo de impossibilidade de convivência pacífica de um com outro. Da mesma forma que podem ser extraídas situações ruins dessa relação – como é o caso das interfaces maliciosas –, também é possível a criação de boas experiências, nas quais o *design* pode ser um aliado valioso no trabalho por um uso mais consciente e adequado dos dados pessoais. E essas iniciativas positivas que devem ser o objetivo.

COOKIES E PROTEÇÃO DE DADOS: REFLEXOS DA EXPERIÊNCIA EUROPEIA NO BRASIL



Marcos Vinícius P. Pessin [37]

INTRODUÇÃO

Com a vigência[38] da Lei n.º 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), os *cookies* tornaram-se cada vez mais populares entre os usuários de internet no Brasil, os quais passaram a ser impactados frequentemente com avisos sobre o uso dessa tecnologia logo após acessarem *sites* destinados ao público brasileiro.

Os *cookies*, no entanto, não são uma novidade tecnológica, já que sua origem remonta ao ano de 1994, quando foi criado como uma solução para um problema técnico envolvendo a impossibilidade de os *sites* armazenarem informações da navegação de usuários[39], o que inviabilizava, por exemplo, a existência de funcionalidades básicas da atualidade, como permanecer autenticado em um *e-mail* ou incluir diversos produtos em um carrinho de compras de um *e-commerce*.

Antes de tal tecnologia, não havia o conceito de sessão de navegação em um *site*, ou seja, a cada novo clique para uma página diferente, toda informação anterior sobre a navegação

[37] Bacharel pela Faculdade de Direito da Universidade de São Paulo (USP). Pós-graduando em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ/ITS/CEPED). Advogado.

[38] A LGPD entrou em vigor em 18 de setembro de 2020, exceto quanto aos seus artigos 52, 53 e 54, referentes às suas sanções administrativas, vigentes desde 1º de agosto de 2021.

[39] SCHWARTZ, John. Giving the Web a memory cost its users privacy. *New York Times*, 2001. Disponível em: http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html. Acesso em: 20 nov. 2021.

era perdida[40]. No contexto do carrinho de compras de um *e-commerce*, por exemplo, a cada clique em um novo produto a informação referente ao clique anterior não era armazenada, impossibilitando aos usuários escolherem diversos produtos em um mesmo acesso ao *site*.

Embora não seja uma tecnologia recente, os *cookies* ainda são atuais, sendo utilizados de modo amplo pelos principais *sites* de empresas e entes do poder público ao redor do mundo, inclusive no Brasil, onde muitos usuários de internet só tiveram contato com o termo "*cookies*" após a vigência da LGPD.

As finalidades do uso da referida tecnologia, entretanto, passaram a ser múltiplas desde sua criação para tal problema técnico, quase sempre baseadas no rastreamento constante das atividades de navegação de usuários na internet.

Ao navegar na internet para ouvir música, ver vídeos, realizar uma compra ou ler notícias, as empresas responsáveis pelos *sites* acessados para tais finalidades, bem como eventuais terceiros autorizados por elas, provavelmente estão rastreando essa navegação por meio dos *cookies*, o que inclui saber onde o usuário clicou, por quanto tempo permaneceu nos *sites* visitados, qual navegador e dispositivo eletrônico está usando, dentre diversas outras informações.

Os *cookies* também permitem, portanto, o monitoramento das atividades de usuários na internet e, por isso, são classifi-

[40] SCHWARTZ, John. Giving the Web a memory cost its users privacy. ***New York Times***, 2001. Disponível em: http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html. Acesso em: 20 nov. 2021.

cados como tecnologias de rastreamento, as quais, inclusive, multiplicaram-se com o crescimento exponencial da internet[41].

Desse modo, tendo em vista o recente impacto de tal tecnologia na experiência dos usuários de *sites* destinados ao público brasileiro e a relevância do tema para a proteção de dados pessoais, este artigo propõe-se a abordar os principais reflexos da experiência do modelo regulatório europeu no uso de *cookies* no Brasil, a partir de uma análise teórica e prática, de acordo com a legislação brasileira e europeia, com a ressalva de que há muito a ser compreendido com a aplicação e a interpretação da LGPD pelos órgãos de fiscalização no Brasil, em especial pela Autoridade Nacional de Proteção (ANPD).

1. COOKIES

Os *cookies* são pequenos arquivos de texto que podem ser enviados por um *site* e armazenados no dispositivo eletrônico do seu usuário. A cada nova página acessada durante a navegação neste *site* ou em um acesso futuro após fechar o navegador, os *cookies* armazenados anteriormente são identificados e analisados pelo mesmo *site*, o que permite a utilização desta tecnologia para diversas finalidades relacionadas às informações de navegação do usuário.[42]

[41] Além dos ***cookies***, há outras tecnologias de rastreamento, como ***web beacons***, ***tracking pixels***, ***flash cookies*** e ***fingerprinting***, as quais, embora também ofereçam riscos à privacidade e à proteção de dados dos usuários de internet, não serão objeto deste artigo.

[42] KRISTOL, David M. HTTP Cookies: Standards, privacy, and politics. ***ACM Transactions on Internet Technology (TOIT)***, v. 1, n. 2, p. 151-198, 2001, p. 154.

Apesar de conhecidos apenas como *cookies*, estes possuem uma diversidade ampla de espécies e recebem classificações relevantes para entendê-los, as quais são, inclusive, utilizadas nas políticas de privacidade de diversos *sites*.

Quanto ao período de duração no dispositivo do usuário, os *cookies* podem ser de sessão ou permanentes. Os primeiros não possuem data de validade, pois são automaticamente excluídos do dispositivo eletrônico do usuário quando o navegador é fechado. Estes *cookies* são utilizados, por exemplo, para manter um usuário conectado ao seu *e-mail* enquanto utiliza o navegador, exigindo uma nova autenticação após este ser fechado. Os permanentes, por sua vez, possuem prazo de validade para serem eliminados do dispositivo eletrônico do usuário e podem durar horas, dias, meses ou até anos, sendo utilizados, a título de exemplo, para saber a preferência de idioma do usuário de um *site*, de modo a dispensá-lo de configurar o idioma toda vez que o acessar, inclusive após ter fechado o navegador.[43]

Já em relação a quem é responsável pelos *cookies* enviados ao dispositivo do usuário e tem acesso aos dados coletados por meio deles, esses pequenos arquivos de texto podem ser primários (*first-party cookies*) ou de terceiros (*third-party cookies*). Os primeiros são de responsabilidade do próprio *site* que o usuário está acessando, enquanto os de terceiros são aqueles de responsabilidade de *sites* diferentes do acessado pelo usuário, como de redes sociais ou de empresas de publicidade parceiras do *site*.[44]

---

[43] KOCH, Richie. Cookies, the GDPR, and the ePrivacy Directive. *GDPR.EU*. Disponível em: https://gdpr.eu/cookies/. Acesso em: 20 nov. 2021.

[44] KOCH, Richie. Cookies, the GDPR, and the ePrivacy Directive. *GDPR.EU*. Disponível em: https://gdpr.eu/cookies/. Acesso em: 26 nov. 2021.

Não obstante os riscos à proteção de dados relacionados aos *cookies* primários, os de terceiros destacam-se, porque não são enviados pelo *site* acessado pelo usuário, mas por terceiros associados ao *site*, os quais, em geral, estão fora da expectativa dos usuários. Nesse sentido, em virtude de os *cookies* de terceiros serem considerados invasivos, o Google prevê o bloqueio dessa tecnologia em seu navegador Google Chrome até 2023[45], seguindo a postura dos navegadores Safari e Firefox, que já adotaram tal medida[46].

Por fim, os *cookies* também são classificados de acordo com a sua função em necessários ou opcionais, sendo talvez esta a forma mais popular na atualidade. *Cookies* necessários são os essenciais para o funcionamento do *site*, sem os quais este pode deixar de funcionar corretamente, como os responsáveis por permitir a autenticação de usuários nas contas de *e-mail* ou a seleção de diversos produtos para o carrinho de compras em sites de *e-commerce*. Por outro lado, os cookies opcionais são todos os outros utilizados para as demais finalidades, como para fins de performance (coletam informações sobre como o *site* é utilizado pelo usuário, permitindo identificar quais as páginas mais acessadas), funcionalidade (guardam informações sobre eventuais preferências do usuário, como idioma) e publicidade (coletam dados específicos para criação de perfil do usuário, o que permite a veiculação específica

[45] GOEL, Vinay. An updated timeline for Privacy Sandbox milestones. ***Google: The Keyword***. Disponível: https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/v. Acesso em: 20 nov. 2021.

[46] WATERS, Richard. Google delays plan to phase out third-party cookies by 2 years. ***Financial Times***. Disponível em: https://www.ft.com/content/b42db1db-8cfd-4247-90f5-3c6f934b5b3d. Acesso em: 20 nov. 2021.

de determinado conteúdo publicitário para aquele usuário, conforme seus gostos e preferências)[47].

Exceto quando as informações coletadas forem anonimizadas, como pode ocorrer com *cookies* de performance, cujo propósito é capaz de ser atendido com dados estatísticos, os *cookies* são considerados dados pessoais, pois identificam ou permitem identificar uma determinada pessoa natural por meio das informações vinculadas a eles[48] e, por isso, estão sujeitos às leis de proteção de dados, inclusive as do Brasil, como a LGPD.

Inspirada na experiência europeia sobre proteção de dados, mais especificamente no Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* – EU 2016/679 - GDPR)[49], a LGPD resultou em efeitos práticos e aparentes em relação aos *cookies* no Brasil, uma vez que, desde sua vigência, os usuários de internet passaram a ser impactados com avisos solicitando o consentimento para a utilização dessa tecnologia.

A mudança recente pelos *sites* voltados para brasileiros, no entanto, apresenta algumas contradições derivadas dos reflexos da experiência europeia sobre o tema no Brasil, sendo necessário compreender o que motivou a maioria deles a

[47] KOCH, Richie. Cookies, the GDPR, and the ePrivacy Directive. *GDPR.EU*. Disponível em: https://gdpr.eu/cookies/. Acesso em: 20 nov. 2021.

[48] Conforme art. 5º, inc. I, LGPD.

[49] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.* Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 20 nov. 2021.

adotarem essa postura para os tratamentos de dados pessoais via *cookies*.

2. COOKIES NA REGULAÇÃO EUROPEIA

No âmbito da União Europeia, a utilização de *cookies* é regulada pela Diretiva 2002/58/CE, também chamada de e*Privacy Directive*, a qual foi instituída com o objetivo de definir regras específicas para a proteção da privacidade nas comunicações eletrônicas, sendo aplicável às redes de comunicação públicas.[50]

Em 2009, a *ePrivacy Directive* foi alterada pela Diretiva 2009/136/EC, conhecida como *Cookie Directive*, tendo em vista seu impacto na regulação do uso desta tecnologia ao exigir o consentimento do usuário para o envio e armazenamento de *cookies* em seus dispositivos eletrônicos (art. 5(3), *ePrivacy Directive*). [51]

Embora tenha instituído o consentimento do usuário como necessário para o armazenamento de *cookies*, o texto alterado da *ePrivacy Directive* não dispôs sobre os requisitos para a obtenção de tal autorização, o que só ocorreu em 2018 com a vigência do GDRP.

Além disso, a *ePrivacy Directive* também prevê uma exceção ao consentimento para os *cookies* necessários, isto é, aque-

[50] UNIÃO *EUROPEIA. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002.* Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=ENv. Acesso em: 20 nov. 2021.

[51] UNIÃO EUROPEIA. *Diretiva 2009/136/CE do Parlamento Europeu e do Conselho*, de 25 de Novembro de 2009. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN. Acesso em: 20 nov. 2021.

les utilizados para a prestação dos serviços solicitados pelos usuários ou quando forem exigidos para a transmissão de uma comunicação pela internet (art. 5(3), *ePrivacy Directive*).

Em razão da alteração legislativa da *ePrivacy Directive*, grande parte dos *sites* da União Europeia começaram a utilizar os *cookies banners*, também conhecidos no Brasil como avisos ou barras de *cookies*, por meio dos quais os usuários são informados sobre a utilização de *cookies* e têm seu consentimento solicitado.

O Grupo de Trabalho do Artigo 29º para Proteção de Dados *(Article 29 Data Protection Working Party – WP29)*, em 2012, emitiu a *Opinion* nº 4/2012 sobre as exceções do consentimento para os *cookies*, na qual indicou algumas situações de dispensa para os *cookies* necessários, como aqueles utilizados para a prestação dos serviços oferecidos pelo *site,* e de funcionalidades, que armazenam as preferências do usuário, como o idioma para o *site* ser exibido.[52]

No ano seguinte, o *WP 29* emitiu o *Working Document* nº 2/2013, prevendo diretrizes para a obtenção do consentimento para *cookies*. Neste cenário anterior ao GDPR, o documento trouxe parâmetros para o consentimento, o qual deve ser: (i) específico (informações completas sobre a finalidade); (ii) prévio (obtido antes do armazenamento dos *cookies*); (iii) inequívoco (obtido por meio de uma ação ativa do usuário que

[52] ARTICLE 29 DATA PROTECTION WORKING PARTY. ***Opinion 04/2012 on Cookie Consent Exemption***. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf. Acesso em: 20 nov. 2021.

não deixe dúvidas sobre a intenção); e (iv) livre (resultado de uma escolha real do usuário). [53]

De acordo com o Comitê Europeu de Proteção de Dados (*European Data Protection Board* – EDPB), substituto do WP 29 desde 2018, em sua *Opinion* nº 5/2019, apesar da entrada em vigor do GPDR prevendo outras bases legais para o tratamento de dados pessoais, as disposições referentes aos *cookies* da *ePrivacy Directive* continuam sendo aplicáveis e prevalecem em relação ao GDPR sobre este tema, pois se trata de um normativo específico sobre o assunto, sendo o consentimento, portanto, obrigatório, salvo nas exceções previstas na própria *ePrivacy Directive*. [54]

A experiência europeia sobre *cookies* resultou em precedentes, sendo o *Case C-673/17*, conhecido como *Planet* 49, julgado pelo Tribunal de Justiça da União Europeia (*European Court of Justice* – ECJ)[55], relevante para a compreensão das práticas esperadas para os *sites* estarem em conformidade com os requisitos do consentimento no âmbito da União Europeia.

---

[53] ARTICLE 29 DATA PROTECTION WORKING PARTY. ***Working Document 02/2013 providing guidance on obtaining consent for cookies***. Disponível: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf. Acesso em: 20 nov. 2021.

[54] EUROPEAN DATA PROTECTION BOARD. ***Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities***. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf. Acesso em: 20 nov. 2021.

[55] EUROPEAN COURT OF JUSTICE. ***Judgment of the Court of 1 October 2019, Case C-673/17, ECLI:EU:C:2019:801***. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0673&from=EN. Acesso em: 20 nov. 2021.

A empresa alemã de jogos *online "Planet GmbH"* adotou em um formulário de inscrição de seu *site* uma caixa de seleção já assinalada, a qual autorizava o tratamento de dados por meio de *cookies* e era opcional, isto é, o usuário poderia concluir o formulário normalmente se resolvesse desassinalar tal caixa.

Em 2014, a Federação das Centrais de Defesa do Consumidor (*Verfahren des Verbraucherzentrale Bundesverfahrens* - VZBV) ajuizou uma demanda judicial contra a *Planet49*, com base no não atendimento aos requisitos do consentimento para o armazenamento de *cookies* nos dispositivos eletrônicos dos indivíduos.

Com o andamento do processo na Alemanha, o caso alcançou o ECJ para *preliminary ruling* em 2019, o qual decidiu que (i) as caixas de seleção assinaladas previamente para autorizar o uso de *cookies* não constituem consentimento válido; (ii) quando o consentimento for necessário para *cookies* nos termos da *ePrivacy Directive*, aplicam-se os requisitos do consentimento do art. 4(11) do GDPR: manifestação de vontade livre, informada e inequívoca; (iii) a *ePrivacy Directive* aplica-se a qualquer informação instalada ou acessada no dispositivo eletrônico de um usuário, como *cookies*, independente de ser dado pessoal ou não; (iv) os usuários devem ser informados sobre a duração do armazenamento dos *cookies* em seus dispositivos, bem como se terceiros terão acesso a eles.[56]

A decisão consolidou entendimentos já esperados após a vigência do GDPR, como a invalidade do consentimento

[56] EUROPEAN COURT OF JUSTICE. *Judgment of the Court of 1 October 2019, Case C-673/17, ECLI:EU:C:2019:801*. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62017CJ0673&from=EN. Acesso em: 20 nov. 2021.

implícito – selecionado previamente – para *cookies* opcionais dos *sites*, o que inclusive já está previsto como exemplo no Considerando n.º 32 do GDPR.

Em 2020, o EDPB emitiu uma atualização[57] das *Guidelines 05/2020* para consentimento do GDPR, na qual abordou especificamente duas questões sobre a validade do consentimento do usuário para *cookies*, como quando: (i) o acesso ao serviço ou funcionalidade de um *site* é condicionado ao consentimento, utilizando-se a famosa "*cookie wall*"; (ii) o consentimento é considerado obtido mediante a ação de rolagem da barra do navegador em um *site*.[58]

De acordo com o EDPB, quanto à primeira situação, o acesso a serviços e funcionalidades de um *site* não deve ser condicionado ao consentimento de um usuário para o armazenamento de informações ou a coleta das já armazenadas em seu dispositivo eletrônico. Tal prática é chamada de "*cookie wall*" e resulta em consentimento inválido, pois deixa de ser uma escolha real do usuário e, portanto, livre. [59]

Em relação ao segundo caso, por sua vez, haveria violação do requisito de manifestação inequívoca do consentimento, a qual requer uma ação afirmativa clara e distinguível de outras

[57] A atualização teve como base as diretrizes publicadas pelo seu antecessor, o *WP29*, as quais já tinham sido endossadas pelo EDPB em 2018.

[58] EUROPEAN DATA PROTECTION BOARD. *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.pdfv. Acesso em: 20 nov. 2021.

[59] EUROPEAN DATA PROTECTION BOARD. *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: 20 nov. 2021.

ações, conforme o Considerando 32 do GDPR. Logo, um *site* não pode concluir que o usuário consentiu com os *cookies* apenas porque rolou a barra do navegador ou quaisquer outras atividades similares, porque não se trata de uma ação claramente distinguível de outras que o usuário possa ter ao acessar o *site*.

Ainda sobre "*cookie wall",* em 2019, seguindo recomendação do EDPB em *Statement* de 2018[60], a *Commission Nationale de l'Informatique et des Libertés* (CNIL), autoridade de proteção de dados da França, vedou tal prática em suas *Guidelines* sobre *Cookies*. No entanto, em 2020, o Conselho de Estado (*Conseil d'*État) francês anulou essas disposições que proibiam de forma geral e absoluta a prática de "*cookie walls*", considerando que a mencionada vedação não seria possível por meio de *guidelines,* que são instrumentos de "*soft law*". [61] No mesmo ano, a CNIL atendeu à decisão do Conselho de Estado e atualizou suas *Guidelines* sobre *cookies*[62].

A necessidade de atualização de tais *Guidelines* pela CNIL evidencia que esses instrumentos não possuem status de lei,

---

[60] EUROPEAN DATA PROTECTION BOARD. *Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications*. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf. Acesso em 20 nov. 2021.

[61] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Cookies and other tracking devices*: the Council of State issues its decision on the CNIL guidelines. Disponível em: http://www.cnil.fr/en/cookies-and-other--tracking-devices-council-state-issues-its-decision-cnil-guidelinesv. Acesso em: 20 nov. 2021.

[62] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Cookies et autres traceurs*: la CNIL publie des lignes directrices modificatives et sa recommandation. Disponível em: http://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandationv. Acesso em: 20 nov. 2021.

inclusive quando publicados pelo EDPB, o que pode resultar em outras abordagens sobre "*cookie wall*" em cada Estado-membro da União Europeia[63].

Nesse sentido, os *sites* destinados ao público europeu buscaram adequar suas práticas relacionadas aos *cookies* com base nas experiências do seu modelo regulatório, o qual passou a exigir o consentimento para *cookies* opcionais com a *ePrivacy Directive* e vem evoluindo desde então com a interpretação pelas entidades competentes no âmbito da União Europeia e de cada um de seus Estados-membros.

A popularização dos avisos ou das barras de *cookies* nesses *sites*, portanto, decorre do cumprimento da regulação europeia, sendo uma solução desenhada para informar e obter o consentimento dos usuários logo após o acesso ao *site*.

3. REGULAÇÃO DE COOKIES NO BRASIL

Não há no ordenamento jurídico brasileiro nenhuma regulação específica sobre *cookies*, exceto quando são aplicáveis as normas sobre proteção ao consumidor, direito à informação, privacidade e proteção de dados em geral.

A LGPD, apesar de se inspirar no GDPR, deixou de abordar os *cookies*, optando por focar em normas gerais que podem ser interpretadas para desenvolver posicionamentos aplicáveis também a esta tecnologia.

[63] Além da CNIL, outras autoridades de proteção de dados dos Estados-membros já abordaram o "*cookie wall*", como a da Espanha em seu *Guide on use of cookies* de 2021. Disponível em: http://www.aepd.es/sites/default/files/2021-01/guia-cookies-en.pdf. Acesso em: 20 nov. 2021.

Como o conceito de dado pessoal é amplo, incluindo quaisquer dados que permitam identificar direta ou indiretamente um indivíduo, a maioria dos *cookies* estão sujeitos às leis brasileiras sobre proteção de dados.

Há cookies, então, que não são considerados dados pessoais, porque não armazenam essas informações, mas apenas dados anônimos necessários, por exemplo, para soluções técnicas dos *sites*. Para estes *cookies*, as leis brasileiras sobre proteção de dados não são aplicáveis, inexistindo qualquer restrição ao seu uso, desde que se garanta o tratamento de informações que não sejam dados pessoais, o que pode ser desafiador tendo em vista a amplitude desse conceito.

Assim, diferente da *ePrivacy Directive*, aplicável a quaisquer *cookies*, conforme detalhado acima, no Brasil apenas os *cookies* considerados dados pessoais estão sujeitos à regulação brasileira sobre proteção de dados.

Antes da entrada em vigor da LGPD, a Lei nº 12.965/2014 (Marco Civil da Internet - MCI) disciplinava as regras de proteção de dados aplicáveis aos *cookies* no Brasil, exigindo o consentimento do usuário para qualquer tratamento de dados pessoais, sendo esta a única base legal prevista no MCI (art 7º, inc. VII e IX, MCI)

Apesar da exigência do consentimento prevista no MCI, na prática, seu cumprimento não foi observado pela maioria dos *sites* brasileiros, os quais já deveriam obter a autorização dos usuários para o tratamento de dados pessoais por meio de *cookies* no cenário regulatório anterior à LGPD.

Com a vigência da LGPD, entende-se que, como lei específica sobre proteção de dados, ela prevalecerá em relação ao

MCI no que diz respeito ao tratamento de dados pessoais[64], inclusive por meio de *cookies*.

A LGPD prevê, em seu artigo 7º, dez bases legais para o tratamento de dados pessoais, inexistindo qualquer hierarquia entre elas. Por isso, os *sites* destinados ao público brasileiro passaram a poder se utilizar de outras bases legais para justificar o tratamento de dados pessoais via *cookies*, em especial o legítimo interesse do controlador ou de terceiros.

O cenário da LGPD é, assim, mais amplo para os *cookies* quando comparado ao anterior à sua vigência no ordenamento jurídico brasileiro, que se assemelhava mais ao modelo regulatório europeu com a exigência de consentimento do MCI.

Apesar dessa mudança no cenário regulatório, muitos *sites* vêm adotando o consentimento como base legal para o tratamento de dados pessoais via *cookies* opcionais, o que tem cooperado significativamente para o efeito já citado de proliferação de barras de *cookies* nos *sites*.

A escolha dos *sites* pelo consentimento nestes casos não é equivocada, sendo inclusive uma alternativa mais protetiva aos usuários dentre as demais bases legais da LGPD. A opção por tal base legal, entretanto, precisa ser consciente, tendo em vista a necessidade dos requisitos da LGPD serem cumpridos.

Para muitas empresas multinacionais, por exemplo, as ferramentas de adequação do *site* são adotadas em nível global,

[64] Nesse sentido: PALHARES, Felipe. Cookies: contornos atuais; LEONARDI, Marcel. Aspectos controvertidos entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet. In: PALHARES, Felipe (coord.). ***Temas atuais de proteção de dados***. São Paulo: Thomson Reuters Brasil, 2020, p. 9-60; 217-243.

considerando o padrão da União Europeia, o que parece justificar tal escolha, desde que essas soluções também estejam adequadas à legislação brasileira.

Não é tarefa difícil encontrar *sites* em desconformidade com os requisitos para o consentimento ser válido. Por exemplo, diversos *sites* incluem em suas barras de *cookies* mensagens contendo declarações como: (i) usamos cookies e outras tecnologias semelhantes para melhorar a sua experiência em nossos serviços, personalizar publicidade e recomendar conteúdo de seu interesse. Ao utilizar nossos serviços, você concorda com tal monitoramento; (ii) utilizamos cookies essenciais e tecnologias semelhantes de acordo com a nossa Política de Privacidade e, ao continuar navegando, você concorda com estas condições.

De acordo com a LGPD, o consentimento deve ser manifestação livre, informada e inequívoca para finalidade determinada. Não parece que nos exemplos acima o usuário tenha uma escolha real sobre autorizar ou não o tratamento de seus dados pessoais via *cookies*, uma vez que apenas a navegação pelo *site* já presume sua concordância, o que viola a exigência de o consentimento ser livre e, por isso, quando obtido por meio destes textos será nulo.

O consentimento também deve ser inequívoco e não há como afirmar que a ação de navegar pelo *site* ou descer a barra de rolagem do navegador, conforme situação explorada pelo EDPB, distinguiria de quaisquer outras interações do usuário, impossibilitando determinar se o consentimento foi inequívoco.

Ainda, palavras que expressam manifestação de vontade nas barras de *cookies*, como "Ok", "Concordo", "Aceito", devem ser utilizadas com cautela: apenas quando o *site* deseja de fato

obter o consentimento do usuário. Por outro lado, quando a proposta for somente garantir transparência sobre o tratamento de dados por *cookies*, pode-se recorrer a outras expressões, tais como "Avançar", "Fechar", "Continuar", de modo a se evitar qualquer presunção da obtenção de autorização do usuário.

Nesse sentido, tais práticas merecem ser revistas pelos *sites* para atender aos requisitos do consentimento da LGPD ou para avaliar a adoção de outra base legal.

Ademais, as empresas precisam analisar suas condutas em relação ao risco para tratamento de dados pessoais em geral, de modo a garantir compatibilidade entre a tomada de decisão envolvendo a definição das bases legais: se para determinado tratamento de dados com risco mais elevado o consentimento não é a base legal utilizada, parece adequada sua utilização apenas para *cookies*? É importante que este racional esteja envolvido no momento de tal escolha.

O legítimo interesse, por sua vez, parece viável para o tratamento de dados pessoais por *cookies* opcionais. O tratamento de dados pessoais com fundamento no legítimo interesse do controlador ou de terceiros, todavia, apenas pode ser utilizado quando tal interesse não se sobrepuser aos direitos e às liberdades fundamentais do titular dos dados, os quais sempre deverão prevalecer em qualquer situação.

Desse modo, caso o interesse legítimo não prevaleça sobre tais direitos e liberdades do titular, o controlador poderá valer-se dessa base legal para legitimar o tratamento dos dados.[65]

[65] PESSIN, Marcos Vinícius P.; LILLA, Paulo. Relatório de Impacto à proteção de dados e avaliação de legítimo interesse. In: BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (Coords.). ***Data Protection***

Assim, o legítimo interesse requer a realização de um teste de proporcionalidade para ponderar se o interesse do controlador – ou de terceiros – irá ou não se sobrepor aos direitos e liberdades fundamentais dos titulares.

Na Europa, ainda na vigência da norma antecessora ao GDPR, a Diretiva nº 95/46/EC, o WP29 propôs um teste de proporcionalidade em sua *Opinion* 06/2014[66], conhecido como *Legitimate Interest Assessment* (LIA), recomendado para controladores de dados pessoais que utilizem a base legal "legítimo interesse" em suas operações de tratamento (art. 6º (f), GDPR).

Conforme destaca Bioni, "o fio condutor de toda essa avaliação é 'balancear' os direitos em jogo. De um lado, do titular dos dados e, de outro lado, de quem faz uso das suas informações"[67].

O art. 10 da LGPD parece ter se inspirado no GDPR, bem como na referida *Opinion n.º 06/2014* do WP29, ao estabelecer elementos que podem indicar um caminho para esse teste ou análise de proporcionalidade.

A LGPD prevê que o legítimo interesse do controlador somente poderá ser utilizado como base legal quando o tratamento de dados pessoais tiver finalidades legítimas, conside-

---

Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020, p. 105-134.

[66] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Direct 95/46/EC*. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em: 20 nov. 2021.

[67] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 235-236.

radas a partir de situações concretas, que incluem, mas não se limitam a: (i) apoio e promoção de atividades do controlador (art. 10, I); e (ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e as liberdades fundamentais (art. 10, II). Ademais, somente os dados pessoais estritamente necessários para a finalidade pretendida podem ser tratados (art. 10, §1º), bem como medidas para garantir transparência devem ser adotadas pelo controlador (art. 10, §2º).

Desde que atendidas essas balizas trazidas pelo art. 10 da LGPD, as quais, basicamente, levam à elaboração do LIA, entende-se que o legítimo interesse também possa fundamentar o tratamento de dados pessoais por meio de *cookies*.

Por fim, quanto à transparência exigida pelo legítimo interesse[68], as soluções abordadas parecem satisfazê-la, seja dando transparência na política de privacidade ou por meio das barras de *cookies*, sendo esta última ferramenta mais transparente, já que informa o titular assim que o tratamento de dados será realizado, isto é, quando este acessa o *site*.

CONSIDERAÇÕES FINAIS

Cookies estão presentes em *sites* por toda a internet. Apesar dessa tecnologia ter sido criada no final do século XX, seu uso ainda continua intenso, sendo ampliado, inclusive, por outras tecnologias de rastreamento com potencial ainda mais invasivo, como *web beacons*, *tracking pixels*, *flash cookies* e *fingerprinting*.

[68] Conforme art. 10, §2º, LGPD.

As empresas parecem dividir opiniões sobre qual seria a melhor proposta em relação aos riscos oferecidos pelos *cookies* à proteção de dados dos usuários de internet. Três navegadores de internet relevantes (Google Chrome, Mozilla Firefox e Safari), todavia, já se posicionaram e, nos próximos anos, os *cookies* de terceiros devem estar bloqueados em todos eles, dando espaço para outras tecnologias preocupadas com os dados pessoais.

Mesmo com o possível "fim" dos *cookies* de terceiros, todos os demais explorados neste artigo ainda continuariam sendo utilizados, tendo em vista que garantem a conhecida "memória" da internet[69], a qual é essencial para o funcionamento dos *sites* como conhecemos hoje.

Enquanto alternativas menos invasivas para *cookies* de terceiros são discutidas, observa-se que, no Brasil, a experiência europeia resultou em reflexos indevidos nas medidas implementadas por algumas empresas para adequação dos tratamentos de dados pessoais via *cookies* à LGPD. Estes reflexos decorrem da adoção equivocada de soluções inspiradas no modelo regulatório europeu, mas que sequer cumprem a LGPD, bem como da disseminação de entendimentos pautados na suposta obrigatoriedade do consentimento para *cookies* opcionais, antes mesmo de qualquer posicionamento dos entes competentes brasileiros sobre o tema.

[69] SCHWARTZ, John. Giving the Web a memory cost its users privacy. *New York Times*, 2001. Disponível em: http://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html. Acesso em: 20 nov. 2021.

PERSONALIDADE HACKEADA: CONSIDERAÇÕES SOBRE PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS, VIGILÂNCIA DIGITAL E DISCRIMINAÇÃO

Ramon Silva Costa[70]

INTRODUÇÃO

O documentário "Privacidade Hackeada"[71], lançado em 2019, aborda o escândalo da empresa Cambridge Analytica (CA), especializada em tratamentos de grandes bancos de dados pessoais -*big datas*-, que na eleição presidencial estadunidense de 2016, realizou uma campanha orientada por dados, levando Donald Trump à vitória. A CA utilizou-se de mecanismos de publicidade on-line para coletar milhões de dados de usuários do Facebook, que foram analisados pelo modelo de personalidade "Big Five"[72], fornecendo um quadro da personalidade dos eleitores para além das variáveis demográficas tradicionais[73]. O documentário explora a partir deste caso, como um simples *like* em uma postagem pode influenciar muito naquilo que passaremos a consumir nas redes e até mesmo naquilo que teremos acesso, o que definitivamente

[70] Doutorando em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Integrante do Legalite, núcleo multidisciplinar de ensino, pesquisa e inovação em Legal Informatics da PUC-Rio. Advogado especialista em Privacidade e Proteção de Dados Pessoais do NIC.br.

[71] PRIVACIDADE HACKEADA. Direção: Karim Amer; Jehane Noujaim. Produção: Karim Amer; Jehane Noujaim; Pedro Kos; Geralyn Dreyfous; Judy Korin. Estados Unidos: Netflix, 2019. 114 minutos.

[72] O psicólogo Michael Kosinski desenvolveu este método que classifica pessoas com base em suas redes sociais. Sua pesquisa teve como campo o Facebook. O cientista afirmou não ter qualquer relação com a Cambridge Analytica e com o escândalo das eleições, mas reconhece que a empresa pode ter se baseado nos métodos de seu estudo para influenciar eleitores. Conteúdo retirado de: SUMPTER, David. ***Dominados pelos números***. Rio de Janeiro: Bertrand Brasil, 2019, p. 45.

[73] SUMPTER, David. ***Dominados pelos números***. Rio de Janeiro: Bertrand Brasil, 2019, p. 45.

nos influenciará em alguma medida, até mesmo em processos democráticos e eleitorais.

Nossas atividades nas redes alinhadas aos dados pessoais que fornecemos ao criar um perfil revelam muito de nossa subjetividade. Portanto, além da privacidade invadida e violada por tratamentos indevidos, o que temos é nossa personalidade hackeada[74], em detalhes que sequer imaginamos. Nesse sentido, são constantes as discussões sociojurídicas acerca da proteção das pessoas diante de tecnologias de vigilância, com algoritmos cada vez mais potentes. Com isso, surgem novas legislações específicas para a proteção dos dados pessoais. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD- Lei 13.709/2018) entrou em vigor em setembro de 2020 e tem como objetivo a proteção dos dados de pessoas naturais, fornecendo direitos aos titulares e regulando operações de tratamento realizadas por entidades públicas e privadas.

Diante disso, o presente artigo preocupa-se em não somente avaliar a proteção de dados pessoais como um direito da personalidade de nosso tempo, mas explorar os impactos discriminatórios efetivados por tratamentos ilegais de dados, analisando o cenário de vigilância digital a partir de uma lente voltada para os marcadores sociais da diferença, como raça, gênero e sexualidade. Assim, questiona-se: Como a proteção de dados pessoais, enquanto direito da personalidade, relacio-

[74] O termo hackeada é utilizado com a conotação popular negativa de invasão. Contudo, o termo "cracker" foi criado para designar um hacker criminoso, como forma de distinção dos hackers que atuam no desenvolvimento de sistemas de segurança, mas não de forma ilegal e que foram fundamentais no desenvolvimento da internet. Conceito retirado de: CASTELLS, Manuel. *A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade.* Rio de Janeiro: Zahar, 2003.

na-se com a diversidade em um contexto de ampla vigilância digital? O trabalho enfrenta uma questão exploratória, com o objetivo de trazer uma compreensão crítica sobre os distintos efeitos e apropriações das tecnologias digitais, partindo da ideia de que a proteção de dados pessoais enquanto direito da personalidade enfrenta dinâmicas para sua efetivação, a depender do contexto individual e social do titular de dados, ou seja, o artigo pretende tensionar a figura de um sujeito de direito neutro e universal, evidenciando as dinâmicas de discriminação que estão por trás da vigilância digital.

A pesquisa exploratória permite uma aproximação investigativa em torno do problema, o tornando mais explícito e facilitando o levantamento de hipóteses e dados. Esse tipo de pesquisa depreende, em grande parte, a análise bibliográfica (GIL, 2007). Por isso, enquanto proposta ensaística, o artigo parte de uma metodologia qualitativa com o uso da técnica de revisão bibliográfica de autores que debatem sobre personalidade, proteção de dados e marcadores sociais da diferença. Além disso, a exploração bibliográfica é contextualizada com exemplos de casos de tratamento de dados discriminatório e ilegal, publicados na mídia ou em pesquisas, como modo de enfatizar a necessidade do desenvolvimento de mecanismos plurais de proteção das pessoas.

1. CONSIDERAÇÕES SOBRE PERSONALIDADE E PROTEÇÃO DE DADOS PESSOAIS

Os direitos da personalidade visam tutelar aspectos subjetivos que todas as pessoas possuem e carregam desde o nascimento e referem-se a todas as relações personalíssimas estabelecidas por elas, acompanhando a experiência humana no âmbito de

seu desenvolvimento[75]. Dessa forma, o legislador brasileiro, por meio da centralidade constitucional dada à dignidade humana, estabeleceu a proteção da personalidade incluindo os processos subjetivos que possam surgir, como a proteção de dados pessoais frente aos desafios de sociedades digitais.

As plataformas digitais ocupam espaço de protagonismo na digitalização das relações sociais, mas possuem como principal contrapartida os dados pessoais fornecidos pelos usuários. Nesse sentido, a personalidade também é digitalizada, pois a partir do momento que entregamos informações pessoais "estamos clicando nossa personalidade" para dentro das redes a todo momento, dizendo para elas como nos sentimos, o que gostamos e revelando nossos desejos de consumo[76].

Sean Parker, primeiro financiador do Facebook, já declarou que os criadores de redes como Facebook e Instagram, basearam seus negócios na capacidade que as plataformas têm para gerar reconhecimento entre os usuários. Além disso, os criadores estavam cientes de que esse modelo de negócio transformaria as relações interpessoais e sociais. Parker enfatiza: "É um *loop* de validação social, exatamente o tipo de coisa que um hacker como eu poderia explorar, porque tira proveito de um ponto fraco da psicologia humana"[77]. Nesse contexto, os dados tornam-se uma fonte valiosa de conhecimento sobre

[75] PERLINGIERI, Pietro. ***La personalità umana nell'ordinamento giuridico***. Camerino: Jovene, 1972. TEPEDINO, Gustavo. ***A tutela da personalidade humana no ordenamento civil constitucional brasileiro***. Rio de Janeiro: Renovar, 2004.

[76] SUMPTER, David. ***Dominados pelos números***. Rio de Janeiro: Bertrand Brasil, 2019, p. 41.

[77] LANIER, Jaron. Dez argumentos para você deletar agora suas redes sociais. Rio de Janeiro: Intrínseca, 2018, p. 10.

grupos sociais, o que desperta interesses econômicos. Como indica Soshana Zuboff[78], a sociedade da vigilância tem como vertente o atual capitalismo de vigilância, que utiliza toda experiência humana, incluindo personalidades e emoções que estão contidas em nossos dados pessoais. Os dados pessoais são controlados e capitalizados como dados comportamentais para os mais diversos mercados embasados nas informações que nos são retiradas de forma gratuita por meio de nossos rastros digitais deixados em nossas redes sociais, pelas nossas pesquisas na internet, ou pelos nossos registros de compra on-line. Portanto, a economia movida a dados e o capitalismo de vigilância estão imbricados de forma substancial, pois a extensão do mercado baseado em dados pessoais utiliza-se da expansão da vigilância[79].

A privacidade enquanto elemento formador da proteção da personalidade recebe novos contornos sociais e de tutela jurídica frente aos desafios de uma sociedade da vigilância. A concepção clássica do *right to privacy*- direito à privacidade, desenvolvida por Warren e Brandeis (1890), como uma ideia de direito a ser deixado só[80], não responde por completo às

[78] ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2020, p. 8.

[79] COSTA, Ramon S.; OLIVEIRA, Samuel R. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva*, v. 5, n. 2, jul/dez 2019 p. 26.

[80] O *right to be alone*- direito de ser deixado só- foi mencionado pelo magistrado Thomas McIntyre Cooley em seu Treatise of law of torts de 1888. Este conceito foi utilizado na primeira concepção de direito à privacidade trazida pelos juristas Louis Brandeis e Samuel Warren no artigo *The right to privacy*, de 1890, publicado na Harvard Law Review. Tal artigo marca o início da linha evolutiva acerca do direito à privacidade.

demandas para a tutela da pessoa em todas as dimensões de sua personalidade, que são afetadas pelo intenso fluxo de informações dispostas nos meios tecnológicos. Nesse cenário, a proteção de dados pessoais configura-se como uma tutela ampla da pessoa, não apenas de sua privacidade, pois o objetivo é protegê-la de controles abusivos e ações discriminatórias pelo tratamento de seus dados, com a finalidade de "garantir a integridade de aspectos fundamentais de sua própria liberdade pessoal"[81].

Nesse sentido, a proteção de dados pessoais ergue-se como um direito da personalidade de extrema relevância na sociedade contemporânea, na qual as tecnologias digitais estipulam um cenário de novos desafios para a tutela da personalidade humana. Isso inclui o sistema de economia movida a dados, operado a partir das atividades de controle e armazenamento de dados pessoais, no qual as personalidades são mapeadas por "signos identificadores" das pessoas. Estamos diante de uma nova identidade que os controladores de dados precisam classificar, de acordo com a personalidade do titular das informações. Essa é a justificativa dogmática para a inserção dos dados pessoais na categoria de direitos da personalidade[82]. Os dados pessoais constituem elementos substanciais da singularidade humana, por isso são capazes de nos identificar em nossas particularidades e enquanto seres sociais. Disso decorre a importância de elevar a proteção de dados pessoais a um status de direito fundamental da personalidade, o que foi alçado em 2022 pela Emenda Constitucional (EC) 115/2022, que

[81] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019, p. 23-24.

[82] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2018, p. 65.

alterou a CF/88 para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, fixando a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais, tendo sua aplicabilidade imediata por força de norma constitucional.

Nesse ponto, a LGPD ao enfatizar a tutela das situações existenciais dos titulares de dados, aproxima-se de uma concepção de proteção de dados pessoais como "direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante"[83].

Desse modo, a tutela jurídica da personalidade compreende de modo substancial a proteção dos dados pessoais, tendo a própria LGPD estabelecido o livre desenvolvimento da personalidade como um de seus fundamentos em seu art. 2º, VII. Logo, a ideia evolutiva da privacidade inclui a proteção de dados pessoais e seu sentido de autodeterminação informativa, ou seja, de controle do titular sobre suas informações[84]. Isso não significa dizer que a proteção de dados pessoais é uma simples extensão do direito à privacidade, mas evidencia a importância de um entendimento da proteção de dados como uma garantia que reveste toda a personalidade humana.

Assim, o livre desenvolvimento da personalidade pode ser alçado como principal fundamento constitucional para a

[83] FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). ***Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro***. São Paulo: Thomson Reuters Brasil, 2019, p. 100.

[84] RODOTÀ, S. ***A vida na sociedade da vigilância: a privacidade hoje.*** Rio de Janeiro: Renovar, 2008, p. 17.

normatização de um direito fundamental à proteção de dados pessoais, tendo em vista que integra diretamente o princípio da dignidade da pessoa humana e o direito geral de liberdade, que assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade[85].

Contudo, a efetividade da proteção dos cidadãos diante dos possíveis danos à personalidade produzidos pela vigilância digital tem como obstáculo um aspecto inerente a todas as pessoas: a diferença. O Brasil possui grande diversidade étnica, racial, regional cultural e social, muitas vezes traduzida em desigualdades estruturais que nos posiciona de modos distintos no que tange às possibilidades de reconhecimento e disposição de direitos. Dessa forma, é preciso descortinar uma produção universalista da legislação de proteção de dados e entender melhor desafios sociais na construção de uma cultura de proteção de dados pessoais no país. Para tanto, o estudo da proteção de dados pessoais deve levar em conta marcadores sociais da diferença como raça, classe, gênero, sexualidade e geração. Com o intuito de exemplificar e debater a potencialidade lesiva de tratamentos de dados discriminatórios e ilegais aborda-se a seguir esse contexto.

2. PARA ALÉM DA NORMATIVIDADE: UM DEBATE SOBRE VIGILÂNCIA DIGITAL E DISCRIMINAÇÃO

A vigilância sobre as pessoas não é um processo novo, mesmo que esteja sendo constantemente renovado e potencializado pelas tecnologias digitais. Em seus estudos sobre a

[85] SARLET, Ingo W.; SAAVEDRA, Giovani A. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais. *Revista Direito Público-RDP*, Brasília, 2020, v.17, n. 93, p. 43.

sociedade disciplinar, Michel Foucault[86] já indicava o percurso histórico de uso de ferramentas de conhecimento sobre a sociedade moderna como uma forma de exercer poder e impor controle sobre as populações. O chamado biopoder compreende a sistemática reunião de informações pessoais sobre a saúde e condições gerais de vida dos indivíduos, sendo este sistema uma forma de determinação sobre os corpos, práticas e comportamentos considerados saudáveis, ou não.

Nos atuais debates sobre diversidade, a ideia de "normatividade" é utilizada para caracterizar a condição imposta por normas sociais e comportamentais que recaem sobre as pessoas como forma de classificá-las como "adequadas", no sentido de atenderem às expectativas construídas historicamente sobre quais corpos e condutas são legítimos, saudáveis e até mesmo humanizados. Nesse cenário, o racismo, sexismo e lgbtifobia ascendem não apenas como formas de opressão, mas de categorização, discriminação e marginalização. Assim, não é difícil imaginar que informações sobre pessoas que historicamente são vigiadas e categorizadas de modo negativo, muitas vezes são tratadas de forma a aumentar a vulnerabilidade dessas populações.

A LGPD, inspirada no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, traz a categoria de dados sensíveis, como forma de garantir maior proteção no contexto de tratamento de dados que podem ser tratados de forma potencialmente discriminatória. O art. 5º, II, da LGPD define como sensíveis os dados pessoais sobre raça, etnia, religião, opinião política, filiação a sindicato ou a organização de ca-

[86] FOUCAULT, Michel. *História da Sexualidade 1: a vontade de saber*. 3. ed. São Paulo: Paz e Terra, 2015, p. 151.

ráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Desse modo, a criação da categoria de dados sensíveis parte de um processo de observação pragmática acerca dos distintos efeitos causados pelo tratamento desses dados em relação aos demais. Nessa esteira, observa-se igualmente a necessidade de tutela do princípio da igualdade material, como fundamento para a proteção da pessoa[87].

A própria seleção sobre quais dados seriam sensíveis demonstra que a circulação de determinadas informações pode acarretar maior potencial lesivo aos seus titulares, em uma determinada configuração social[88]. Partindo desse pressuposto, a compreensão sobre os mecanismos que devem ser empregados na proteção de dados sensíveis perpassa um entendimento sobre as dinâmicas discriminatórias que são articuladas na sociedade. Pensando nisso, a seguir serão apresentados três exemplos e seus respectivos debates acerca da discriminação e da vigilância com recortes para marcadores sociais de raça, gênero e sexualidade.

3. MULHERES NEGRAS

Em um vídeo do TED (conferência online) de 2017, a cientista da computação, Joy Buolamwini, estudante do MIT (*Massachusstes Institute of Technology*), mostrou como algumas tecnologias munidas de inteligência artificial não reconheciam seu rosto. Ela

[87] RODOTÀ, S. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 85.

[88] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019, p. 143.

conduz diversos estudos sobre racismo e sexismo em tecnologias digitais, propondo uma análise racializada da tecnologia, como forma de compreensão e correção de máquinas, robôs e ferramentas tecnológicas discriminatórias. A cientista relata sobre seu projeto para auditar algoritmos, que analisa tecnologias de reconhecimento facial que possuem menor precisão em faces de mulheres negras. Contudo, o estudo demonstra que o mesmo não acontece quando a visibilidade é negativa, visto que as tecnologias demonstram ser extremamente eficazes para indicar pessoas negras para resultados negativos[89].

Já a pesquisadora Safiya Noble[90] evidenciou em suas pesquisas os resultados de busca em plataformas como o Google, na qual a procura pelo termo "garotas negras" resulta expressivamente em conteúdos pornográficos. Nesse campo, os algoritmos discriminam e subalternizam a representação de mulheres negras, sendo algo perceptível até mesmo na ferramenta de complementação textual do Google, que escancara misoginia, sexismo e racismo em suas sugestões. Noble aponta que essa realidade é um efeito de fortalecimento das estruturas de poder reproduzidas pelas tecnologias e entende como uma possibilidade de enfrentamento desse problema, a articulação de uma epistemologia feminista, que amplie os sentidos de desenvolvimento e apropriação dessas tecnologias, visto que são embasadas na experiência de homens brancos e burgueses, o que as condiciona a uma compreensão parcial e discriminatória sobre outros grupos sociais.

---

[89] BUOLAMWINI, Joy. Como eu luto contra o preconceito em algoritmos-TED. Vídeo. 2017. Disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms . Acesso em: 14 de dez. 2020.

[90] NOBLE, Safiya Umoja. *Algorithms of Oppression: How search engines reinforce racism*. NYU Press, 2018.

A pesquisa "#QUEMCODABR"[91], desenvolvida pelo Pretalab em parceria com a consultoria em softwares Thoughtworks, levantou dados sobre o perfil de profissionais da tecnologia e ocorreu entre 2018 e 2019. Os resultados apontam que os homens representam 68% dos profissionais de tecnologia, enquanto mulheres são 31,5% e pessoas intersexo, 0,3%. Os brancos representam 58,3% dos profissionais, contra 36,9% de negros, 4% de amarelos e 0,3% de indígenas. Além disso, a maior parte dos profissionais são heterosexuais (78,9%), com apenas 10,2% de homossexuais, 7,8% de bissexuais e 2% de pansexuais. As porcentagens demonstram um expressivo contraste no que tange à diversidade racial e de gênero, tendo em vista que a maioria da população brasileira é mulher (51, 5%) e negra (53,9%)[92].

Portanto, o fato do perfil comum do profissional de tecnologia ser um homem branco, heterossexual e cisgênero impacta na produção tecnológica e no grau de atenção à diversidade nos meios que produzem, controlam e fornecem tecnologias para a sociedade. Esse cenário vincula-se a um contexto social no qual as identidades não normativas vivenciam uma relação complexa com o avanço do desenvolvimento das tecnologias digitais. Isso porque, se por um lado cada vez mais vivenciamos uma expansão das possibilidades e usos da tecnologia, por outro, populações vulneráveis tendem a vivenciar discriminações proporcionadas pelas tecnologias, que reproduzem, em certa medida, a cultura na qual são criadas e difundidas.

[91] Disponível em: https://www.pretalab.com/dados

[92] IBGE. IBGE, Pesquisa Nacional por Amostra de Domicílios 2015. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv98887.pdf Acesso em: 19 jul. 2021.

Acompanhando essa discussão, o pesquisador Scott Skinner-Thompson[93] explora a historicidade discriminatória que divide as pessoas em termos de condições de garantia da privacidade. Segundo ele, a vigilância opressiva e sistemática tem sido historicamente destinada às minorias raciais, principalmente aos negros, definindo suas condições de vida. Nesse ponto, Simone Browne[94] destaca que a vigilância não é uma novidade para pessoas negras, é um controle estabelecido pelo "sistema anti-negritude"[95].

A autora chama de "vigilância racializante" o processo de vigilância de pessoas negras, não apenas como uma ferramenta de monitoramento e controle social, mas também para a produção da "negritude" como categoria, permitindo ainda mais o monitoramento e a categorização com base na divisão racial. Essa conjuntura é o que vem sendo reproduzido no desenvolvimento e apropriação de tecnologias digitais, tendo em vista que essas inovações são moldadas na ideologia de mercado capitalista dos países ditos desenvolvidos, que estabelecem a lógica da supremacia branca e que encontra ressonância no racismo colonialista de países como o Brasil, que possui seus próprios contextos históricos de opressão e desigualdade racial.

---

[93] SKINNER-THOMPSON, Scott. *Privacy at margins*. Cambridge: Cambridge University Press, 2021, p. 24.

[94] BROWNE, Simone. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press Books, 2015.

[95] Dentre os exemplos históricos de vigilância sobre pessoas negras, Browne (2015) documenta ações como a marcação de negros como escravos, o uso de toras de navios para categorizar os negros como mercadorias junto com outras cargas, a vigilância e violência perpetrada por "feitores" contra escravos negros e os anúncios sobre escravos fugitivos.

Nesse contexto, a pesquisadora Bianca Kremer[96] discorre sobre a necessidade de uma perspectiva afrocentrada no estabelecimento de uma cultura de proteção de dados pessoais no Brasil. A questão é que a lei é moldada a partir da suposta neutralidade jurídica, que não se demonstra verdadeira quando observamos as instituições e indivíduos munidos de poder para articularem e efetivarem a lei. Nesse sentido, a LGPD pode ser utilizada como uma revisão do racismo estrutural em plano jurídico, visto que "segue lida e construída – teórica e jurisprudencialmente – por trás de uma suposta neutralidade e igualdade formal".

4. PESSOAS TRANS

Em suas pesquisas, Skinner-Thompson[97] revela outras dimensões do que ele chama de "privacidade nas margens", referindo-se aos constructos históricos e socioculturais que embasam a relação entre vigilância e privacidade para populações vulneráveis. O pesquisador debate as possibilidades de segurança da vida privada e liberdade de pessoas homossexuais e transexuais, enfatizando que historicamente pessoas não heteronormativas, no sentido de não atenderem às normas sociais de gênero e sexualidade, enfrentam contextos de vigilância e restrições sociais. O próprio Estado utiliza-se de

[96] KREMER, Bianca. LGPD em vigor: por que racializar a proteção de dados é tão importante? *Jota*, 01 de out. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-em-vigor-protecao-dados-importante-01102020 Acesso em: 10 de jul. 2021.

[97] SKINNER-THOMPSON, Scott. *Privacy at margins*. Cambridge: Cambridge University Press, 2021.

poder de polícia para demarcar fronteiras sobre quais espaços e condutas pessoas LGBTI+[98] podem vivenciar.

É importante compreender que mesmo com o avanço na garantia de direitos civis, os corpos não normativos ainda são os mais perseguidos e violentados. Segundo levantamentos feitos pela Associação Nacional de Travestis e Transexuais (ANTRA), em 2020 foram 175 travestis e mulheres transexuais assassinadas, número que representou alta de 41% em relação ao ano anterior (124 homicídios) e 78% das vítimas eram negras e 72% delas eram profissionais do sexo[99]. Diante desse cenário, informações sobre a identidade de gênero, quando não tratadas de forma adequada, pode ocasionar grave violação à personalidade e até mesmo à integridade física e à vida.

As pesquisadoras Mariah Rafaela Silva e Joana Varon[100] desenvolveram um estudo sobre o uso de reconhecimento facial no setor público brasileiro e as identidades trans, no qual alertam sobre um processo de implementação da tecnologia no país, sem a devida transparência, o que dificulta uma mensuração acerca dos efeitos danosos para a população trans, levando-se em conta ainda, questões socioeconômicas, raciais e territoriais. Nesse contexto, a tecnologia de reconhecimento

---

[98] Sigla referente às pessoas lésbicas, gays, bissexuais, transexuais, intersexuais e outras identidades não heteronormativas.

[99] BENEVIDES, Bruna; NOGUEIRA, Sayonara. *Dossiê dos assassinatos e da violência contra travestis e transexuais brasileiras em 2020*. São Paulo: Expressão Popular, ANTRA, IBTE, 2021.

[100] SILVA, Mariah Rafaela; VARON, Joana. *Reconhecimento facial no setor público e identidades trans: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território*. Codin Rights: Rio de Janeiro, 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 29 jun. 2021.

facial, muitas vezes caracterizada como neutra, pode não ser eficiente em suas avaliações. Assim, tendo em vista que não há muita transparência sobre a efetiva margem de erro da tecnologia, pessoas trans podem sofrer processos de exclusão de direitos e serviços públicos, tornando suas vidas ilegítimas.

O dado sobre identidade de gênero, conjugado com outras informações sensíveis configuram um conjunto de informações, que quando tratados de modo inadequado, pode ocasionar graves danos às pessoas trans no Brasil, que já tendem a serem perseguidas, violentadas e marginalizadas na sociedade. Isso pode ainda ser agravado pelo uso de tecnologias avançadas no tratamento de grandes bancos de dados, que carregam falhas quanto à percepção e acurácia sobre a diversidade humana.

Esses exemplos contribuem para a compreensão das dinâmicas de opressão e vulnerabilidade que atingem pessoas não enquadradas na normatividade binária e cisgênera. Assim, é importante identificar a identidade de gênero como uma informação munida de grande sensibilidade, apresentando aspectos fundamentais para sua interpretação enquanto dado sensível, quais sejam: (i) informação personalíssima; (ii) potencial discriminatório; e (iii) potencialidade danosa

O tratamento do dado sobre identidade de gênero deve levar em conta o contexto no qual essa informação está inserida e está sendo tratada, bem como requer atenção para a pessoa titular desse dado. Desse modo, pessoas trans podem ter informações sobre suas identidades de gênero tratadas de modo a aumentar a discriminação, aspecto que contraria por completo a noção trazida pelos princípios da LGPD, bem como o objetivo central da legislação, que é a proteção da pessoa, na integralidade de sua personalidade.

5. HOMENS GAYS

Na esteira das plataformas digitais de relacionamento, outra população que tem sofrido graves violações à personalidade por tratamento irregular de dados pessoais são os homens homossexuais, grupo que concentra o maior número de usuários nessas redes, tendo em vista a expressiva socialização da busca sexual entre gays por meio do uso dos apps geolocalizados[101].

Em 2020, a Senacon (Secretaria Nacional do Consumidor) do Ministério da Justiça notificou o Grindr e o Tinder por venderem dados pessoais de usuários para outras empresas melhorarem a eficiência dos anúncios publicitários. A ação da Senacon foi motivada pelo relatório *Out of Control*- Fora de Controle, divulgado pelo Conselho de Consumidores da Noruega, que alerta sobre diversas irregularidades cometidas pelas empresas publicitárias e as redes sociais. Em razão desse relatório, o app Grindr recebeu uma multa equivalente a R$ 63,8 milhões na Noruega[102]. Esse relatório levou a Autoridade de Proteção de Dados da Noruega a multar o Grindr em 6,5 milhões de euro em 2021[103].

Já em 2018, foi revelado que o Grindr repassou dados pessoais de seus usuários para as empresas Apptimize e Localytics, dentre os dados repassados estavam o status de Vírus

[101] MISKOLCI, Richard. ***Desejos Digitais: uma análise sociológica da busca por parceiros on-line***. 1. Ed. Belo Horizonte: Autêntica Editora, 2017.

[102] LARA, Mahila. A. Governo notifica Tinder e Grindr por vender dados pessoais de usuários. ***Poder 360***. 15 jan. 2020. Disponível em: <https://www.poder360.com.br/midia/governo-notifica-tinder-e-grindr-por-vender-dados-pessoais-de-usuarios/> Acesso em 15 jun. 2021.

[103] https://www.raciocinedigital.com.br/lgpd-em-noticias/grindr-recebe-outra-multa-pesada-por-espionar.html.

da Imunodeficiência Humana (VIH ou HIV, do inglês *Human Immunodeficiency Virus*), localização, e-mail e telefone das pessoas. A irregularidade foi descoberta por Antoine Pultier, cientista da Organização não governamental norueguesa SINTEF, que conseguiu "quebrar a criptografia" dos dados de forma não tão complexa e revelou que ocorria o envio dos dados para terceiros[104].

O dado sobre HIV é munido de extrema sensibilidade, não só por tratar-se de um dado sensível referente à saúde dos indivíduos, mas pelo contexto em que é tratado, em um app como o Grindr, majoritariamente utilizado por homens gays. Isso porque, o próprio movimento político e social de pessoas LGBTI+ foi abalado pela associação entre a AIDS-SIDA (Síndrome da Imunodeficiência Adquirida) e homens homossexuais e mulheres trans e travestis, acentuada pela epidemia da doença que era considerada a "peste gay" nos anos 1980 e meados dos anos 1990, o que ocasionou uma esfera discriminatória e odiosa na sociedade contra essas pessoas[105].

Como exemplifica Rodotà[106], um empregador ou companhia seguradora que ao obterem uma informação sobre uma pessoa que vive com HIV podem discriminá-la em um processo seletivo, demiti-la, recusar uma promoção ou negar

[104] BARIFOUSE, Rafael. App de relacionamento gay Grindr compartilhou status de HIV de usuários com empresas. ***BBC Brasil***, São Paulo, 03 de abr. de 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43620447. Acesso em 10 jul. 2021.

[105] COSTA, Ramon S. ***Entre taps e direitos: proteção de dados pessoais, privacidade e liberdade no aplicativo Grindr.*** Dissertação (Mestrado em Direito). Universidade Federal de Juiz de Fora. 185 p. 2020, p. 38.

[106] RODOTÀ, S. ***A vida na sociedade da vigilância: a privacidade hoje***. Rio de Janeiro: Renovar, 2008, p. 70.

um contrato de seguro. Isso aconteceria pelo estigma, desinformação e preconceitos vinculados ao vírus. Dessa maneira, o tratamento indevido do dado sobre HIV deve ser encarado como um problema para além da privacidade, pois envolve um contexto de expressiva estigmatização de toda uma coletividade já vulnerável.

Ademais, o cenário de apps de relacionamento integram dinâmicas bastante intensivas de tratamento de dados sensíveis, tendo em vista que os algoritmos dos apps buscam por combinações e apresentam opções de pretendentes que de alguma maneira estejam relacionadas com nosso perfil comportamental nas redes. Nesse sentido, a pesquisadora Cathy O'Neil[107] destaca o papel dos algoritmos na produção e reprodução de discriminações. Isso porque, os modelos algorítmicos utilizados nos apps acabam por moldar a experiência das pessoas nessas redes, mas são construções humanas limitadas. O'Neil classifica os algoritmos como possíveis "armas de destruição matemáticas", justamente por serem baseados em escolhas de seres humanos falíveis, o que ocasiona impactos sociais extremamente nocivos, especialmente a discriminação de populações mais vulneráveis

No entanto, quando O'Neil (2020) descortina diversos processos de aplicação discriminatória de modelos algorítmicos, o que fica evidente é que os algoritmos sempre errarão em algum nível, pois são simplificações incapazes de lidarem com toda complexidade do mundo real ou da comunicação humana. Nesse ponto, é possível vislumbrar os impactos de

[107] O'NEIL, Cathy. *Algoritmos de destruição em massa*. Como o big data aumenta a desigualdade e ameaça a democracia. São Paulo: Editora Rua do Sabão, 2020.

tratamentos de dados irregulares sobre informações relacionadas às sexualidades destoantes do padrão heteronormativo.

Nessa conjuntura, o exemplo de possíveis discriminações danosas que podem ser produzidas no âmbito do tratamento de dados em apps de relacionamento possui ressonâncias distintas de acordo com a identidade sexual do titular afetado. Podemos pensar que um conjunto de dados sensíveis de um homem gay pode ser utilizado para justificar decisões embasadas em tecnologias irrigadas pela heteronormatividade. Isso significa que a sexualidade, enquanto dado sensível, inevitavelmente tem repercussões diferentes quando comparamos heterossexuais e outras orientações sexuais

É mais fácil que um titular de dados homossexual receba tratamentos discriminatórios em virtude da sua sexualidade, visto que essa já é a realidade para as sexualidades dissidentes da heterossexualidade. Essa diferenciação precisa ser destacada quanto tratamos dos dados sensíveis referentes à vida sexual porque os mecanismos de proteção devem ser proporcionais aos contextos de tratamento e não apenas uma aplicação generalizante de um dispositivo legal, que não contempla a complexidade da diversidade sexual e, consequentemente, não é capaz de entregar uma interpretação atenta a todas as possibilidades de danos que um titular pode sofrer em razão de sua identidade.

6. POR UMA INTERPRETAÇÃO INCLUSIVA DA CATEGORIA DE DADOS SENSÍVEIS

Diante dos contextos abordados, podemos vislumbrar, em alguma medida, como populações vulneráveis potencialmente sofrem significativos danos à personalidade em tratamentos

indevidos e abusivos de dados. Nesse sentido, as pesquisadoras Caitlin Mulholland e Bianca Kremer[108] indicam a necessidade de um olhar para a diversidade em um processo de efetivação da tutela dos dados sensíveis. Isso porque, uma proteção substancial dessa categoria de dados é um instrumento efetivo na defesa de direitos fundamentais no cenário digital. Contudo, o direito também precisa ser mobilizado para a aplicação dos princípios da igualdade e não discriminação, rompendo "com o manto da desigualdade formal, e a perversa utilização de características étnico-raciais, sexuais e de gênero como mecanismos de exclusão".

No entanto, o Brasil ainda está em um processo inicial de implementação da LGPD e de criação de uma cultura de proteção de dados, pois a lei apenas entrou em vigor por completo em agosto de 2021. Assim, a ANPD ainda não regulamentou ou especificou interpretações para a categoria de dados sensíveis. Por isso, há um debate relevante sobre a taxatividade ou não dos dados expressos no art. 5º, II da lei. A interpretação taxativa restringe a aplicação direta do regime de dados sensíveis aos dados contemplados no dispositivo. Em contrapartida, é possível uma extensão interpretativa daqueles dados que mesmo inicialmente não entendidos como sensíveis demonstrem sensibilidade a depender de seu contexto de tratamento, o que é possibilitado pelo art. 11, § 1º.

Contudo, como observado nos exemplos de tratamento discriminatório trazidos neste artigo, a configuração de um

[108] MULHOLLAND, Caitlin; KREMER, Bianca. Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. In: Rodrigo da Guia Silva; Gustavo Tepedino. (Org.). *O Direito Civil na era da inteligência artificial*. São Paulo: Revista dos Tribunais, 2020, p. 580.

dado como sensível e a consequente aplicação de um regime legal mais rigoroso para seu tratamento, requer atenção para o contexto em que esses dados são tratados, bem como para seus titulares. Isso porque, os efeitos discriminatórios não estão no dado em si, mas nos usos que são feitos dele[109]. Porém, determinados tipos de informação configuram um contexto maior de vulnerabilidade para seus titulares. Grupos vulneráveis tendem a serem mais prejudicados por tratamentos ilícitos e discriminatórios, visto que o uso irregular de suas informações impactam diretamente no aumento da vulnerabilidade.

É relevante demarcar que uma interpretação do rol de dados sensíveis como explicativo visa, em primeiro lugar, garantir que a legislação cumpra seu objetivo de uma proteção ampla da pessoa contra violações de seus dados pessoais, tendo a categoria de dados sensíveis uma maior robustez protetiva, em consonância com o princípio da não discriminação estabelecido na lei. Ou Seja, o entendimento do rol do art. 5º, II, da LGPD como taxativo limita as possibilidades de interpretação e percepção das dinâmicas de violação à personalidade e à dignidade humana, pois não é possível dimensionar o modo como os aplicadores da lei e controladores de dados irão interpretar determinadas situações em que populações vulneráveis possam estar expostas, mas não necessariamente estarão contempladas pela listagem presente na lei, como é o caso da identidade de gênero de pessoas trans. Do mesmo modo, a aplicação de uma interpretação contextual, como possibilitado pelo art. 11, § 1º, mesmo quando cabível, não

[109] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019, p. 144.

necessariamente será articulada de forma concreta para a proteção do titular

Assim, é importante que os agentes de tratamento de dados tenham em vista as dinâmicas de diversidade e vulnerabilidade presentes nas informações que estão tratando. Tal entendimento se justifica porque a categoria de dados sensíveis compreende os dados pessoais "especialmente suscetíveis de utilização para fins discriminatórios, como estigmatização, exclusão ou segregação", podendo causar violações à dignidade das pessoas, à identidade pessoal e à privacidade[110]. Assim, é possível compreender que não há o estabelecimento de um rol taxativo de dados sensíveis na LGPD, pois esses dados são classificados de acordo com o nível de lesividade que apresentam em determinado tratamento

Contudo, há a discussão acerca da presença do dano para o enquadramento de um dado como sensível. Tal vinculação entre dano e sensibilidade restringe o âmbito de aplicação do art. 11. Isso porque, há uma dificuldade para que o titular comprove o dano de forma concreta. Além disso, os efeitos danosos são, em grande medida, refletidos na coletividade e não na subjetividade dos titulares. Todavia, quando pensamos em contextos de tratamento ilícito de dados como raça, gênero e sexualidade, o que temos é um cenário capaz de gerar danos particulares e coletivos

Portanto, interpretar um dado como sensível também inclui uma perspectiva de que qualquer dado sensível, quando tra-

[110] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (coords). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*.1 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 455.

tado fora das hipóteses legais do art. 11, I, II, da LGPD, "gerará sempre danos de natureza personalíssima por violação dos direitos de privacidade, liberdade ou identidade, fundamentos da proteção de dados". Desse modo, o dano seria *in re ipsa*, sem necessidade de comprovação sobre outras consequências jurídicas, o que não retira a possibilidade de uma pessoa arguir a existência de um dano concreto sobre sua personalidade[111].

Sendo assim, a extensão da categoria de dados sensíveis para uma interpretação ampla deve estar ancorada na LGPD, no sentido de observar a configuração de tratamentos ilícitos, discriminatórios e que causam danos aos titulares. Isso porque, é possível que dados sejam tratados de forma discriminatória, no sentido de atribuições distintas a depender das informações, mas isso pode ocorrer de forma lícita e sem causar danos aos titulares. Além disso, a aplicação do regime de dados sensíveis deve observar a complexidade das operações de tratamento, bem como o contexto pessoal e social atribuídos a uma informação, o que está diretamente relacionado a um comprometimento de combate à discriminação e promoção da diversidade e dignidade humana na construção de uma cultura de proteção de dados no Brasil.

CONCLUSÃO

Na introdução deste artigo, o exemplo do uso de dados na eleição estadunidense trouxe à tona um dos pontos centrais abordados: a vigilância digital sobre nossos dados pessoais e os impactos decorrentes disso. Todavia, seja em termos

[111] MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, Caitlin (org). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020, pp. 131-132.

privados ou coletivos, a vigilância digital operada a partir de tratamento de dados pessoais gera consequências distintas entre as pessoas. A diferença, fator inerente ao ser humano, muitas vezes é posta como desigualdade na sociedade. Marcadores como raça, gênero e sexualidade foram abordados como uma forma de alertar para uma leitura mais diversa da proteção dos titulares de dados, que estão longe de passarem pelas mesmas dinâmicas de opressão e de terem as mesmas chances de autodeterminação informativa em uma sociedade marcada por discriminações e violações de direitos fundamentais de populações vulneráveis.

De todo modo, é preciso reconhecer que os exemplos abordados foram articulados para o formato de um artigo, o que significa que foi apresentada apenas uma discussão parcial sobre um contexto muito mais complexo e repleto de questões e especificidades sociojurídicas que podem ser mais elaboradas e debatidas em outras pesquisas. Contudo, o que deve ser posto e salientado neste texto, é que a personalidade violada, aqui dita hackeada, é um problema de todos os cidadãos, porém com repercussões e desenvolvimentos históricos muito diferentes. Mulheres, pessoas negras e LGBTI+ sofrem um hackeamento violador de suas personalidades, de maneira que as informações sobre suas vidas e identidades são utilizadas para categorizá-las em posições sociais de desprestígio e violência

É evidente que as tecnologias reproduzem os contextos discriminatórios difundidos na sociedade, tanto entre os desenvolvedores de tecnologia e controladores de dados, quanto na realidade dos titulares de dados. Porém, a dinâmica discriminatória não pode ser entendida como algo simplesmente posto. Essa reprodução discriminatória pode ser interrompida

e mitigada por meio de mecanismos de inserção de pessoas diversas no debate e produção da tecnologia e seus impactos. Somado a isso, é importante o estabelecimento de uma via educacional, no sentido de contestação dos parâmetros normativos que cerceiam direitos fundamentais e restringem a condição humana de pessoas vulneráveis em termos de gênero, sexualidade, raça, classe socioeconômica e outros marcadores que configuram um quadro desproporcional no que tange à efetiva proteção de dados pessoais.

A efetivação da proteção de dados pessoais como um direito fundamental da personalidade e a devida interpretação dos dados sensíveis requer um olhar atento e constante sobre a diversidade, com a participação de todos os atores, principalmente com o apoio da sociedade civil na elaboração de parâmetros protetivos guiados pelos princípios da não discriminação e dignidade humana. Assim, é possível abandonar uma concepção restrita de proteção da privacidade em termos privativos e alcançar uma dimensão de participação coletiva na construção de uma cultura de proteção de dados que contemple a diversidade brasileira.

OS DESAFIOS DA ADMINISTRAÇÃO PÚBLICA NA ADEQUAÇÃO DA LGPD: UMA ANÁLISE ACERCA DE SUA COMPATIBILIDADE COM A LAI E O AMPLO COMPARTILHAMENTO DE DADOS

Fernanda Alves Corrêa[112]

INTRODUÇÃO

É sabido que vivenciamos a era da sociedade hiper conectada, com intenso fluxo de dados circulando em frações de segundos e para além das fronteiras, sem quaisquer controles por parte de seus titulares acerca de sua correlata finalidade e tratamento. Nesse contexto, os dados têm se tornado o grande ativo de muitas empresas e governos,[113] na medida que o lucro com suas vendas cresce em caráter exponencial, seja para influenciar padrões de comportamentos de potenciais consumidores, personalizar serviços, ou até mesmo, influenciar nas acirradas disputas eleitorais.

O escândalo da *Cambridge Analytica*[114] alertou o mundo para a necessidade da autodeterminação informativa dos titulares, a saber, o direito do próprio indivíduo de decidir acerca da divulgação e utilização de seus dados pessoais, a fim de proteger sua privacidade e não ficar refém da atual cultura do *Surveillance Capitalism*[115] acentuada pela era digital, muito pelo

[112] Pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ). Advogada.

[113] Nas palavras do matemático britânico Clive Humby: "Os dados são o novo petróleo". No original: "Data is the new oil"; THE ECONOMIST. The world's most valuable resource is no longer oil but data. May 6th, 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-world-s-most-valuable-resource-is-no-longer-oil-but-data . Acesso em 18.05.21.

[114] BBC NEWS. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em 18.05.21.

[115] Uma análise interessante pode ser encontrada em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/sorria-o-estado-brasileiro-esta-de-olho-em-voce-26052021 Acesso em 27.05.21.

qual, "nenhum homem é considerado livre, se não dispuser de garantia de inviolabilidade da esfera de privacidade que o cerca",[116] posto assim, como o núcleo central da dignidade humana.

Neste toar, nasce na Europa o Regulamento Geral Sobre a Proteção de Dados (*General Data Protection Regulation- GDPR),* que serviu de posterior inspiração para a promulgação em nosso ordenamento da Lei Geral de Proteção de Dados, disposta sob o nº 13.709/18 (LGPD)[117]. Ressalta-se que a Carta Magna de 88, já respalda como direito fundamental, em seu artigo 5ª, inciso X,[118] a inviolabilidade da vida privada, contudo, inexiste expressamente a proteção aos dados de maneira específica.[119]

No entanto, inicialmente, é somente com o julgado da medida cautelar em ação direta de inconstitucionalidade (ADIN)

---

[116] DI FRANCO, Carlos Alberto. Jornalismo, Ética e Qualidade. São Paulo: Vozes,1996.

[117] BRASIL. Lei nº 13.709. ***Planalto***, Brasília, 14 de ago. de 2020. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 09.05.21.

[118] Art. 5º, inciso 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;

[119] Em que pese o inciso XII disponha sobre a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, setores representantes da sociedade civil se uniram para propor a EC n° 19 (PEC) a fim de complementar o referido artigo. Recentemente, a referida PEC foi aprovada em 2 turnos, recebendo 64 votos no 1º e 76 no 2º, sendo o mínimo exigido de 49. O texto agora irá para promulgação (ainda sem data), contemplando a proteção de dados pessoais inclusive no meio digital. Disponível em: COMISSÃO DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA (camara.leg.br) Acesso em 05.11.21.

n° 6387[120] que a discussão ganhou corpo e relevância, ao cabo de elevar a proteção dos dados pessoais ao patamar de direito fundamental.

A jornada de adequação à LGPD será longa, especificamente no que tange ao tema do poder público, detentor da maior rede de dados existente. Notoriamente, desde a concepção do *Welfare State,* pós 2ª guerra mundial, o Estado passou a demandar de seus administrados, uma gama de dados para estudos e confecções de políticas públicas, seja na seara educacional, na área de seguridade social, saúde, tributação, dentre outros.

[120] O cerne do julgado gira em torno do questionamento do repasse de dados concedidos pelos titulares à empresas de telefonia, por conta da prestação de serviço contratada, à entidades da administração pública como o IBGE para traçar monitoramentos para a situação emergencial da COVID-19. Afirma a relatora Rosa Weber: "se pode extrair do texto constitucional, em particular das garantias expressas de proteção à dignidade da pessoa humana, à privacidade, à intimidade e ao sigilo dos dados pessoais, uma "tutela constitucional do direito à autodeterminação informativa". Afirmando assegurada, na Constituição da República, "uma tutela autônoma aos dados pessoais e não apenas ao conteúdo das comunicações", sustenta que "a medida provisória em análise viola o sigilo de dados dos brasileiros e invade a privacidade e a intimidade de todos, sem a devida proteção quanto à segurança de manuseio, sem justificativa adequada, sem finalidade suficientemente especificada e sem garantir a manutenção do sigilo". Enfatizando a ampliação dos riscos à privacidade na sociedade de informação atual, observa que "o mau uso de dados compartilhados pode servir à campanha de ***fake news*** e até mesmo de manipulação da vontade do eleitorado, comprometendo a liberdade democrática". Nesse contexto, assevera constituir dever de um Estado democrático de direito garantir, em face da realidade tecnológica, "adequada e efetiva proteção dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais." Disponível em: downloadPeca.asp (stf.jus.br) .Acesso em 18.05.21.

Destaca-se que o mesmo dispõe de dados das declarações anuais da Receita Federal dos contribuintes e seus dependentes, sigilos fiscais e bancários mantidos pelo Banco Central, bem como do gerenciamento de dados dos trabalhadores brasileiros pela Caixa Econômica Federal -CEF, através do Fundo de Garantia por Tempo de Serviço (FGTS); do amplo cadastro de dados sensíveis de serviços de saúde da base do Sistema Único de Saúde- SUS, cujo histórico de tratamento também é compartilhado com hospitais conveniados.

Não obstante, possui ampla disposição de informações armazenadas oriundas de sua tutela sobre os processos judiciais e administrativos, arquivos eletrônicos da Justiça Eleitoral com dados de eleitores, dados dos seus segurados do sistema de previdência social administrados pela entidade autárquica do Instituto Nacional do Seguro Social (INSS) e, sem pretensão de esgotar o tema, ainda há a questão do arquivamento de imagens oriundo do reconhecimento facial implementado pelos serviços sofisticados de segurança pública.

Na assertiva de Regis Fernandes:

Se sei quem é o outro, se conheço seu patrimônio, se percebo sua cultura, sua formação intelectual, os dados de sua vida anterior (eventualmente qualquer tipo de constrangimento por que passou) isso dá ao interessado uma situação privilegiada. [121]

[121] DE OLIVEIRA, Regis Fernandes. Os Fundamentos da Lei de Proteção de Dados Pessoais. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p.167.

A sociedade da pós-modernidade, reestruturou o processamento das informações, os papéis deram lugares ao armazenamento "nas nuvens" linkados a provedores e processados por *softwares* cada vez mais potentes. Na mesma linha, evidentemente, seguiu a administração[122] pública, a fim de facilitar seus canais de transparência e desburocratizar o sistema. Hoje, órgãos e entidades de todas as esferas já viabilizam o acesso aos seus cidadãos até mesmo por aplicativos.[123][124]

A problemática do presente estudo, está na constatação da incapacidade do Governo de prover a segurança dos dados de seus cidadãos.[125] Ao instalar tais '*apps',* logo se depara com uma ficha de informações para preencher e, assim, se ter o acesso liberado, como CPF, *e-mail,* nome completo, RG etc.

Indaga-se: Como o Estado trata tais dados? Ele os utiliza apenas à finalidade destinada? Esta finalidade é transparente? Assim sendo, a transparência é realizada de modo adequado? Os dados requisitados são todos necessários à finalidade?

---

[122] Imperioso mencionar o recente Decreto nº 10.332/20, instituído para estabelecer um governo digital até 2022 de maneira unificada em todo o país. Disponível em: D10332 (planalto.gov.br). Acesso em 20.05.21.

[123] ABREU, Jaqueline de Souza; LAGO, Lucas; MASSARO, Heloisa. Internet Lab. ESPECIAL| Por que se preocupar com o que o Estado faz com nossos dados pessoais? Disponível em: https://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/ . Acesso em 19.05.21.

[124] Entre os quais temos o e-Título, E-social, a CNH digital, Meu Imposto de Renda, Meu INSS, Bolsa Família, CAIXA, SNE Denatran, além dos próprios sistemas do IRPF, CNIS, Consumidor.Gov, DNI criado pela Lei Nacional de Identidade n° 13.444/17, e outros.

[125] Os tribunais, ministérios e demais órgãos têm sofrido recorrentes ataques cibernéticos em seus sistemas por parte de ***hackers.*** Disponível em: https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/ Acesso em 20.05.21.

Como os armazena e até quanto tempo? Quais normas e técnicas de padrão de segurança faz uso para evitar vazamentos? Esses são alguns dos questionamentos que se pretende abordar nesta temática.

No mais, muito além do comportamento dos indivíduos de não ler as políticas de privacidade e termos de uso corroborar com a conjuntura atual, existem os perigos da adoção do compartilhamento de dados sem a devida governança corporativa entre as esferas de poder. Por fim, e não menos importante, o *modus operandi* pelo qual a administração pública realiza a transparência exigida de um Estado democrático de Direito[126], será profundamente afetado com a entrada da LGPD em vigor.

1. TRATAMENTO DE DADOS PESSOAIS PELO SETOR PÚBLICO: CONCEITOS E FUNDAMENTOS

Seguindo a linha da tendência mundial, a LGPD, acertadamente, abarcou um capítulo exclusivo ao poder público, muito embora tenha havido fortes coalizões contra a sua implementação na Lei.

Preliminarmente, para que seja possível a análise acerca da proteção de dados pelo poder público, é necessário compreender os objetivos principiológicos trazidos pela Lei. A fim de proteger os direitos fundamentais de liberdade, intimidade e privacidade constitucionalmente previstos, além de definir dados pessoais e sensíveis[127], a lei tratará de forma clara em

[126] Art.37: "A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência(...)"

[127] Art. 5º: Para os fins desta Lei, considera-se: I - dado pessoal: informação

seu artigo 6º, os requisitos primordiais para que exista o tratamento.[128] Assim dispõe:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade:[129] realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem

---

relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[128] Art.5º : (...)- X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[129] Nota-se que a finalidade é a primeira dentre os 10 princípios. Busca-se que os dados sejam utilizados para as finalidades as quais foram coletadas, e não àquelas não relacionadas diretamente com à política pública ou competência legal com a qual se pretenda. Para tanto, a *accountability* neste processo é imprescindível. Já sob a égide da LGPD, o Tribunal de Justiça de São Paulo, em ação civil pública proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em face da Concessionária Da Linha 4 Do Metrô De São Paulo S.A. (Via Quatro) - que embora seja empresa privada, incide no cap. de regime público da norma, vide art. 24 c/c 173 da CF- resolveu condenar a ré, acolhendo parcialmente o mérito. Com base na LGPD, arts. 2º e 6º, I, a magistrada reconheceu nos autos que houve captação de imagens de usuários, inclusive crianças, sem o conhecimento ou consentimento dos mesmos, para fins comerciais que beneficiavam a ré e a empresa por ela contratada, "o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, ambos elencados no artigo 6º, III e IV do Código de Defesa do Consumidor" "Ainda, a finalidade do tratamento deve ter propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I)". SÃO PAULO. Tribunal de Justiça de São Paulo- TJSP. 37ª

possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

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;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Vara Cível da Comarca de São Paulo, Autos n. 1090663-42.2018.8.26.0100. Juíza de Direito Patrícia Martins Conceição. Julgado em 07.05.2021.

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nessa perspectiva, tem-se como evidente, a tentativa de equilibrar a relação cidadão- Estado, colocando o indivíduo como elemento central da norma, oferecendo ao mesmo, maiores mecanismos de proteção e controle sobre suas informações.[130]

Para cada tratamento, seja no âmbito digital ou físico, haverá de ter uma base legal para fundamentar a atividade do operador e/ou controlador.[131] Ao setor público, a base legal a que se lhe destina, será a hipótese prevista nos artigos 7,

[130] Nesse mesmo sentido, merece atenção a disposição acerca da amplitude da LGPD em relação à Lei do *Habeas Data*. Disponível em: JUNIOR, Francisco Gabriel Pacheco. O tratamento de dados pessoais pelo setor público e o alcance da LGPD -. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 317-319.

[131] Art.5º: (...)VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; IX - agentes de tratamento: o controlador e o operador;

inciso III e artigo 11, II, "b". Ambas aduzem expressamente que: A administração pública poderá tratar e fazer uso compartilhado de dados quando 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.

Todavia, Miriam Wimmer[132] entende que a leitura de tais artigos devem ser feitas conjuntamente ao *Caput* do artigo 23 da Lei- interpretando-se de acordo com a alínea "a" do artigo 11[133]- uma vez que não somente de políticas públicas trata o Estado, mas também de dados dos seus próprios servidores e gestores públicos, bem como de dados no exercício de suas atribuições cotidianas legais. Portanto, o tratamento de dados pelo setor público deverá observar as suas competências legais e a execução de políticas públicas.

No entanto, a Lei é rodeada de subjetividade e normativas em branco, a saber, é necessário consultas em outros diplomas jurídicos, como, por exemplo, a doutrinas de direito administrativo, para que haja a correta incidência da norma. É imprescindível conhecimento técnico acerca do conceito

[132] WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades, p.131-2. Revista do advogado, Ano XXXIX, n.144, p.126-133, nov. 2019.

[133] Art. 11: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II- sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: A) cumprimento de obrigação legal ou regulatória pelo controlador. B) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.

de políticas públicas,[134] administração pública e pessoas de direito público.[135]

Antes fosse apenas este o obstáculo. Uma leitura no aludido artigo 23 faz urgir uma demanda de se delimitar o termo "interesse público". Veja-se:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (...)

[134] Entende-se por política pública, nas palavras de Bandeira de Mello: "um conjunto de atos unificados por ato condutor que os reuniria ao objetivo, meta ou alvo comum de realizar um projeto de governo para o país." BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. São Paulo: Malheiros, 2013, PP. 830-831.

[135] Preceitua o artigo 1º da Lei: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." Às pessoas de direito público, enquadram-se todas aquelas referidas no art. 1º da Lei de Acesso à informação -LAI. Veja-se: "(...)Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios." Ressalta-se que às atividades delegadas à serviços privados, como a de registro notariais, se incidirá o mesmo regime jurídico aplicável ao poder público, pois o que importa é a atividade exercida e não a espécie de entidade, assim ocorre com as estatais que operacionalizam políticas públicas.

Historicamente, a alegação da supremacia do interesse público tem vencido sobre interesses privados. Sendo o interesse público[136] e a finalidade pública os norteadores do tratamento de dados pelo Estado, poderá haver inúmeras justificativas arbitrárias sob o pretexto daquele, a ponto de se ferir o princípio da minimização dos dados com o intenso volume de dados cruzados, armazenados e expostos a público sem critério ou utilidade. O que se verá a seguir.

2. UM DIÁLOGO ENTRE A LEI DE ACESSO À INFORMAÇÃO E A LGPD.

A LAI e a LGPD, ressalvadas pequenas semelhanças, possuem objetivos eminentemente opostos. Enquanto a primeira visa a divulgação e o acesso aos dados abertos[137] aos cidadãos,

[136] "Interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de o serem. Não se trata do interesse de um todo abstrato, mas sim da faceta coletiva dos interesses individuais." BANDEIRA DE MELLO, *Op. Cit.,* 25.ed.,2008, p.61. No entanto, ressalta-se que o interesse público não pode jamais se confundir com o da administração pública e tampouco com o do agente público. BUCAR, Daniel; OLIVEIRA, Rafael Carvalho Rezende. A Lei Geral de Proteção de Dados e a Administração Pública: por uma convergência da privacidade com o interesse público. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 898. "(...) A definição do que é o interesse público, e de sua propalada supremacia sobre os interesses particulares, deixa de estar ao inteiro arbítrio do administrador, passando a depender de juízos de ponderação proporcional entre direitos fundamentais e outros valores e interesses metaindividuais constitucionalmente consagrados(...)." BINENBOJM, Gustavo. *Da supremacia do interesse público ao dever de proporcionalidade: um novo paradigma para o direito administrativo.* In: SARMENTO, Daniel (org.) *Interesses públicos x interesses privados: desconstruindo o princípio da supremacia do interesse público.*2.tir.Rio de Janeiro: Editora Lumen Juris,2007,p.128.

[137] O decreto n° 8777 institui o conceito e política de dados abertos. Dis-

como forma de cumprir com a transparência exigida de um Estado republicano[138] - seja de maneira ativa ou passiva- a segunda, tem por primordial, a tentativa de minimização da exposição dos dados pelo poder público, fazendo jus à defesa dos direitos da privacidade.[139]

Ocorre que, na LAI[140]- assim vista como o grande marco regulatório do artigo 5º, inciso XXXIII, da CF/88, que estabeleceu a necessidade de transparência no país, ainda sendo uma cultura muito recente- dados pessoais e sensíveis podem ser considerados abertos e não incidirem no âmbito da LGPD, mediante exceção prevista no artigo 31, § 3º. Em uma dessas exceções, encontra-se o referido interesse público e geral preponderante, *vide* inciso V.

---

ponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm .

[138] Estado em que se exige um "governo do poder visível, em que nada pode permanecer confinado no mistério" BOBBIO, Norberto. O futuro da democracia: uma defesa das regras do jogo. Trad. Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra,1986, p.83 e 84. Adicionalmente, nas palavras de Bandeira de Mello: "Não pode haver em um Estado Democrático de direito, no qual o poder reside no povo, ocultamento aos administrados dos assuntos que a todos interessam, e muito menos em relação aos sujeitos individualmente afetados por alguma medida." Op cit.2013, p.114, edição digitalizada.

[139] GLASSMAN, Guillermo. Interfaces Entre o Dever de Transparência e a Proteção dos Dados Pessoais no Âmbito da Administração Pública-. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 863; RIBEIRO, Giovana Bellini. Compatibilidade Entre a Proteção de Dados Pessoais e o Dever De Transparência Pública -. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p.293.

[140] BRASIL. Lei nº 12.527. ***Planalto***, Brasília, 18 de novembro de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em 09.05.21.

É bem verdade que a transparência aumenta o controle social[141] por parte dos administrados e fomenta a participação democrática nos atos administrativos. Contudo, há exposições que são questionáveis, sobretudo nos meios eletrônicos.

A resolução n° 269 de 2018 dispõe acerca da divulgação de dados pessoais dos candidatos a concursos públicos. O artigo 2º prescreve que "Em todos os concursos públicos do Poder Judiciário, os tribunais divulgarão apenas o nome completo e o número de inscrição dos concorrentes à(s) vaga(s) pública(s)." No entanto, parece que a divulgação nominal se torna inadequada por conta do princípio da minimização, podendo apenas ser divulgado o número de inscrição.

Em uma ponderação entre o interesse público e a privacidade, conclui-se que o receio de sofrer discriminações e represálias em empregos privados pela exposição, se sobressai frente aos anseios sociais.

---

[141] Todavia, permitindo-se fazer referência ao direito comparado, a transparência não deve ser interpretada como somente a disposição desenfreada de todas as informações nos sítios eletrônicos. A prefeitura de Aleksandrów Kujawski, na Polônia, que tinha o costume de divulgar suas informações em uma espécie de boletim, o BIP (*Biuletyu Informacji Publicznej*), além de transmitir ao vivo as sessões do Conselho Municipal pelo *Youtube*, que ficavam gravadas, foi condenada a uma multa de 50 mil reais por entender a Autoridade que o Município e o prefeito violaram a *GDPR* ao "não possuir um contrato com a empresa que gerenciava o BIP; ao não manter políticas relevantes quanto ao armazenamento, finalidade e exclusão de dados; ao não realizar uma análise de risco quanto à utilização do Youtube; ao manter os vídeos apenas no Youtube, sem uma cópia de segurança; Ao não possuir um registro com data planejada de exclusão do site das informações". PEDROSO, Lucas Aluísio Scatimburgo. Tratamento de dados pessoais pelo Poder Público: o que esperar segundo a experiência europeia? -. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 336.

Embora o § 2º discorra que os tribunais deverão utilizar a tecnologia no *follow* ou ferramenta similar para inibir a atuação de buscadores de informação nas páginas eletrônicas em que constarem dados pessoais dos candidatos, uma simples busca pelo nome completo, ainda assim, recorrentemente, expõe nome e tipos de inscrição dos mesmos. Se há um interesse público nessa questão, giraria em torno de candidatos com condenação criminal transitada em julgado inscritos em concursos. Contudo, seria papel inviável do Ministério Público averiguar cada uma delas, ao passo que, mesmo por denúncias, restaria mais bem resolvido na própria fase de investigação social dos certames.

Constatação relevante também se dá na questão da ausência de regulamentação da publicidade dos processos judiciais eletrônicos para que se incida a LGPD. Há a disponibilidade de dados básicos em consulta pública livre na *internet* [142] e aquela dos processos na íntegra, mas com acesso restrito. Existe uma gama infinita de dados de titulares dispostas nos processos públicos, como extratos

[142] O presente artigo não pretende explorar o fenômeno da desindexação, o que é matéria que necessita de análise complexa, não cabível no momento. No entanto, é imprescindível mencionar o IRDR n° 70082616665 instaurado no TJRS, que circunda diretamente sob a temática da publicidade, quando discute acerca da responsabilidade civil de startups que atuam como buscadores de informações processuais dispostas publicamente nos diários oficiais. O processo originário discute acerca da "divulgação de informações nos sites de busca ESCAVADOR e GOOGLE de reclamatória trabalhista, cujo objeto era o pagamento de indenização por danos morais, bem como a retirada permanente dos dados das páginas." Baseado na insegurança jurídica causada pelas decisões conflitantes pelo país acerca desse contexto, o STF está, no momento da divulgação deste artigo, para julgar a repercussão geral no ARE 1307386- Tema 1141.

bancários, CPF, endereço, que até mesmos advogados não habilitados nos autos podem acessar facilmente[143], o que já amplia consideravelmente o número de pessoas visualizando dados alheios pelo país.

De fato, por mais que a forte cultura de publicidade existente auxilie tais advogados e à comunidade jurídica como um todo, como por exemplo, no caso de uma nova propositura de ação em face do titular do dado a qual não se conseguia achar sua atual residência, conseguida através de dado de processos recentes, ou até mesmo no envio de mandados e precatórias ao correto endereço, ademais da listagem de processos nos buscadores contribuir e ser determinante aos consumidores e empregadores para fechamento de negócios e empregos, há de se existir um método empregado para redução de exposição de dados.

Sabe-se que a ampla regra difundida é a publicidade, a não ser que exista segredo de justiça decretado nos autos. Contudo, a LGPD, como visto, já é direito constitucionalmente reconhecido e assume posição no ordenamento jurídico brasileiro. É de todo interesse que publicidade e privacidade andem lado a lado na medida do possível, visto que a divulgação de dados pessoais e sensíveis podem representar riscos dos mais variados níveis aos cidadãos, o que não se coadunaria com o fundamento do artigo 1º, III, da constituição[144].

---

[143] *Vid*e art.3º, § 1º da Res. nº 121 de 05/10/2010 do CNJ c/c artigo 11, § 6º e 7º da Lei n° 11.419/06.

[144] "Se a dignidade da pessoa humana não for observada, poderá o Estado continuar na persecução do interesse público? Certamente que não." NEVES, Edmo Colnaghi. Dados pessoais e interesse público. In: LGPD &

Acredita-se que o posicionamento de 2015 do STF no julgamento do ARE n° 652.777, acerca da divulgação nominal junto ao vencimento de servidores possa sofrer alteração. Neste impasse, a corte entendeu que a divulgação dos nomes e cargos junto ao salário nos portais de transparência é um ônus a qual o servidor se submeteu previamente e anuiu quando de sua escolha. Para alguns, a exposição do nome serve para satisfazer a mera curiosidade alheia, para outros, o dado pessoal é imprescindível para sua finalidade, a transparência.

Diferentemente do que ocorre no caso dos inscritos em concursos públicos, parece que faz jus o voto do ministro relator Teori Zavascki, que assim explicita "(...)a negativa de prevalência do princípio da publicidade administrativa implicaria, no caso, inadmissível situação de grave lesão à ordem pública"[145]. A possível futura troca de nome por apenas matrícula junto aos vencimentos, impacta o controle social de forma direta, na medida que pode ensejar casos de pagamentos de servidores fantasmas ao não conseguir se identificar o beneficiário das verbas públicas.

Um diálogo entre as duas leis será aferido caso a caso pelo poder judiciário, mediante forte análise técnica, pelo método comumente utilizado de ponderação dos princípios.[146]

Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 202.

[145] Disponível eletronicamente em: paginador.jsp (stf.jus.br) , p.12.Acesso em 07.06.21.

[146] Sobre a ponderação, recomenda-se fortemente a leitura integral do artigo: CANHADAS, Fernando Augusto Martins. A Lei de Acesso à infor-

3. O RISCO DO IRRESTRITO COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS E ENTIDADES

Primordialmente, é preciso ter em mente que o termo "finalidade" disposto no artigo 23 é diferente do disposto no artigo 6º, I. A primeira se refere a elemento vinculado do ato administrativo e a adequação pelo poder público aos princípios basilares da administração pública, - como legalidade e impessoalidade, - já a segunda, se refere exclusivamente ao objetivo da coleta dos dados.

Até 2016, antes da edição do decreto n° 8.789/16, o compartilhamento de dados entre órgãos e entidades se valia da necessidade prévia de acordos ou convênios. O posterior decreto n° 10.046/19[147], a qual substitui o de 2016, e institui o Cadastro Base do Cidadão, tem como alguns dos principais objetivos : (I) Simplificar a oferta de serviços públicos; (II) Orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;(III) Possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;(IV) Promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e (V) Aumentar a qualidade e a eficiência das operações internas da administração pública federal.

---

mação e a Lei Geral de Proteção de Dados: a transparência proibida-. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p.425-441.

[147] BRASIL. Lei nº 10.046. ***Planalto***, Brasília, 09 de outubro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm . Acesso em 08.06.21.

Inicialmente, esse Cadastro contará com dados cadastrais, atributos biográficos e atributos biométricos provenientes da base de dados do CPF, mas será acrescido, posteriormente, de informações provenientes de outras bases temáticas (...) Com o CBC, não apenas os antigos dados cadastrais podem ser compartilhados livremente e de forma automática entre órgãos e entidades, mas uma ampla variedade de dados pessoais produzidos e coletados pelo Estado no curso da execução e implementação de políticas públicas, inclusive dados sensíveis.[148]

O grande questionamento se dá quando há a percepção de que tal política fere o próprio princípio de finalidade da LGPD. Os administrados concedem seus dados para atuação em cada repartição específica e para propósitos informados, de modo que o intercâmbio deles sem distinções prévias, a fim de facilitar a gestão estatal[149], pode fugir do escopo inicial a qual os dados foram coletados.

Apesar da própria LGPD garantir em seu artigo 25 que os dados sejam tratados em formato estruturado e interoperável, é preciso que o Estado, além de garantir a segurança da informação e os devidos cuidados para evitar acessos não

[148] FRAGOSO, Nathalie; MASSARO, Heloisa. Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina? Disponível em: https://www.internetlab.org.br/pt/privacidade-e-vigilancia/cadastro-base-e-amplo-compartilhamento-de-dados-pessoais-a-que-se-destina/ Acesso em 08.06.21.

[149] Uma norma que autoriza o compartilhamento de dados não protegidos por sigilo fiscal pela Secretaria da Receita Federal do Brasil, a órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional é a portaria n° 1384 da RFB de 09/09/16. Disponível em: Port. RFB Nº 1384 - 2016 (fazenda.gov.br) . Acesso em 14.06.21.

autorizados[150], atenda integralmente ao disposto no artigo 6° da Lei, em específico à finalidade, sempre se atentando à boa fé e a transparência do tratamento[151], não bastando apenas o pretexto de se valer de dados compartilhados para reduzir a imagem de uma administração engessada, sob pena de esvaziar o objetivo da Lei.

CONCLUSÃO

Para que a inserção da LGPD seja uma realidade no cotidiano da administração pública, é necessária uma ampla atuação dos encarregados juntamente ao escalão de gestão de cada órgão.

Sendo o encarregado aquele que fará a intermediação entre os titulares dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) e o controlador, é imprescindível que ele tenha autonomia para tanto, e o mais importante,

[150] Interessante trazer um caso de desvio de finalidade ocorrido na Bélgica em 2018, onde, em época de eleições, um prefeito se utilizou ***de e-mails*** trocados entre a repartição e 2 cidadãos, que tinha o objetivo finalístico de pleitear a mudança de um plano urbanístico, para no ano seguinte, enviar-lhes ***e-mails*** pedindo votos. O mesmo ocorreu com outro prefeito que aproveitou os dados coletados nas reuniões realizadas em seu mandato para pedir votos posteriormente. PEDROSO, Lucas Aluísio Scatimburgo. Tratamento de dados pessoais pelo Poder Público: o que esperar segundo a experiência europeia? Op. Cit. p. 340.

[151] KUJAWSKI, Fábio Ferreira; CASTELLANO, Ana Carolina Heringer. Compartilhamento de Dados Pessoais No Âmbito Da Administração Pública Sob a Égide da Lei Geral de Proteção de Dados-. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 321; MOREIRA, Patrícia Prieto. Tratamento e Uso Compartilhado de Dados Pessoais Pela Administração Pública na Execução de Políticas Públicas-. In: LGPD & Administração pública: Uma análise ampla dos impactos-Rio de Janeiro: Revista dos Tribunais, 1ª ed., 2020, p. 275.

não acumule cargos, ora que, nitidamente, já sendo o mesmo servidor público ou DPO, impactaria substancialmente em suas atribuições.

Infelizmente, a LGPD ainda é uma Lei bastante principiológica, que necessitará de maiores complementos e limitações dadas pela ANPD[152], onde inclusive, tem sua independência frente ao governo questionada por doutrinadores. Sua estruturação ainda está sendo composta, estando para discutir possíveis sanções aplicadas ao poder público, visto que, ao mesmo não caberá pagamento de multa por descumprimento da Lei.

Conclui-se que será necessário, além de investimentos em sistemas de informação[153], a incorporação da política do *Privacy by Design,* com a inserção de ações educativas para a conscientização de todo o corpo de servidores acerca da privacidade dos dados,[154] mediante treinamentos a estabe-

[152] Recentemente, foi publicada no Diário Oficial da União (DOU), a primeira regulamentação oficial da ANPD. Resolução/CD/ANPD n° 1, de 28 de outubro de 2021 que aprova o regulamento do processo de fiscalização e do processo Administrativo Sancionador no âmbito da ANPD. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de--28-de-outubro-de-2021-355817513. Acesso em 05.11.21.

[153] Em se falando de tecnologia, o poder judiciário de Santa Catarina se tornou o pioneiro no país na implementação da LGPD. Com um projeto-mais especificamente o aplicativo 'LGPDJUS'- desenvolvido pelo Instituto de Tecnologia e Sociedade (ITS) em parceria com o Laboratório de Inovação e Inteligência da Associação dos Magistrados Brasileiros (AMBLab) e com apoio do Ministério de Relações Exteriores e Desenvolvimento do Reino Unido (Foreign Commonwealth and Development Office – FCDO). Disponível em LGPDJus: aplicativo para solicitações sobre proteção de dados pessoais é lançado neste 30/07 (itsrio.org) . Acesso em 10.11.21.

[154O] STF, em complementação a sua resolução de n° 363 de 12.01.21, instituiu por meio da resolução n° 724 de 02.03.21 o comitê Executivo de

lecer regras internas de supervisão e mitigação de riscos, além de medidas a serem tomadas no caso de incidentes de segurança, padrões técnicos e normas de segurança, seguidos de muito comprometimento e monitoramento contínuo.

Proteção de Dados para identificar e implementar as medidas necessárias à adequação da LGPD no Tribunal. Disponíveis em: https://atos.cnj.jus.br/files/original181204202101196007 20f42c02e.pdf e Res_724_2021_STF.pdf (stj.jus.br). Na mesma linha, o município do Rio de Janeiro, através do recente Decreto n° 49.558/2021, passou a estabelecer regras e procedimentos para a Administração Pública Municipal na fase de adaptação a nova Lei. Caberá à Procuradoria do Município a criação de cláusulas padrão a serem adotadas por toda a administração pública direta e indireta, além da aplicação de questionários para avaliação da maturidade de todos os órgãos e entidades; realização de relatório de impacto à proteção de dados e ainda a designação do encarregado (DPO). Disponível em: Editora Roncarati - DECRETO MUNICIPAL (RJ) Nº 49.558, DE 06.10.2021 | Diário Oficial. Acesso em 10.11.21.

A PROTEÇÃO DE INFORMAÇÕES PESSOAIS NA CHINA: ANÁLISE À LUZ DO NOVO CÓDIGO CIVIL CHINÊS DE 2021

Larissa Chen Yi Qian [155]

1. INTRODUÇÃO AO PENSAMENTO JURÍDICO CHINÊS

A República Popular da China é um Estado socialista subordinado à ditadura democrático-popular da classe operária e assente na aliança dos operários e camponeses. [156]Para compreender o Estado chinês é preciso esclarecer que o cenário jurídico da China moderna ainda está sendo escrito.

Nas últimas décadas, o Sistema Jurídico Chinês passou por uma rápida modernização, emergindo como um sistema híbrido da tradição legal imperial, Direito ocidental e Direito socialista soviético.[157] Devido à sua cultura ancestral, adquiriu uma tradição legal *sui generis* de modo que muitas questões sobre o tema não podem ser respondidas somente com base em estudos sobre Estado de Direito (*rule of law*); é necessário examinar a cultura, os costumes, as tradições e as atitudes das pessoas em relação ao Direito e a autoridades. [158]

---

[155] Pós- graduanda em Direito Digital pela Universidade do Estado de Rio de Janeiro em parceria com o Instituto de Tecnologia e Sociedade. Graduada em Direito pelo Instituto Brasileiro de Mercado de Capitais de RJ. Pesquisadora no Projeto CyberBricks do Centro de Tecnologia e Sociedade/FGV. Advogada com atuação na área consultiva.

[156] The Peoples Republic of China is a socialist state under the people´s democratic dictatorship led by the working class and based on the alliance of workers and peasants. Disponível em: < http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_12372963.htm>.

[157] PEREIRA, Venício Branquinho. Direito constitucional na China. In: POLIDO; Ramos, 2015, p. 149.

[158] FERRARI, Leandro. Introdução ao pensamento jurídico chinês: estudo histórico-crítico. Canoas: Consultor Editorial, 2017. p. 52.

Desde a época do império, a filosofia confucionista foi a principal responsável por influenciar todos os ramos sociais e culturais da China. Assim, as regras de conduta e os ritos trazidos por Confúcio expressam-se em grande medida na agremiação de práticas costumeiras e não escritas. Esse conjunto de normas sociais é traduzida pelo conceito de *Li* [*礼*], [159] e acreditava-se que seriam suficientes para manter a paz social, sendo indesejável a condução de soluções por meio de um direito posto e institucionalizado de sanções, conhecido como *Fa* [法][160], que seriam traduzidos como as normas escritas pelo Estado defendidas pela escola do legalismo.

Por outro lado, tem-se a filosofia do taoísmo que se traduz na expressão *Dao* [*道*] o qual significa o "caminho a seguir", a qual foi copilada principalmente na obra conhecida como *"Dao de Jing"* [*道德经*], contendo os ensinamentos do *Lao Zi* [*老子*], juntamente com os do *Zhuang Zi* [*庄子]*.[161] Pelo taoísmo, preconiza-se a existência de uma ordem espontânea de equilíbrio do universo, propiciado pelo embate equânime entre as forças *Yin* e *Yang*[162]. Por isso, diferentemente do confucionismo, o taoísmo prega pelo não controle e pela regulação espontânea.

[159] BIAZI, João Pedro de Oliveira de: (org.) Qian, Larissa Chen Yi (trad.). Código Civil Chinês- 1. Ed.- São Paulo: Edulex, 2021. p. 13.

[160] VICENTE, Dário Moura. Direito Comparado, 4. Ed., v.1, Edição Brasileira, São Paulo, Almeida, 2018, p. 452,

[161] BIAZI, João Pedro de Oliveira de: (org.) Qian, Larissa Chen Yi (trad.). Código Civil Chinês- 1. Ed.- São Paulo: Edulex, 2021. p. 13.

[162] ROCHA, Rafael Machado da. Raízes do pensamento chinês: confucionismo, taoísmo e legalismo. In: POLIDO, Fabrício Bertini Pasquot; Ramos, Marcelo Maciel (coord.) Direito chinês contemporâneo, São Paulo, Almedina, 2015, p. 37.

Durante o período do Século XX, o Direito Chinês sofreu influências marxista-leninistas em que teve um efeito devastador para o direito chinês, tendo uma ruptura abrupta com o passado. O ponto mais marcante foi que a advocacia foi abolida e as diretrizes políticas tomaram lugar da lei como fundamento das sentenças. [163]

Somente a partir do Governo de *Deng XiaoPing [邓小平]* e com a vigência da Constituição de 1982, que se reinicia um movimento de construção de um Sistema Jurídico verdadeiramente chinês. Apesar de sofrer ainda grandes influências do direito imperial baseado no confucionismo, houve a influência do pragmatismo e da globalização dos estudos em direito na China, de tal forma que algumas notas do pensamento jurídico ocidental foram incluídas.[164]

Essa é a base do pensamento jurídico que suportou os trâmites e discussões do Código Civil Chinês, uma tradição jurídica que reflete orientações filosóficas tradicionais, porém sem ignorar as diretrizes fornecidas por um pensamento mais contemporâneo do direito civil. [165]

Antes do Código Civil, a legislação de direito privado na China era espalhada em estatutos esparsos. O principal objetivo do Código consiste na organização de todas essas legislações de direito privado em um único texto normativo, para conferir maior operabilidade e compreensão do seu conteúdo.

---

[163] VICENTE, Dário Moura. Direito Comparado. 4. Ed., v. 1, Edição Brasileira, São Paulo, Almedina, 2018, p. 455.

[164] VICENTE, Dário Moura. Direito Comparado. 4. Ed., v. 1, Edição Brasileira, São Paulo, Almedina, 2018, p. 458.

[165] BIAZI, João Pedro de Oliveira de: (org.) Qian, Larissa Chen Yi (trad.). Código Civil Chinês- 1. Ed.- São Paulo: Edulex, 2021. p. 15.

A elaboração do Código começou em 2014 e foi dividida em duas fases de trabalho. A primeira foi destinada à elaboração da "Parte Geral", que foi finalizada em 2017. Na segunda parte, os grupos de trabalho passaram a cuidar da elaboração das seis "Partes separadas" do Código, o que equivale à Parte Especial do Código Civil Brasileiro. Finalmente, ela entrou em vigência em 1º janeiro de 2021. [166]

Destaca-se que a Parte Geral sofreu influências dos países de codificações romano-germânicas. No que se refere à parte especial, chama a atenção a divisão dos capítulos específicos de acordo com os diferentes assuntos da vida civil. Em especial, chama a atenção o Capítulo VI do Livro IV em que trata dos direitos à privacidade e proteção de informações pessoais[167] como um direito da personalidade, tema que será abordado ao longo do presente artigo.

Portanto, considera-se o Direito Contemporâneo Chinês como uma aliança entre a cultura milenar chinesa com sua preferência de um controle social fora do direito, e o pensamento jurídico moderno alinhado com as expectativas normativas próprias de uma economia global e em franco crescimento. [168] A codificação trouxe ao país uma unificação das legislações civis esparsas, constituindo o Código Civil mais moderno que

[166] BIAZI, João Pedro de Oliveira de: (org.) Qian, Larissa Chen Yi (trad.). Código Civil Chinês- 1. Ed.- São Paulo: Edulex, 2021. p. 16.

[167] A Lei Geral de Proteção de Dados brasileira usa o termo de "proteção de dados", por outro lado, no Código Civil Chinês optou pelo uso do termo de" proteção de informações pessoais" devido a sua literalidade na tradução. Apesar desta diferença, pode-se constatar que o termo de proteção de informações pessoais equivale ao de proteção de dados pessoais.

[168] BIAZI, João Pedro de Oliveira de: (org.) Qian, Larissa Chen Yi (trad.). Código Civil Chinês- 1. Ed.- São Paulo: Edulex, 2021. p. 15.

existe nos dias de hoje[169]. Assim, é de se esperar que preveja normas basilares para a Proteção de Informações Pessoais.

2. PRINCIPAIS MOTIVOS QUE ENSEJARAM A ADOÇÃO DA PROTEÇÃO DE INFORMAÇÕES PESSOAIS

Com a globalização, consequentemente com o aumento do fluxo de informações entre os países, o tema de proteção de informações pessoais ganhou especial destaque na China. Para tal, serão analisados os motivos principais que ensejaram a proteção de informações pessoais no Código Civil Chinês.

Atualmente a China é considerada o país com maior número de usuários de Internet, isto por si só já constitui interesse na regulamentação das informações que são trocadas através da rede. Conforme o Relatório 48 Estatísticos sobre o Desenvolvimento da Internet na China (Relatório), divulgado na data de 27 de agosto de 2021, o número de usuários de Internet atingiu 1,011 bilhão com um aumento de 21,75 milhões em relação a dezembro de 2020. [170]

O crescimento exponencial de acesso se deve ao crescente mercado consumidor da China e ao desenvolvimento da Economia Digital. O diretor do Centro de Informações de Rede de Internet da China (CNNIC) *Zeng Yu*, afirma que no momento da Economia Digital, a Internet se tornou uma nova força motriz para o crescimento econômico e novos modelos

169ROSPIGLIOSI, Enrique Varsi. El primer Código Civil de la República Popular de China [Parte I]. Produção Enfoque Derecho. Disponível em < https://www.youtube.com/watch?v=9s6Nw3e7J9I>. Acessado em 12/05/2021.

[170] ZHANG Gang. WANG Kai: O 48º Relatório Estatístico sobre o Status de Desenvolvimento da Internet na China. Disponível em < http://www.chinanews.com/gn/2021/08-27/9552404.shtml> Acessado em 28/10/2021.

de negócios estão surgindo a toda hora. No mesmo sentido, o vice-diretor do CNNIC entende que durante a pandemia causada pelo vírus Covid-19, a Internet desempenhou um papel de suma importância na garantia do consumo, do emprego, da educação e da promoção de retomada de todas as atividades de produção. [171]

Os fatos que contribuíram para o aumento no acesso da Internet foram primordialmente os seguintes: (i) a melhoria contínua da construção das infraestruturas tecnológicas, o qual possibilitou a China em construir a maior rede de fibra óptica e comunicação móvel do mundo; (ii) o desenvolvimento da Economia Digital que viabilizou o crescimento das compras online e que teve uma grande procura durante a pandemia; e, (iii) finalmente a maior integração dos aplicativos com a vida cotidiana da sociedade devido ao aumento das suas funções que demandam o acesso a rede da internet. [172]

O ex-secretário-geral adjunto da *Internet Society of China*, *Sun Yongge* relata que há outros fatores que auxiliaram no aumento do uso da Internet e no rápido desenvolvimento dos principais campos da tecnologia, tais como o *Blockchain*, IPV6, 5G, Inteligência Artificial e *Big Data*.

Em relação a melhoria das infraestruturas tecnológica, segundo o Relatório 48º a proporção de usuários de banda larga de fibra óptica na China aumentou para 94%, a velocidade de

[171] ZHANG Huai Yin. Análise da proteção de informações pessoais na era do Big Data. Disponível em < http://www.xinhuanet.com/politics/2020-04/28/c_1125915967.htmv>. Acessado em 11/05/2021.

[172]ZHANG, Huai Yin. Análise da proteção de informações pessoais na era do Big Data. Disponível em < http://www.xinhuanet.com/politics/2020-04/28/c_1125915967.htm>. Acessado em 11/05/2021.

experiência do usuário ponta a ponta da banda larga fixa atingiu 51,2 Mbps e a velocidade da rede móvel ocupa o quarto lugar entre 139 países e regiões em o mundo. Consolidando assim, a maior rede de informação e comunicação do mundo.

No que se refere ao desenvolvimento da Economia Digital, desde a pandemia, os negócios de entrega imediata, representado por alimentos frescos e medicamentos, desenvolveu-se rapidamente junto com os serviços de entrega de alimentos, tais fatores ajudaram na subsistência das pessoas. Conforme o Relatório 48, a China atingiu 456 milhões em junho de 2021, um aumento de 49,76 milhões em relação a dezembro de 2020. Isto posto, é inquestionável que na Era da Economia Digital, os dados tornaram-se o recurso competitivo mais importante no desenvolvimento do país.

Outro fato interessante, refere-se ao aumento de escritórios digitais, em junho de 2021, o número de usuários de escritórios online na China atingiu 381 milhões, um aumento de 35,06 milhões em relação a dezembro de 2020, e a taxa de utilização de usuários da Internet é de 37,7%. Os aplicativos de segmentação de escritório online continuam a se desenvolver, e a taxa de utilização de vídeo / teleconferência online e edição colaborativa de documentos online é de 23,8%. Por um lado, à medida que a transformação digital das empresas continua a avançar, o modelo de trabalho flexível representado pelo escritório online continuará a inovar e se desenvolver.[173]

Em contrapartida, o aumento de casos de vazamento de dados e o uso indevido de informações pessoais na China

[173] ZHANG Gang. WANG Kai: O 48º Relatório Estatístico sobre o Status de Desenvolvimento da Internet na China. Disponível em < http://www.chinanews.com/gn/2021/08-27/9552404.shtml> Acessado em 28/10/2021.

continental teriam contribuído também para a aceleração de mecanismos de proteção de informações pessoais. Vale citar como por exemplo o caso que aconteceu em março de 2020, em que as informações pessoais de mais de 538 milhões de usuários da *Sina Weibo* foram colocadas na dark web e em outros sites online para venda ao público.[174]

O desenvolvimento da Proteção de Informações Pessoais não se esgota apenas nos motivos acima citados, nem tampouco se restringe apenas como uma resposta à tendência mundial, mais sim como o resultado do autoaperfeiçoamento e autodesenvolvimento do Sistema Jurídico Chinês ao longo dos 20 anos.

Dessa forma, constata-se que antes da previsão no Código Civil Chinês o Direito de Proteção à Informações Pessoais já constava em outros documentos legislativos tais como a Lei de Segurança Cibernética, a Lei de Proteção dos Direitos do Consumidor, a Lei de Comércio Eletrônico e a Lei Criminal. [175]

Portanto, percebe-se que os esforços da China em construir uma estrutura legislativa sólida tem como objetivo estimular a economia interna e internacional, promover o bem-estar social colocando o ser humano como o centro das suas relações jurídicas e conferir maior Segurança Jurídica a todos àqueles que interajam com o país.

---

[174] As dez maiores violações de dados em 2020. Disponível em: https://www.secrss.com/articles/28972. Acessado em 01/11/2021.

[175] Congresso Nacional da China. O significado de longo alcance da Lei de Proteção de informações pessoais: China e o Mundo. Disponível em: < http://www.npc.gov.cn/npc/c30834/202108/1fee8d19bae14f9f9766c50ab1e53c0f.shtml> Acessado em: 28/10/2021.

3. A PROTEÇÃO DE INFORMAÇÕES PESSOAIS

A partir da análise dos motivos que levaram a China a almejar a proteção de informações pessoais, é inquestionável a relevância do tema para os dias atuais. Assim sendo, o Código dedicou um capítulo específico para regular o direito à privacidade e proteção de informações pessoais, constituindo o único Código Civil do mundo a tratar do tema.

Antes da vigência do Código Civil Chinês já existiam leis dispersas que tutelavam as informações pessoais, porém não as equiparava aos direitos fundamentais da pessoa física. A título de exemplo, no ano de 2017 entrou em vigor a Lei de Cibersegurança que proibiu os fornecedores dos serviços online de recolherem e venderem os dados dos usuários, sem o consentimento prévio destes. Em outras palavras, a sua aplicação é limitada apenas como indicação de conformidade para fornecedores dos serviços online, para que as autoridades chinesas concedam às empresas as autorizações e certificados necessários, mas não defendem na prática os usuários da Internet. Denota-se a inexistência da tutela ao direito à proteção de informações pessoais como um direito fundamental.[176]

Somente com o advento do Código Civil Chinês, que o direito à privacidade e proteção de informações pessoais foi apresentado na Parte Geral do livro como um Direito Civil e especificamente no Livro IV capítulo VI foi elencado como um Direito Fundamental.

176CARREIRA, Rui. Nova legislação de proteção de dados na China. Disponível em < https://globalnews.pt/sociedade/nova-legislacao-de-protecao-de-dados-na-china/v>. Acessado em: 28/10/2021.

A Parte Geral do Código dispõe que a proteção de informações pessoais é um Direito Civil da pessoa natural conforme o art. 111[177] em que deve ser garantida a segurança das informações pessoais, pelas pessoas físicas ou jurídicas, não devendo coletar, usar, processar ou transmitir ilegalmente, assim como veda a sua comercialização, fornecimento ou divulgação ilegal a terceiros. Em caso de violação à norma supracitada, cabe à vítima solicitar a responsabilidade civil do infrator conforme o art.120. [178]Ressalta-se, que no artigo 111 não especifica as figuras do processador e operador de informações tal qual na GPDR[179] ou LGPD[180], portanto ainda deverá aguardar a edição de lei específica que trate sobre o tema. [181]

No Capítulo I do Livro IV do Código confere especial proteção aos direitos da personalidade conforme disposto no art. 989[182]. No art. 990[183] determina que os direitos da personalidade

[177] Art. 111: As informações pessoais da pessoa natural serão protegidas por lei. A organização ou pessoa natural deve garantir a segurança na obtenção de informações pessoais de uma outra pessoa natural não devendo coletar, usar, processar, ou transmitir ilegalmente as informações pessoais de terceiros, assim como não deve comercializar, fornecer ou divulgar ilegalmente as informações pessoais de terceiros.

[178] Art. 120: Na violação dos direitos e interesses civis, cabe à vítima o direito de solicitar a responsabilização do infrator.

[179] *General Data Protection Regulation* (The Regulation 2016/679). Disponível em: < https://gdpr-info.eu/>. Acessado em 28/10/2021.

[180] Lei Geral de Proteção de Dados. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acessado em 28/10/2021

[181] Art. 127: Quando a lei tiver disposições sobre a proteção de dados e propriedade virtual da rede, siga essas disposições.

[182] Art. 989: Este capítulo regula as relações civis decorrentes do gozo e proteção dos direitos da personalidade.

[183] Art. 990: Os direitos de personalidade são usufruídos por sujeitos civis e abrangem os direitos à vida, corpo, saúde, nome, títulos, retrato, reputação,

serão usufruídos por sujeitos civis e abrangem os direitos à vida, corpo, saúde, nome, imagem, honra, privacidade dentre outros. Além disso, as pessoas físicas gozam de outros direitos de personalidade e interesses decorrentes da liberdade e da dignidade humana. A partir desta descrição, percebe-se que o código adotou uma postura centralizada nos direitos fundamentais e a dignidade humana, esses dois elementos conferem maior sistematicidade do Direito e Segurança Jurídica, farão com que a Sociedade chinesa continue sua trajetória em prol do desenvolvimento humano.

Dentro do Livro IV, especificamente, no Capítulo VI está previsto o Direito à Privacidade e à proteção de informações pessoais. O art. 1032[184] dispõe que as pessoas físicas possuem direito à privacidade. A definição de privacidade da pessoa física possui dois principais significados: a tranquilidade de uma vida privada e o espaço privado, atividades privadas e informações privadas que não querem ser reveladas a terceiros. [185]

---

honra, privacidade dentre outros. Além dos direitos da personalidade, as pessoas físicas gozam de outros direitos de personalidade e interesses decorrentes da liberdade e da dignidade humana.

[184] Art. 1032: as pessoas físicas possuem direito à privacidade. Nenhuma organização ou indivíduo pode infringir os direitos à privacidade de terceiros, espionando, assediando, divulgando ou outras formas. A privacidade abrange a tranquilidade da vida privada e o espaço privado que não deseja ser conhecido por outras pessoas, atividades privadas e informações privadas.

[185] O professor *Wang Chun Hui* explica que o direito à tranquilidade na vida privada ela sempre existiu no debate dentro da Teoria do Direito Civil, entende que é um direito especial conferido às pessoas físicas e o Código o incorporou como um direito fundamental. Cabe ainda, a responsabilidade civil em decorrência da violação do direito à vida privada, podendo ser exigido indenização pelos prejuízos sofridos em decorrência das circunstâncias fáticas de cada caso. No que se refere ao espaço, atividade e informações privadas, a lei não se limitou apenas aos espaços físicos como

O art. 1033[186] enumera seis tipos de atos que violam a privacidade das pessoas físicas, abarcando as cinco primeiras modalidades minuciosamente descritivas e a última modalidade é mais abrangente que admite maior interpretação. Paralelamente, a lei confere um conceito em aberto de violação à privacidade a ser definido em cada caso concreto. Insta salientar, que não constituirá violação à privacidade quando houver disposição em contrário em lei ou com o consentimento expresso do titular do direito.

No que se refere especificamente à definição de dados pessoais, o Código prevê no art. 1034[187] que as informações

---

a residência, quartos em hotel dentre outros, ela inclui também os diários pessoais e espaços virtuais. A liberdade de comunicação e a confidencialidade das comunicações é um direito concedido pela própria Constituição chinesa, e somente poderá ser limitada em casos de segurança nacional ou de perseguições penais. WANG, Chun Hui. Interpretação aprofundada da privacidade do Código Civil e a proteção de informações pessoais. Disponível em: < http://paper.cnii.com.cn/article/rmydb_15820_298769.html#:~:text=%E3%80%8A%E6%B0%91%E6%B3%95%E5%85%B8%E3%80%8B%E7%AC%AC%E4%B8%80%E5%8D%83%E9%9B%B6%E4%B8%89%E5%8D%81%E5%9B%9B%E6%9D%A1,%E5%81%A5%E5%BA%B7%E4%BF%A1%E6%81%AF%E3%80%81%E8%A1%8C%E8%B8%AA%E4%BF%A1%E6%81%AF%E7%AD%89%E3%80%82>. Acessado em: 19/05/2021.

[186] Salvo disposição em contrário por lei ou com o consentimento expresso do titular do direito, nenhuma organização ou indivíduo pode realizar as seguintes ações: (1) Invadir a vida privada de outras pessoas através de telefonemas, mensagens de texto, ferramentas de mensagens instantâneas, e-mails, folhetos, ou outros meios; (2) Entrar, filmar e espiar em espaços privados, como casas de outras pessoas e quartos de hotel; (3) Fotografar, espionar, ouvir e divulgar as atividades privadas de terceiros; (4) Fotografar, espionar as partes íntimas dos corpos de outras pessoas; (5) Processar as informações privadas de terceiros; (6) Violar a privacidade de outras pessoas de outras maneiras.

[187] Art. 1034: As informações pessoais de pessoas físicas são protegidas por lei. Informações pessoais são uma variedade de informações registradas eletronicamente ou de outras maneiras que permitam a identificação de

pessoais de pessoas físicas serão protegidas por lei, ou seja, a interpretação é de que a norma contida no Código Civil seja mais abstrata, a lei específica "*Personal Information Protection Law*" (PIPL)[188] prevê maiores detalhes. Observa-se, que o art. 1034 ao especificar as informações registradas eletronicamente ou de outras maneiras, o Código Civil garante maior escopo de proteção que aquela prevista no art. 76 Lei de Segurança Cibernética[189] de 2017. Destaca-se ainda, que o Código Civil não é uma lei específica para regulamentar as informações pessoais confidenciais, logo, deverão ser aplicados regula-

pessoa física específica individualmente ou em combinação com outras informações, incluindo o nome da pessoa física, data de nascimento, número de identificação, número biométrico, endereço, número de telefone, endereço de e-mail e saúde, informações sobre a localização ou outras informações. Para informações pessoais privadas, aplicar-se-ão os regulamentos relativos aos direitos de privacidade; se não houver regulamentos, serão aplicáveis os regulamentos relativos à proteção de informações pessoais.

[188] Atualmente, já está em vigência a Lei de Proteção de Informações Pessoais PIPL, ela apresenta semelhanças estruturais com a Lei 13.709 (LGPD) e o Regulamento nº 2016/679 (RGPD). A PIPL possui 70 artigos e está dividido em 08 capítulos que tratam sobre (i) disposições gerais (ii) requisitos para o tratamento de informações pessoais (iii) transferência internacional de dados informações pessoais (iv) direito dos titulares (v) deveres dos agentes de tratamento (vi) obrigações e responsabilidades dos departamentos de proteção de informações pessoais (vii) responsabilidade legal e (viii) disposições suplementares. Insta salientar, que o Estado possuirá um papel preponderante na implementação das estruturas dos sistemas de proteção de informações pessoais e no desenvolvimento de uma cultura relacionada ao tema.

[189] Art. 76: Informações pessoais referem-se a todos os tipos de informações que possam identificar a identidade pessoal de uma pessoa física isoladamente ou em combinação com outras informações, incluindo, mas não se limitando ao nome, data de nascimento número de identificação, informações biométricas pessoais, endereço, número de telefone dentre outras informações da pessoa física

mentos relativos aos direitos de privacidade, na ausência deste, serão aplicados os regulamentos relativos à Proteção de Informações Pessoais.

O art. 1035[190] do Código, traz consigo os princípios e condições no tratamento de informações pessoais. Ela elenca três princípios: a Legalidade, Legitimidade e Necessidade. Além disso, estabelece que as informações processadas deverão seguir às condições de obtenção de consentimento do titular ou do seu representante, respeito às regras de tratamento público de informações, declarar a finalidade, método e abrangência do processamento de informações, e não violar as disposições legais, regulamentos administrativos ou acordos entre as partes. Para o Código, o processamento de informações inclui a coleta, armazenamento, uso, processamento, transmissão, fornecimento e divulgação. Logo, todos aqueles que realizem tais atividades deverão seguir os princípios e condições supracitados, sob pena de responsabilidade civil do agente.

Em seguida, o art. 1036[191] estabelece as exceções em que o processador não se responsabiliza civilmente no processamento

[190] Art. 1035: O processamento de informações pessoais deve seguir os princípios de legalidade, legitimidade e necessidade, não devendo processar informações a mais, as informações processadas deverão atender às seguintes condições: (1) Obtenção do consentimento da pessoa física ou de seu tutor, salvo disposição em contrário em leis regulamentos administrativos; (2) Respeito às regras de tratamento público de informações; (3) Declaração clara da finalidade, método e abrangência do processamento de informações; (4) Não violação das disposições em leis, regulamentos administrativos e o acordo entre as partes.

[O] processamento de informações pessoais inclui a coleta, armazenamento, uso, processamento, transmissão, fornecimento e divulgação de informações pessoais.

[191] Art. 1036: O processador não se responsabiliza civilmente em nenhuma

de informações pessoais. Ressalta-se aqui que, o Código não especifica a figura do controlador e do operador como no GDPR ou no LGPD, mas o termo específico seria "*handlers*" ou "*entrust part*" conforme previsão na lei específica PIPL[192]. Assim, dentre as situações excepcionais que excluem a responsabilidade civil, estão os atos praticados com o consentimento do titular ou do seu representante, as informações divulgadas pelo titular ou outras informações legalmente divulgadas e outros praticados razoavelmente para proteger o interesse público ou os direitos legais do titular.

O professor *Wang Chun Hui* entende que o primeiro inciso, diz respeito aos atos praticados com o consentimento da pessoa física, inclui o consentimento de pessoas adultas, representantes legais de menores e pessoas com doenças mentais. As informações processadas limitar-se-ão àquilo acordado entre as partes, não podendo ser processados de forma excessiva. O inciso segundo possui dois significados, isto é, o primeiro trata das informações pessoais que a própria pessoa física divulgou ou aquelas que já estão divulgadas legalmente, como

---

das seguintes situações no processamento de informações pessoais: (1) Atos razoamento executados no âmbito do consentimento da pessoa física ou de seu tutor; (2) informações razoavelmente divulgadas pela própria pessoa física ou outras informações divulgadas legalmente, salvo se a pessoa física se recuse ou trata explicitamente as informações que violem seus principais interesses; (3) outros atos praticados razoavelmente para proteger o interesse público ou os direitos legais da pessoa física.

[192] No caso, o Código Civil Chinês adotou o termo de "processadores" para abranger o controlador e o operador. A PIPL, por sua vez, adotou os termos "***handle***r" e "***entrust part***" para se referir aos processadores, tanto que previu no seu capítulo V os deveres dos "***handlers***". ***Personal Information Law***. Disponível em: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> . Acessado em: 01/11/2021.

por exemplo quando o titular revela o seu nome, endereço, número de telefone etc. Por outro lado, também há informações que o titular não deseja ser revelados pois prejudicaria seus principais interesses, assim, o processador não deveria divulgá-las sob pena de responsabilidade civil.

Por fim, o inciso terceiro estabelece informações que podem ser divulgadas em para proteger o interesse público ou interesses do titular, observa-se a prevalência da primazia do interesse público em detrimento do direito privado em determinados casos. Neste viés, o exemplo mais recente seria o uso de informações pessoais pelo governo chinês no controle e prevenção da pandemia causado pelo Covid-19, a China autorizou as instituições médicas o processamento de informações pessoais. Em termos, o controle é estritamente limitado a populações-chave, como casos confirmados, suspeitos e contatos próximos, e geralmente não visa todas as populações em uma área específica. O objetivo é evitar a discriminação contra pessoas em uma área específica.[193]

Em relação aos direitos do titular das informações, estão previstos no art. 1037[194], os quais permitem a consulta

[193] WANG, Chun Hui. Interpretação aprofundada da privacidade do Código Civil e a proteção de informações pessoais. Disponível em: < http://paper.cnii.com.cn/article/rmydb_15820_298769.html#:~:text=%E3%80%8A%E6%B0%91%E6%B3%95%E5%85%B8%E3%80%8B%E7%AC%AC%E4%B8%80%E5%8D%83%E9%9B%B6%E4%B8%89%E5%8D%81%E5%9B%9B%E6%9D%A1,%E5%81%A5%E5%BA%B7%E4%BF%A1%E6%81%AF%E3%80%81%E8%A1%8C%E8%B8%AA%E4%BF%A1%E6%81%AF%E7%AD%89%E3%80%82>. Acessado em: 26/05/2021.

[194] Art. 1037: As pessoas físicas podem consultar ou copiar suas informações pessoais dos processadores de informações, desde que em conformidade com a lei; se forem encontrados erros nas informações, o titular das informações terá direito de levantar objeções, solicitar correções oportunas

e cópia das informações dos processadores, desde que em conformidade com a lei. Também dispõe sobre o direito de levantar objeções, solicitar correções ou tomar outras medidas necessárias. Em caso de processamento inadequado das informações pessoais, o titular também possui o direito de solicitar a exclusão.

Num outro giro, o art. 1038[195] traz os deveres e medidas de segurança que os processadores devem respeitar. Em primeiro lugar destaca que não devem compartilhar ou adulterar as informações que foram coletadas e armazenadas sem o prévio consentimento do titular. Além disso, veda a divulgação de informações não anonimizadas a terceiros sem o devido consentimento. Em relação às medidas de segurança, os processadores devem adotar formas técnicas e outras medidas necessárias para garantir a segurança dos dados que eles coletam e armazenam. O artigo dispõe ainda que em caso de

ou tomar outras medidas necessárias. Se a pessoa física descobrir que o processador de informações violou as disposições legais, regulamentos administrativos ou o acordo entre as duas partes de tratar suas informações pessoais, ela possuirá o direito de solicitar que o processador de informações as exclua em tempo hábil.

[195] Art. 1038: Os processadores de informações pessoais não devem divulgar ou adulterar as informações pessoais que foram coletadas e armazenadas; sem o consentimento de pessoas físicas, eles não devem fornecer ilegalmente as informações pessoais a terceiros, salvo aquelas informações em que não seja possível identificar indivíduos específicos e serem restaurados após o processamento. Os processadores de informações devem tomar medidas técnicas e outras medidas necessárias para garantir a segurança das informações pessoais que eles coletam e armazenam, além de evitar vazamentos, adulterações e perdas de informações; caso aconteça ou haja possibilidade de acontecer vazamento, adulteração ou perda de informações pessoais, medidas corretivas devem ser tomadas em tempo hábil e as pessoas físicas devem ser notificadas de acordo com os regulamentos e relatadas às autoridades competentes.

possibilidade de vazamento, adulteração ou perda dos dados, os processadores devem notificar os titulares e às autoridades competentes em tempo hábil.

Finalmente, o art. 1039[196] traz o tratamento de informações pessoais por órgãos públicos e seus funcionários, exigindo que estes mantenham a confidencialidade das informações pessoais das pessoas físicas obtidas no exercício da função.

Portanto, o Código Civil já traz o conceito de informações pessoais, os princípios a serem seguidos no processamento, a responsabilidade civil os processadores assim como as formas de exclusão dela, os direitos dos titulares das informações pessoais, os deveres dos processadores, o consentimento prévio do titular para processamento das informações pessoais, a anonimização, medidas técnicas em caso de vazamento e a notificação ao titular. Aspectos de extrema relevância para que o país caminhe na direção de adotar um sistema adequado de proteção de informações pessoais. Atualmente já existe a lei específica, "*Personal Information Protection Law*", portanto é recomendável que o Código Civil seja utilizado de forma subsidiária às determinações da PIPL.

CONSIDERAÇÕES FINAIS

O Sistema Jurídico Chinês passou por uma rápida modernização nas últimas décadas, considerado como um sistema híbrido da tradição legal imperial, Direito ocidental e Direito

[196] Art. 1039: Os órgãos do Estado e os seus funcionários estatutários que desempenhem funções administrativas, devem manter confidenciais a privacidade e as informações pessoais das pessoas físicas obtidas no exercício das suas funções, não as divulgando ou transmitindo ilegalmente a terceiros.

socialista soviético. Devido à sua cultura milenar, adquiriu uma tradição legal *sui generis*, portanto, para o seu estudo é necessário conhecer a cultura, os costumes e a evolução histórica do país.

Com base em todas essas influências ao longo da história, houve a elaboração do novo Código Civil Chinês, que entrou em vigor em 1 de janeiro de 2021. O diploma normativo faz a compilação de todas as leis civis esparsas, e o texto foi dividido em Parte Geral e Parte Especial. O Capítulo VI do Livro IV oferece destaque ao direito à privacidade e proteção de informações pessoais como um direito fundamental. A partir disso, verifica-se que a China demonstra especial enfoque no avanço da economia digital e a regulamentação seria a resposta digna para a solução das lides contemporâneas relacionadas ao grande fluxo de informações.

A China vem planejando ao longo dos últimos 20 anos uma estrutura rígida de proteção de informações pessoais. Os principais motivos que ensejaram a China a estimular o desenvolvimento de legislações protetivas às informações pessoais se resumem em melhorar a economia nacional e internacional, aprimorar a segurança cibernética evitando o uso ilegal de informações e assegurar o bem-estar social colocando o ser humano no centro das relações jurídicas.

Dessa forma, a China não perdeu a oportunidade de elencar a proteção de informações pessoais como um Direito Civil Fundamental na Parte Geral e como um Direito Fundamental na parte especial. Dentro do Capítulo de Privacidade e Proteção de Informações Pessoais, os artigos 1034 a 1039 trazem conceitos essenciais para a elaboração de um sistema de proteção de informações. Dentre quais destacam-se o conceito

de informações pessoais, os princípios a serem seguidos no processamento, a responsabilidade civil os processadores assim como as formas de exclusão dela, os direitos dos titulares das informações pessoais, os deveres dos processadores, o consentimento prévio do titular para processamento das informações pessoais, a anonimização, medidas técnicas em caso de vazamento e a notificação ao titular.

Por fim, ressalta-se que o Código ao prever a Proteção de Informações Pessoais como um Direito Fundamental é um grande avanço tanto para Sociedade Chinesa quanto para a Sociedade Internacional. Sem dúvidas, coloca a China em um patamar digno de disputa do título de grande potência mundial, através das inovações legislativas em prol da melhoria da Segurança Cibernética e Jurídica.

WHATSAPP COMO PLATAFORMA DE PAGAMENTOS: VANTAGENS E RISCOS AO CONSUMIDOR

Rafaella Fernandes dos Santos[197]

INTRODUÇÃO

O *WhatsApp*, aplicativo da empresa de tecnologia *Facebook* que oferece serviço de mensagens instantâneas e chamadas de áudio e de vídeo, com tecnologia de criptografia ponta a ponta, passou a permitir a realização de pagamentos entre os usuários (*peer-to-peer)*, por meio da ferramenta popularmente conhecida como *WhatsApp Pay*, que promete a mesma facilidade e segurança a custo zero em suas transações, assim como as mensagens de texto.

A escolha do Brasil como um dos países para ser "mercado-teste" do serviço de pagamentos não foi à toa, tendo em vista a expressiva aderência da população ao *WhatsApp*, cuja utilização se tornou mais predominante com a pandemia da Covid-19, que impôs relacionamentos remotos e modificou estruturalmente a rotina das pessoas e a forma de consumir.

Não obstante sua popularidade, o *WhatsApp* enfrenta polêmicas que podem desestimular os usuários à adesão dos pagamentos, como as constantes notícias de tentativas de golpes e compartilhamento de dados pelo *Facebook*, que levou as autoridades regulatórias a suspender temporariamente o serviço para adequações das atividades, relacionadas à competitividade no mercado financeiro e à proteção dos dados dos usuários, que serão analisadas no presente artigo.

[197] Advogada graduada em Direito pela Universidade Federal Fluminense (UFF) e pós-graduanda em Direito Digital pela Universidade do Estado do Rio de Janeiro (Uerj) em parceria com o Instituto de Tecnologia e Sociedade (ITS) e o Centro de Estudos e Pesquisas no Ensino do Direito (Ceped).

Por esse motivo, o presente artigo propõe a discussão sobre impactos das recentes mudanças no meio de comunicação em massa utilizado no país, especialmente sob a ótica do Direito do Consumidor, da Proteção de Dados e do Direito à Concorrência.

1. *WHATSAPP PAY* COMO EXEMPLO DA BANCARIZAÇÃO DAS BIG TECHS E AS QUESTÕES REGULATÓRIAS PARA IMPLEMENTAÇÃO NO BRASIL

1.1. BREVES EXPLICAÇÕES SOBRE O WHATSAPP PAY E SUA FUNÇÃO COMO INICIADOR DE TRANSAÇÕES DE PAGAMENTO

A premissa do *WhatsApp Pay* é proporcionar serviço de transferências financeiras entre pares dentro do próprio aplicativo de mensagens, com limite de transações de mil reais, mediante cadastro de cartão de débito ou pré-pago ligado a um banco local, permitindo a transferência de valores de conta bancária para contatos do aplicativo, sendo autorizado somente por inserção de PIN cadastrado pelo usuário.

O serviço de pagamentos do *WhatsApp* foi habilitado a operar mediante a subsidiária *Facebook Pagamentos*, instituição iniciadora de transação de pagamento autorizada pelo Banco Central, modalidade também conhecida como PISP, da expressão em inglês *payments initiation service provider,* regulamentada pela Resolução nº 24 do BACEN[198] em outubro de

[198] BRASIL. Presidência da República. Ministério da Economia. Banco Central do Brasil. Diretoria Colegiada. ***Resolução BCB nº 28***, de 23 de outubro de 2020. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-bcb-n-28-de-23-de-outubro-de-2020-284724060v. Acesso em: 11 jul. 2021.

2020, com a finalidade de iniciar, a partir da ordem do usuário, transações mediante débito em conta, porém sem ingerência sobre os fundos transferidos na prestação do serviço.

Por ser uma iniciadora de pagamentos, o *WhatsApp Pay* envia as informações da transação e pode obstar a operação caso seja notificado sobre saldo insuficiente em conta corrente ou conta de pagamento para cobrir o valor da transação. Neste diapasão, o *WhatsApp Pay* pretende se apresentar como uma opção tão conveniente e segura quanto o PIX, destacando-se a possibilidade de estorno das transações suspeitas, algo que ainda não é possível no arranjo do Banco Central.[199]

1.2. *WHATSAPP PAY* COMO VETOR DE INCLUSÃO DE "DESBANCARIZADOS" NO CONTEXTO DO *OPEN BANKING* E EXPRESSÃO DE TENDÊNCIA DO MERCADO DIGITAL

O PISP foi autorizado pelo Banco Central como uma das etapas da implementação do *Open Banking*, sistema de interoperabilidade e portabilidade de dados, que irá permitir o compartilhamento de informações e serviços financeiros pelos clientes bancários em plataformas de tecnologia, instituído por fases pelo Banco Central como fomento à inovação e à concorrência na prestação de serviços de pagamento.[200]

---

[199] VACCAREZA, Joana. *Whatsapp Pay*: o que esperar após autorização do BC. *Instituto Propague*. 2021. Disponível em: https://institutopropague.org/noticias/whatsapp-pay-o-que-esperar-apos-autorizacao-do-bc/. Acesso em: 6 jul. 2021.

[200] SIMÃO, Edna. Depois do Pix, BC aprova PISP, nova modalidade de pagamento. *Valor Investe*, 2020. Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/10/22/depois-do-pix-bc-aprova-pisp-nova-modalidade-de-pagamento.ghtml. Acesso em: 11 jul. 2021.

Sob o ponto de vista socioeconômico, o *WhatsApp Pay* pode ser considerado como uma etapa do *Open Banking*, trazendo a muitos usuários a oportunidade de maior inclusão financeira, tendo em vista a possibilidade de cadastro de conta corrente e contas de pagamento, cuja adesão entre os brasileiros aumentou exponencialmente no período de pandemia, sendo para muitos a primeira oportunidade de "bancarização", necessidade que se tornou presente aos beneficiários do auxílio emergencial no contexto da pandemia de Covid-19[201], além da própria consolidação da ideia de *cashless society*, isto é, a desmaterialização do papel-moeda, que traz maior controle e segurança às transações.[202]

Neste contexto, a virtualização dos meios de pagamento vem se tornando o "novo normal", atraindo a atenção não apenas de governos, bancos tradicionais e carteiras digitais, como também de empresas do varejo e até mesmo de tecnologia, a exemplo do próprio *Facebook*, em tendência de mercado conhecida como *banking as a service,* cuja estratégia é promover a melhor experiência do usuário com personalização de serviço, buscando maior aproximação e confiabilidade do consumidor.[203]

---

[201] TAVARES, Yasmim. Sistema Pix e open banking trazem desafios para a inclusão dos desbancarizados. ***Valor Investe***, 2020. Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/09/16/sistema-pix-e-open-banking-trazem-desafios-para-a-inclusao-dos-desbancarizados.ghtml. Acesso em: 15 jul. 2021.

[202] FILIPIAK, Piotr. COVID-19: the viral spread of cashless society? ***Financial Times.*** Disponível em: https://www.ft.com/partnercontent/comarch/covid-19-the-viral-spread-of-cashless-society.htmlv. Acesso em: 15 jul. 2021.

[203] STRANGE, Angela. Any Company Can Offer Financial Services. ***YouTube***, 21 jan. 2020. Disponível em: https://www.youtube.com/watch?v=DjUMfhT0o64&ab_channel=a16z. Acesso em 11 de jul. 2021.

Em suma, pode-se concluir que há uma verdadeira tendência de "fintechzação" das plataformas digitais, com a adoção de modelo de negócios voltados aos serviços financeiros e processos fundados em tecnologia, para a realização de atividades antes inerentes aos bancos tradicionais, como reação à economia digital e à busca do consumidor por inovação, agilidade e transparência, com o menor custo possível.[204]

Contudo, a ideia de uma sociedade livre de papel-moeda significa a maior dependência de dispositivos móveis para tarefas básicas do cotidiano, em uma economia cada vez mais voltada para a exploração de dados dos usuários como modelo de negócios, com potencial de provocar riscos ao direito de privacidade dos consumidores.

Além disso, a concentração do sistema de pagamentos no setor privado, em especial no caso de grandes conglomerados de tecnologia, acarreta considerável risco concorrencial ao sistema financeiro. Deste modo, torna-se imprescindível a intervenção dos órgãos reguladores em prol do equilíbrio econômico diante dos avanços tecnológicos no setor financeiro, na medida em que não há norma vigente acerca da atuação destas empresas.[205]

---

[204] LIMA, Rafael Pereira; SILVEIRA, Daniel Barile. Fintech e o Direito do Consumidor. *Revista de Direito, Governança e Novas Tecnologias*, Salvador, v. 4, n. 1, p. 109-128, 2018. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/4350. Acesso em: 10 jul. 2021.

[205] ALMEIDA, Daniel Veloso; BADRA, Daniel Dutra; PAIXÃO, Ricardo Fernandes. A nova figura do Iniciador de Transação de Pagamento. *Jota*, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-nova-figura-do-iniciador-de-transacao-de-pagamento-17032021. Acesso em: 30 jun. 2021.

1.3. REFLEXÕES SOBRE AS QUESTÕES REGULATÓRIAS CONCERNENTES AO BANCO CENTRAL E AO CADE PARA A AUTORIZAÇÃO DO *WHATSAPP PAY* NO BRASIL

O *Facebook* anunciou o lançamento do *Whatsapp Pay* em junho de 2020, porém foi oficialmente liberado no Brasil em 15 de junho de 2021, uma vez que a implementação do serviço de pagamento ocorreu sem o devido escrutínio das autoridades nacionais, o que provocou a suspensão imediata por ordem do Banco Central e do Conselho Administrativo de Defesa Econômica (Cade), diante de possíveis danos irreparáveis ao Sistema de Pagamentos Brasileiro (SPB), conforme disposições da Lei nº 12.865/2013, bem como à competição, eficiência e privacidade de dados.

Especulou-se à época entre especialistas em direito regulatório que a suspensão pelo Banco Central foi motivada pelos preparativos para a implementação do PIX, cujo lançamento coincidiu com a empreitada do *Facebook* e possui vantagens muito parecidas com as ofertadas pelo *WhatsApp Pay*, como anteriormente mencionado.[206]

Com efeito, há o fundado receio da introdução das *big techs* no setor de pagamentos e a urgência pela regulação deste tipo de atividade, diante do risco à competitividade, considerando que a infraestrutura destas plataformas por vezes é controlada

[206] COUTINHO, Diogo; GONÇALVES, Priscila Briolio; KIRA, Beatriz. Pagamentos por WhatsApp: por que o Banco Central e o Cade se preocupam? *Jota*, 2020. Disponível em: https://www.jota.info/tributos-e-empresas/regulacao/pagamentos-por-whatsapp-por-que-o-banco-central-e-o-cade-se-preocupam-30062020. Acesso em: 30 jun. 2021.

pela mesma empresa de tecnologia, a exemplo do próprio *Facebook*, dentro do contexto de *marketplace*.[207]

Inclusive, cogita-se que o próprio Banco Central editou a Resolução nº 24, que instituiu a figura do Iniciador de Transação, para abarcar os pagamentos pelo *WhatsApp* no Sistema de Pagamentos Brasileiro (SPB), em resposta à movimentação agressiva do *Facebook* em território nacional.[208]

Já o Conselho Administrativo de Defesa Econômica (Cade) suspendeu brevemente a funcionalidade em dezembro de 2020, notificando o *Facebook* sobre a instauração de procedimento administrativo para apuração de ato de concentração e de possíveis efeitos concorrenciais que podem gerar danos de difícil reparação, tendo em vista a parceria com a credenciadora *Cielo* e a suspeita de *joint venture* disfarçada, que precisaria de análise e autorização prévia na forma da Lei nº 12.529/2011, que dispõe sobre Sistema Brasileiro de Defesa da Concorrência.[209]

De fato, a autorização da operação de um serviço do porte do *WhatsApp Pay* requer maior precaução com os riscos advindos da rapidez inerente às transformações tecnológicas e do impacto no modo como consumidores adquirem ou

---

[207] COUTINHO, Diogo; GONÇALVES, Priscila Briolio; KIRA, Beatriz. ***Ibidem.***

[208] ALMEIDA, Daniel Veloso; BADRA, Daniel Dutra; PAIXÃO, Ricardo Fernandes. A nova figura do Iniciador de Transação de Pagamento. ***Jota,*** 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-nova-figura-do-iniciador-de-transacao-de-pagamento-17032021. Acesso em: 30 jun. 2021.

[209] WIZIACK, Julio. Cade e BC barram acordo que prevê pagamentos via ***WhatsApp. Folha de S. Paulo,*** 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/06/cade-e-bc-barram-acordo-que-preve-pagamentos-via-whatsapp.shtml. Acesso em: 5 jul. 2021.

utilizam determinados produtos ou serviços, razão pela qual a regulação é essencial ao equilíbrio do mercado.[210]

Portanto, faz-se adequada a análise dos impactos ao consumidor pelo viés do direito concorrencial e de proteção de dados, na medida em que foram as motivações principais para a suspensão temporária do serviço do *WhatsApp Pay* no Brasil.

2. ANÁLISE DOS IMPACTOS AO CONSUMIDOR DE PRÁTICAS DO *WHATSAPP PAY* PELA ÓTICA ANTITRUSTE E DE PROTEÇÃO DE DADOS PESSOAIS

2.1. POLÊMICA COM A POLÍTICA DE PRIVACIDADE DO *WHATSAPP* QUE ABRANGE OS SERVIÇOS DE PAGAMENTOS INSTANTÂNEOS

A partir do anúncio da nova política de privacidade do *WhatsApp* no início de 2021, rapidamente surgiram críticas às práticas de compartilhamento de dados pessoais dos usuários com empresas do grupo econômico do Facebook e consentimento forçado, em contrariedade à Lei Geral de Proteção de Dados (LGPD), cuja repercussão negativa provocou o adiamento da implementação das políticas e pedidos de esclarecimentos e recomendações de órgãos de fiscalização.[211]

[210] MIRAGEM, Bruno. Novo Paradigma Tecnológico, Mercado de Consumo e o Direito do Consumidor. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (org.). ***Direito digital***: direito privado e internet. 3. ed. rev. atual. e ampl. São Paulo: Editora Foco, 2020. [livro eletrônico].

[211] SHINOHARA, Gabriel. WhatsApp vai continuar permitindo acesso de usuários que não concordaram com nova política de privacidade por 90 dias. ***O Globo***, 2021. Disponível em: https://bityli.com/p05nd. Acesso em: 13 jul. 2021.

No contexto do *WhatsApp Pay*, os regramentos internos que dispõem sobre tratamento de dados se complementam com a finalidade de "operar, fornecer, aprimorar, entender, personalizar, dar suporte e comercializar o recebimento e envio de pagamentos, além de detectar, impedir ou lidar com questões relacionadas a fraudes, à segurança, à proteção, a abusos ou a outras más condutas".[212]

Em geral, os termos possuem previsões que remetem à aplicação da Lei Geral de Proteção de Dados (LGPD), como informações do período de armazenamento e do direito ao acesso, correção, portabilidade, eliminação e confirmação de tratamento de dados. No entanto, há excesso de regramento que dificulta a compreensão do usuário quanto às questões de privacidade relacionadas à função de pagamento, o que traz a reflexão sobre a denominada "fadiga do consentimento".[213]

Ao utilizar o serviço de pagamento, o usuário permite a coleta, o uso, o compartilhamento de informações com as próprias empresas do *Facebook* e com instituições financeiras que atuam como processadores de pagamento, como forma de pagamento, preferências de segurança, dados do remetente ou do destinatário do pagamento, *status* da conta e suficiência de saldo, além de alertas de fraude.[214]

---

[212] Política de Privacidade de Pagamentos no *Whatsapp*. *WhatsApp*. Disponível em: https://www.whatsapp.com/legal/payments/privacy-policy. Acesso em: 11 jul. 2021.

[213] OLIVEIRA, Caio César; FILHO, Paulo César Tavares. A LGPD e o início do fim da cultura do consentimento. *Jota*, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-o-inicio-do-fim-da-cultura-do-consentimento-28062021. Acesso em: 15 jul. 2021.

[214] Política de Privacidade de Pagamentos no *Whatsapp*. *WhatsApp*. Disponível em: https://www.whatsapp.com/legal/payments/privacy-policy.

Decerto, o processamento de informações pessoais é necessário para o aprimoramento de uma plataforma digital, especialmente no contexto de prevenção a fraudes e da previsão de tratamento de dados pessoais sensíveis sem necessidade de consentimento do titular na forma do artigo 11, inciso II, alínea "g" da Lei nº 13.709/2018[215], contudo sem perder de vista a razoabilidade na coleta dos dados e a transparência ao usuário.

Com efeito, o compartilhamento de dados dos usuários do *WhatsApp* com o *Facebook* não é novidade, eis que ocorre desde 2016, porém tomou maior destaque com a atualização da Política de Privacidade da empresa. Diante da imprecisão dos impactos à privacidade dos usuários, a Autoridade Nacional de Proteção de Dados (ANPD) instaurou processo administrativo para avaliação técnica da nova política de privacidade do WhatsApp, em atuação conjunta com o Conselho Administrativo de Defesa Econômica (Cade), a Secretaria Nacional do Consumidor (Senacon) e o Ministério Público Federal (MPF)[216]

Nesse processo, foram realizados questionamentos sobre a finalidade do tratamento dos dados compartilhados e recomendações para conferir maior transparência acerca da atualização da política de privacidade, efetividade aos direitos

Acesso em: 11 jul. 2021.

[215] BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. ***Lei Geral de Proteção de Dados Pessoais (LGPD)***. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 jul. 2021.

[216] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. ***Nota técnica nº 02/2021/CGTP/ANPD***. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

elencados na LGPD e respaldo aos usuários contra qualquer prática de discriminação em hipóteses de não concordância aos termos.[217]

Dentre os dados coletados para compartilhamento entre empresas do conglomerado e prestadores de serviço terceirizados, estão informações da conta e dados de transações e pagamentos, o que traz a preocupação sobre o grande poder analítico do Facebook, especialmente porque a Política de Privacidade não esclarece se o *Facebook* é capaz ou não de usar as mensagens do *WhatsApp* para outros fins. [218]

Em que pese o *Facebook* garanta que não há acesso ao número e ao código de segurança do cartão utilizado para o serviço de pagamentos, é relevante a preocupação com o compartilhamento de tantas informações sobre os usuários a outras empresas do próprio conglomerado, a ponto de possibilitar às *big techs* medidas de mercado questionáveis, como a previsão de comportamento e extração de informações sobre poder aquisitivo dos usuários.[219]

---

[217] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. *ANPD divulga orientações aos usuários sobre nova política de privacidade do Whatsapp*. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/a-nova-politica-de-privacidade-do-whatsapp. Acesso em: 24 nov. 2021.

[218] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. *Nota técnica nº 02/2021/CGTP/ANPD*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

[219] POOLER, Michael; MURPHY, Hannah. WhatsApp person-to-person payments return to Brazil. *Financial Times*, 2021. Disponível em: https://www.ft.com/content/9c862d5f-e9fd-4503-a8e4-2952a8676b98. Acesso em: 4 jul. 2021.

2.2. A EXPLORAÇÃO DE DADOS PESSOAIS COMO VANTAGEM COMPETITIVA ÀS *BIG TECHS*

Com efeito, a atuação de *big techs* no sistema financeiro mostra que a exploração dos dados é o meio que as empresas de tecnologia ganham vantagens competitivas entre si. Nas palavras de Ana Frazão, "a violação da privacidade e dos dados pessoais torna-se um lucrativo negócio que, baseado na extração e na monetização de dados, possibilita a acumulação de um grande poder que se retroalimenta indefinidamente".[220]

Considerando o poder das plataformas de armazenar grande montante de dados, na busca de vantagens a partir deste "ativo", não é exagero cogitar a possível utilização dos dados fornecidos para utilização do serviço de pagamentos para outras finalidades, como publicidade em outras plataformas do *Facebook*.

Se por um lado a captação de dados pode aumentar a segurança, conforme mencionado, por outro, concentra nas mãos do *Facebook* um conjunto poderoso de informações sobre os usuários que pode ser compartilhada com outras empresas do grupo, possuindo mecanismos capazes de tornar os usuários totalmente dependentes de seus produtos, a ponto de encontrar tudo o que precisam em uma única plataforma, possibilitando compras, pagamentos, troca de mensagens, ligações de voz e de vídeo; tudo sem sair do aplicativo.

[220] FRAZÃO, Ana. ***Big Data*** e Aspectos Concorrenciais do Tratamento de Dados Pessoais. *In:* DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; JUNIOR, Otavio Luiz Rodrigues (org.). ***Tratado de proteção de dados pessoais***. Rio de Janeiro: Forense, 2021. p. 537.

Neste contexto, o *Facebook* planeja expandir pagamentos entre pessoas e empresas mediante o *WhatsApp Business* (WAB), um serviço dirigido a empresas que "ajuda a se conectarem pessoalmente aos seus clientes", com a premissa de coleta de dados do usuário coletados nos últimos anos para traçar a "melhor experiência de compra". Recorda-se que o Banco Central não concedeu a autorização para transações comerciais mediante o *WhatsApp Pay.*[221]

Não obstante as facilidades e a garantia de segurança do aplicativo mediante criptografia ponta-a-ponta e autenticação por dois fatores, esse controle apenas anonimiza as mensagens, porém não blindam o compartilhamento de metadados ou do conteúdo das comunicações às empresas do conglomerado e/ou empresas terceiras que oferecem serviços ao *Facebook,* tal como no uso do *WhatsApp Business,* que funciona como porta de entrada para desvio de tratamento se não for assegurada a transparência ao usuário. [222]

Deste modo, é notável que o *WhatsApp Pay* não foi desenvolvido com base no *privacy by design,* isto é, a ideia de que a privacidade deve orientar a concepção de um produto ou serviços, com tecnologias que facilitem o controle e a prote-

[221] PASCUAL, Manuel. Brasil e Índia encabeçam a rebelião mundial contra as novas condições do WhatsApp. *El País,* 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-05-15/brasil-e-india-encabecam-a-rebeliao-mundial-contra-as-novas-condicoes-do-whatsapp.html. Acesso em: 13 jul. 2021.

[222] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. *Nota técnica nº 02/2021/CGTP/ANPD.* Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

ção de dados pessoais[223], que invista na união da experiência do usuário e da autodeterminação informativa. Não há, por exemplo, informações sobre técnicas de anonimização e/ou pseudonimização ou limites de coleta e tratamento dos dados.[224]

Sabendo que estamos vivendo a transição da sociedade de consumo para uma sociedade de vigilância, essas são questões relevantes ao consumidor e que evidenciam a vulnerabilidade nas relações de consumo via internet.

2.3. ASPECTOS DO DIREITO CONCORRENCIAL E SUA IMPORTÂNCIA PARA A TUTELA DOS DIREITOS DO CONSUMIDOR

A tutela dos dados pessoais permeia as mais variadas searas jurídicas, mas é possível entender a correlação com o Direito da Concorrência, especialmente quando estamos diante de uma economia digital movida a dados, em um modelo de negócio cada vez mais presente na sociedade do século XXI, convencionando-se a denominar tal fenômeno como "Capitalismo de Vigilância", termo cunhado por Shoshana Zuboff.[225]

---

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

[224] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. ***Nota técnica nº 02/2021/CGTP/ANPD***. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

[225] FRAZÃO, Ana. ***Big Data*** e Aspectos Concorrenciais do Tratamento de Dados Pessoais. ***In:*** DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; JUNIOR, Otavio Luiz Rodrigues (org.). ***Tratado de proteção de dados pessoais***. Rio de Janeiro: Forense, 2021. p. 537.

Em razão desta dinâmica complexa, sustentada pela exploração de dados pessoais, indaga-se se a abrangência do Código de Defesa do Consumidor (CDC) e da Lei Geral de Proteção de Dados (LGPD) é o suficiente para a tutela do consumidor em uma plataforma como o *WhatsApp*, ou se outras áreas do Direito, como o antitruste, deveriam também endereçar esforços ao agigantamento exponencial de agentes econômicos às custas de violações da privacidade e da autodeterminação informativa dos cidadãos-consumidores.[226]

Além disso, ressalta-se a importância do Marco Civil da Internet, que assegura a aplicação do próprio CDC às relações de consumo viabilizadas pelo meio eletrônico (art. 7, XIII da Lei 12965/2014).

3. OS IMPACTOS DA UTILIZAÇÃO DO *WHATSAPP PAY* NO ATUAL MERCADO DE CONSUMO PAUTADO NA EXPLORAÇÃO DE DADOS PESSOAIS DOS USUÁRIOS

3.1. MUDANÇA DE PARADIGMA SOBRE O DIREITO DO CONSUMIDOR DIANTE DE NOVOS MODELOS DE NEGÓCIO EM UMA ECONOMIA *DATA-DRIVEN*

É correto afirmar que o Código de Defesa do Consumidor (CDC) possui forte apelo na sociedade civil, muito por conta dos prejuízos causados ao consumidor, de ordem material e moral, decorrentes de práticas comerciais que não se coadunam com a boa-fé objetiva, isto é, a lealdade necessária em todas as fases do contrato, no intuito de não frustrar a legítima

[226] FRAZÃO, Ana. *Op. cit.*, p. 537.

confiança entre as partes e de estabelecer o equilíbrio nas relações jurídicas.[227]

Neste esteio, não se pode perder de vista os princípios e normas previstas na referida legislação, uma vez que o intenso fluxo de informações no contexto das *big techs* pode trazer desequilíbrio à ordem econômica e refletir de forma negativa à prestação dos serviços aos usuários, com risco de submeter os usuários a uma concentração de poder nas mãos de poucas empresas de tecnologia.

O potencial do *WhatsApp Pay* na promoção de mudanças estruturantes no modo de consumir de seus usuários, tal como um típico serviço disruptivo oferecido por uma *big tech*, evoca a reflexão sobre os novos riscos aos consumidores decorrentes da evolução do mercado e da rapidez das novas formas de consumo potencializadas pela internet.

Assim, a hipossuficiência do consumidor pode ser mais agravada diante das características e riscos das relações de consumo via internet, haja vista os avanços tecnológicos que permeiam as relações entre consumidores e fornecedores em novas formas de oferta e contratação impactadas pelas transformações do mercado.[228]

---

[227] ROSENVALD, Nelson. Dignidade humana e boa-fé no Código Civil. São Paulo: Saraiva. *In*: LIMA, Rafael Pereira; SILVEIRA, Daniel Barile. Fintech e o Direito do Consumidor. ***Revista de Direito***, Governança e Novas Tecnologias. Salvador, v. 4, n. 1, p. 109-128, 2018. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/4350. Acesso em: 10 jul. 2021.

[228] MIRAGEM, Bruno. Novo Paradigma Tecnológico, Mercado de Consumo e o Direito do Consumidor. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (org.). ***Direito digital***: direito privado e internet. 3. ed. São Paulo: Editora Foco, 2020. [livro eletrônico].

Desta forma, os tempos atuais trazem uma necessária mudança de paradigma do direito do consumidor, dialogando com outros princípios constitucionais atinentes à ordem econômica para fortalecimento da tutela ao consumidor, como a defesa da concorrência e a proteção de dados.

3.2. POSSÍVEIS APLICAÇÕES DO CÓDIGO DE DEFESA DO CONSUMIDOR NO ÂMBITO DO *WHATSAPP PAY*

Com a aplicação do *WhatsApp Pay* apenas entre pessoas, sem fins comerciais, não se cogita aplicação do Direito do Consumidor entre os usuários, contudo há inegavelmente relação de consumo entre usuários e o *Facebook*, devendo ser garantida a reparação de eventual dano decorrente da violação de dever jurídico, em razão da prestação de serviço de pagamentos pelo aplicativo.

A exemplo do próprio *WhatsApp Pay*, as plataformas digitais apresentam diversos termos de uso e de privacidade que dispõem sobre cláusulas de exclusão da responsabilidade do intermediador de pagamentos sobre falhas na transação, sempre lançando ao consumidor a culpa pelo dano, com base no disposto no art. 14, §3º do CDC.

Hipoteticamente, em casos de fraudes, a indevida utilização de dados do usuário e subsequente desvio de valores mediante o sistema de pagamento deve ser considerada como fortuito interno, em razão da natureza da atividade desenvolvida pelo *WhatsApp Pay*.

Neste diapasão, embora não haja retenção de fundos da transação pelo sistema de pagamento no *WhatsApp*, a empresa obviamente é remunerada pelas empresas parceiras para

a iniciação do pagamento, decorrente da própria atividade bancária da *big tech,* no contexto do *banking as a service*.

Por operar como iniciadora de transações de pagamento, o *Facebook* deve ser tratado em pé de igualdade com instituições financeiras, inclusive no tocante à responsabilidade civil por falha na prestação de serviço, considerando que a instituição de pagamentos integra a cadeia de consumo e, por isso, deve responder solidariamente por eventuais danos, conforme artigo 25, §1º do CDC.

Desta forma, se a aferição de lucros ou vantagens de uma atividade bancária exercida por uma empresa de tecnologia decorre de uma prestação de serviço defeituosa, questiona-se a aplicação por equiparação da teoria do risco do empreendimento, prevista no artigo 927 do Código Civil[229] e consolidada pelo Enunciado 479 da Súmula do Superior Tribunal de Justiça (STJ): "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

Certamente tais reflexões não possuem uma resposta correta e necessitam de uma construção doutrinária e jurisprudencial acerca da responsabilização do *Facebook* por danos decorrentes de eventual falha na segurança e a caracterização do usuário como consumidor por equiparação, na forma do artigo 17 do Código de Defesa do Consumidor.

---

[229] BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 10.406, de 10 de janeiro de 2002. ***Código Civil***. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 jul. 2021.

3.3. A IMPORTÂNCIA DO DEVER DE INFORMAÇÃO E TRANSPARÊNCIA AO USUÁRIO EM RELAÇÃO AOS MECANISMOS DE SEGURANÇA E TRATAMENTO DE DADOS

Outro ponto de destaque tanto no âmbito consumerista como na tutela dos dados pessoais é o direito à informação, que impõe ao fornecedor o dever de repassar, de forma clara, as características de produtos e serviços, de modo que as cláusulas contratuais decorrentes destas relações precisam ser interpretadas de forma benéfica ao consumidor.[230]

Além disso, o *WhatsApp* apresenta fatores que podem causar receio aos usuários quanto à vulnerabilidade dos dados bancários em um aplicativo com altas taxas de estelionato virtual, como tentativas de golpes e clonagem de conta, sobretudo durante a pandemia. Comumente, a técnica dos criminosos é a engenharia social, solicitando aos usuários os dígitos de autenticação, seja por falsificação de identidade em meios digitais (*spoofing),* seja por envio de *links* com falsas vantagens ao usuário, por meio de mensagens disfarçadas de páginas e perfis da internet e em redes sociais (*phishing),* no intuito de roubar dados pessoais e aplicar golpes financeiros pelo aplicativo. [231]

[230] LIMA, Rafael Pereira; SILVEIRA, Daniel Barile. Fintech e o Direito do Consumidor. *Revista de Direito, Governança e Novas Tecnologias*, Salvador, v. 4, n. 1, p. 109-128, 2018. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/4350. Acesso em: 10 jul. 2021.

[231] BOTTINO, Raphael. Pagamentos no *WhatsApp*: entenda segurança e privacidade na ferramenta. *Tecmundo*, 2020. Disponível em: https://www.tecmundo.com.br/seguranca/154838-pagamentos-whatsapp-entenda-seguranca-privacidade-ferramenta.htm. Acesso em: 11 jul. 2021.

Embora o *WhatsApp* seja alvo constante de tentativas de golpe, é necessário reconhecer que o aplicativo possui mecanismos de segurança, como a autenticação por duas etapas e, no âmbito dos pagamentos, o limite de transação até R$ 1 mil. Contudo, no Brasil ainda não há conscientização forte sobre segurança da informação para a redução do número de vítimas de estelionatos por meio virtual, sendo necessário intensificar a educação da população sobre os riscos da engenharia social.

Deste modo, é imprescindível ao *Facebook,* como empresa de tecnologia, empenhar iniciativas de conscientização da segurança cibernética em linguagem simples e direta, em referência ao artigo 8º do Código de Defesa do Consumidor[232], como meio de prevenção da ocorrência de danos em virtude do tratamento de dados pessoais, conforme artigo 6º, inciso VIII, da LGPD, para estimular um ambiente confortável aos usuários para a utilização da ferramenta, sem receio de falhas de segurança.

Dentre as bases legais que autorizariam o compartilhamento de dados pelo *WhatsApp,* estão a necessidade contratual (artigo 7º, inciso V, da LGPD) e o legítimo interesse (artigo 7º, inciso IX, da LGPD)[233]. Esta última está intimamente ligada ao princípio da transparência, que se correlaciona, em suas

[232] BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 8.078, de 11 de setembro de 1990. ***Código de Defesa do Consumidor (CDC)***. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 jul. 2021

[233] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. ***Nota técnica nº 02/2021/CGTP/ANPD.*** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

devidas proporções, ao dever de informação garantido pela legislação consumerista, conforme preconizado no artigo 10, §2º da LGPD, diante da exigência de divulgação sobre o tratamento dos dados de forma clara, adequada e ostensiva.[234]

Neste sentido, o legítimo interesse como base legal necessita da transparência no tratamento dos dados, previsto no artigo 9º, inciso VII, da LGPD[235], a fim de possibilitar a efetivação de outros princípios legais, como a prestação de contas e a responsabilização por incidentes de segurança, bem como garantir a autodeterminação informativa para efetivo exercício dos direitos de titular do usuário, elencados no artigo 18 da LGPD.

Em suma, não se trata apenas de segurança da informação, mas também o controle da privacidade das informações. Por isso, é importante que as *big techs* como o *Facebook* se engajem na adoção de medidas a minimizar o impacto do tratamento com base no legítimo interesse, tais como a correlação de categoria de dados tratados com suas finalidades e registros de compartilhamento de dados entre operadores, controladores e/ou terceiros[236]

---

[234] Art. 10, parágrafo segundo, da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018): "O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse."

[235] Art. 9º, inciso VII, da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018): "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei."

[236] BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. *Nota técnica nº 02/2021/CGTP/ANPD*. Disponível em: https://www.

Portanto, cabe ao *WhatsApp,* assim como a outras empresas de tecnologia que exercer atividades bancárias, a realização de um trabalho de blindagem, com mecanismos de controle e auditoria do sistema, buscando processos de identificação e correção de eventuais deficiências no tratamento dos dados[237], realizando a exploração de dados com a devida razoabilidade ao consumidor, como fator de maior garantia da autodeterminação informativa e segurança aos usuários do aplicativo.

CONCLUSÃO

O mercado brasileiro está receptivo às modalidades de pagamentos digitais, como visto no caso do PIX, de modo que o *WhatsApp Pay* se apresenta como uma forma de inclusão financeira daqueles recentemente "bancarizados", visto que o aplicativo aceita cadastro de contas de pagamento em carteiras digitais.

Contudo, a confiabilidade dos usuários no serviço de pagamentos do aplicativo é questionável, considerando que o aplicativo é alvo constante de tentativas de fraudes, especialmente durante a pandemia, consolidando o Brasil como um dos países com maiores taxas de estelionatos por meio virtual.

Por isso, torna-se necessário que o *Facebook* invista em seu dever de informação em suas plataformas e redes so-

gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas--noticias/NOTATECNICADACGTP.pdf. Acesso em: 24 nov. 2021.

[237] PINHEIRO, Patricia Peck. Os desafios com a chegada do Pix e do open banking ao país. *Noomis CIAB FEBRABAN*, 2020. Disponível em: https://noomis.febraban.org.br/especialista/patricia-peck-pinheiro/os-desafios--com-a-chegada-do-pix-e-do-open-banking-no-pais. Acesso em: 11 jul. 2021.

ciais sobre os mecanismos de segurança disponíveis, como a autenticação de dois fatores, repassando, de forma simples e clara, orientações sobre como identificar uma tentativa de golpe e como proceder no próprio aplicativo para proteger os dados do usuário.

Além disso, as conjecturas com o tratamento de dados inseridos para a transação de pagamentos se relacionam com polêmicas relacionadas à política de privacidade do aplicativo, que também envolve o sistema de pagamentos e autoriza o compartilhamento de dados com outras empresas do *Facebook*, em potencial risco de monopólio do poder econômico de uma única empresa de tecnologia.

Deste modo, não obstante a inclusão social do *WhatsApp Pay* e a eficiência das transações mediante conversas no aplicativo, a falta de regulação específica para a introdução de *big techs* ao mercado financeiro gera riscos ao consumidor e à concorrência, o que pode maximizar a vulnerabilidade do usuário na plataforma de pagamentos.

Desta forma, o estudo de caso do *WhatsApp Pay* nos incita à reflexão sobre a necessária convergência entre defesa da concorrência, de proteção de dados e do consumidor quando se trata de pagamentos digitais, que tiveram um crescimento exponencial de adesão desde o início da pandemia de Covid-19, para que os benefícios oriundos da ferramenta não sejam ofuscados pelos riscos ao sistema financeiro, no sentido de garantir a competição no setor e melhoria na qualidade dos serviços.

Apenas o tempo dirá se o Banco Central e o Cade agiram corretamente ao liberarem o serviço no Brasil, e se o serviço irá se expandir para transações comerciais, visto que atual-

mente está habilitado apenas entre pessoas. Enquanto isso, é fundamental que as autoridades regulatórias e concorrenciais intervenham quando necessário para mitigar os riscos apresentados pelas plataformas digitais como instituições de pagamento, especialmente envolvendo grandes empresas de tecnologia, como o *Facebook*.

ENTRE A VOZ E A RESPONSABILIDADE: A ERA DO PROCESSO E A VALORIZAÇÃO DA BOA-FÉ NA MODERAÇÃO DE CONTEÚDO EM PLATAFORMAS DIGITAIS

Júlia de Paula Cople[238]

INTRODUÇÃO

Em 06 de janeiro de 2021, enquanto congressistas norte-americanos se reuniam no Capitólio para certificar o resultado das eleições presidenciais de 2020, milhares de pessoas irresignadas com a vitória do democrata Joe Biden invadiram a sede do Legislativo federal dos Estados Unidos. Havia semanas, em postagens impulsionadas por curtidas e compartilhamentos nas redes sociais, o candidato à reeleição derrotado Donald Trump atacava oponentes e convocava partidários, sem apresentar provas, a reagirem à fraude eleitoral[239]. Orquestrada e inflamada previamente em plataformas digitais de comunicação, a ação violenta não "saiu" das telas para as ruas, como destaca Carlos Affonso Pereira de Souza[240]. O caso evidenciou como não há mais separação entre os mundos virtual e real: a turba queria ser vista, compartilhada e validada pelos pares em fóruns digitais, numa integração dos universos *online* e *off-line*. A violência em Washington manifestou fisicamente

[238] Pós-graduanda em Direito Digital pelo ITS/Ceped Uerj. Graduanda em Direito na UFF. Bacharela em Comunicação Social pela PUC-Rio. Jornalista. E-mail: coplej@gmail.com.

[239] LAKIER, Genevieve; TEBBE, Nelson. After the "Great Deplatforming": reconsidering the shape of the First Amendment. LPE Project, 03 jan. 2021. Disponível em: <https://bit.ly/3v703x7>. Acesso em: 16 jun. 2021. Disponível em: https://bit.ly/3v703x7. Acesso em: 16 jun. 2021.

[240] SOUZA, Carlos Affonso Pereira de. Invasão ao Capitólio não "saiu da internet"; esta separação não existe mais. UOL. Coluna Tilt. 09 jan. 2021. Disponível em: <https://bit.ly/3u4Jcef>. Acesso em: 25 ago. 2021.

a polarização política[241] e a desordem informacional[242] que se espraiaram por ciberespaços de debate público.

Diante dessa simbiose violenta, as plataformas digitais de comunicação[243] reforçaram o monitoramento em tempo real de interações entre usuários. O *Facebook*, por exemplo, destacou na ocasião que passara à "busca ativa" de conteúdos e perfis considerados promotores de violência e violadores de políticas da rede e implementara medidas adicionais "para manter as pessoas seguras"[244]. A estratégia envolveu inclusive a aplicação de inteligência artificial para reduzir o alcance de conteúdos que "provavelmente violassem as políticas da empresa"[245] e o banimento de usuários, como Donald Trump, numa iniciativa de moderação da arena digital sem precedentes em termos de escala e repercussão[246].

---

[241] BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. Network Propaganda: manipulation, desinformation and radicalization in American politics. New York: Oxford University Press, 2018.

[242] Claire Wardle e Hossein Derakhshan incluem na categoria de "desordem informacional" a "mis-information" (informação enganadora, sem intenção de causar dano); a "dis-information" (falso contexto, manipulado ou fabricado); e a "mal-information" (assédio moral, discurso de ódio) para conformar a ideia de um paradoxo democrático na circulação de informações em plataformas digitais. Vide WARDLE, Claire; DERAKSHAN, Hossein. Information disorder: towards an interdisciplinary framework for research and policy making. Council of Europe Report. Strasbourg: Council of Europe, 2017. Disponível em: <https://bit.ly/2KbfguJ>. Acesso em: 29 abr. 2021.

[243] Em que pese a multiplicidade de conceitos e modelos de "plataformas digitais", neste artigo, recortamo-nos àquelas mais conhecidas como redes sociais, tais quais *Facebook* e *Twitter*.

[244] ROSEN, Guy; BICKERT, Monika. Our Response to the Violence in Washington, 06 jan. 2021. Disponível em: <https://bit.ly/3aoJUee>. Acesso em 17 jun. 2021.

[245] *Ibid.*, 2021.

[246] LAKIER; TEBBE, 2021.

A invasão do Capitólio e a reação das plataformas evidenciaram a erosão da qualidade do debate público nos fóruns digitais, mas também o poder de atores privados sobre a voz e a visibilidade dos usuários e a transparência no processo de moderação de conteúdos e comportamentos nas redes. Para Richard Rogers[247], destaca-se uma progressiva adoção, por parte das plataformas de comunicação, de medidas restritivas como resposta a comportamentos tóxicos de usuários, não necessariamente alinhadas com leis locais. Marina Estarque, João Victor Archegas, Celina Bottino e Christian Perrone[248] ressaltam que, em pouco mais de uma década, as plataformas assumiram papel vital na moderação do debate público – e muitos usuários até estão cientes disso, mas não de regras e princípios que regem o processo.

O advento da internet, a partir dos anos 1990, trouxe expectativa de mais igualdade e participação nas trocas comunicativas e, com isso, de expansão da produção e do livre consumo de informação, arte e cultura, antes filtrados por déspotas ou por detentores dos meios de produção das mídias de comunicação de massa, explica Clara Keller[249]. Neste

[247] ROGERS, Richard. Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. European Journal of Communication, v. 35(3), p. 213–229, 2020.

[248] ESTARQUE, Marina; ARCHEGAS, João Victor; BOTTINO, Celina; PERRONE, Christian. Redes sociais e moderação de conteúdo: criando regras para o debate público a partir da esfera privada. Rio de Janeiro: Instituto de Tecnologia e Sociedade, 2021. Disponível em: <https://itsrio.org/pt/publicacoes/redes-sociais-e-moderacao-de-conteudo/>. Acesso em: 07 jul. 2021.

[249] KELLER, Clara Iglesias. Democracia e Liberdade de Expressão na Internet – de onde viemos e para onde vamos? In: CRUZ, Adriana; FREIRE, Alonso; PIRES, Thiago Magalhães. O Direito Público por Elas: homenagem à professora Jane Reis. Rio de Janeiro: Lumen Juris, 2018.

período, segundo a autora, a literatura especializada passou a atrelar a potencialização da participação política à expansão do exercício da liberdade de expressão no ambiente *online*, pois as pessoas poderiam assumir a postura ativa de usuários da rede, com alcance global e baixo custo.

No entanto, a própria arquitetura da internet se revelou um obstáculo à democratização do debate e conduziu a uma concentração de poder dos novos intermediários. Lawrence Lessig[250] ressalta que o código binário da internet se impôs como fonte de regulação de relações jurídicas no ambiente *online* e passou a concorrer com a regulação operada por normas jurídicas, normas sociais e leis de mercado.

Na lição de Lessig, como principal fonte de regulação, inclusive incidente sobre as demais, o ordenamento jurídico estatal coexiste com usos e costumes de dadas comunidades para determinadas circunstâncias; com a condução mercadológica que responde ao atendimento de necessidades humanas e afeta o acesso a bens econômicos; e com a regulação da estrutura da internet, considerada a mais eficaz e inflexível, que programa o grau de abertura de camadas e de acesso a informações no ciberespaço. Assim, os quatro eixos contribuem ou restringem o exercício de liberdades individuais de usuários.

Nesta coexistência de regulações, dados o atual estado da técnica e a natureza jurídica privada das plataformas, boa parte das medidas coercitivas aplicáveis pelo mercado e pelo código para induzir comportamentos na internet hoje implica, sem prévio escrutínio social, alguma limitação à liberdade de ex-

[250] LESSIG, Lawrence. Code: and Other Laws of Cyberspace, Version 2.0. Nova York: Basic Books, 2006.

pressão do usuário (vide as alternativas de redução do alcance, de remoção de postagens e até de exclusão de perfis). Neste ponto, o sistema de moderação autorregulado sofre pressão de diferentes espectros políticos[251]: conservadores acusam a plataforma de restringir com mais intensidade conteúdos e comportamentos ligados à direita, e progressistas questionam a concentração de poder das empresas e uma alegada leniência para com discursos de ódio.

Convocado a prestar esclarecimentos sobre a atuação da empresa frente à violência em Washington a uma comissão do Congresso norte-americano, o *CEO* do *Facebook*, Mark Zuckerberg, defendeu[252] a decisão de restringir conteúdos e suspender usuários, mas concordou com a necessidade de parâmetros regulatórios e de alguma revisão na imunidade (garantida nos Estados Unidos) dos intermediários para a gestão do debate público nas redes sociais. O empresário ponderou, porém, a importância da preservação da liberdade de expressão, já que usuários devem poder questionar o sistema e as leis sob os quais vivem.

Em suma, a moderação do debate público nas plataformas digitais implica um choque de direitos no ciberespaço: colidem a livre iniciativa da plataforma, no sentido da sua liberdade de contratar e estabelecer as regras da sua atividade, e as liberdades fundamentais de expressão e desenvolvimento da personalidade dos usuários. Neste diapasão, impõe-se o

[251] ESTARQUE; ARCHEGAS; BOTTINO; PERRONE, 2021.

[252] A sessão do Comitê foi transmitida pelo YouTube. ENERGY AND COMMERCE COMMITTEE. Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation. YouTube, 25 mar. 2021. Disponível em: <https://www.youtube.com/watch?v=dw6wJ7dFiPs>. Acesso em: 09 jun. 2021.

debate se as plataformas digitais podem ou mesmo devem moderar conteúdos e comportamentos de usuários em meio ao debate público no ambiente digital e se podem fazê-lo segundo seus termos globais de serviço, sem decisão judicial ou escrutínio social que legitime o processo.

Projetos de lei em tramitação no Congresso Nacional[253] brasileiro visam a alterar o Marco Civil da Internet (MCI, Lei 12.965/2014) no sentido de condicionar a moderação do ambiente *online* a decisões judiciais ou prever hipóteses de nulidade de cláusulas contratuais de suspensão de conteúdo ou ainda responsabilizar plataformas pela atividade moderadora que censurar ou rotular postagens como "enganosas" ou "questionáveis". Em maio de 2021, o Executivo federal anunciou que preparava um decreto para, em prol da "liberdade" dos usuários, restringir a livre iniciativa das plataformas ao proibir, por regra, a tomada de medidas de moderação sem ordem judicial, com limitadas exceções, sob o argumento de que as políticas das empresas "afrontam o ordenamento jurídico nacional" [254].

O presente trabalho, nesta esteira, sem a pretensão de esgotar o tema, se propõe a investigar: a moderação operada por iniciativa própria das plataformas digitais de comunicações fere o ordenamento jurídico brasileiro? Demarcado o

[253] Projeto de Lei nº 213/2021; Projeto de Lei nº 291/2021; e Projeto de Lei nº 246/2021; entre outros.

[254] VARGAS, Mateus. Bolsonaro prepara decreto, considerado ilegal, para limitar retirada de posts e perfis das redes sociais. Folha de São Paulo, São Paulo, 20 mai. 2021. Caderno Poder, online. Disponível em: <https://www1.folha.uol.com.br/poder/2021/05/governo-prepara-decreto-para-limitar-retirada-de-posts-e-perfis-das-redes-sociais.shtml>. Acessado em 05 jul. 2021.

problema, para realizar o esforço intelectual sugerido, primeiro serão descritos o histórico e o estado da arte da moderação de conteúdos e comportamentos das plataformas digitais para depois serem abordados o enquadramento legal aplicado no Brasil e o choque entre liberdade de expressão e livre iniciativa neste processo. Por fim, discute-se a centralidade do direito fundamental ao devido processo e da boa-fé objetiva no bojo da relação contratual usuário-plataforma.

1. DA MODERAÇÃO DE CONTEÚDO

John Bowers e Jonathan Zittrain[255] dividem o processo histórico de moderação de conteúdos nas plataformas digitais em três fases, distribuídas no correr de três décadas. De início, firmou-se uma fase privilegiadora de direitos na rede, com foco na promoção da liberdade de expressão e de inovações tecnológicas e na proteção contra incursões estatais. Neste momento, as plataformas adotaram uma postura de evitar ao máximo restringir discursos, mas, observados os impactos sociais desse grau de liberdade, sobreveio o que os autores classificam como uma fase da saúde pública.

Sobre esta transição, operada nos anos 2010, Kate Klonick[256] e Jack Balkin[257] explicam que as empresas privadas, pressionadas por governos nacionais ante a circulação de ilícitos no

[255] BOWERS, John; ZITTRAIN, Jonathan. Answering impossible questions: Content governance in age of disinformation. Harvard Kennedy School (HKS) Misinformation Review, n.1, v.1. 2020. Disponível em: <https://bit.ly/3gPHc5u>. Acesso em: 29 abr. 2021.

[256] KLONICK, Kate. The New Governors: the people, rules, and processes governing online speech. Harvard Law Review, v. 131, p. 1598-1670, 2018.

[257] BALKIN, Jack. Free Speech is a Triangle. Columbia Law Review, v. 118, p. 2011-2056, 2018.

ambiente *online*, migraram "quase sem querer" da postura de canal da "voz" dos usuários, sem juízo de conteúdo, para o de governantes do discurso *online*, na tentativa de retardar regulações externas, legitimar a autorregulação, atender as expectativas dos usuários e evitar que eles se desengajassem por se sentirem inseguros ou ofendidos.

Em 2019, em ponto alto dessa guinada, o *Facebook* atualizou os "valores" dos seus Padrões de Comunidade. No anúncio da medida, a diretora Monika Bickert destacou que, por mais de uma década, a rede social focou em "dar voz às pessoas, manter um ambiente seguro e aplicar as políticas de forma consistente e justa pelo mundo"[258], mas que a partir de então, segundo ela, a plataforma passaria a considerar os valores de voz, autenticidade, segurança, privacidade e dignidade na elaboração e na aplicação das regras do negócio.

Segundo Balkin, os provedores de aplicações se viram na posição de organizar esses espaços, até para que as pessoas continuassem ativas na rede – norte dos seus modelos de negócio – e fizeram-no por meio de "uma combinação de contrato e código"[259]. Para Bowers e Zittrain, a fase da saúde pública na internet colocou sob discussão global a responsabilização das plataformas e recrudesceu o dilema quanto à imposição privada de limites à liberdade de expressão nesse espaço virtual[260] – historicamente celebrado por seu potencial

[258] BICKERT, Monica. Updating the Values That Inform Our Community Standards. 12 set. 2019. Disponível em: <https://bit.ly/3x3FHq9>. Acesso em: 18 abr. 2021.

[259] BALKIN, 2018, p. 2021.

[260] BOWERS; ZITTRAIN, 2020.

democratizante de discursos[261], nada obstante os obstáculos colocados pela própria codificação privada da *web*[262]. Na visão de Balkin, foi instalado um sistema de moderação autorregulado autocrático, sem transparência nem devido processo, com exceções para pessoas e organizações influentes[263].

James Grimmelmann[264] conceitua a moderação de conteúdos como "o conjunto de mecanismos de governança que estruturam a participação em uma plataforma para facilitar cooperação e prevenir abusos"[265], num processo que se materializa numa comunidade *online* entre proprietários da infraestrutura, moderadores dessa comunidade, autores e leitores do conteúdo. Para o autor, tal processo pode gerar consequências morais, ao expandir o acesso ou, de maneira inversa, excluir pessoas da comunidade e do conhecimento que ela produz. Nesta esteira, o autor vincula a abertura da comunidade à democracia na moderação, isto é, à participação dos atores no processo, na formulação das políticas de moderação e até na possibilidade de opinar sobre as decisões de aplicação dessas políticas.

No Brasil, o Marco Civil da Internet (MCI, Lei 12.965/2014) não estabelece requisitos para a remoção de conteúdo ou suspensão de contas: como ensinam Carlos Affonso de Souza e Chiara de Teffé[266], não há dever de monitoramento prévio de

---

[261] KELLER, 2018.

[262] LESSIG, 2006.

[263] BALKIN, 2018, p. 2025.

[264] GRIMMELMANN, James. The Virtues of Moderation. Yale Journal on Law & Technology, v. 17, p. 42-109, 2015.

[265] *Ibid.*, p.47-48.

[266] SOUZA, Carlos Affonso Pereira de; TEFFÉ, Chiara Spadaccini de. Respon-

atos de terceiros e a normativa específica, em seu artigo 19, condiciona a responsabilidade civil dos provedores à omissão frente a uma ordem judicial específica[267]. No entanto, ressaltam eles, a legislação não veda que tais atores, na gestão de suas atividades, disciplinem o que pode ou não ser publicado ou mantido na plataforma, com base nos próprios termos de serviço, cuja natureza contratual de adesão é reconhecida pacificamente pela doutrina e pela jurisprudência nacionais.

O MCI tampouco imuniza esses provedores por eventuais lesões a direitos decorrentes de ato próprio: isto é, podem ser responsabilizados se abusarem da liberdade de gerir aquele ambiente *online* e estabelecerem restrições arbitrárias a usuários, de modo que "devem tomar o exercício da liberdade de expressão como vetor de suas atividades, sendo medidas de filtragem, bloqueios ou remoção uma solução excepcional"[268].

Para fins de comparação, nos Estados Unidos, berço da doutrina da liberdade de expressão, a *Section 230* da *Communications Decency Act* – hoje também sob discussão de mudança naquele país – prevê ampla imunidade a intermediários de serviços *online*, de maneira que as plataformas digitais não

---

sabilidade dos provedores por conteúdos de terceiros na internet. Revista Eletrônica Consultor Jurídico, 23 jan. 2017.

[267] Pende de decisão no Supremo Tribunal Federal questionamento sobre a constitucionalidade do artigo 19 do MCI (tema de repercussão geral 987 ligado ao *leading case* RE 1.037.396/SP), notadamente sobre o atual regime de responsabilidade civil subjetiva por omissão. Adota-se neste artigo, porém, a visão de que as plataformas não podem ser responsabilizadas por danos decorrentes de atos de terceiros sob pena de se incentivar um monitoramento prévio de conteúdos e se colocar em risco a liberdade de expressão na rede. Discute-se neste artigo a legalidade da moderação de conteúdos por iniciativa própria dos provedores.

[268] SOUZA; TEFFÉ, 2017.

são responsabilizadas por danos decorrentes de conteúdo de terceiros e, pela chamada cláusula do "bom samaritano", podem restringir livremente, sem responsabilização, postagens e contas que considerem obscenas e ofensivas[269].

Dada a capilaridade das plataformas digitais na vivência social e política dos usuários, a moderação de conteúdos e comportamentos nesses espaços se torna condição para a qualidade do serviço e para a garantia de direitos fundamentais e do ambiente democrático, segundo Juliano Maranhão, Ricardo Campos, Matthias Kettemann, Juliana Abrusio e Giovanni Sartor[270]. Neste sentido, porém, segundo os autores, os termos de uso desses provedores devem convergir com a ordem jurídica estatal nas democracias constitucionais contemporâneas, de modo que as regras que regem a relação plataforma-usuário ultrapassem a relação contratual e incorporem ditames legais e constitucionais.

Com a invasão do Capitólio, autores norte-americanos recuperaram o contexto de aprovação e aplicação da Primeira Emenda para destacarem como a moderação autorregulada das plataformas não viola a liberdade de expressão à luz da Constituição do país, uma vez que o ditame constitucional restringe a ação de atores estatais – e não de atores privados – sobre discursos de cidadãos[271]. No Brasil, porém, Maria

[269] ESTARQUE; ARCHEGAS; BOTTINO; PERRONE, 2021.

[270] MARANHÃO, Juliano; CAMPOS, Ricardo; KETTEMANN, Matthias; FLORÊNCIO, Juliana Abrusio; SARTOR, Giovanni. Como regular a moderação privada de conteúdo nos novos espaços públicos? Revista Eletrônica Consultor Jurídico, *online*, p. 1 - 1, 01 set. 2020.

[271] LAKIER; TEBBE, 2021.

Celina Bodin de Moraes[272] ensina que uma reviravolta jurídica pôs valores existenciais acima de interesses econômicos e passou a admitir a aplicação direta das normas e dos valores constitucionais nas relações privadas, numa eficácia horizontal dos direitos fundamentais.

Carlos Affonso de Souza[273] destaca que o MCI foi aprovado como uma afirmação de direitos em meio a iniciativas de se regular a internet no Brasil sob a perspectiva de tutela dos direitos fundamentais. Neste aspecto, para o autor, a legislação conferiu especial tratamento à liberdade de expressão, positivada como princípio, como condição de exercício de direitos na rede e como parâmetro interpretativo para a responsabilização por eventuais danos.

Além disso, para o autor, a inscrição desta liberdade no caput do artigo 2º do MCI sugere a sua posição prevalente entre os fundamentos da disciplina do uso da internet no Brasil, na esteira de sua interpretação como fundamento para o exercício de outras liberdades individuais. Lenio Streck e Marcelo Andrade Cattoni de Oliveira[274] ponderam que tal liberdade não pode acabar por legitimar violências incompatíveis com a democracia – e, portanto, com a ordem constitucional bra-

[272] BODIN de MORAES, Maria Celina. A caminho de um direito civil constitucional. Revista de Direito Civil, Imobiliário, Agrário e Empresarial, p. 21-32, jul. 1993.

[273] SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no marco civil da Internet. In: DE LUCCA, Newton, et al. (org.). Direito & Internet III – Marco Civil da Internet: Lei 12.965/2014. São Paulo: Quartier Latin, 2015.

[274] STRECK, Lenio Luiz; CATTONI DE OLIVEIRA, Marcelo Andrade. Pode-se, em nome da democracia, propor a sua extinção? Revista Eletrônica Consultor Jurídico, São Paulo, p. 1-4, 22 jun. 2020. Disponível em: <https://bit.ly/37afjPy>. Acesso em: 29 jul. 2021.

sileira. Os autores sustentam que a liberdade de expressão não se refere apenas ao emissor e deve considerar também o destinatário, o contexto e a história da fala, de maneira a se distinguir – dada a essencialidade dessa liberdade para a conformação do Estado Democrático de Direito – uma ilegítima mordaça e a legítima posterior responsabilização.

Na lição de Jack Balkin, a liberdade de expressão na internet "é um triângulo" entre os Estados nacionais, os agentes privados e os usuários. Dessa relação, decorrem três riscos, na análise do autor: 1) a possibilidade de imposição de regulações que impliquem censura colateral e restrições prévias ao ambiente digital; 2) o abuso de burocracias privadas que "governam" arbitrariamente usuários, sem devido processo nem transparência; e 3) a vigilância digital que facilita a manipulação de visões de mundo[275].

Estarque, Archegas, Bottino e Perrone apontam a dificuldade, num serviço global de comunicações, de se equilibrar diferentes tradições de liberdade de expressão na gestão de discursos, com diferentes contextos culturais e réguas de ilicitude conforme o país de atuação. Assim, para os autores, a tarefa dos governantes do ambiente *online* de estabelecer limites e critérios "sempre será, até certa medida, arbitrária"[276]. Neste contexto, a fim de se preservar a liberdade de expressão e se conter a concentração de poder, Balkin[277] sugere, de início, regulações estruturais pró-concorrência e contra a discriminação, mas também a imposição de garantias de devido processo

[275] BALKIN, 2018, p. 2055. Para fins deste artigo, nos debruçamos sobre os dilemas 1 e 2.

[276] ESTARQUE; ARCHEGAS; BOTTINO; PERRONE, 2021, p. 27.

[277] BALKIN, 2018.

na curadoria de conteúdo e o reconhecimento de deveres de lealdade, confiança e boa-fé nas relações plataforma-usuários.

2. DOS DIREITOS E OBRIGAÇÕES

Vê-se, pela discussão da seção anterior, que a moderação de conteúdos por iniciativa própria das plataformas não implica necessariamente violação à "voz" de usuários. Neste sentido, iniciativas legais ou executivas que privilegiem a liberdade de expressão dos falantes, em desconsideração da posição dos ouvintes e em detrimento desproporcional da livre iniciativa, não conduzem a uma maior proteção dos usuários.

A Constituição Federal vigente no Brasil destaca a fundamentalidade da liberdade de expressão, independentemente de censura ou licença (art. 5º, inciso IX), mas também registra a livre iniciativa como fundamento da República (art. 1º, IV) e da ordem econômica do país, conforme os ditames da justiça social e observada a função social da propriedade (art. 170, caput e inciso III)[278]. Para equilibrar os direitos, cartilhas internacionais e as próprias empresas, como o *Facebook*, têm defendido o incentivo à inovação e a aplicação de testes de proporcionalidade e necessidade das medidas de moderação[279].

Ainda que não configure censura, a moderação interfere em manifestações individuais e altera holisticamente as condições sociais do discurso – e não de forma neutra, mas por critérios baseados em interesses políticos e econômicos das plataformas –, pelo que deve ser operada sob uma ótica

[278] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Centro Gráfico, 1988.

[279] ESTARQUE; ARCHEGAS; BOTTINO; PERRONE, 2021.

de transparência e devido processo, na visão de Lahis Kurtz, Paloma do Carmo e Victor Vieira[280]. Esta visão se alinha no Brasil – na ponderação de direitos fundamentais em quaisquer relações jurídicas, considerada a eficácia horizontal – com o direito fundamental ao devido processo do artigo 5º, LIV, da Constituição Federal[281]. Segundo Kurtz, Do Carmo e Vieira, porém, as legislações nacionais, como a brasileira, carecem da previsão de obrigações robustas de transparência no processo, com parâmetros obrigatórios de devido processo e de publicidade de critérios de restrição e decisões, sejam humanas ou automatizadas.

Neste escopo de críticas ao estado da arte da moderação, Bowers e Zittrain[282] apontam a vinda de uma terceira fase: a era do processo. Ante as dificuldades práticas da governança do ambiente *online*, como a disputa política sobre como ela deve ser operada e a quantidade de conteúdo circulante, a nova etapa mira, segundo os autores, incentivos à clareza na elaboração e na aplicação de regras de conduta e de moderação. Em detrimento do mero juízo valorativo de discursos, apontar-se-ia para o juízo de proporcionalidade, para a necessidade de fundamentação das decisões e de transparência na aplicação de medidas restritivas, além da criação de mecanismos de reclamação e revisão de decisões.

[280] KURTZ, Lahis Pasquali; DO CARMO, Paloma Rocillo Rolim; VIEIRA, Victor Barbieri Rodrigues. Transparência na moderação de conteúdo: tendências regulatórias nacionais. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: <https://bit.ly/3xjAUka>. Acesso em: 08 jul. 2021.

[281] BRASIL, 1988.

[282] BOWERS; ZITTRAIN, 2020.

Logo, as plataformas digitais podem operar, por iniciativa própria, a moderação de discursos *online*, mediante um devido processo para o equilíbrio da liberdade de expressão e da livre iniciativa. Resta investigar, porém, se não são responsabilizadas senão pelo descumprimento de ordem judicial específica, por que elas moderariam? Há dever de moderar?

Como visto anteriormente, as plataformas digitais estruturaram um sistema de governança privada via código, na programação de suas funcionalidades[283], e contrato, na elaboração de termos de serviço e padrões de comunidade aos quais cada usuário deve aderir para participar dela[284]. Segundo Claudia Lima Marques[285], a adesão a serviços desta espécie inaugura uma relação de consumo compartilhado. Num modelo de negócio concentrado em acesso e uso em comum das utilidades, segundo a autora, o intermediário desaparece na tecnologia, mas se coloca muito presente no local de encontro entre as partes e na imposição de regras sobre esse encontro.

Destaca Marques que tal modelo de economia digital se estrutura sobre uma relação de confiança entre todas as pontas da cadeia de compartilhamento, de maneira que se gera responsabilidade para todas elas pela confiança criada. Na lição da autora, a posição da plataforma como organizadora do

[283] LESSIG, 2006.

[284] BALKIN, 2018.

[285] MARQUES, Cláudia Lima. A nova noção de fornecedor no consumo compartilhado: um estudo sobre as correlações do pluralismo contratual e o acesso ao consumo. REVISTA DE DIREITO DO CONSUMIDOR, v. 111, p. 247, 2017.

compartilhamento contamina toda a relação como de consumo e reforça os deveres de boa-fé para toda a rede de contratos[286].

Flávio Tartuce[287] ensina que o direito civil, o direito processual civil e o direito consumerista valorizam o princípio da boa-fé objetiva e os ditames constitucionais (como as liberdades e o devido processo) nas fases pré, durante e pós-contrato. Dada essa principiologia una, o autor destaca a progressiva aplicação do diálogo das fontes para a complementaridade das normas e o atendimento das finalidades da ordem jurídica no Brasil. Assim, as relações privadas reclamam atenção à vulnerabilidade das partes, aos deveres de confiança, ao equilíbrio contratual e a um padrão ético de conduta (a boa-fé objetiva), tendo esta última a função limitadora da liberdade contratual[288]. Nas relações desenvolvidas na internet, este sistema ainda se complementa com as normativas do Marco Civil da Internet, a Lei nº 12.965/2014.

Cristiano Chaves de Farias e Nelson Rosenvald[289] reforçam que, na evolução do direito brasileiro, para evitar que se transformasse num instrumento de pressão, o contrato foi "impregnado pela justiça e pela solidariedade"[290] e passou a ser visto não como um ato isolado, mas uma relação inserida em processos econômico-sociais. Assim, ao analisarem o contrato como um

[286] ***Ibid.***, p. 254.

[287] TARTUCE, Flávio. Direito civil: teoria geral dos contratos e contratos em espécie. 10ª ed. São Paulo: Método, 2015. v. 1. 730p.

[288] MARQUES, 2017 ***apud*** TARTUCE, 2015.

[289] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. Curso de Direito Civil: Volume 4 - Contratos, Teoria Geral e Contratos em Espécie. 7ª ed. Salvador: JusPodivm, 2017. v. 4. 1131p.

[290] ***Ibid.***, 2017, p. 46.

veículo de livre desenvolvimento da personalidade e meio de realização da dignidade humana, os autores sustentam que tanto a liberdade contratual (o conteúdo da relação) quanto a liberdade de contratar (o estabelecimento do negócio jurídico) se submetem à realização de uma função social, nos termos do art. 421 do Código Civil[291].

O desequilíbrio prévio da liberdade contratual nos contratos de adesão (como os firmados entre usuários e plataformas) não afasta a sua contratualidade nem a sua natureza de instrumento de intercâmbio de bens e serviços e espaço de afirmação da pessoa humana, na visão de Farias e Rosenvald, mas legitima uma intervenção externa mais intensa para assegurar a paridade, em conjugação com a normal geral de interpretação da boa-fé. Como apontou Marques[292], sendo a plataforma uma rede de contratos, há que se considerar o dever de confiança e de boa-fé objetiva em todas as pontas da cadeia, sem que se afaste a possibilidade de interferência externa para garantir o equilíbrio e a realização da função social.

Se a liberdade de expressão é o norte do Marco Civil da Internet, a boa-fé é o elo essencial do diálogo de fontes no Brasil. A partir da positivação do direito consumerista, Farias e Rosenvald destacam como a boa-fé assumiu o posto de modelo de comportamento no direito brasileiro, a ser coordenado, para ser concretizado, com outras normas do ordenamento. Desta maneira, em vista da generalidade do princípio, alarga-se o conceito de adimplemento das obrigações, a abarcar também o atendimento dos chamados deveres anexos e a ensejar, inclusive, em caso de violação dos mesmos, "o nascimento da

[291] FARIAS; ROSENVALD, 2017, p. 352.

[292] MARQUES, 2017.

pretensão reparatória ou do direito potestativo à resolução do vínculo"[293].

Neste ponto, ainda que fossem constitucionais, os termos minutados no decreto do Executivo federal para limitar a livre iniciativa das plataformas ainda dariam azo à moderação privada, como no artigo 2º-B, parágrafo único, I, que prevê a autorização para a exclusão de contas em caso de "inadimplência do usuário"[294]. Considerado esse alargamento do conceito de adimplemento das obrigações à luz do princípio da boa-fé objetiva, ainda se encontraria fundamento para restringir comportamentos de usuários que violassem os deveres assumidos para com a plataforma e para com os demais usuários da comunidade.

Farias e Rosenvald[295] explicam que o sistema obrigacional brasileiro vigente amplia a noção de inadimplência para reconduzir o atendimento de necessidades das partes e da função social dos contratos na concretude de cada relação. Como aponta Marques[296], a economia digital possibilita a constituição de um pluralismo de vínculos, isto é, uma pluralidade não só intersubjetiva (com solidariedade interna desta cadeia), mas uma interdependência atávica nos contratos entre o intermediador digital e os pares que compartilham o serviço.

Trata-se, nesta esteira, de uma rede com pontas unidas e conexas, pelo que não há que se exigir a prevalência irrestrita da liberdade de expressão de usuários de má-fé, nem há que

[293] FARIAS; ROSENVALD, 2017, p. 193.

[294] VARGAS, 2021.

[295] FARIAS; ROSENVALD, 2017.

[296] MARQUES, 2017, p. 258.

se cogitar o que seria, na prática, um direito fundamental de abusar de liberdades e violar regras de uma comunidade compartilhada digitalmente.

CONSIDERAÇÕES FINAIS

A análise do choque de direitos fundamentais frente à governança privada de discursos nas plataformas digitais e a breve revisão bibliográfica sobre a história e o estado da arte deste processo evidenciam que as plataformas não só podem, como devem moderar discursos e comportamentos no ambiente *online*: trata-se de parte do adimplemento das obrigações assumidas para com as pontas da rede de contrato. Neste sentido, o ato de o provedor governar o ciberespaço não viola, por essência, o ordenamento jurídico brasileiro.

A posição preferencial conferida em primeiro momento à liberdade de expressão não se confunde com uma liberdade irrestrita, imune a uma posterior responsabilização, tampouco bloqueia o exercício da livre iniciativa dos gestores do espaço. Os provedores de aplicações podem moderar, na gestão de suas atividades, e devem governar os seus canais de circulação de informações em atenção à centralidade, no direito brasileiro, do princípio da boa-fé objetiva.

No entanto, também por boa-fé e pela eficácia horizontal dos direitos fundamentais, a moderação não pode ser arbitrária. O direito brasileiro já oferece parâmetros de partida para necessárias regulações adicionais na "era do processo": a governança do ambiente *online* deve privilegiar a liberdade de expressão e, para limitá-la, ser operada mediante um devido processo, com base em cláusulas e critérios transparentes, juízo de proporcionalidade e possibilidade de reclamação e

revisão de termos e decisões, sendo certo que as plataformas não estão imunes à responsabilidade por violações decorrentes de atos próprios nessa moderação.

Na lição de Lawrence Lessig, qualquer pretensão regulatória congrega as leis do código, as leis de mercado, as normas sociais e as normas jurídicas. Condicionar os eixos de código e mercado a decisões judiciais poderia inviabilizar o endereçamento de problemas próprios à sociedade e à economia digital, como a efetiva contenção da desordem informacional no ciberespaço e a sua manifestação em violência como na invasão do Capitólio em Washington, de maneira a colocar em xeque o exercício de liberdades nas redes e nas ruas como um todo.

A LIBERDADE DOS VEÍCULOS DE COMUNICAÇÃO DIGITAIS DE REALIZAR DEBATES ELEITORAIS

Amanda Perli Golombiewski[297]

INTRODUÇÃO

A Lei n. 9.504/97 faculta às emissoras de radiodifusão, aqui compreendidas as emissoras de rádio e as emissoras de televisão (sujeitas à concessão pública, conforme art. 223, da Constituição Federal), a realização de debates e entrevistas entre os candidatos a cargos eletivos em um determinado pleito eleitoral.

O art. 46, do referido diploma geral, estabelece regras para a realização de debates a serem transmitidos por emissoras de rádio ou de televisão (tanto entre candidatos, quanto entre pré-candidatos, conforme art. 36-A, I, da mesma lei), inclusive prevendo a obrigatoriedade de convite para candidatos cujos partidos políticos ou coligações detenham, no mínimo, cinco parlamentares no Congresso Nacional.

A Lei Geral de Eleições é, contudo, aparentemente por escolha do legislador, omissa quanto à possibilidade de realização e de transmissão de debates por veículos de comunicação via internet, o que, ao mesmo tempo em que permite concluir que o espaço online é predominantemente livre, gera certa insegurança jurídica.

[297] Graduada em Direito pela Faculdade de Direito de Curitiba, do Centro Universitário Curitiba. Especialista em Direito Civil e Processual pelo Centro Universitário Curitiba e pós-graduanda em Direito Digital pelo ITS Rio/UERJ.

1. A SISTEMÁTICA DOS DEBATES ELEITORAIS NA LEI N. 9.504/97

O direito à informação é um direito fundamental positivado na Constituição Federal de 1988, em seu art. 5º, XIV. Os veículos de comunicação concretizam o direito à informação, levando ao conhecimento da sociedade fatos de interesse público, assim considerados como aqueles "que dizem respeito às escolhas que a pessoa deve fazer como membro de sua comunidade, que interessam às demais e nelas interfiram, bem como que influenciem e interfiram no que pertine à sua organização política e social"[298].

Durante o período eleitoral, o direito à informação e a liberdade de comunicação adquirem maior relevância, na medida em que "é através da imprensa que os cidadãos se conscientizam dos problemas comuns da polis; ela é fundamental na orientação e dos quadros dirigentes da nação, e quanto ao juízo a que todos nós temos direito de fazer acerca das políticas públicas implementadas pelos governantes eleitos"[299].

[298] STROPPA, Tatiana. As dimensões constitucionais do direito de informação e o exercício da liberdade de informação jornalística. Belo Horizonte: Fórum, 2010, p. 164.

[299] BRASIL. Supremo Tribunal Federal. Arguição de descumprimento de preceito fundamental n. 130/DF. Arguinte: Partido Democrático Trabalhista – PDT. Arguido: Presidente da República e outros. Relator: Ministro Carlos Ayres Britto. Brasília, 30/04/2009. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605411. Acesso em 22/11/2021.

Para além disso,

> Para que a vontade coletiva possa ser exprimida por meio do voto e para que os representantes eleitos possam continuar responsivos à vontade da cidadania, não basta o procedimento formal da votação. É necessário que haja um espaço público que garanta o livre fluxo de informações e ideias e que permita que os cidadãos possam, não apenas selecionar os representantes, mas discutir continuamente temas de interesse público, fiscalizar a influenciar a atuação dos representantes. A democracia não se limita, assim, ao exercício do direito ao voto. Ela envolve um permanente processo participativo, que permite a formação da vontade coletiva, a partir do engajamento de seus cidadãos, seja para expressar suas ideias, seja para ouvir aquelas que são divulgadas pelos seus pares ou pelas mídias: democracia é a participação no debate político.[300]

A Lei n. 9.504/97, na esteira das normas constitucionais, e o Tribunal Superior Eleitoral, por intermédio de suas resoluções e normativas editadas a cada pleito, procuraram regulamentar o exercício da atividade dos veículos de comunicação de modo a harmonizar o direito de informar e à informação com os demais princípios inerentes ao processo eleitoral, impondo, por exemplo, restrições à programação normal das emissoras de radiodifusão, como aquelas trazidas pelo art. 45, I, Lei n. 9.504/97[301].

---

[300] OSÓRIO, Aline. Direito eleitoral e liberdade de expressão. Belo Horizonte: Fórum, 2017, p. 71.

[301] "Com tais restrições, pretende-se privilegiar os princípios da imparcialidade e da impessoalidade na prestação de serviço público, bem como

Com os debates eleitorais, não foi diferente. Exatamente por serem de suma importância para que o eleitor tome conhecimento das propostas de cada candidato e veja o embate entre os concorrentes ao cargo eletivo em disputa, a Lei n. 9.504/97 estabeleceu regras para sua realização e veiculação em emissoras de rádio e televisão.

Inicialmente, é importante que se conceitue o debate como "um encontro face a face entre candidatos correntes (normalmente) a cargos do Poder Executivo, em que lhes são feitas perguntas e apresentados temas e problemas diversos para suas apreciações e respostas"[302], com a ressalva de que é possível a realização de debates entre pré-candidatos, conforme previsto no art. 36-A, I, da Lei n. 9.504/97.

A doutrina faz importante resgate histórico, ensinando que o primeiro debate eleitoral televisionado de que se tem notícia foi veiculado nos Estados Unidos da América, na campanha presidencial de 1960. Já no Brasil, teria sido realizado em 1982[303], tornando-se a partir daí parte tradicional do período eleitoral[304] e, inclusive, aguardada pelos candidatos.

---

da isonomia e do equilíbrio entre os participantes do certame, impedindo-se que uns sejam beneficiados em detrimento de outros. Tendo em vista que o rádio e a televisão constituem serviços públicos cuja realização pelo particular depende de concessão do Poder Público, há mister que o concessionário aja com imparcialidade perante os candidatos e as agremiações participantes do certame." (GOMES, José Jairo. Direito eleitoral. 12. ed. São Paulo: Atlas, 2016, p. 516).

[302] GOMES, José Jairo. Direito eleitoral. 12. ed. São Paulo: Atlas, 2016, p. 519.

[303] GOMES, José Jairo. Direito eleitoral. 12. ed. São Paulo: Atlas, 2016, p. 520.

[304] "Quanto aos debates, matéria vertida no art. 46, da Lei de Eleições, é preciso ter presente, em primeiro plano, que, embora se esteja a tratar de regulamentação mínima sobre atividade privada – serviços de radiodifusão sonora, e de sons e imagens, explorado diretamente ou mediante con-

Na Lei Geral de Eleições, o art. 46 regulamenta a realização de debates eleitorais pelas emissoras de rádio e televisão, nos seguintes termos:

> Art. 46. Independentemente da veiculação de propaganda eleitoral gratuita no horário definido nesta Lei, é facultada a transmissão por emissora de rádio ou televisão de debates sobre as eleições majoritária ou proporcional, assegurada a participação de candidatos dos partidos com representação no Congresso Nacional, de, no mínimo, cinco parlamentares, e facultada a dos demais, observado o seguinte:
>
> I - nas eleições majoritárias, a apresentação dos debates poderá ser feita:
>
> a) em conjunto, estando presentes todos os candidatos a um mesmo cargo eletivo;
>
> b) em grupos, estando presentes, no mínimo, três candidatos;
>
> II - nas eleições proporcionais, os debates deverão ser organizados de modo que assegurem a presença de número equivalente de candidatos de todos os partidos e coligações a um mesmo cargo eletivo, podendo desdobrar-se em mais de um dia;
>
> III - os debates deverão ser parte de programação previamente estabelecida e divulgada pela emis-

---

cessão, permissão ou autorização –, sequer havendo obrigatoriedade na realização dos debates, o ordinário é a sua realização, sendo que tal atividade é essencialmente de caráter público, podendo interferir gravemente na disputa eleitoral e, assim, no processo de construção da democracia." (STF – ADI 5487 – Rel. Min. Luis Roberto Barroso – J. 25.08.2016).

sora, fazendo-se mediante sorteio a escolha do dia e da ordem de fala de cada candidato, salvo se celebrado acordo em outro sentido entre os partidos e coligações interessados.

§1º. Será admitida a realização de debate sem a presença de candidato de algum partido, desde que o veículo de comunicação responsável comprove havê-lo convidado com a antecedência mínima de setenta e duas horas da realização do debate.

§2º. É vedada a presença de um mesmo candidato a eleição proporcional em mais de um debate da mesma emissora.

§3º. O descumprimento do disposto neste artigo sujeita a empresa infratora às penalidades previstas no art. 56.

§4º. O debate será realizado segundo as regras estabelecidas em acordo celebrado entre os partidos políticos e a pessoa jurídica interessada na realização do evento, dando-se ciência à Justiça Eleitoral.

§5º. Para os debates que se realizarem no primeiro turno das eleições, serão consideradas aprovadas as regras, inclusive as que definam o número de participantes, que obtiverem a concordância de pelo menos 2/3 (dois terços) dos candidatos aptos, no caso de eleição majoritária, e de pelo menos 2/3 (dois terços) dos partidos ou coligações com candidatos aptos, no caso de eleição proporcional[305].

[305] BRASIL. Lei n. 9.504/97, art. 46.

Nota-se, pela leitura do artigo, que os debates eleitorais deverão fazer parte da grade de programação das emissoras de radiodifusão, que, por sua vez, deverão estabelecer regras para o seu funcionamento, as quais deverão ser aprovadas por pelo menos dois terços dos candidatos aptos a participar do evento.

Mas quem são os candidatos aptos a participar do evento? São aqueles cujas coligações ou cujos partidos políticos[306] a que pertençam detêm, no mínimo, cinco parlamentares no Congresso Nacional. Estes candidatos têm participação assegurada no debate eleitoral, podendo, naturalmente, declinar do convite, caso assim prefiram. O convite aos demais, ou seja, àqueles que não atingirem o número mínimo de representantes no Parlamento, é uma faculdade das emissoras. Foi como esclareceu o Tribunal Superior Eleitoral ao responder à consulta n. 62-75.2016.6.00.0000/DF:

> CONSULTA. PROPAGANDA ELEITORAL. ART. 46 DA LEI N° 9.504/97. NOVA REDAÇÃO. LEI N° 13.165/2015. INTERPRETAÇÃO. DEBATE. CANDIDA-

[306] "A referência ao número mínimo de deputados contida no art. 46 da Lei n. 9.504/97 deve ser compreendida como a quantidade de deputados federais pertencentes aos quadros de determinado partido político, o qual, quando superior a nove, impõe a obrigatoriedade de o candidato filiado a tal agremiação ser convidado para participar dos debates realizados pelas emissoras. No caso de coligações, o número mínimo de deputados federais previsto no art. 46 da Lei n° 9.504/97 deve ser aferido, quando se tratar de eleição proporcional, pela soma de todos os representantes dos partidos políticos que compõem a coligação na Câmara dos Deputados e, quando se tratar de eleição majoritária, pelo total de deputados federais dos seis maiores partidos que compõem a coligação." (TSE – Consulta n. 491-76.2015.6.00.0000 – Rel. Min. Henrique Neves da Silva – J. 17.03.2016).

TOS. PARTICIPAÇÃO. CONVITE. OBRIGATORIEDADE. REPRESENTATIVIDADE. CÂMARA DOS DEPUTADOS. COLIGAÇÃO. POSSIBILIDADE. PARTIDO POLÍTICO. EQUIPARAÇÃO.

1. É facultada ao candidato a prefeito ou a vereador a participação em debates, caso a coligação partidária que integre seja formada por partidos que, somados, atendam, no mínimo, à exigência legal de representatividade partidária superior a nove[307] cadeiras na Câmara dos Deputados.

2. As emissoras de rádio e televisão podem convidar candidato a prefeito ou a vereador para participar de debates, mesmo que o partido pelo qual concorra não preencha a representatividade mínima exigida por lei de dez deputados federais.

3. A norma contida no caput do art. 46 da Lei n° 9.504/97 deve ser interpretada levando-se em consideração, no caso de eleição proporcional, a representatividade de todos os partidos que compõem uma determinada coligação e, no caso de eleição majoritária, a soma dos representantes dos seis maiores partidos que integrem a coligação, semelhante ao que ocorre no caso de distribuição do tempo de propaganda eleitoral gratuita, prevista no art. 47, §20, 1, da Lei n° 9.504/97.

[307] O número de cadeiras no Congresso Nacional alterou-se em sucessivas mudanças legislativas. A redação original do artigo estipulava número mínimo de um parlamentar, a fim de assegurar a presença do candidato nos debates em radiodifusoras. Em 2015, sobreveio alteração legislativa que aumentou este número para nove. Em 2017, reduziu-se novamente, passando-se a se exigir cinco parlamentares.

> 4. Consulta respondida afirmativamente quanto ao primeiro e ao segundo itens e julgada prejudicada no tocante ao terceiro.[308]

Tal critério foi considerado constitucional pelo Supremo Tribunal Federal que, no julgamento da ação direta de inconstitucionalidade n. 5.487, entendeu que

> 2.1. As emissoras de tv e rádio têm a faculdade de realizar debates eleitorais. Optando, no entanto, por promovê-los, têm de obedecer a diretrizes mínima fixadas em lei, com a finalidade de assegurar (i) o pluralismo político (democracia), (ii) a paridade de armas entre os candidatos na disputa eleitoral (isonomia), e (iii) o direito à informação dos eleitores (liberdade de expressão).
>
> 2.2. Em relação à definição dos participantes dos debates, é válida a fixação, por lei, de um critério objetivo que conceda a parcela dos candidatos (os "candidatos aptos") direito subjetivo à participação nos debates, não podendo a emissora de tv ou de rádio a ele se opor, ainda que com a concordância de outros candidatos. O critério adotado pela legislação brasileira, tal como interpretado pelo TSE, assegura a participação nos debates dos candidatos de partidos ou coligações que tenham representatividade mínima de 10 deputados fede-

[308] BRASIL. Tribunal Superior Eleitoral. Consulta n. 62-75.2016.6.00.0000. Consulente: Sarney Filho. Relatora: Ministra Luciana Lóssio. Brasília, 17/03/2016. Disponível em: http://inter03.tse.jus.br/sjur-consulta/pages/inteiro-teor--download/decisao.faces?idDecisao=52945&noChache=341700368. Acesso em 22/11/2021.

> rais. Trata-se de critério razoável, coerente com as normas relativas à propaganda eleitoral vigentes no país e que cumpre as finalidades constitucionais acima citadas.
>
> 2.3. Todavia, o legislador não fechou as portas do debate político a candidatos de partidos ou coligações que tenham menos de 10 deputados federais, tampouco tolheu por completo a liberdade de programação das emissoras de tv e rádio. Unindo essas duas preocupações, a Lei no 9.504/1997 facultou que as emissoras convidem para os debates candidatos com representatividade inferior à exigida na lei. No caso de competidores bem colocados nas pesquisas de intenção de voto, é razoável concluir que as emissoras terão estímulos para promover a sua inclusão, tanto como forma de aumentar a audiência, quanto de garantir a credibilidade do programa. Esta é a interpretação que já se extraía da legislação eleitoral antes da minirreforma de 2015 e que deve permanecer possível diante do atual cenário normativo, bastando que se confira interpretação conforme a Constituição à nova redação do art. 46, § 5o, da Lei no 9.504/1997 dada pela Lei n. 13.165/2015.[309]

Estas regras, que restringem a liberdade editorial das emissoras de radiodifusão, são aplicadas exclusivamente a estes veículos de comunicação, como art. 46, da Lei n. 9.504/97, dispõe. Ocorre que, com o avanço tecnológico e a migração da atenção da sociedade para a internet e as mídias sociais,

[309] BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade n. 5487/DF. Requerente: Partido Socialismo e Liberdade – PSOL e outros. Relator para acórdão: Ministro Roberto Barroso. Brasília, 25/08/2016. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=14222692. Acesso em 22/11/2021.

somados ao aumento do número de usuários com acesso à rede mundial de computadores[310], passou-se a questionar acerca da possibilidade de realização de debates ao vivo a serem transmitidos pela internet – seja em redes sociais, seja em veículos de comunicação digitais.

A discussão, que parece simples, não o é. Discutiu-se se a internet seria assemelhada aos veículos de comunicação impressos (tais como jornais, submetidos a regras eleitorais mais brandas, podendo um portal de notícias, inclusive, declarar apoio a uma determinada candidatura) ou às emissoras de radiodifusão.

Em 2010, o então deputado federal Miro Teixeira formulou consulta ao Tribunal Superior Eleitoral tendo por objeto, precisamente, a possibilidade de realização de debates a serem transmitidos pela internet com pré-candidatos ao pleito, na dicção do art. 36-A, I, da Lei n. 9.504/97. Questionou:

> a) se portais eletrônicos e jornais impressos podem realizar debates com pré-candidatos em qualquer época;
>
> b) se tais debates podem ser transmitidos ao vivo, pela internet;

[310] Pesquisa realizada pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), vinculado ao Comitê Gestor da Internet no Brasil, indicou que três em cada quatro brasileiros estão conectados à internet. Fonte: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. Acesso em 18/06/2021, às 20h10min.

> c) se podem ser convidados a participar somente os pré-candidatos considerados viáveis sob a óptica jornalística, a critério dos realizadores;
>
> d) se pré-candidatos que participem dos debates podem sofrer sanções;
>
> e) se pré-candidatos que compareçam aos debates e não peçam votos podem sofrer sanções.[311]

A resposta do Tribunal Superior Eleitoral foi no sentido de ser plenamente possível a realização de debates pela internet, seja entre pré-candidatos, seja entre candidatos, mas com um adendo: "para a internet não existe esta necessidade de tratamento isonômico", na medida em que este meio de comunicação não seria semelhante ao rádio e à televisão, mas, sim, aos veículos escritos de imprensa. Naquele mesmo ano, foi realizado o primeiro debate entre candidatos à Presidência da República, organizado pelo jornal Folha de São Paulo e pelo portal de notícias Universo Online (UOL)[312].

A não submissão dos veículos de comunicação exclusivamente digitais ao dever de conferir tratamento isonômico aos candidatos – imposto às emissoras de radiodifusão – é relevantíssima para se garantir a liberdade na definição dos

[311] BRASIL. Tribunal Superior Eleitoral. Consulta n. 796-36.2010.6.00.0000/DF. Consulente: Miro Teixeira. Relator: Ministro Marco Aurélio. Brasília, 16/06/2010. Disponível em: https://tse.jusbrasil.com.br/jurisprudencia/16794423/consulta-cta-79636-df/inteiro-teor-103580087. Acesso em 22/11/2021.

[312] CARVALHO, Douglas Belchior de; MOREIRA, Diogo Rais Rodrigues. Debate eleitoral na internet. Disponível em: http://eventoscopq.mackenzie.br/index.php/jornada/xvijornada/paper/view/1860/1325. Acesso em 18/06/2021, às 20h29min.

formatos e dos convidados a participar de um debate eleitoral a ser transmitido exclusivamente pela internet. Um portal de notícias pode, portanto, decidir convidar apenas aqueles candidatos que contarem com mais de 20% (vinte por cento) das intenções de votos em uma determinada pesquisa eleitoral sem cometer nenhuma infração à legislação eleitoral. Nesse sentido,

> A realização de debate por mídias, jornais e revistas virtuais não é objeto de específica regulamentação na Lei n. 9.504/97. Não há, pois, proibição do que seja realizado e exibido na web. No que for cabível, pode-se cogitar a aplicação por analogia do disposto no artigo 46 daquela norma, mormente seu §4º, segundo o qual 'o debate será realizado segundo as regras estabelecidas em acordo celebrado entre os partidos políticos e a pessoa jurídica interessada na realização do evento, dando-se ciência à Justiça Eleitoral'. Saliente-se, porém, não ser imperiosa a formulação de convite e a efetiva participação de todos os candidatos, nem mesmo a de todos os candidatos 'dos partidos com representação na Câmara de Deputados'.[313]

A ausência de regulamentação dos debates realizados pela internet adveio da revogação do art. 45, §3º, da Lei n. 9.504/97, pela Lei n. 12.034/2009, que previa que: "As disposições deste artigo aplicam-se aos sítios mantidos pelas empresas de comunicação social na internet e demais redes

[313] GOMES, José Jairo. Direito eleitoral. 12. ed. São Paulo: Atlas, 2016, p. 514.

destinadas à prestação de serviços de telecomunicações de valor adicionado.". A partir de sua revogação, assumiu-se que a internet seria um espaço livre de discussão pública, assemelhado aos veículos de comunicação impressos, como já dito anteriormente.

Na prática, infelizmente, a ausência de regulamentação tem imposto dificuldades aos veículos de comunicação. Cita-se, por exemplo, caso ocorrido nas eleições municipais de Curitiba/PR, no qual atuei pessoalmente como procuradora do representado, em que um debate organizado por um portal de notícias acabou por ser cancelado, em razão de reiteradas decisões judiciais que o inviabilizaram[314].

Neste caso, o jornal Gazeta do Povo propôs-se a realizar debate entre os oito candidatos à Prefeitura de Curitiba mais bem colocados em pesquisa de opinião anteriormente divulgada, adotando como critério de desempate o menor índice de rejeição. Explica-se: naquela eleição, disputada por dezesseis candidatos, seis deles encontravam-se empatados em oitavo lugar[315], com um por cento das intenções de votos, o que exigia a estipulação de um critério de desempate para que se definisse quem seria o oitavo participante do ciclo de debates.

[314] Disponível em: https://www.gazetadopovo.com.br/eleicoes/2020/curitiba-pr/justica-eleitoral-suspende-debates-gazeta-do-povo-a-pedido-do-pt/ e https://www.gazetadopovo.com.br/eleicoes/2020/curitiba-pr/liminares-suspendem-debates-da-gazeta-do-povo-com-candidatos-a-prefeitura-de-curitiba/. Acesso em 20/06/2021, às 20h42min.

[315] Disponível em: https://www.gazetadopovo.com.br/eleicoes/2020/pesquisa-eleitoral/ibope=-pesquisa-prefeito-curitiba-pr-outubro2020-/?ref-link-interno-materia. Acesso em 20/06/2021, às 20h54min.

Ao analisar representação eleitoral movida por um dos candidatos empatados em oitavo lugar, o juízo da 177ª Zona Eleitoral de Curitiba/PR entendeu que:

> (...) em se tratando de veiculação, por meio da mídia social (Youtube) a ser veiculada pelo portal da empresa representada, em que o conteúdo fica disponível, na hora que quiser e quanta (sic) vezes quiser, assim entendo que a regra de rádio e tv, para o caso em mesa deve ser aplicado (sic) também".[316]

Partindo desta premissa, o magistrado entendeu que "sendo 16 (dezesseis) candidatos que estão por ora aptos a concorrer ao cargo de Prefeito de Municipal e convidar somente os oito melhores colocados e como critério de desempate os de menor rejeição, está em dissonância com o regramento legal"[317], que determinaria, no entender do julgador, o dever de tratamento isonômico dos concorrentes ao pleito.

O Tribunal Regional Eleitoral do Paraná, analisando mandado de segurança impetrado pela Gazeta do Povo e concedendo a liminar para determinar a realização do ciclo de debates, reconheceu que

[316] BRASIL. Juízo da 177ª Zona Eleitoral de Curitiba/PR. Representação eleitoral n. 0600292-70.2020.6.16.0004. Requerente: Partido Comunista do Brasil – PcdoB. Requerida: Editora Gazeta do Povo S.A. Relator: Juiz. Rodrigo Domingos Peluso Junior. Curitiba, 04/11/2020.

[317] BRASIL. Juízo da 177ª Zona Eleitoral de Curitiba/PR. Representação eleitoral n. 0600292-70.2020.6.16.0004. Requerente: Partido Comunista do Brasil – PcdoB. Requerida: Editora Gazeta do Povo S.A. Relator: Juiz. Rodrigo Domingos Peluso Junior. Curitiba, 04/11/2020.

> (...) não se ignora que a cada dia a Internet com seus serviços de streaming, com suas mídias interativas, vídeos etc, cada vez mais vem substituindo o papel que o rádio e a televisão sempre tiveram, no entanto o legislador ainda não entendeu ser o tempo de se equiparar por completo esses meios de comunicação, pois se o quisesse poderia tê-lo feito alterando expressamente a legislação.[318]

Os debates acabaram por ser cancelados, pois, a cada decisão impeditiva que era cassada liminarmente por mandado de segurança, seguia-se uma nova. O direito à informação da sociedade, ao final de tal celeuma, saiu prejudicado, na medida em que os eleitores curitibanos deixaram de ter acesso a importante instrumento para um voto consciente.

Assim, tem-se que, apesar de a jurisprudência ter se consolidado no sentido de serem os portais de notícias e demais provedores de aplicação são assemelhados aos veículos de comunicação impressos e, portanto, não estão sujeitos às restrições e aos deveres impostos às emissoras de radiodifusão, a ausência de regulamentação aparentemente repercute de alguma maneira na compreensão do Judiciário sobre a matéria, o que impossibilita, na prática, o pleno acolhimento das potencialidades dos debates em meio online e dificulta o pleno exercício do direito à informação do eleitor, prejudicando, ao fim e ao cabo, toda a sociedade.

[318] BRASIL. Tribunal Regional Eleitoral. Mandado de segurança n. 0600636-63.2020.6.16.0000. Impetrante: Editora Gazeta do Povo S.A. Impetrado: Juízo da 177ª Zona Eleitoral de Curitiba/PR. Requerida: Editora Gazeta do Povo S.A. Relator: Desembargador Rogério de Assis. Curitiba, 04.11.2020.

CONSIDERAÇÕES FINAIS

A omissão da Lei n. 9.504/97 quanto à realização e transmissão de debates por veículos de comunicação digital foi uma escolha do legislador, que entendeu pela revogação do art. 45, §3º, em 2009. O intuito por detrás desta opção legislativa está em fazer da internet um espaço de amplo debate, no qual o eleitor possa buscar elementos que orientem seu voto consciente.

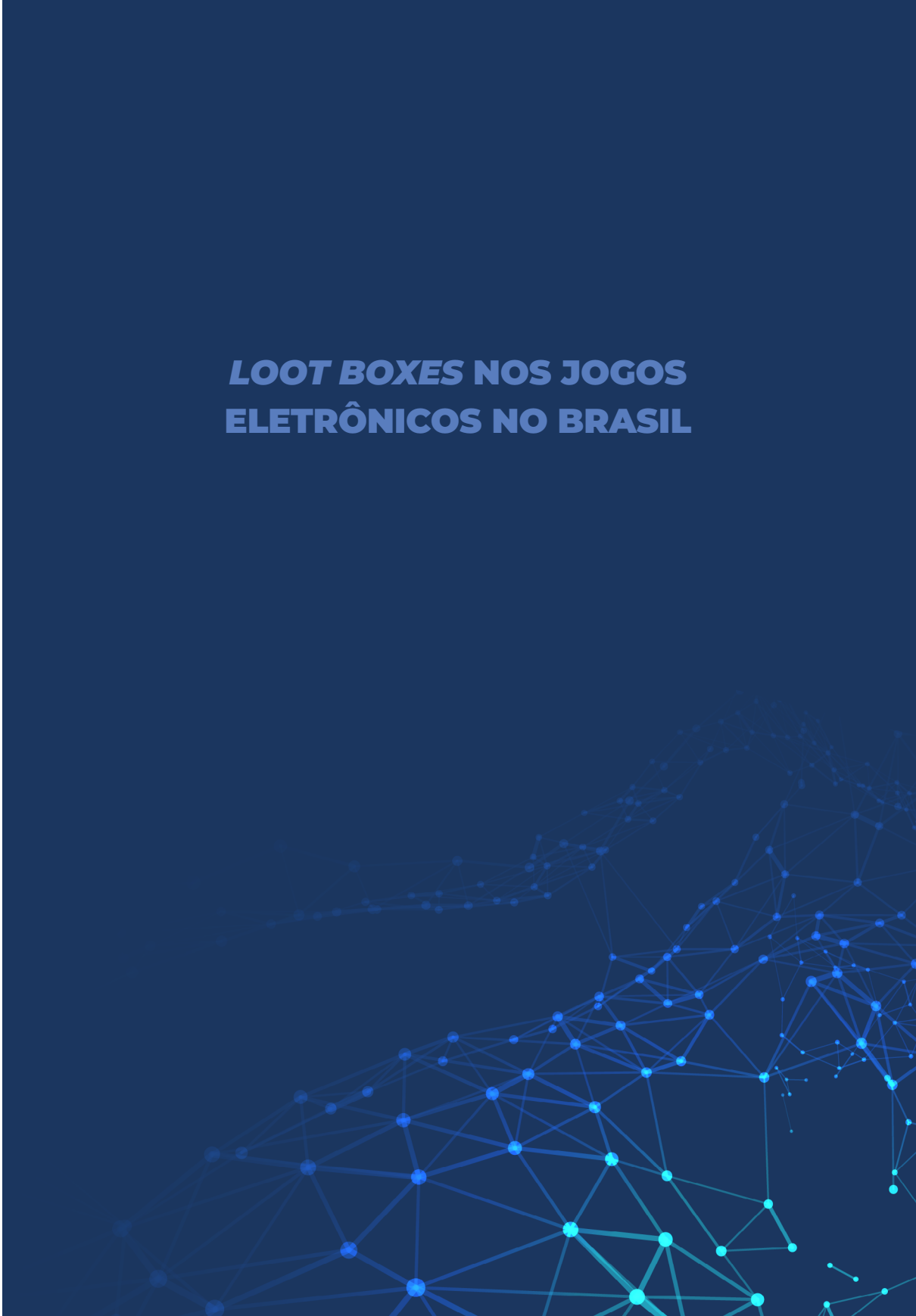
Esta acertada escolha iguala os veículos de comunicação virtuais com os impressos, na medida em que é necessária uma postura ativa do eleitor para buscar o conteúdo, em contraposição com as emissoras de radiodifusão que, por sua capilaridade, permitem ao telespectador ou ao ouvinte uma posição mais passiva[319]. Ou seja, para que se encontre um determinado assunto na internet, é necessária uma ação, um buscar, um acessar.

O Tribunal Superior Eleitoral fez esta diferenciação entre os veículos de comunicação de rádio e televisão e impressos e internet, destacando que a estes últimos não se aplicariam as restrições aplicáveis aos primeiros, sendo-lhes possível até mesmo manifestar apoio a determinada candidatura.

[319] "(...) a regulação mais robusta também se fundamenta na maior intrusão dessas mídias na vida das pessoas e na maior influência que exercem sobre a formação da opinião pública. A ideia é que a imprensa escrita tem menor alcance e exige uma atitude mais proativa do leitor, enquanto as mensagens difundidas pelo rádio e televisão teriam maior abrangência e seriam mais ostensivas, impondo-se a um elevado número de espectadores, sem exigir grande participação." (OSÓRIO, Aline. Direito eleitoral e liberdade de expressão. Belo Horizonte: 2017, p. 287/288).

Apesar desta premissa, fixada em 2010, a omissão legislativa implica em insegurança jurídica aos veículos de comunicação virtuais, que, como ocorreu no caso Gazeta do Povo, podem ver seus debates inviabilizados por compreensões equivocadas da legislação eleitoral. Uma mudança na Lei Geral de Eleições, com foco em garantir a liberdade editorial dos veículos de comunicação via internet poderia vir a solucionar esta questão, garantindo acesso dos eleitores a este importante mecanismo de debate entre os candidatos ao pleito.

LOOT BOXES NOS JOGOS ELETRÔNICOS NO BRASIL



Ana Paula Vasconcellos da Silva[320]

INTRODUÇÃO

O avanço da indústria dos videogames no Brasil e no mundo vem trazendo desafios não apenas para os pais e educadores, mas também para os operadores do Direito ao trazer inovações que desafiam os conceitos jurídicos tradicionalmente estabelecidos. Um desses desafios é a ideia dos *loot boxes*, que, em tradução livre, significa "caixas de recompensa". Embora seja uma funcionalidade comum no mundo dos jogos eletrônicos, esses itens trazem consigo importantes discussões acerca da aplicabilidade do direito do consumidor, da caracterização como possível jogo de azar embutido nos *games* e das questões relativas à proteção das crianças e adolescentes – particularmente vulneráveis a este tipo de prática.

Este artigo busca explorar o que existe de mais atual e relevante nos temas acima mencionados, sendo estruturado nos seguintes tópicos: *loot boxes*: o que são e como funcionam; a proteção ao direito das crianças e a ação da ANCED; se as *loot boxes* poderiam ser caracterizadas como uma modalidade de contravenção penal; o que diz o direito do consumidor aplicado a jogos eletrônicos; e as conclusões tiradas a partir dos pontos debatidos ao longo do texto.

[320] Possui Doutorado pelo Programa de Pós-Graduação em Políticas Públicas, Estratégias e Desenvolvimento do Instituto de Economia da UFRJ, Mestrado em Direito pelo Programa de Pós-graduação Stricto Sensu em Direito da UERJ e Bacharelado em Direito pela UFF e Letras Inglês/Literaturas de Língua Inglesa pela UERJ. Pós-graduação em Direito Digital em andamento, com previsão de conclusão em junho/2022.

1. O QUE SÃO LOOT BOXES E COMO ELAS FUNCIONAM NOS JOGOS ELETRÔNICOS

Os videogames vêm sofrendo uma evolução acelerada desde o início da sua criação. Se, nos anos 1970, assistiu-se à "Era de Ouro do Arcade", com os jogos sendo jogados fora de casa e sendo remunerados pela "moedinha" colocada nas máquinas de árcade, hoje o que se observa é que os jogos eletrônicos são quase todos jogados dentro de casa, centrados nos *gadgets* que permitem jogá-los a qualquer momento, local ou circunstância – e, com essas mudanças, novas formas de rentabilização foram desenvolvidas. Conforme aponta Sean Kane em sua recente apresentação sobre o tema para a FTC[321], o smartphone passou a ser uma plataforma de jogos e os *games* passaram a ser um centro de serviços (*Game as a Service*), nos quais estão embutidas funcionalidades gratuitas e pagas disponíveis de maneira muito fácil dentro do jogo – embora o modo de funcionamento dessas funcionalidades nem sempre seja muito claro para o jogador.

A indústria dos *games* se sofisticou e cresceu de modo exponencial. Segundo estimativa da empresa Superdata[322], o mercado de jogos eletrônicos em 2019 movimentou aproximadamente U$120 bilhões – mostrando um crescimento de 4% em relação a 2018. Contudo, a despeito de ser um

[321] KANE, Sean. *Loot Boxes. FTC. Inside the game: Unlocking the consumer issues surrounding loot boxes*. Estados Unidos da América, 2019. Disponível em: https://www.ftc.gov/system/files/documents/public_events/1511966/slides-lootbox-8-7-19.pdf . Acesso em 01/11/2021.

[322] SARMIENTO, Angelo. *Indústria de games movimentou mais de US$ 120 bilhões em 2019*. Disponível em: https://www.tecmundo.com.br/cultura-geek/148956-industria-games-movimentou-us-120-bilhoes-2019.htm. Acesso em 01/11/2021.

mercado milionário, com custos de produção cada vez mais elevados, o preço desses jogos para o consumidor individual continua baixo, sendo comuns que estejam disponíveis para *download* de forma gratuita. Isso significa, como aponta Sean Kane, que os produtores de jogos vêm sendo remunerados com modelo de negócios e formas de se agregar valor cada vez mais inovadoras e criativas – como é o caso das estratégias por trás das microtransações.

Microtransações são funcionalidades ativadas nos jogos através do pagamento em dinheiro (geralmente pequenas quantias) que implicam em itens ou vantagens especiais que melhoram a experiência do jogador. Em geral são utilizadas nos *games* disponíveis gratuitamente, que permitem que o jogador tenha acesso ao jogo e suas funções principais sem custos, mas que, para obter a experiência completa, o jogador precisa realizar o pagamento dessas funcionalidades. As *loot boxes* são, então, uma dessas estratégias de microtransações. Tratam-se de "caixas de recompensas" adquiridas nos jogos (por meio de recursos próprios dos *games* ou de dinheiro real), que contêm itens que são de interesse do jogador, mas que, a princípio, não é possível saber quais benefícios efetivamente trarão. Conforme aponta José Higídio[323], o jogador tem a garantia de que receberá algo, mas só conhece os detalhes após comprá-las e abri-las. Assim, a recompensa pode envolver desde os itens mais raros disponíveis no jogo até os mais banais possíveis.

[323] HIGÍDIO, José. *Advogados rejeitam proibição de loot boxes, mas defendem ajustes*. Disponível em: https://www.conjur.com.br/2021-abr-19/advogados-rejeitam-proibicao-loot-boxes-defendem-ajustes. Acessado em 01/11//2021.

As *loot boxes* tiveram sua origem nos "baús de tesouro" dos jogos de RPG e fantasia. É um tipo de estratégia existente em quase todos os gêneros de jogos eletrônicos e se popularizou com o avanço dos *games* disponíveis para dispositivos *mobile*. Embora sejam frequentes em jogos, alguns países já baniram essa prática, como a Bélgica e a Holanda, que aplicam multas e prisão para os jogos que possuírem estes dispositivos. As autoridades estão atentas em razão dos valores vultuosos envolvidos: segundo estimativa da *Juniper Research*, os jogadores de videogame em todo o mundo devem gastar cerca de US$ 20 bilhões com as *loot boxes* até 2025[324].

O mercado aquecido se justifica por ser uma prática bastante comum em jogos eletrônicos. Alguns exemplos de jogos que utilizam esta prática são: Saint Seya, League of Legends, Fifa, Dota 2, Free Fire, Counter Strike: Global Offensive, Pokemon Go, Genshin Impact, Fortnite, entre outros. São jogos que possuem centenas de milhares de jogadores e são populares em muitos países do mundo – especialmente no Brasil. A questão é que a mecânica de funcionamento das *loot boxes* em cada um desses jogos é diferente – e essas variações fazem toda a diferença na experiência do jogo.

Segundo o site especializado em jogos eletrônicos The Enemy[325], alguns modelos de *loot boxes* mais comuns no mercado são os seguintes:

---

[324] TUNHOLI, Murilo. *Ação judicial para banir loot boxes no Brasil tem apoio do Ministério Público*. Disponível em: https://www.terra.com.br/diversao/games/acao-judicial-para-banir-loot-boxes-no-brasil-tem-apoio-do-ministerio-publico,1dc027b17fa1113e8dd45297713f25efa0ikxll0.html. Acesso em 01/11/2021.

[325] SARMENTO, Angelo. *O que mudaria com as loot boxes banidas no Brasil?*

- Counter-Strike: Global Offensive, da empresa Valve: as armas possuem "skins" que aumentam seu poder de fogo. É possível comprá-las com dinheiro real. Recentemente foi lançado um dispositivo que torna possível ver o que tem dentro das caixas, descaracterizando, assim, como uma *loot box* propriamente dita. Porém, o jogador só pode usá-lo novamente depois de abrir a caixa em que o jogador usou o dispositivo pela primeira vez – independente de o item ser bom ou ruim;

- FIFA, da empresa EA: o jogador podia investir dinheiro real para ter acesso a jogadores com melhor performance. Contudo, após um vazamento de documentos internos demonstrando que o jogo induzia os jogadores em direção ao modo "Ultimate Team"[326], a estratégia da empresa foi remover completamente a opção de compra das moedas internas com dinheiro real nos EUA. Essa vedação acaba sendo facilmente burlada, principalmente dentro do cenário competitivo do FIFA, que possui um dos campeonatos de *E-sports* mais competitivos do mundo. Mais recentemente, foi adicionada nova funcionalidade que permite "espiar" o conteúdo das caixas antes de adquiri-las[327];

Disponível em: https://www.theenemy.com.br/mobile/loot-boxes-banidas-brasil-o-que-muda . Acesso em 01/11/2021.

[326] TREFILO, Daniel. *EA está induzindo jogadores ao consumo de loot boxes em FIFA, indicam documentos*. Disponível em: https://www.theenemy.com.br/playstation/fifa-21-compra-loot-boxes-documentos . Acesso em 01/11/2021.

[327] EMBOAVA, Valdecir. *EA permitirá que jogadores vejam itens de loot boxes em FIFA*. Disponível em: https://meups.com.br/noticias/electronic-arts-ver-itens-do-loot-box-fifa/ . Acesso em 01/11/2021.

- Genshin Impact, da empresa MiHoYo: neste jogo, a aquisição de novos personagens – que é uma parte essencial da experiência do jogo – é exclusivamente via *loot boxes,* o que exige um fator de sorte quase punitivo dadas as probabilidades para se conseguir os personagens mais raros, fazendo com que a aquisição de *loot boxes* seja fundamental para se obter progresso no jogo.

- Fortnite, da empresa Epic Games: o jogo já possui um sistema de monetização baseado em venda de itens separadamente em sua loja, além do Passe de Batalhas. Porém, até 2019 existiam, no modo "Save the World", as *loot boxes* na forma de lhamas coloridas que podiam ser adquiridas com dinheiro e que ofereciam itens e "skins", mas sem que o jogador soubesse qual recompensa viria. Em 2021 um acordo feito em uma ação judicial apresentada na Corte Superior da Carolina do Norte, nos Estados Unidos[328], estabeleceu que a empresa distribuiria aproximadamente U$8,00 para todos os jogadores que adquiriram *loot boxes*. A versão atual do jogo não possui mais essa funcionalidade.

- Pokemon Go, da empresa Niantic em conjunto com a Nintendo: os monstrinhos podem ser capturados no ambiente do jogo ou podem ser chocados em ovos obtidos gratuitamente após executar certas ações no jogo. Contudo, não é possível identificar a princípio

[328] KELLY, Makena. *Epic Games will settle Fortnite loot box lawsuits in V-Bucks*. Disponível em: https://www.theverge.com/2021/2/22/22295676/epic-games-fortnite-loot-box-lawsuit-settlement-rocket-league-v-bucks. Acesso em 01/11/2021.

> quais Pokemons virão no ovo antes de ele chocar, além de ser possível comprar itens com dinheiro real para acelerar o processo de "chocagem" dos ovos. Os Pokémons obtidos nos ovos podem ser encontrados no ambiente normal do jogo, não sendo fundamental para o progresso no jogo. Recentemente, a empresa mudou a dinâmica para permitir que os jogadores visualizem quais possíveis Pokémons podem advir dos ovos, mesmo antes de chocá-los.

Como se pode observar no panorama feito acima, são diversos os modelos de negócio possíveis envolvendo as microtransações do tipo *loot boxes*. Alguns são mais agressivos, obrigando o jogador a necessariamente investir dinheiro real em um item cuja recompensa não se sabe qual será, enquanto outros jogos possuem itens mais cosméticos ou mecanismos que permitam que o jogador visualize os itens possíveis e qual a probabilidade de se obtê-los antes de abrir as caixas. As empresas vêm buscando se adaptar às demandas feitas pelos jogadores, suavizando construções mais predatórias para mecanismos em que o jogador possui um pouco mais de controle. Ainda assim, mesmo as versões mais suaves de *loot boxes* podem trazer problemas na sua utilização, especialmente para jogadores menores de idade. É o tema que se discutirá com maior profundidade no tópico a seguir.

2. PROTEÇÃO DE CRIANÇAS E ADOLESCENTES E A AÇÃO JUDICIAL DA ANCED

As *loot boxes* trazem recompensas que são importantes para os jogadores dentro dos jogos, mas há outro aspecto que as tornam tão atraentes. Frequentemente são itens que geram cenas coloridas, com muito som e muito brilho quando

as caixas são abertas, gerando um efeito semelhante ao de um cassino (mais adiante será abordada a similaridade entre as *loot boxes* e os jogos de azar). É um dispositivo extremamente atraente e prazeroso para o jogador.

Essa atratividade especial das *loot boxes* gera preocupação principalmente em relação ao público infantil dos jogos, uma vez que o modelo de negócio que se assemelhe a um cassino acarreta o receio de estimular o vício em jogos de azar para jogadores jovens. Segundo a NBC News[329], esta prática tem chamado a atenção de psicólogos e grupos de defesa das crianças contra jogos de azar. A preocupação se justifica porque, segundo Relatório publicado pela Comissão de Jogos do Reino Unido[330], três em cada dez crianças tiveram acesso a *loot boxes* em algum tipo de jogo eletrônico. Além da facilidade em encontrar jogos com esse mecanismo, também há incentivos de outros jogadores (muitos deles menores de idade) para que as crianças adquiram e abram as *loot boxes* nos *games*. Existem muitos vídeos no YouTube de pessoas abrindo caixas de itens e discutindo seus conteúdos - incluindo jogadores muito jovens, com evidente expressão de felicidade quando encontram um item raro ao abrir uma caixa.

[329] SCHERER, Luisa. *Loot Boxes e o vício em jogos*. Disponível em: https://truthandtales.app/pt/loot-boxes-viciam-criancas-em-jogos/ . Acesso em 01/11/2021.

[330] PU, Benjamin. *What are loot boxes? FTC will investigate $30B video game industry*. Disponível em 05/07/2021. https://www.nbcnews.com/tech/tech-news/loot-boxes-gambling-video-games-ftc-look-it-n941256. Acesso em 01/11/2021.

Conforme aponta o advogado João Pedro Ferraz Teixeira[331], "as crianças não têm a clara percepção de que, ao adquirir uma *loot box*, estão, na verdade, entrando em uma espécie de *jogo de azar*, bem como não possuem a devida clareza ou entendimento sobre o valor despendido para tanto, tornando-se, assim, vulneráveis às práticas perpetradas nos jogos virtuais". Dessa forma, os menores de idade são mais suscetíveis a esta microtransação, uma vez que não conseguem compreender claramente as consequências financeiras de se abrir uma caixa colorida do jogo.

A legislação brasileira possui um dispositivo legal para proteger as crianças e adolescentes de jogos que envolvam apostas. Conforme dispõe o Estatuto da Criança e do Adolescente:

> Art. 80. **Os responsáveis por estabelecimentos que explorem comercialmente bilhar, sinuca ou congênere ou por casas de jogos, assim entendidas as que realizem apostas**, ainda que eventualmente, cuidarão para que não seja permitida a entrada e a permanência de crianças e adolescentes no local, afixando aviso para orientação do público. (grifou-se)

Importante destacar que a aplicação deste dispositivo aos jogos eletrônicos é complicada, uma vez que as crianças fazem *download* dos jogos para os seus próprios dispositivos

[331] HIGÍDIO, José. *Advogados rejeitam proibição de loot boxes, mas defendem ajustes*. Disponível em: https://www.conjur.com.br/2021-abr-19/advogados--rejeitam-proibicao-loot-boxes-defendem-ajustes . Acesso em 01/11/2021.

eletrônicos com o consentimento dos pais, não adentrando em algum estabelecimento em que jogos de azar estivessem acontecendo de qualquer forma. Assim, embora seja discutível a comparação das *loot boxes* com jogos de azar (que será melhor abordado na seção seguinte deste artigo), a aplicação do Estatuto da Criança e do Adolescente (ECA) para a proteção de menores do uso indiscriminado das *loot boxes* é adequada, em razão da proteção integral às crianças prevista nos artigos 1º e 3º do Estatuto. Defendendo este argumento, existe uma ação judicial questionando a existência desses mecanismos no território brasileiro justamente alegando violação ao ECA.

A Associação Nacional dos Centros de Defesa dos Direitos da Criança e do Adolescente (ANCED) entrou em março de 2021 com ações propostas em face das empresas Activision; EA Games; Garena Brasil; Nintendo Brasil; Riot Games; Ubisoft; Konami; Valve Corporation; e Tencent, além das empresas que hospedam os jogos em suas plataformas: Apple, Microsoft, Google e Sony. Segundo consta no site da entidade[332], ao todo são 7 ações protocoladas na Vara da Infância e da Juventude do Distrito Federal, com pedidos, no total, de 19 bilhões e meio de Reais em indenizações por danos morais coletivos e individuais.

O pedido feito em uma das ações já recebeu parecer positivo do Ministério Público do Distrito Federal. Em seu parecer,

[332] *ANCED entra na justiça pedindo proibição de sorteios ilegais em jogos eletrônicos*. Disponível em: https://www.ancedbrasil.org.br/anced-entra-na-justica-pedindo-proibicao-de-sorteios-ilegais-em-jogos-eletronicos/. Acesso em 01/11/2021.

a promotora de justiça Luisa de Marillac Xavier dos Passos declara que[333]:

> A presente ação, e as outras seis a ela associadas por determinação deste Juízo [...] **são uma oportunidade para que o sistema de Justiça se debruce sobre a questão, com a possibilidade de se inaugurar medidas que possam ampliar a proteção de crianças, adolescentes e famílias, principalmente considerando que as atividades de passatempo ou lazer voltados a crianças e adolescentes devem não somente ter, preferencialmente, caráter pedagógico e contribuir para o seu pleno desenvolvimento, mas preservar sua integridade física, psíquica e moral**. (...) Se de um lado há inúmeros estudos versando sobre os efeitos prejudiciais de jogos eletrônicos e virtuais para crianças e adolescentes, é bem verdade que, de outro, há usos pedagógicos excelentes dos mesmos recursos", diz o parecer do MP. (...) Nesse sentido, seria muito controvertido se dispor em uma decisão judicial sobre a adequação ou não de jogos virtuais para crianças e adolescentes, genericamente falando. **No entanto, o recorte da presente ação é o do uso de mecanismo considerado como "jogo de azar" e, portanto, reconhecidamente ilícito, cujo dano está implícito na própria ilicitude**. [334]

[333] FERREIRA, Victor. *Ministério Público aceita abrir processo para banir vendas de loot boxes*. https://www.theenemy.com.br/pc/ministerio-publico-processo-loot-boxes-brasil . Acesso em 01/11/2021.

[334] FERREIRA, Victor. *Ministério Público aceita abrir processo para banir vendas de loot boxes.* Disponível em: https://www.theenemy.com.br/pc/ministerio-publico-processo-loot-boxes-brasil. Acesso em 01/11/2021.

Assim, o Ministério Público reconhece o potencial danoso desse tipo de microtransação dentro do mundo dos videogames, especialmente quando crianças e adolescentes são os jogadores. Embora a interpretação do art. 80 do ECA para o enquadramento das *loot boxes* seja um pouco complicada, ainda assim é possível defender que os jovens menores de idade são vulneráveis e, portanto, merecem uma proteção especial do ordenamento jurídico, cabendo a eles a proteção integral mencionada nos artigos 1º e 3º do ECA. Especialmente caso se enquadre as *loot boxes* como um tipo de jogo de azar – que é o tema a ser debatido na próxima seção.

3. LOOT BOXES PODEM SER CARACTERIZADAS COMO CONTRAVENÇÃO PENAL?

Na ausência de uma legislação específica para jogos eletrônicos no Brasil, busca-se aplicar as normas vigentes. Um dos institutos jurídicos que pode ser avocado para aplicação no caso em tela é o enquadramento das *loot boxes* como jogos de azar, uma vez que existe um forte componente de sorte na obtenção do prêmio a ser recebido. Na grande maioria dos jogos, as chances de se obter um item de valor são baixíssimas, sendo que nem é possível saber qual probabilidade está construída no algoritmo. Contudo, como o jogador recebe algum tipo de recompensa, ele continua insistindo cada vez mais na compra desses itens, na expectativa de que "na próxima rodada ele terá mais sorte", semelhante ao que ocorre nos jogos de um cassino.

A Lei de Contravenções Penais assim dispõe:

> Art. 50. Estabelecer ou explorar jogo de azar em lugar público ou acessível ao público, mediante o pagamento de entrada ou sem ele: (...)
>
> § 3º Consideram-se, jogos de azar:
>
> **a) o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte**;
>
> b) as apostas sobre corrida de cavalos fora de hipódromo ou de local onde sejam autorizadas;
>
> c) as apostas sobre qualquer outra competição esportiva. (grifou-se)

A redação do art. 50 da Lei de Contravenções Penais coloca como centro da aplicação da norma a questão da preponderância da sorte na obtenção de ganho. Trata-se de uma redação bastante ampla, permitindo, assim, que sua interpretação abranja as *loot boxes*. Porém, é importante destacar que se trata de uma legislação antiga, que não reflete a realidade dos novos tempos nem consegue dar conta das especificidades do mundo virtual. Segundo o advogado João Vitor Gomes Corrêa[335], a caracterização como jogo de azar dependerá da forma como a empresa apresenta o mecanismo da *loot box* dentro do jogo: "por exemplo, no jogo Dota 2, da desenvolvedora Valve, no qual as *loot boxes* aparecem na tela com um visual de roleta de cassino, praticamente se assumindo como um jogo de azar."[336]

---

[335] HIGÍDIO, José. *Advogados rejeitam proibição de loot boxes, mas defendem ajustes*. https://www.conjur.com.br/2021-abr-19/advogados-rejeitam-proibicao-loot-boxes-defendem-ajustes. Acesso em 01/11//2021.

[336] HIGÍDIO, José. Advogados rejeitam proibição de loot boxes, mas de-

Ainda, as modalidades *pay-to-win* podem ser equiparadas a jogos de azar, segundo Côrrea, "visto que influenciam diretamente na performance do jogador no momento da partida, o que realmente pode estimular o interesse por aquisição de uma quantidade maior de *loot boxes* para obtenção de vantagens competitivas".

As empresas desenvolvedoras dos jogos argumentam que as *loot boxes* não seriam jogos de azar porque seus itens permanecem dentro dos jogos e não podem ser sacados. E, como se demonstrou anteriormente neste artigo, nem todas as caixas podem ser adquiridas com dinheiro real, podendo ser obtidas com recursos dos próprios jogos. Além disso, existem dispositivos em alguns jogos que demonstram quais são os itens que podem aparecer ao se abrir a caixa, disponibilizando informação acerca da probabilidade de se obter um item desejado, descaracterizando, assim, a dependência exclusiva ou principal do elemento sorte no jogo.

Compreende-se o argumento das empresas de que esses mecanismos de microtransação são fundamentais para financiar as desenvolvedoras, especialmente quando se tratam dos jogos com *download* gratuito. Contudo, os custos de financiamento dos jogos não têm o condão de afastar a caracterização da sorte no ganho ou perda, conforme consta da Lei de Infrações Penais. Assim, dependendo do modelo de negócio que orienta a utilização das *loot boxes* nos jogos, defende-se que este tipo de microtransação pode ser caracterizado como jogo de azar, correndo o risco de o jogo ser banido no Brasil se insistir na utilização desta prática.

---

fendem ajustes. https://www.conjur.com.br/2021-abr-19/advogados-rejeitam-proibicao-loot-boxes-defendem-ajustes. Acesso em 01/11/2021.

Além da discussão da caracterização das *loot boxes* como contravenção penal, é importante destacar que a relação do jogador com a empresa desenvolvedora do jogo é uma relação consumerista. Como se verá a seguir, o Código de Defesa do Consumidor possui um sistema de proteção que também abrange os jogadores nessa situação específica.

4. A LEGISLAÇÃO DE PROTEÇÃO AO CONSUMIDOR E A APLICABILIDADE NAS *LOOT BOXES*

Os jogos eletrônicos, entendidos como um centro de serviços (*Game as a Service*), podem ser compreendidos como o fornecimento de um serviço, uma vez que se trata da venda de uma experiência, que se desenvolve através da disponibilidade de novos conteúdos *online* e de forma permanente, para ser usufruída no longo prazo. O desenvolvedor dos jogos é um fornecedor e o jogador é um consumidor, e a eles se aplicam a legislação de proteção ao consumidor, a despeito de esta relação de consumo se desenvolver pela internet.

O acesso dos jogadores à internet, contudo, não necessariamente faz com que o jogador obtenha mais informações acerca do que se está adquirindo. Conforme aponta Anderson Schreiber[337], embora "a contratação via internet realize-se de modo cada vez mais veloz, sem a adequada pesquisa sobre

[337] SCHREIBER, Anderson. *Contratos eletrônicos e consumo*. RBDCivil, v. 1, n. 01, 2014, p. 99. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/132#:~:text=O%20artigo%20anal isa%20o%20tratamento,-tamb%C3%A9m%20na%20experi%C3%AAncia%20j ur%C3%ADdica%20estrangeirav. Acesso em 01/11/2021https://rbdcivil.ibdcivil.org.br/rbdc/article/view/132#:~:text=O%20artigo%20analisa%20o%20tratamento,-tamb%C3%A9m%20na%20experi%C3%AAncia%20jur%C3%ADdica%20estrangeira. Acesso em 01/11/2021.

as características do produto ou serviço contratado, sobre a qualidade do fornecedor ou sobre as próprias condições do contrato (...), o fato é que o consumidor eletrônico não sabe muitas vezes o quê está contratando." Assim, a legislação brasileira aplica-se, oferecendo a garantia dos direitos básicos do consumidor hipossuficiente, principalmente acerca da proteção contra a publicidade enganosa e abusiva, bem como contra práticas abusivas no fornecimento de serviços, conforme consta dos art. 6º, IV, do Código de Defesa do Consumidor, incidente no caso dos jogos eletrônicos e das *loot boxes*.

Contudo, não significa dizer que todas as práticas de *loot boxes* podem ser consideradas como práticas abusivas inseridas nos jogos eletrônicos. Conforme defende o advogado João Vitor Gomes Corrêa, deve-se garantir a proteção do consumidor-jogador ao se analisar, caso a caso, se as caixas são utilizadas de maneira abusiva: "A partir do momento que se garante transparência, para que o jogador compre uma *loot box*, mas consiga auditar seus números e entender como funciona, é possível eliminar essa característica de abuso"[338]. Portanto, o fornecimento de informações claras acerca das probabilidades de se obter cada item é fundamental para que se descaracterize as *loot boxes* como uma infração às regras de proteção ao direito do consumidor.

Além da informação clara acerca das probabilidades de cada item aparecer, outras características que podem ajudar na proteção ao consumidor, segundo o especialista Jeff Heynes[339],

[338] HIGIDIO, José. *Advogados rejeitam proibição de loot boxes, mas defendem ajustes*. Disponível em: https://www.conjur.com.br/2021-abr-19/advogados-rejeitam-proibicao-loot-boxes-defendem-ajustes. Acesso em 01/11/2021.

[339] HAYNES, Jeff. *Loot Boxes. FTC. Inside the game: Unlocking the consumer*

seriam: (i) a obtenção dos itens advindos das *loot boxes* não pode ser fundamental para se concluir todo o jogo; (ii) pagar pelos jogos em vez de usar jogos gratuitos, retirando, assim, a necessidade das microtransações para o financiamento dos jogos; (iii) utilizar os mecanismos de controle parental para impedir que as crianças e adolescentes possam investir dinheiro real no jogo; (iv) os pais devem conversar com as crianças e adolescentes sobre as compras no jogo e estabelecer regras claras do que os filhos podem ou não fazer no jogo. Existem, portanto, diversas estratégias que aumentam o controle da parte dos consumidores e tornam a experiência do jogo mais clara e transparente para o jogador, evitando, assim, as práticas abusivas.

Conforme se pode observar da análise feita, o modo como as *loot boxes* são utilizadas nos jogos é fundamental para se identificar se os direitos dos jogadores estão sendo respeitados, descaracterizando-as como práticas abusivas, em observância com o que dispõe o Código de Defesa do Consumidor.

CONCLUSÃO

As *loot boxes* são mecanismos de microtransações comuns nos jogos eletrônicos, especialmente naqueles que são adquiridos gratuitamente e jogados em dispositivos móveis, havendo diferentes modelos de negócios para a utilização nos diferentes *games*. Alguns jogos utilizam estratégias mais suaves, em que os itens adquiridos são meramente estéticos ou formatos em que é possível identificar os itens que podem vir a ser obtidos

issues surrounding loot boxes. Estados Unidos da América, 2019. Disponível em: https://www.ftc.gov/system/files/documents/public_events/1511966/slides-lootbox-8-7-19.pdf . Acesso em 01/11/2021.

ao se abrir as caixas. Em outros modelos, as *loot boxes* são fundamentais para que se possa completar a história ou oferece uma vantagem excessiva ao jogador, havendo alguns abusos na utilização desse mecanismo por parte dos desenvolvedores de alguns jogos.

A legislação de proteção das crianças e adolescentes, embora não tenha um dispositivo que se aplique especificamente à questão dos jogos eletrônicos, prevê a proteção integral dos menores de idade, razão pela qual deve haver uma preocupação especial com os jogadores nessa faixa etária, como por exemplo mecanismos de controle parental para impedir que os jogadores mais vulneráveis possam investir dinheiro real nos jogos.

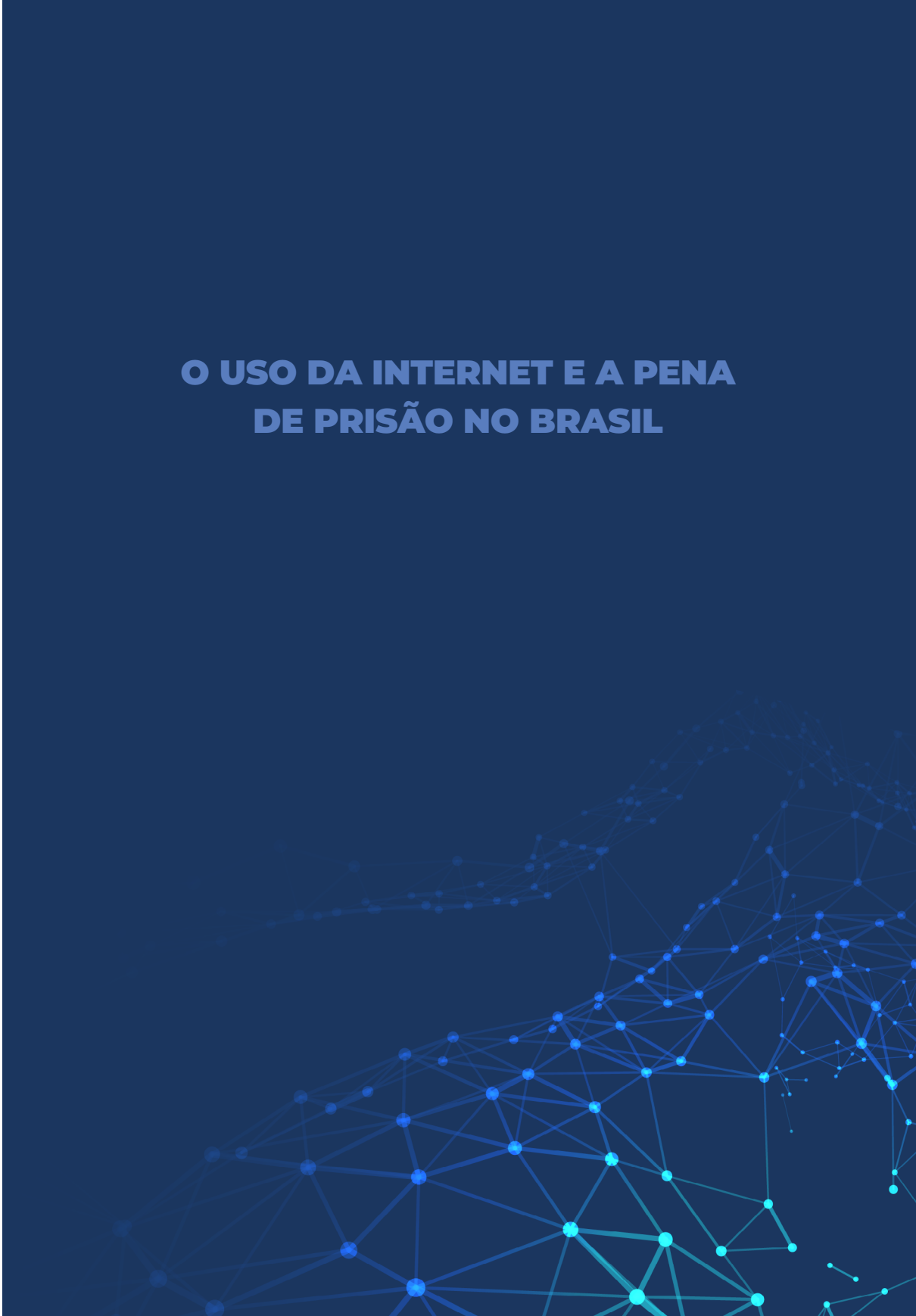
Já a legislação de contravenções penais, ao estabelecer que pode ser caracterizada como contravenção o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte – o que pode ocorrer dependendo do modelo de negócio que orienta a utilização das *loot boxes* –, permite a caracterização deste tipo de microtransação como jogo de azar.

Por fim, a legislação consumerista também garante proteção aos jogadores contra práticas abusivas, o que pode ocorrer dependendo do formato como é feita a utilização das *loot boxes* nos jogos. A informação clara aos jogadores é fundamental para descaracterizar uma violação ao Código de Defesa do Consumidor, especialmente quanto à probabilidade de cada item aparecer ao se abrir a caixa.

Embora a indústria dos videogames envolva valores cada vez maiores, representando as *loot boxes* uma parte significativa das transações financeiras realizadas, é fundamental que a indústria dos jogos eletrônicos aperfeiçoe seus modelos de

negócios e amplie a transparência e o controle sobre este tipo de microtransação. Afinal, o objetivo não é impedir os jogadores de acessarem todas as funcionalidades dos seus jogos favoritos, mas sim permitir que a diversão aconteça da forma mais transparente e com melhor controle possível, descaracterizando, assim, as *loot boxes* como violação aos direitos das crianças e adolescentes, ou como jogos de azar ou ainda como práticas abusivas.

O USO DA INTERNET E A PENA DE PRISÃO NO BRASIL



Marcelo Batista Gomes da Cruz[340]

INTRODUÇÃO

O artigo 2º da Lei 12.965/2.014 (Marco Civil da Internet - MCI) enuncia os fundamentos da "disciplina do uso da internet no Brasil", dentre os quais destaca-se "os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais" (inciso II) e "a finalidade social da rede" (inciso VI). Embora possa se apontar o caráter vago e abstrato dos termos adotados pela legislação, é inquestionável que o legislador brasileiro concretizou no ordenamento jurídico pátrio a importância da internet como instrumento de formação e desenvolvimento da personalidade humana e do convívio social. A própria exposição de motivos do MCI cita o amplo e crescente uso das redes informáticas no país como motivo para atenção em relação aos "desafios para que a Internet realize seu potencial social"[341].

Visto isso, na mais recente Pesquisa Nacional por Amostra de Domicílios (PNAD), o IBGE apurou que 78,3% dos brasileiros utilizavam a internet no ano de 2019, dentre os quais 98,6% o

[340] Bacharel em Direito pela Universidade de São Paulo (USP). Pós-graduando em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ), Instituto de Tecnologia e Sociedade (ITS Rio) e Centro de Estudos e Pesquisas no Ensino do Direito (CEPED). Assistente jurídico na 12ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo (TJSP).

[341] Exposição de motivos nº 00086 de 25 de abril de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/projetos/expmotiv/emi/2011/86-mj%20mp%20mct%20mc.htm Consultado em 03/07/2021.

faziam por meio de telefones celulares[342]. Ademais, a utilização por cidadãos entre os 20 e 40 anos é superior a 90%[343].

Por sua vez, aproximadamente 90% da população carcerária brasileira é composta por indivíduos entre os 18 e os 45 anos de idade, que totalizam mais de meio milhão de pessoas[344]. Para estas, contudo, o uso da internet é proibido por lei.

Nem a Constituição Federal, ao prever as modalidades de pena no Direito brasileiro (artigo 5º, XLVI), nem o Código Penal, ao tratar dos efeitos da condenação (artigos 91 e 92), preveem a perda do direito à comunicação por meios telemáticos ou do acesso à internet.

Ainda assim, a Lei de Execução Penal considera falta grave a posse, uso ou fornecimento de "aparelho telefônico, de rádio ou similar, que permita a comunicação com outros presos ou com o ambiente externo" (Art. 50, inciso VII), ao passo que o Código Penal criou espécie de prevaricação qualificada para o Diretor de Penitenciária e o agente público que deixar de cumprir o dever de "vedar ao preso o acesso a aparelho telefônico, de rádio ou similar, que permita a comunicação com outros presos ou com o ambiente externo" (Art. 319-A). No mais, a reprovação social generalizada ao uso de apare-

---

[342] IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento. *Pesquisa Nacional por Amostra de Domicílios Contínua 2018/2019*, 2021, p.01. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101794_informativo.pdf. Consultado em 03/07/2021.

[343] Ibidem, p. 09

[344] SISDEPEN. População Prisional por Faixa Etária, período de janeiro a junho de 2020. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiMjU3Y2RjNjctODQzMi00YTE4LWEwMDAtZDIzNWQ5YmIzMzk1IiwidCI6ImViMDkwNDIwLTQ0NGMtNDNmNy05MWYyLTRiOGRhNmJmZThlMSJ9. Consultado em 03/07/2021.

lhos eletrônicos com acesso à internet por parte de cidadãos encarcerados no Sistema Penitenciário Nacional é notória e frequentemente objeto de matérias jornalísticas cobertas de indignação.

Sendo assim, o panorama acima delineado expõe evidente contradição: o mesmo ordenamento jurídico que reconhece a importância social do uso da internet exclui o acesso à ferramenta em relação à população carcerária, contrariando, inclusive, tendência social natural de difundida utilização das redes por parte de cidadãos na mesma faixa etária.

Por certo, não é vedado que a Lei promova discriminações quando, para tanto, se utilizar de critério idôneo. Tampouco se ignora que uma série de comportamentos das pessoas encarceradas – como o gerenciamento de organizações criminosas e a aplicação de "golpes" por meio de celulares – sugere haver idoneidade para a diferenciação empregada.

Entretanto, é justamente esse paradigma que será contestado pelo presente artigo, tendo em vista que, conforme será demonstrado, o acesso à internet por parte de indivíduos reclusos em penitenciárias estatais, em determinadas condições, pode ser instrumento fundamental para aprimorar os pretensos objetivos da pena privativa de liberdade.

1. O SISTEMA PRISIONAL E A ILUSÃO DA RESSOCIALIZAÇÃO

A temática das finalidades da pena é, provavelmente, uma das mais antigas e exaustivamente debatidas no campo do direito penal e da criminologia. Não à toa, Alexis Couto de

Brito proclama que: "O problema da finalidade da pena nasceu com o Direito Penal"[345].

O tema deu origem a inúmeras correntes doutrinárias, cujo conteúdo não concerne ao escopo deste artigo, ao qual importa apenas a finalidade adotada de forma preponderante pelo ordenamento jurídico brasileiro em relação à execução penal.

Em seu artigo 1º, a Lei nº 7.210/1984 (Lei de Execução Penal - LEP) enuncia: "A execução penal tem por objetivo efetivar as disposições de sentença ou decisão criminal e proporcionar condições para a harmônica integração social do condenado e do internado".

Sendo assim, parece correto o entendimento de que o legislador pátrio resumiu as demais finalidades da pena em um mandamento geral de efetivação da sentença penal condenatória, oferecendo maior destaque a um fim específico da reprimenda, qual seja: a prevenção especial positiva. Trata-se da designação de corrente teórica que concebe a pena enquanto instrumento de correção do apenado, o qual busca promover as ideologias "re" (ressocialização, repersonalização, reeducação, reinserção social etc.)[346].

Tais ideologias, por sua vez, decorrem de formulações teóricas calcadas em dois pressupostos comuns: o primeiro é que o autor do fato criminoso é um ser passível de correção; o

[345] BRITO, Alexis Couto de. ***Execução Penal***, 6ª ed., São Paulo: Saraiva Educação, 2020, p.46

[346] ZAFFARONI, E. Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. ***Direito Penal Brasileiro: primeiro volume – Teoria Geral do Delito***, 4ª ed., Rio de Janeiro: 2011, p. 116

segundo é que a execução da pena, sobretudo a pena privativa de liberdade, constitui meio idôneo para corrigi-lo.

Quanto à primeira premissa, não compete a este estudo debruçar-se sobre a fragilidade de seus pressupostos teóricos face às evidências empíricas, tema amplamente explorado pelas escolas criminológicas contemporâneas. Mais relevante para a argumentação que se busca construir é a análise do segundo pressuposto.

O paradigma da pena privativa de liberdade como forma de correção se corrobora pelas concepções da criminologia clínica, a qual, grosso modo, visa "avaliar os desdobramentos possíveis dos comportamentos problemáticos" de indivíduos submetidos à execução penal e "formular estratégias que contribuam para que elas tenham um sucesso saudável, quando de seu retorno ao convívio social livre, inclusive através da conquista de um melhor equilíbrio interno e em sua relação com seu contexto social"[347]. Porém, o que tal corrente criminológica ignora, em suas formulações clássicas, são os vícios estruturais do cárcere que, por sua própria configuração, pode provocar perniciosos efeitos sobre a psique do encarcerado.

Nesse sentido, Erving Goffman esclarece que a prisão é uma "instituição total", conceito que se refere a um estabelecimento caracterizado pela "barreira à relação social com o mundo externo e por proibições à saída que muitas vezes estão incluídas no esquema físico – por exemplo, portas fechadas, paredes altas, arame farpado"[348]. São locais que preenchem a

[347] AUGUSTO DE SÁ, Alvino. *Criminologia clínica e execução penal: proposta de um modelo de terceira geração*, 2ª ed., São Paulo: Saraiva, 2015, p. 71.

[348] GOFFMAN, Erving. *Manicômios, prisões e conventos*, São Paulo: Edit. Perspectiva, 1974, p. 16

totalidade do tempo dos indivíduos, os quais realizam ali todas as suas atividades cotidianas, em conjunto de outras pessoas submetidas às mesmas condições e segundo um conjunto de normas que visa atender o objetivo da instituição[349].

Tal objetivo, para Foucault, seria criar pessoas "dóceis e úteis" à sociedade[350], por meio do isolamento, de tratamentos específicos às suas individualidades e de vigilância e disciplina constantes. Assim, o apenado se transformaria em peça apta ao trabalho, disciplinado de acordo com normas sociais incontestáveis.

No entanto, até mesmo essa pretensão raramente é atingida. Como explica Shecaira, dentro da prisão o ser humano "sofre progressivamente uma série de rebaixamentos, humilhações, degradações pessoais e profanações do eu"[351]. Nessa linha, Goffman defende que as instituições prisionais possuem efeitos criminógenos, em razão de um processo de aniquilação da identidade individual do preso ("mortificação do eu").

O processo em questão ocasiona o abandono aos comportamentos próprios do indivíduo, na medida em que passa a aderir às normas da instituição[352]. Uma vez no cárcere, o apenado "é estimulado pela necessidade de se manter vivo e, se possível, ser aceito no grupo. Portanto, longe de estar

[349] Ibidem, pp. 17-18.

[350] FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*, Petrópolis: Vozes, 1987, p. 260.

[351] SHECAIRA, Sérgio Salomão. *Criminologia*, 7ª ed., São Paulo: Thomson Reuters Brasil, 2018, p. 265

[352] GOFFMAN, Erving. *Op, cit.*, p. 24.

sendo ressocializado para a vida livre, está, na verdade, sendo socializado para viver na prisão"[353].

Em outras palavras, o cárcere não origina pessoas reconfiguradas para o convívio em sociedade, mas, na verdade, indivíduos institucionalizados, portadores de identidade nova, formada a partir da internalização de regras cotidianas da instituição e do convívio constante com os outros detentos. Nesse sentido, a troca do mundo social externo à instituição total pelo mundo particular dentro dela criado inclui o abandono completo de atividades sociais cotidianas ou sua reconfiguração aos moldes do sistema prisional.

Atualmente, seria impossível não incluir entre tais atividades, a interação social por meio da internet e o acesso a informações e conteúdo em plataformas digitais. Ocorre que essa nova forma de interação ultrapassa as fronteiras físicas do isolamento ao permitir a comunicação à distância e em tempo real. As portas fechadas, paredes altas e arame farpado citados por Goffman não são suficientes para impedir a transmissão de ondas de rádio de dispositivos eletrônicos.

Assim, inicia-se no âmbito da administração carcerária uma custosa guerra antitecnológica, travada com bloqueadores de sinal[354], detectores de metal e até mesmo armas para intercep-

[353] PIMENTEL, Manoel Pedro. *O crime e a pena na atualidade*, p. 158, apud, SHECAIRA, Sérgio Salomão. *Op. cit.*, p. 267

[354] Sobre referida tecnologia, vale dizer que seu uso afeta não apenas o uso de celulares em unidades prisionais, mas também em seu entorno, podendo dificultar a comunicação telemática de cidadãos não encarcerados, impedindo o acesso, por exemplo, a serviços de emergência. Neste sentido: GSMA. *Segurança e privacidade no ecossistema móvel. Principais temas e implicações para políticas públicas*. 2017, p. 44. Disponível em: https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safe-

tação de drones[355]. Diante das novas ameaças ao isolamento social, o sistema prisional age desesperadamente para manter o *status quo* estrutural que o compõe, avesso às mudanças e fiel às bases que o originaram.

Contudo, o "custo bélico" mencionado não é apenas financeiro, mas também social, na medida em que o processo de degradação mental e de perda da sociabilidade já existente no cárcere torna-se ainda mais relevante quando se lhe acresce a perda do acesso às redes. De outro modo: em um mundo conectado, a desconexão da vida em sociedade provocada por um "encarceramento *offline*" é ainda maior.

2. DOS USOS DA INTERNET NA EXECUÇÃO DA PENA DE PRISÃO: MEDIDAS EXISTENTES

Diante das robustas evidências quanto aos efeitos despersonalizantes do cárcere, alguns teóricos do tema passam a assumir as falhas estruturais do sistema prisional como pressuposto e se inclinam a uma vertente político-criminal de "desinstitucionalização"[356]. Nessa linha, valorizam-se estratégias que busquem atenuar ou dirimir o citado processo de "mortificação do eu", como a reinserção gradual do preso à sociedade (por meio da progressão de regime ou do livramento

ty-privacy-and-security-across-the-mobile-ecosystem_PORTUGUESE-BR.pdf. Acesso em: 19/11/2021

[355] Assessoria de Imprensa da Secretaria da Administração Penitenciária do Estado de São Paulo. ***Presídios de SP terão tecnologia antidrone contra envio de drogas e celulares.*** Disponível em: http://www.sap.sp.gov.br/noticias/not2066.html. Acesso em: 19/11/2021.

[356] SHECAIRA, Sérgio Salomão. ***Op. cit.***, p. 271

condicional), a adoção de penas não privativas de liberdade ou de regimes prisionais menos rigorosos, dentre outras[357].

Dentro desse panorama, ganha força o modelo de criminologia clínica de inclusão social (ou "de terceira geração"), o qual busca a adoção de medidas capazes de reconstruir o vínculo entre a parte encarcerada da comunidade e a parcela liberta[358], a fim de que a primeira volte a se enxergar como parte integrante da última. Simultaneamente, pretende-se reformular a consciência da sociedade e de suas instâncias de controle em relação aos indivíduos reclusos[359].

No direito brasileiro, a preservação dos vínculos entre detento e sociedade não é desprezada pelo legislador – que previu o direito à visita e à correspondência[360], por exemplo – e tampouco pela jurisprudência, que, em relação ao exame criminológico para concessão de benefícios prisionais, valoriza a menção aos vínculos familiares preservados como elemento de constituição do requisito subjetivo[361].

No entanto, as tecnologias da comunicação desbravaram um novo horizonte de possibilidades para reforçar as relações do detento com o mundo exterior sem prejudicar a estrutura carcerária de disciplina e controle. Além disso, criaram ferramentas que possibilitam a expansão de atividades educativas,

[357] Ibidem, pp. 275-281

[358] AUGUSTO DE SÁ, Alvino. *Op. cit,* pp. 349-351

[359] Ibidem, pp. 358-359

[360] Artigo 41 da Lei de Execução Penal

[361] Nessa linha: TJSP; Agravo de Execução Penal 0002883-79.2019.8.26.0154; Relator (a): Amable Lopez Soto; Órgão Julgador: 12ª Câmara de Direito Criminal; Data do Julgamento: 30/01/2020.

culturais, de saúde e jurisprudenciais que podem ser implementadas no sistema prisional.

No Brasil, contudo, esse uso específico da tecnologia beira a incipiência e recebe pouca ou nenhuma atenção das autoridades estatais e do debate público.

Como já visto, a legislação proíbe a posse, uso e fornecimento de aparelhos telefônicos, de rádio e similares, destinados à comunicação com outros presos ou com o ambiente externo. O uso da comunicação virtual apenas ganhou algum espaço com a instituição, em 2010, das visitas virtuais em penitenciária federais[362]. A medida só foi adotada por outras unidades federativas em razão do advento da pandemia de 2020/2021, quando algumas secretarias estaduais passaram a admitir visitas por meio de videoconferência, além do recebimento de cartas virtuais, enviadas por e-mail[363,364]. Ainda assim, a comunicação não é diária e se sujeita a data e período de duração pré-determinados, fatores que limitam em demasia o potencial da medida.

[362] A medida se encontra normatizada pela Portaria Conjunta DPU/DEPEN nº 500 de 30/09/2010.

[363] Um resumo dessas medidas pode ser encontrado no material "*Medidas concessivas adotadas pelas unidades federativas a familiares/visitantes e presos durante o período de suspensão de visitas, no sistema prisional, para prevenção do coronavírus (covid-19)*", publicado pelo DEPEN em 2020. Disponível em: http://antigo.depen.gov.br/DEPEN/TABELAUNIDADESFEDERATIVASMEDIDASCONCESSIVASAFAMILIARESVISITANTESEPRESOS17.04.2022H1.pdf. Acesso em: 19/11/2021.

[364] No mesmo sentido é o projeto Conexão Familiar, criado pela Secretaria da Administração Penitenciária do Estado de São Paulo.

Também se difundiu, em razão do contexto pandêmico, o exercício da telemedicina no sistema penitenciário[365], a consulta virtual de advogados a seus clientes encarcerados[366], bem como a realização de audiências judiciais por sistema de videoconferência, possibilitando que a pessoa presa seja ouvida pelo juízo dentro da própria unidade prisional[367].

Esse é, no entanto, o atual limite do progresso. Não há, no Brasil, qualquer atividade estatal adicional (ou sequer projetos de políticas públicas em andamento) que busquem o alargamento do acesso à internet por parte da população carcerária.

Isso não significa que há um atraso gritante da legislação pátria em relação ao restante do mundo, tendo em vista que poucos Estados estrangeiros revelam iniciativas mais elaboradas nesse âmbito. Ainda assim, a menção a alguns desses países se mostra pertinente para delinear as possibilidades de alargamento das medidas já adotadas.

Nos Estados Unidos, por exemplo, a empresa JPay, por meio de contratos com o poder público, oferece serviços diversos aos internos de determinadas penitenciárias e seus familiares. A empresa vende *tablets* aos encarcerados que, por meio de um servidor interno e monitorado pela unidade prisional, pos-

---

[365] DEPEN. *Depen disponibiliza atendimento por telemedicina no Sistema Penitenciário Federal.* Disponível em: https://www.gov.br/depen/pt-br/assuntos/noticias/depen-disponibiliza-atendimento-por-telemedicina-no-sistema-penitenciario-federal. Acesso em: 19/11/2021.

[366] Como exemplo, tem-se as medidas de assistência jurídica remota implementadas no Estado de São Paulo. Disponíveis em: http://www.sap.sp.gov.br/noticias/not1689.html. Acesso em: 19/11/2021.

[367] Resolução CNJ nº 329 de 30/07/2020. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/08/Resolucao329_2020-30072020.pdf. Acesso em: 19/11/2021.

sibilitam o envio de e-mails, realização de ligações telefônicas rastreadas e videochamadas pré-agendadas, além da aquisição de músicas, jogos eletrônicos, livros e cursos educacionais[368].

Os produtos e serviços são inteiramente custeados pelos internos ou seus familiares, modelo distante do ideal, tendo em vista que a população carcerária é composta, majoritariamente, por pessoas de reduzido poder aquisitivo. Ainda assim, a iniciativa merece destaque por possibilitar maior interação dos detentos com pessoas fora dos muros do cárcere, bem como por permitir-lhes escolher atividades de lazer, cultura e educação que maior se adequem às suas preferências e necessidades pessoais.

Na Bélgica, por sua vez, um número reduzido de penitenciárias possui celas individuais com computadores e acesso ao sistema "PrisonCloud", que permite a realização de ligações telefônicas, cursos educacionais, gestão de atividades cotidianas e contato a serviços internos da unidade[369],[370]. Além disso, o uso diário de telefones instalados no corredor das celas é permitido aos internos, às suas custas e com monitoramento, unicamente, da identidade do interlocutor e tempo da chamada[371]. Em 2019, seguindo o planejamento divulgado

[368] Disponível em: https://www.jpay.com/FriendsFamily.aspx. Acesso em: 19/11/2021.

[369] Service Public Fédéral – *Justice. Inauguration de la nouvelle prison de Beveren. Disponível em:* https://justice.belgium.be/fr/nouvelles/communiques_de_presse/inauguration_de_la_nouvelle_prison_de_beveren. Acesso em: 19/11/2021.

[370] Maiores detalhes técnicos sobre o PrisonCloud em: https://www.computerweekly.com/news/1522598/A-prisons-virtual-desktops-keep-inmates-plugged-in. Acesso em: 19/11/2021.

[371] Informações disponíveis em: https://justice.belgium.be/fr/themes_et_dos-

no Relatório Anual da Direção Geral de Estabelecimentos Prisionais de 2016[372], algumas penitenciárias passaram a contar com telefones dentro das celas, ampliando o espectro de liberdade conferido aos internos[373].

Diferentemente do que se observa nos Estados Unidos, as iniciativas belgas se baseiam em infraestrutura custeada por recursos públicos, com serviços específicos pagos pelo detento. Portanto, em que pese as dificuldades orçamentárias que o modelo possa acarretar, é de se ressaltar sua maior acessibilidade aos destinatários do projeto.

Visto isto, outros exemplos poderiam ser citados no plano internacional, mas não seriam numerosos e tampouco mais relevantes do que os acima expostos. Isso demonstra que, mesmo em países desenvolvidos, a implementação de políticas carcerárias voltadas ao uso da internet ainda é reduzida.

A informação, contudo, não surpreende. A pena de prisão é estruturada sobre os princípios de vigilância e disciplina constantes, bem como preserva, na maioria dos países, a ideia de que estabelecimentos prisionais precisam ser constituídos enquanto ambientes desagradáveis que mais se assemelham às masmorras medievais.

---

siers/prisons/vivre_en_prison/contacts_avec_le_monde_exterieur/telephone. Acesso em: 19/11/2021.

[372] Service Public Fédéral – Rapport annuel 2016, Direction Générale des Etablissements Pénitentiaires. Disponível em: https://justice.belgium.be/sites/default/files/bat_ra_2016_fr_light.pdf. Acesso em: 19/11/2021.

[373] The Bulletin. *Belgian prisons to start adding phones inside cells*. Disponível em: https://www.thebulletin.be/belgian-prisons-start-adding-phones-inside-cells. Acesso em: 19/11/2021.

Os ideais de reinserção social podem ter sido positivados no ordenamento jurídico, mas é de fácil constatação que a majoritária opinião popular e, consequentemente, dos gestores públicos ainda não consegue desassociar a pena de suas finalidades puramente retributivas[374]. No Brasil, a existência de celas insalubres e superlotadas provavelmente gera menos indignação popular do que haveria caso fossem propostas políticas públicas como as acima enunciadas.

Ainda assim, conforme será demonstrado, o cenário de escassos exemplos práticos não impede a formulação de propostas teóricas ainda inéditas, desde que minimamente concretizáveis.

3. NOVAS POSSIBILIDADES PARA O USO DA INTERNET APLICADO À PENA DE PRISÃO

O primeiro e mais importante uso da internet dentro dos estabelecimentos prisionais seria a interação frequente com familiares e amigos do apenado. Em artigo de opinião publicado pelo jornal The Guardian, o detento Jarvis Jay Masters, preso há quase quarenta anos no sistema prisional norte-americano, expôs suas considerações sobre o uso de telefones celulares no ambiente carcerário[375]. A partir de sua longa vivência na instituição total, Masters observou que a simples ocupação do tempo ocioso por meio do uso de ce-

[374] Em relação à temática dos fins das penas, as teorias absolutas ou retributivas formulam a sanção enquanto um "mal justo", que retribui o "mal injusto" do crime.

[375] The Guardian. *Letting prisoners use cellphones makes sense – now more than ever*. Disponível em: https://www.theguardian.com/commentisfree/2020/may/22/coronavirus-prisons-covid-pandemic-cellphones. Acesso em: 19/11/2021

lulares reduz as condutas violentas praticadas contra outros detentos ou contra o corpo funcional da prisão.

O autor também cita a importância de manter-se atualizado sobre os acontecimentos da vida de seus familiares, reduzindo, por exemplo, a ansiedade causada pela falta de notícias de parentes adoecidos ou a frustração pela perda do nascimento de um filho. Ademais, o contato mais frequente entre filhos e pais encarcerados poderia atenuar os impactos negativos da ausência de figuras parentais no cotidiano de crianças e adolescentes.

São inúmeras as ferramentas que possibilitam a interação diária e até mesmo imediata entre indivíduos dentro e fora das unidades prisionais. A administração penitenciária poderia escolher entre aplicações de trocas de mensagens, SMS e até mesmo e-mails, de acordo com a maior ou menor facilidade para monitoramento de conteúdo caso este se mostre imprescindível.

Por certo seria necessário o dispêndio de recursos públicos para implementação de sistemas de monitoramento ou para fornecimento de *hardwares* habilitados para o uso dos detentos. No entanto, não se mostra impossível a adoção de medidas semelhantes às implementadas no sistema prisional norte-americano, por meio do fornecimento oneroso de determinados aparelhos celulares ou *tablets* para consumo da população carcerária. Todavia, a depender da eficiência do controle e monitoramento – tanto realizados presencialmente pelos agentes penitenciários quanto virtualmente por sistemas públicos próprios – seria possível permitir o uso de telefones celulares particulares, minimizando os custos do erário e do próprio recluso.

Do mesmo modo, possibilitar-se-ia utilizar os meios de comunicação telemática para flexibilizar as consultas jurídicas feitas a advogados e defensores públicos, bem como permitir acesso direto a dados processuais de interesse do condenado.

Sob outro ponto de vista, a implementação do acesso à internet permitiria a ampliação das atividades educacionais. Nesse âmbito, a Lei de Execução Penal já admite a remição de pena por meio de estudos realizados por ensino à distância (art. 126, §2º), mas não a transmissão do conteúdo por meio eletrônico, seja de forma gravada ou telepresencial.

Em pesquisa voltada a medidas de combate à reincidência criminal por meio de atividades de ensino, verificou-se que os principais obstáculos à implementação de programas educacionais no sistema prisional norte-americano eram de matriz logística e financeira, como a dificuldade de encontrar espaço e profissionais adequados[376]. O mesmo estudo observou que tais entraves seriam facilmente solucionados por meio da adoção de plataformas que disponibilizassem conteúdo *online* para o acesso dos detentos[377].

Com efeito, a adoção de programas de ensino *online* revela flexibilidade incomparável às formas educativas tradicionais, tanto para os emissores quanto para os receptores do conhecimento. Elimina-se a necessidade de deslocamento de educadores ao interior da unidade prisional, bem como a exigência de ambiente específico e de compatibilização da disponibilidade horária de reclusos, professores e agentes

[376] GORGOL, Laura E., SPONSLER, Brian A. *Unlocking Potential: Results of a National Survey of Postsecondary Education in State Prisons*. Institute for Higher Education Policy: 2011, pp. 16-17

[377] Ibidem.

penitenciários. Uma mesma aula gravada em sistema audiovisual, por exemplo, pode ser acessada em penitenciárias de todo o país, seja por meio de acesso remoto em dispositivos de uso individual ou de transmissão coletiva em televisores.

Por fim, imaginando-se a existência de um sistema penitenciário no qual indivíduos submetidos à pena privativa de liberdade tivessem acesso a *smartphones* de uso individual com acesso a determinadas mídias sociais, inevitavelmente registros do cárcere seriam compartilhados via internet[378]. Os sons e imagens da prisão seriam acessados pela população em geral e as condições precárias do sistema penitenciário brasileiro não seriam apenas conhecidas, mas sim presenciadas. O tema poderia ganhar um espaço maior e mais sensível no debate público e, consequentemente, alavancar importantes reformas legislativas[379].

4. RESSALVAS NECESSÁRIAS

É evidente que as propostas supracitadas podem ser encaradas como fruto de idealismo e ingenuidade. O sistema prisional brasileiro apresenta deficiências de caráter muito

[378] A título de exemplo, no ano de 2021, um detento do Presídio Dalton Crespo, no Rio de Janeiro, criou perfil no TikTok para compartilhar vídeos sobre seu cotidiano no cárcere. Em 19 de novembro de 2021, o perfil "@ wlfdllinha" possuía mais de 15 mil seguidores e mais de 86 mil curtidas na referida plataforma.

[379] Trata-se de posição defendida por Walter Pavlo em artigo de opinião publicado na revista Forbes, na qual o autor cita episódios em que a divulgação de determinados vídeos difundiu importantes discussões na sociedade norte-americana, o que poderia se refletir em relação ao sistema penitenciário. Disponível em: https://www.forbes.com/sites/walterpavlo/2020/04/19/will=-cell-phones-be-the-downfall-of-prisons/?sh-14bb40531be4. Acesso em: 19/11/2021.

mais básico[380] e que, seja pela falta de recursos públicos ou pelo descaso estatal, ainda parecem distantes de solução definitiva.

Ainda assim, não há prejuízo para que se levantem discussões teóricas acerca do tema, tendo em vista que sua eclosão à arena pública, diante do constante avanço das tecnologias da informação e a expansiva permeação da internet pela vida social, é mera questão de tempo.

Por outro lado, também podem ser formuladas prontas objeções à adoção das iniciativas propostas em razão de possíveis riscos à segurança pública. A vedação a meios de comunicação imposta a determinados indivíduos é condição necessária para a contenção de facções criminosas, uma vez que suas lideranças podem comandar a atuação do grupo mesmo do interior de unidades prisionais[381]. Ademais, o uso de meios de comunicação telemática também permite a prática de outros diversos delitos, como atividades ligadas ao tráfico de drogas, crimes patrimoniais, ameaças, entre outros.

Contra tais objeções, cabem três argumentos.

O primeiro é que nenhuma medida de acesso à internet precisa ser implementada de forma igualitária em todas as

---

[380] Nesse sentido: ESTADO DE MINAS GERAIS. ***Associação denuncia falta até de absorvente em presídios femininos de MG***. Disponível em: https://www.em.com.br/app/noticia/gerais/2021/03/05/interna_gerais,1243738/associacao-denuncia-falta-ate-de-absorvente-em-presidios-femininos-de-mg.shtml. Acesso em 05/07/2021.

[381] Como exemplo, têm-se as execuções ordenadas por lideranças de conhecida facção criminosa, no ano de 2018: ESTADÃO. ***Ação contra o PCC expõe ordens para matar agentes públicos***. Disponível em: https://sao-paulo.estadao.com.br/noticias/geral,acao-contra-o-pcc-expoe-ordens-para-matar-agentes-publicos,70002351010. Acesso em: 19/11/2021

unidades prisionais. Pode haver vedações especiais a unidades de segurança máxima, detentos submetidos ao regime disciplinar diferenciado e até mesmo a determinados pavilhões dentro de uma mesma unidade.

O segundo argumento é que o monitoramento de rede por parte do Estado visa, justamente, coibir o mau uso da internet. Trata-se da mesma lógica presente no sistema meritocrático da execução penal, no qual o comportamento do indivíduo durante o cumprimento de sua pena é considerado tanto para premiá-lo (por meio de progressão de regime, livramento condicional, remição e outros benefícios) quanto para puni-lo (mediante aplicação de faltas graves, revogação de determinados direitos e benefícios, etc). Desse modo, a violação às diretrizes impostas poderia levar à perda do direito de acesso ou a transferência para pavilhão ou unidade desprovida de conexão à rede, sem prejuízo da responsabilização cível e criminal da conduta.

Por fim, o terceiro argumento é de ordem prática: o uso ilegal de celulares no sistema prisional já é amplamente difundido e, em que pese os esforços e recursos estatais empregados para combatê-lo, não tende a diminuir. Isso porque, como demonstrado no início deste artigo, a dependência do acesso à internet é tendência natural das sociedades contemporâneas, o que apenas se confirma pelo fato de que os detentos se sujeitem aos riscos da punição apenas para fazer uso de telefone celular.

Presumir que todos os sentenciados que assim o fazem possuem intenção de praticar crimes é negar suas necessidades humanas enquanto indivíduos provenientes de uma sociedade informacional. Outrossim, presumir que o modelo

proibitivo atual ou outros mais rigorosos serão eficientes para combater essa prática revela ingenuidade maior do que qualquer das propostas anteriormente apresentadas.

CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo demonstrar que os usos da internet podem apresentar benefícios aos indivíduos submetidos a penas privativas de liberdade em estabelecimentos prisionais. Desse modo, inicialmente, demonstrou-se a contradição entre as tendências sociais de maior acesso à internet no Brasil e a obstrução de seu uso à população carcerária, bem como o descompasso entre as normas que visam a difusão da internet e aquelas que a proíbem no interior de unidades prisionais.

Em seguida, demonstrou-se que a finalidade da pena escolhida pelo legislador brasileiro para nortear a execução penal conflita com problemas estruturais do cárcere enquanto instituição total, que não apenas falha em seus objetivos "ressocializadores" como também promove um processo de degradação da individualidade humana.

Tal processo se mostra ainda mais pernicioso em razão da obstrução aos meios de comunicação impostos pelo cárcere nas sociedades contemporâneas. Por outro lado, a própria existência de tais meios de comunicação permite a adoção de medidas que reduzam o impacto do aprisionamento sobre a estrutura psicológica individual a partir da manutenção de laços afetivos e da facilidade de acesso a diversos tipos de conteúdo.

Nessa linha, explorou-se o atual panorama de uso da internet pelo sistema prisional brasileiro, em comparação a

sistemas estrangeiros, concluindo-se que, apesar do maior atraso no plano nacional, as políticas públicas nessa área são mundialmente incipientes. Sendo assim, passou-se a um exercício teórico-especulativo quanto a possibilidades concretas do uso da internet em unidades prisionais.

Por fim, foram feitas ressalvas quanto à existência de outras necessidades mais prementes do sistema prisional e expostas objeções às propostas apresentadas, as quais foram, a seguir, rebatidas.

Como visto, as tendências tecnológicas e sociais do mundo contemporâneo implicam no avanço de temáticas relativas ao uso da internet sobre todos os campos da vida humana. Portanto, é inevitável que, tal qual já ocorre em outros países, essa temática permeie os debates sobre o direito de execução penal e a política criminal carcerária. Assim, o presente artigo buscou lançar holofotes sobre o tema, demonstrando, em linhas gerais, sua importância, incipiência e os entraves que o rodeiam.

Diante de um sistema penitenciário que já reúne antigos e numerosos problemas, parece necessário cogitar novas soluções.

VIGIAR E PUNIR 4.0? OS SISTEMAS DE RECONHECIMENTO FACIAL E VIGILÂNCIA ESTATAL E A NECESSIDADE DE IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA PÚBLICA QUE DIALOGUE COM OS DIREITOS HUMANOS

Bárbara Schelble[382]

"A internet não nos rouba a humanidade, é um reflexo dela. A internet não entra em nós, ela mostra o que há ali."

Zygmunt Bauman

INTRODUÇÃO

Em fevereiro de 1996, durante a Conferência de Davos, John Perry Barlow divulgou ao mundo um manifesto reconhecido como a "Declaração de Independência do Ciberespaço"[383]. Segundo Barlow, a então desconhecida internet[384] seria um lugar livre, sem regramento estatal, mais humana e justa. Passados vinte e cinco anos e diante das surpreendentes mudanças ocasionadas pela disseminação do uso das novas tecnologias e da rede mundial de computadores, a regulação e os limites do uso dessas ferramentas passaram a ser objeto de amplo debate na sociedade e nas principais organizações internacionais.[385]

---

[382] Graduada em Direito pela UFRJ e em Relações Internacionais pela Universidade Estácio de Sá, pós-graduanda em Direito Digital e Inovação no Setor Público pela UERJ e ITS Rio, MBA em Transformação Digital e o Futuro dos Negócios pela PUC/RS, Corregedora do Departamento de Ações Socioeducativas do Rio de Janeiro, Advogada, Delegada de Polícia Federal aposentada.

[383] BARLOW, John Perry. *A Declaration of the Independence of Cyberspace*. *Eletronic Frontier Foundation*, 1996. Disponível em: https://www.eff.org/cyberspace-independence. Acesso em: 18 jun. 2021.

[384] *WORLD Wide Web Foundation*. *About us*, c2008-2021. Disponível em: https://webfoundation.org/about/. Acesso em: 18 jun. 2021.

[385] VELOCCI, Carli. Derrubar o acesso à internet viola direitos humanos, segundo a ONU. Gizmodo Brasil, 2016. Disponível em: https://gizmodo.uol.com.br/internet-direito-humano/. Acesso em: 15 jun. 2021.

Temas desafiadores como a implementação de sistemas de reconhecimento facial pelos órgãos de controle estatal (que podem nos levar a um estado de super vigilância indesejado) merecem atenção.

Em recente obra, Bauman cunhou a expressão "vigilância líquida" para expressar o estado de controle e vigilância ao qual todos estamos submetidos na atualidade[386]. Ressalta, ainda, que, se por um lado, a super vigilância pode ser caracterizada como uma ameaça, por outro:

> A condição de ser observado e visto, portanto, foi reclassificada de ameaça para tentação. A promessa de maior visibilidade, a perspectiva de "estar exposto" para que todo mundo veja e observe, combina bem com a prova de reconhecimento social mais avidamente desejada, e, portanto, de uma existência valorizada – "significativa".[387]

Entre um mundo repleto de paradoxos, onde temos a superexposição da vida privada estimulada pelos algoritmos das redes sociais, como conciliar a marcha irrefreável da tecnologia, notadamente da tecnologia de reconhecimento facial, com possíveis ameaças a direitos fundamentais? Como resguardar a tutela do direito à privacidade frente às novas tecnologias de mapeamento facial e vigilância estatal? Em que medida o

[386] BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon *apud* Josh Rose, diretor de criação digital da agência de publicadade Deutsch LA. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. p. 21.

[387] *Ibidem*.

uso dessa tecnologia agravará o problema da superlotação carcerária nos presídios nacionais? Estamos prontos para tanta tecnologia?

Para responder a essas perguntas, pretende-se analisar os principais desafios relacionados à implementação de sistemas de reconhecimento facial pelos órgãos de controle estatal, por meio dos quatro tópicos: 1. Principais direitos e garantias fundamentais ameaçados; 2. Conceito e principais características dos sistemas de monitoramento facial; 3. Como o Brasil, demais países e organismos internacionais vêm tratando o tema à luz da legislação vigente; e, por fim, 4. Análise do possível agravamento da situação prisional no Brasil com a implantação em escala nacional de sistemas de reconhecimento facial.

1. PRINCIPAIS DIREITOS E GARANTIAS FUNDAMENTAIS AMEAÇADOS ("NÃO ENTRE SEM SER CHAMADO...")

Desde a transição democrática, que culminou na promulgação da Constituição Federal de 1988, o Brasil obteve significativos avanços na proteção dos direitos humanos. Flávia Piovesan afirma que "naquele contexto histórico oriundo de duas décadas de regime ditatorial, instalamos uma democracia frágil e ávida por assegurar direitos e garantias fundamentais a seus cidadãos"[388].

Entretanto, mesmo contando com normas protetivas asseguradas pelo texto constitucional, os direitos humanos nunca estiveram tão ameaçados: exclusão digital, crimes cibernéticos, vazamentos de dados pessoais, discurso de ódio, coleta e

[388] PIOVESAN, Flávia. Direitos Humanos e o Direito Constitucional Internacional. Saraiva Jur. Edição do Kindle. 19. ed. São Paulo: Saraiva Educação, 2021. p. 83.

tratamento indevido de dados pessoais, violações ao direito à privacidade e à não discriminação... Se antes as ameaças aos direitos humanos eram reais, hoje enfrentamos um novo inimigo.[389]

1.1. AMEAÇA INVISÍVEL?

A expressão "vigiar e punir"[390] criada por Foucault nunca foi tão atual. A euforia com as novidades digitais, identificada por Bauman[391], ocasionou mudanças comportamentais na sociedade. Se antes prezávamos pela nossa privacidade, hoje lidamos de forma natural com neologismos como nudes, *selfie* e *sharenting*.[392]

Assim, a privacidade não possui mais a mesma simbologia cunhada por Tércio Sampaio Ferraz Jr., nos idos de 1993, em clássico artigo sobre o tema[393], no qual afirma que, na era

[389] PIOVESAN, Flavia; MUNOZ, Lucien. Internet e direitos humanos. Marcos jurídicos têm sido aprovados com a ambição de estabelecer parâmetros, princípios, garantias, direitos e deveres no mundo digital. Ministério da Mulher, da Família e dos Direitos Humanos. Disponível em: https://www.gov.br/mdh/pt-br/sdh/noticias/2016/novembro/internet-e-direitos-humanos. Acesso em: 26 jun. 2021.

[390] FOUCAULT, Michel. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 25ª Edição, 1987.

[391] BAUMAN, Zygmunt, *op. cit.*, p. 6.

[392] BOLESINA, Iuri; FACCIN, Talita de Moura. A Responsabilidade Civil por *Sharenting*. Revista da Defensoria Pública - RS, ano 11, n. 27, jul./dez. 2020. Porto Alegre. Disponível em: https://revista.defensoria.rs.def.br/defensoria/issue/view/22/22. Acesso em: 18 jun. 2021.

[393] FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, *[S. l.]*, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 01 jul. 2021.

moderna, a privacidade surge no contexto de duas novas dicotomias: Estado x sociedade e sociedade x indivíduo.

A assimetria na relação entre os titulares de dados pessoais e os detentores das tecnologias – empresas (tanto *Big Techs*, como *startups* que coletam enorme quantidade de dados pessoais) – é preocupante. Para o filósofo e historiador Harari, se quisermos evitar a concentração de toda a riqueza e de todo o poder nas mãos de uma pequena elite, é preciso regulamentar a propriedade de dados, sob pena da ascensão de verdadeiras "ditaduras digitais baseadas em tecnologias digitais de vigilância" nos próximos anos.[394]

Não menos ameaçadoras são as violações surgidas com a implementação das tecnologias de Inteligência Artificial em decisões automatizadas. Em seu "Parecer sobre a legalidade dos Decretos n.º 10.046/2019 e n.º 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro", Lucia Maria Teixeira Ferreira afirma que "além da falta de transparência, o desenvolvimento dessa tecnologia tem conduzido à opacidade, vieses e injustiças, como denuncia a matemática e cientista de dados Cathy O´Neil"[395], para quem o uso de algoritmos configura ameaça à própria democracia, pois serve como instrumento apto a aumentar as desigualdades socioeconômicas e a discriminação social resultante da raça e da classe social.

---

[394] HARARI, Yuval Noah. 21 Lições para o Século 21; tradução Paulo Geiger. 1ª ed. São Paulo: Companhia das Letras, 2018. p. 107.

[395] FERREIRA, Lucia Maria Teixeira. Elaboração de parecer sobre a legalidade dos Decretos n.º 10.046/2019 e n.º 10.047/2019 em face das normas que disciplinam os direitos fundamentais. Revista do Ministério Público do Estado do Rio de Janeiro n. 75, p. 263. jan./mar. 2020

Relatório organizado por grupo de pesquisadores do Instituto de Tecnologia e Sociedade – ITS assevera que, diante da euforia em torno do uso das tecnologias de reconhecimento facial para identificação de foragidos e suspeitos, é preciso analisar se essas ferramentas são eficazes e aptas aos fins a que se destinam.[396]

Em julho de 2021, o Laboratório de Políticas Públicas e Internet publicou o relatório "Vigilância Automatizada: o uso de reconhecimento facial pela Administração Pública" com o diagnóstico do uso dessa tecnologia pela Administração Pública brasileira e o levantamento dos principais riscos inerentes ao uso indiscriminado das tecnologias de reconhecimento facial. A principal conclusão do relatório é que "o emprego de tecnologias de vigilância não tem sido realizado de forma transparente com a população, o que coloca em risco os direitos e liberdades individuais de cidadãos cujos dados são coletados por esses sistemas". Há ainda pouca confiabilidade envolvendo o uso de tais tecnologias pelo setor público, na medida em que "seu amplo emprego não

[396] Nesse sentido: "A utilização dessas novas ferramentas tecnológicas pelos órgãos públicos, especialmente em um cenário de ausência de legislação específica aplicável, pode criar riscos significativos para os direitos fundamentais dos cidadãos, como privacidade, liberdades de expressão e associação, além da presunção de inocência. Monitoramento em tempo real por câmeras de segurança, identificações equivocadas (falsos positivos), além de decisões automatizadas e enviesadas (discriminatórias e geradoras de exclusão) são apenas algumas das problemáticas existentes". [LEMOS, Alessandra; FERNANDES, Elora; MEDEIROS, Juliana; GUEDES, Paula; SILVA, Priscila. Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial. Instituto de Tecnologia e Sociedade do Rio – ITS. Rio de Janeiro, p. 1. 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf. Acesso em: 01 jul. 2021].

é acompanhado, por exemplo, por regulação específica, por mecanismos de prestação de contas aos cidadãos sobre os seus direitos e tampouco pelo emprego de medidas preventivas adequadas de segurança da informação e proteção de dados". Tampouco sua aplicação tem sido acompanhada de avaliações sobre a proporcionalidade dos impactos que promove em relação aos benefícios que promete para a eficiência da atividade estatal.[397]

Mesmo diante dessas vicissitudes, é inegável que a tecnologia de reconhecimento facial abre novas possibilidades para a Administração Pública, em especial a segurança pública e o controle de fronteiras. O início de testes e do uso dessas tecnologias por diversas autoridades públicas provocou debate intenso a respeito do potencial impacto na proteção dos direitos humanos, já que desafios relacionados à opacidade, vieses e injustiças, foram detectados nas tecnologias de IA utilizadas para reconhecimento facial, como preconizado por Peter Deangelis.[398]

[397] REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: Laboratório de Políticas Públicas e Internet - LAPIN, p. 2. 2021. Disponível em: https://lapin.org.br/download/4136/. Acesso em: 01 jul. 2021.

[398] Nesse sentido: "Racial profiling is not merely wrong because of these consequentialist failings, but also because it violates basic constitutional rights, such as the right to be protected against unreasonable searches and seizures and the right to equal protection of the law." [DEANGELIS, Peter. Racial Profiling and the Presumption of Innocence. Netherlands Journal of Legal Philosophy, v. 1 p. 43, 2014. Disponível em: https://www.bjutijdschriften.nl/tijdschrift/rechtsfilosofieentheorie/2014/1/NJLP_2213-0713_2014_043_001_004.pdf. Acesso em: 01 jul. 2021].

Não sem razão, o uso dessa tecnologia vem sendo questionado por diversos países e cidades do mundo, como São Francisco[399] e Baltimore[400], que desativaram o uso de equipamentos de vigilância, devido à falta de transparência e de mecanismos garantidores de utilização para finalidades exclusivas de segurança, sem riscos a violações a direitos fundamentais, por se tratar de tecnologia de IA invasiva e que não traz garantias quanto à proteção dos dados coletados.

2. CONCEITO E PRINCIPAIS CARACTERÍSTICAS DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

O estudo "Tecnologia de Reconhecimento Facial: considerações de direitos fundamentais no contexto da aplicação da lei", publicado em 21 de novembro de 2019 pela Agência Europeia de Direitos Fundamentais – FRA, define tecnologia de reconhecimento facial como sendo a tecnologia que "permite a identificação automática de um indivíduo pelo cruzamento de duas ou mais imagens faciais de arquivos digitais"[401].

---

[399] BIONI, Bruno Riciardo; LUCIANO, Maria; RIELLI, Mariana. Regulação de reconhecimento facial em São Francisco. DataPrivacyBR, 2019. Disponível em: https://dataprivacy.com.br/regulacao-de-reconhecimento-facial-em-sao-francisco/. Acesso em: 16 jun. 2021.

[400] COLLINS, David. *Court finds Baltimore aerial surveillance unconstitutional. WBALTV*, 2021. Disponível em: https://www.wbaltv.com/article/baltimore-police-spy-plane-unconstitutional-federal-appeals-court/36832093#. Acesso em: 26 jun. 2021.

[401] EUROPEAN Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. Áustria, 2019. p. 7. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf. Acesso em: 20 jun. 2021.

Consta no referido estudo que a tecnologia de reconhecimento facial "abrange a uma infinidade de tecnologias que podem executar diversas tarefas para diferentes propósitos com objetivo de verificação, identificação ou categorização"[402]. Verificação e identificação dizem respeito às características únicas dos indivíduos aptas a determinar sua identidade pessoal. A verificação ou autenticação "é frequentemente referida como correspondência um-para-um na comparação de dois modelos biométricos, para determinar se a pessoa mostrada nas duas imagens é a mesma pessoa"[403]. A categorização classifica os indivíduos por grupo específico com base em suas características biométricas – por exemplo, sexo, idade ou raça.

A identificação pode ser classificada ainda como "fechada", quando as imagens são comparadas com arquivo existente em banco de dados, ou como "conjunto aberto", caso não haja imagem armazenada em banco de dados. Quando usada para identificação, a tecnologia de reconhecimento facial é chamada "Reconhecimento Facial Automatizado" (AFR). Se baseada em imagens faciais obtidas de câmeras de vídeo, denomina-se tecnologia de "Reconhecimento Facial ao Vivo" (LFRT).[404]

O cerne da questão envolvendo a utilização dessas ferramentas é que o seu funcionamento depende quase que exclusivamente da coleta de dados biométricos, considerados dados sensíveis nas principais legislações sobre tratamento de dados pessoais, como a Diretiva sobre Segurança Pública (EU

[402] *Ibidem*.

[403] *Ibidem*.

[404] *Ibidem*.

2016/680) da União Europeia, de 27 de abril de 2016[405], que regula o sistema de proteção de dados pessoais no campo da segurança pública e da cooperação judicial em matéria criminal[406].

Nesse sentido, Chiara de Teffé ressalta, ainda, que os dados biométricos são considerados dados sensíveis e merecem tutela diferenciada e especial, "de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar preconceitos e discriminações ilícitas ou abusivas em face do titular"[407].

Há ainda que se considerar o fato de as imagens faciais serem facilmente capturadas em comparação com outros dados biométricos, como impressões digitais ou DNA, visto

[405] UNIÃO Europeia. Diretiva n.º 2016/680 do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&rid=1. Acesso em: 01 jul. 2021.

[406] Segundo o item 13, do artigo 3º, da Diretiva n.º 2016/608, do Parlamento Europeu e do Conselho (*cf. supra*), imagens faciais são consideradas dados biométricos quando usadas para correspondência biométrica com objetivo de identificação ou autenticação de uma pessoa natural.

[407] 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. O Direito Civil na Era da Inteligência Artificial. 1. ed. São Paulo: Thompson Reuters Brasil, 2020, p. 290. Disponível em: https://www.academia.edu/44127917/Tratamento_de_dados_sens%C3%ADveis_por_tecnologias_de_reconhecimento_facial_prote%C3%A7%C3%A3o_e_limites. Acesso em: 29 jun. 2021.

que um indivíduo se torna praticamente incapaz de impedir a captura e monitoramento da sua imagem em público.[408]

2.1. ERRAR É HUMANO?

O levantamento realizado pela FRA apontou ainda que a tecnologia de reconhecimento facial "tem alta probabilidade de erro quando usada para identificar mulheres ou afrodescendentes, produzindo resultados tendenciosos, que poderiam resultar em discriminação"[409] – isso acontece, porque, muitas vezes, a tecnologia original é treinada em um local específico que nem sempre representa uma amostra diversa da população – e que pode, ainda, impactar negativamente a liberdade de associação e o direito de reunião, caso os indivíduos sintam-se ameaçados de estarem sendo monitorados ao saírem na rua (*chilling effect*[410]).

Questiona, ainda, possível ameaça ao direito à privacidade diante do processamento de larga quantidade de dados e em que ponto essa violação poderia afetar o funcionamento da democracia. Preocupa-se também com o fato de pesquisadores e empresas estarem se dedicando a inferir emoções[411], como

[408] UNIÃO Europeia, ***op. cit.***, p. 7.

[409] EUROPEAN Union Agency for Fundamental Rights, ***op. cit.***, p. 9.

[410] Em um contexto legal, um ***chilling effect*** (em tradução livre, «efeito inibidor» ou «efeito amedrontador») é a inibição ou desencorajamento do exercício legítimo de direitos legais e naturais pela ameaça de sanção legal. [CHILLING effect. *In:* Wikipedia: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Chilling_effect. Acesso em: 01 jul. 2021].

[411] Quanto a isso: "Dados sobre a origem, crenças e relacionados a questões sexuais são especiais diante de históricas perseguições, discriminações e preconceitos em face de pessoas de determinadas origens raciais ou étnicas, com certas crenças ou posições políticas ou, ainda, que tenham

raiva, medo ou felicidade, além de outras características, como orientação sexual[412].

Conforme alertado em matéria veiculada pelo site G1, há ainda o problema de que algoritmos de reconhecimento facial têm diferentes graus de acurácia e precisão. Eles podem gerar falsos positivos, quando pessoas inocentes são reconhecidas como criminosos, ou falsos negativos, quando um criminoso passa despercebido.[413]

Em razão dos questionamentos éticos e da necessidade de regulação e especificação do alcance da tecnologia de reconhecimento facial, muitos países resolveram adiar ou suspender a implementação desses sistemas tanto na Segurança Pública, como em outras áreas da vida em sociedade, como explicitado no estudo do FRA.[414]

---

determinada opção sexual. Os dados corporais, com o avanço da ciência e da tecnologia, apresentam uma sensibilidade também elevada, sendo diversas as suas aplicações e tratamentos, como será analisado em relação aos dados biométricos". [TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad, *op. cit.*, p. 290].

[412] Este último foi pesquisado em fronteiras externas selecionadas da UE (Grécia, Hungria e Letônia) no âmbito do projeto *Integrated Portable Control System - iBorderCtrl* [EUROPEAN Union Agency for Fundamental Rights. *op. cit.*, *loc. cit.*].

[413] TECNOLOGIA de reconhecimento facial apresenta viés e imprecisão, aponta estudo do governo dos EUA. G1, Rio de Janeiro, 20 dez. 2019. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/12/20/tecnologia-de-reconhecimento-facial-apresenta-vies--e-imprecisao-aponta-estudo-do-governo-dos-eua.ghtml. Acesso em: 01 jul. 2021.

[414] EUROPEAN Union Agency for Fundamental Rights, *op. cit.*, p. 9.

2.2. O USO DE TECNOLOGIA DE RECONHECIMENTO FACIAL NO BRASIL

Um mapeamento realizado pela organização Transparência Brasil, denominado "Uso de Inteligência Artificial pelo Poder Público", publicado em fevereiro de 2020, aponta a existência de três tipos de ferramentas de Inteligência Artificial atualmente em uso pelo Poder Público brasileiro: "i) 20 ferramentas para apoio a tomada de decisão direcionadas para os próprios órgãos públicos; ii) 8 ferramentas de decisão direcionadas para o público externo; e iii) 16 ferramentas para aperfeiçoar processos internos dos órgãos, sem envolver tomada de decisão"[415].

Identificou, ainda, violações aos princípios da presunção de inocência, na medida em que o uso generalizado de sistemas de reconhecimento facial incide sobre toda a população que transita pelo local vigiado. Ressaltou também que esses sistemas podem impactar negativamente o princípio da não discriminação quando não programados para detecção de possíveis vieses[416]. Isso, porque "o uso da tecnologia inverte a lógica do direito penal em um Estado Democrático de Direito, em que toda investigação que impacte direitos (no caso, direito à intimidade, privacidade e proteção de dados pessoais) deve partir de uma suspeita fundada"[417].

---

[415] TRANSPARÊNCIA Brasil. Uso de Inteligência Artificial pelo Poder Público. São Paulo, 2019, p. 9. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 20 jun. 2021.

[416] *Ibidem*, p. 15.

[417] *Ibidem*.

Cidades como o Rio de Janeiro e Salvador iniciaram o uso de câmeras de monitoramento com sistemas de reconhecimento facial em 2019 sob a justificativa de identificação de pessoas com mandados de prisão em aberto[418]. Foram identificadas falhas nos sistemas de reconhecimento facial em operação por entidades da sociedade civil[419_420] e órgãos de imprensa, contudo a falta de transparência em relação às falhas ocasionou, à época, a prisão ilegal de inocente, devido ao uso de banco de dados desatualizado para a comparação e identificação das imagens coletadas[421].

418ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *In*: INTERNETLAB. Vigilância Sobre as Comunicações no Brasil. 2. ed. 2017. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso em: 20 jun. 2021.

419 COALIZÃO Direitos Na Rede. Nota sobre projeto de videomonitoramento o Ceará e em defesa de maior debate público, 04 set. 2020. Disponível em: https://direitosnarede.org.br/2020/09/04/nota-sobre-projeto-de-videomonitoramento-no-ceara-e-em-defesa-de-maior-debate-publico/. Acesso em: 18 jun. 2021.

420 LIMA, Mariana. Estudo aponta que 90% dos presos por reconhecimento facial são negros. Observatório do Terceiro Setor, 2019. Disponível em: https://observatorio3setor.org.br/noticias/estudo-aponta-que-90-dos--presos-por-reconhecimento-facial-sao-negros/. Acesso em: 20 jun. 2021.

421 Nesse sentido: "Os testes aqui começaram no carnaval de 2019 e Marcos Vinicius de Jesus Neri, 19 anos, foi preso em um bloco na cidade de Salvador, após ser reconhecido por uma das câmeras. Foram 184 pessoas presas com o uso de reconhecimento facial no Brasil durante o primeiro ano de uso – dessas, mais de 90% eram negras. No Rio de Janeiro, a maioria das câmeras que fazem reconhecimento facial foram instaladas no bairro de Copacabana. No segundo dia do uso, uma mulher foi presa ao ser identificada erroneamente pelo sistema que apontou mais de 70% de semelhança entre ela e Maria Leda, uma pessoa foragida da justiça. No entanto, a verdadeira criminosa estava presa desde 2015. As polícias militar e civil do Rio de Janeiro utilizaram um banco de dados desatualizado. Esse caso é emblemático porque expõe a falha da máquina de leitura biométrica facial e a irresponsabilidade por parte da secretaria de segurança públi-

A falta de transparência, de regulamentação e de auditagem sobre os sistemas de reconhecimento facial causa ainda mais preocupação ao analisarmos o problema em conjunto com os dados do relatório "Situação dos Direitos Humanos no Brasil", publicado pela Comissão Interamericana de Direitos Humanos da OEA, em 12 de fevereiro de 2021[422].

Consta no referido relatório que, em 2019, a sociedade brasileira era composta em sua maioria por afrodescendentes (56,8% da população), além de possuir a terceira maior população carcerária do mundo e uma taxa de superlotação de 170,74% no sistema penitenciário. Em relação aos presos provisórios, a taxa chega a 229.823 (30, 43% da população carcerária[423]. Outro grave problema diagnosticado pela Comissão diz respeito ao "aumento de 22,5% da população carcerária entre 2000 e 2019"[424]. Segundo o entendimento da Comissão:

> [...] o Brasil enfrenta um problema de discriminação racial estrutural histórico, que coloca as pessoas afrodescendentes em um processo de inequidade e exclusão. Em particular, a Comissão

ca." (grifos próprios). [SOUZA, Bruno. Panóptico: reconhecimento facial renova velhas táticas racistas de encarceramento. Rede de Observatórios da Segurança, 2021. Disponível em: http://observatorioseguranca.com.br/panoptico-reconhecimento-facial-renova-velhas-taticas-racistas-de--encarceramento/. Acesso em: 01 jul. 2021].

[422] COMISSÃO Interamericana de Direitos Humanos. Situação dos direitos humanos no Brasil: Aprovado pela Comissão Interamericana de Direitos Humanos em 12 fev. 2021. Disponível em: http://www.oas.org/pt/cidh/relatorios/pdfs/Brasil2021-pt.pdf. Acesso em: 20 jun. 2021.

[423] *Ibidem*, p. 64.

[424] *Ibidem*.

> observa com extrema preocupação a predominância de pessoas afrodescendentes no sistema penitenciário, que constituem 65,9% do total da população carcerária. Esse dado demonstra que a discriminação racial enfrentada por essas pessoas também faz com que elas sejam mais propensas a serem encarceradas.[425]

Silvio Almeida conceitua discriminação racial como "a atribuição de tratamento diferenciado a membros de grupos racialmente identificados"[426]. Tem, portanto, como requisito fundamental o poder, ou seja, a possibilidade efetiva do uso da força, sem a qual não é possível atribuir vantagens ou desvantagens por conta da raça. Em um país predominantemente afrodescendente, com problemas graves na elaboração de políticas de segurança pública efetivas e duradouras, questiona-se se o uso de tecnologias modernas de monitoramento e vigilância, ou de "policiamento preditivo"[427],

---

[425] *Ibidem*.

[426] ALMEIDA, Silvio Luiz de. Racismo Estrutural. São Paulo. Editora Jandaira, 2021, p. 32.

[427] Nesse sentido: "Todavia, um sistema de ***profiling*** policial baseado em algoritmos não monitora apenas um sujeito em potencial, mas categoriza indivíduos de modo que a máquina passe a supor que certos grupos têm maior probabilidade de praticar crimes do que outros, merecendo, portanto, maior atenção por parte das autoridades policiais. Se esse tipo de ***profiling*** levar a uma busca e subsequente prisão, nenhum agente de persecução penal individualmente considerado terá de modo efetivo identificado ***ex ante*** uma justa causa para a prisão. Na verdade, ele ou ela talvez nunca saiba como foi formado o conjunto de dados que resultou na prisão daquele indivíduo. Esse procedimento dificilmente constituiria uma suspeita razoável tal qual a requerida pela CEDH. A fundamentação de uma regra de inadmissibilidade da prova ilícita também se assenta no princípio da igualdade perante a lei, central para qualquer democracia.

seriam eficientes e estariam em consonância com os direitos e garantias fundamentais assegurados na Magna Carta.

Sob esse aspecto, Ferreira cita em seu Parecer a preocupação da *Coding Rights* com a possível ocorrência de abusos por parte de policiais e do setor privado, responsável pela implementação dos sistemas e pelo compartilhamento de dados sensíveis.[428]

Embora a ameaça de violação a direitos fundamentais seja real, notadamente ao direito à não discriminação e à presunção de inocência, a adoção do reconhecimento facial no campo da segurança pública é inevitável. Ao menos 20 estados e municípios brasileiros já tiveram, têm ou estão em processo de licitação de projetos.[429] A Bahia é o estado mais avançado no uso da tecnologia e também o que mais encarcera.

Se a atividade policial é baseada em algoritmos que dividem a população em grupos tendo em vista determinadas características, o resultado será uma mudança fundamental em nosso sistema jurídico, que passará a ser caracterizado por um aumento de buscas e detenções ilegais, além das consequentes violações à privacidade e à liberdade de todos os cidadãos". [GLESS, Sabine. Policiamento preditivo: em defesa dos "verdadeiros-positivos". Tradução de Heloisa Estellita e Miguel Lima Carneiro. Revista Direito GV, v. 16, n. 1, p. 5, jan./abr. 2020].

[428] FERREIRA, Lucia Maria Teixeira, *op. cit.*, p. 262.

[429] MOGNON, Mateus. Brasil é pioneiro no uso de reconhecimento facial em aeroportos. Tecmundo, 2021. Disponível em: https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/219316-brasil-usa-reconhecimento-facial-ter-aeroportos-embarque-digital.htm. Acesso em: 01 jul. 2021.

3. UM OLHAR SOBRE A LEGISLAÇÃO DO BRASIL, DA UNIÃO EUROPEIA E DAS ORGANIZAÇÕES INTERNACIONAIS

3.1. A EVOLUÇÃO DA LEGISLAÇÃO NACIONAL NA ERA DIGITAL

A Lei n.º 12.965, publicada em 24 de abril de 2014[430], instituiu os princípios, garantias, direitos e deveres para o uso da internet no Brasil. O Marco Civil da Internet adota como fundamentos o respeito à liberdade de expressão, os direitos humanos, a pluralidade, a diversidade e a finalidade social da rede. Entre os princípios, destacam-se tanto a garantia da liberdade de expressão como a proteção à privacidade e aos dados pessoais.

Com a edição da Lei n.º 13.709, de 14 de agosto de 2018, denominada LGPD (Lei Geral de Proteção de Dados Pessoais)[431], o Brasil passou a integrar o grupo de mais de 130 países que possuem a sua própria lei de proteção dos dados pessoais. A LGPD foi inspirada na GDPR, Regulação de Proteção de Dados da União Europeia[432]. Ambas firmam bases sólidas no princípio

[430] BRASIL. Lei n.° 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 jun. 2021.

[431] BRASIL. Lei n.° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 jun. 2021.

[432] UNIÃO Europeia. Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho, 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), 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504.

da autodeterminação informativa[433], que visa conceder aos titulares dos dados pessoais real poder sobre as suas próprias informações e um efetivo controle sobre os seus dados.

Em novembro de 2019, o presidente da Câmara dos Deputados determinou a criação de comissão de juristas[434] para elaboração de anteprojeto de lei[435] para os casos de tratamento de dados pessoais para fins de segurança pública e persecução penal[436]. Foi opção do legislador não contemplar o tratamento de dados para segurança pública e investigação criminal no âmbito de aplicação da LGPD, estabelecendo expressamente a necessidade de aprovação de lei específica para esse tema (art. 4, caput, inciso III, alíneas "a" e "d" c/c § 1º, da LGPD).[437]

Acesso em: 01 jul. 2021.

[433] FERREIRA, Lucia Maria Teixeira, *op. cit.*, p. 258.

[434] Nesse sentido: "A opção da comissão de juristas pelo CNJ como autoridade competente no âmbito da LGPD Penal tem como objetivo garantir uma independência necessária para a proteção do cidadão e a colaboração internacional, concentrando os poderes de supervisão em um órgão fora da estrutura do Executivo. Na medida em que o CNJ não possui, até então, subórgão específico competente para analisar questões de regulação de dados, a lei garante a autonomia e expertise técnicas do órgão com a criação da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) dentro da própria estrutura do CNJ." [LEMOS, Alessandra; FERNANDES, Elora; MEDEIROS, Juliana; GUEDES, Paula; SILVA, Priscila, *op. cit.*, p. 3].

[435] BRASIL. Câmara dos Deputados. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, 2019. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 01 jul. 2021.

[436] COSTA, Eduarda; REIS, Carolina. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? Laboratório de Políticas Públicas e Internet – LAPIN, 2021. Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/. Acesso em: 01 jun. 2021.

[437] BRASIL. Lei n.° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de

O principal desafio da comissão foi elaborar um anteprojeto de lei que não inviabilizasse o tratamento de dados nas atividades policiais (típica atividade policial), mas que "garantisse direitos fundamentais e criasse situação de confiança entre Estado e cidadão"[438], tendo em vista que "a utilização de ferramentas tecnológicas no contexto do processo penal para auxílio da colheita de provas e investigação penal são uma realidade"[439].

Conforme explicitado em relatório elaborado pelo ITS:

> [...] o artigo 5º, inciso XXIII, do anteprojeto define tecnologias de monitoramento como sendo equipamentos, programas de computador ou sistema informático que possam ser usados para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio.[440]

O anteprojeto estabeleceu duas proibições no uso de tecnologias de monitoramento, visando coibir o vigilantismo estatal e preservar o direito à proteção de dados na seara da segurança pública. Uma delas diz respeito à necessidade de autorização legal específica prévia para o seu uso (artigo 42, caput[441]), a qual deve ser precedida de relatório de impacto

---

Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 jun. 2021.

[438] COSTA, Eduarda; REIS, Carolina, ***op. cit., loc. cit.***

[439] ***Ibidem***.

[440] LEMOS, Alessandra; FERNANDES, Elora; MEDEIROS, Juliana; GUEDES, Paula; SILVA, Priscila, ***op. cit.***, p. 4.

[441] BRASIL. Câmara dos Deputados, ***op. cit.***

de vigilância (§2º, do mesmo dispositivo[442]) e estabelecer garantias aos direitos dos titulares. A segunda, disposta no artigo 43, proíbe:

> [...] a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.[443]

O objetivo foi garantir que os órgãos responsáveis por atividades de segurança pública detenham segurança jurídica para exercer suas funções com maior eficiência em consonância com as garantias e direitos fundamentais dos titulares de dados, "equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações"[444].

Em Nota Técnica elaborada pelo Laboratório de Políticas Públicas e Internet – LAPIN sobre a LGPD Penal, afirma-se que a proteção de dados pessoais é um direito fundamental autônomo, amparado constitucionalmente pelos direitos à liberdade, à privacidade e ao livre desenvolvimento da personalidade. Entende-se, ainda, que, para a salvaguarda dos direitos fun-

[442] *Ibidem*.

[443] LEMOS, Alessandra; FERNANDES, Elora; MEDEIROS, Juliana; GUEDES, Paula; SILVA, Priscila, *op. cit.*, p. 4.

[444] BRASIL. Câmara dos Deputados, *op. cit.*

damentais, é imprescindível a edição de legislação específica no âmbito penal que delimite e balanceie as fronteiras entre a esfera penal e a garantia de direitos fundamentais.[445]

3.2. A REGULAÇÃO ALÉM-MAR

As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, de 1980, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, na sigla em inglês), foram uma das primeiras normas de proteção de dados e representa um consenso internacional sobre princípios e regras relativos à coleta e ao gerenciamento da informação pessoal, fundamentada em três princípios: democracia pluralista, respeito aos direitos humanos e economias de mercado aberto.[446]

O artigo 8º, da Carta de Direitos Fundamentais da União Europeia (2012/C 326/02), estabelece que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito"[447]. Diversas organizações internacionais, como a Agência Europeia para Direitos Fundamentais, o Grupo de Inteligência Artificial do Alto Comissariado do Comitê Europeu e o Comitê Consultivo da Convenção 108 do Conselho da

[445] LAPIN. Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para a Segurança Pública e Investigação Criminal. Laboratório de Políticas Públicas e Internet – LAPIN, 2021. Disponível em: https://lapin.org.br/wp-content/uploads/2021/03/NT_APJ-para-Seguranca-Publica-e-Investigacao-Criminal.pdf. Acesso em: 01 jul. 2021.

[446] FERREIRA, Lucia Maria Teixeira, *op. cit.*, p. 259.

[447] UNIÃO Europeia. Carta dos Direitos Fundamentais da União Europeia (2012/c 326/02). Jornal Oficial da União Europeia, 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Acesso em: 18 jun. 2021.

Europa, priorizam a formulação de proposições destinadas à regulação ética e jurídica do reconhecimento facial e de outras tecnologias de IA, ressaltando que o desenvolvimento e o uso da IA devem respeitar, em especial, os direitos à privacidade e à proteção dos dados pessoais.

As principais agências internacionais recomendam, ainda, o uso racional da tecnologia de reconhecimento facial e sugerem que sua aplicação seja claramente baseada em leis existentes, considerando que o seu crescimento é alimentado pela inteligência artificial.[448] A jurisprudência ainda é praticamente inexistente sobre o tema, com exceção de um caso ajuizado na Inglaterra ainda sem decisão final.[449]

Há quem seja mais radical, como Margrethe Vestager, vice-presidente executiva de regulação digital da União Europeia (EU, na sigla em inglês), que sugere a proibição do uso do reconhecimento facial nos espaços públicos dos países da União Europeia pelo período de três a cinco anos, até que existam salvaguardas para mitigar os riscos dessa tecnologia.[450]

Importa mencionar que o fenômeno da convergência em torno de leis gerais, na Europa e na América Latina, fundadas em direitos básicos concedidos aos titulares de dados e no conjunto de obrigações aos controladores e processadores

---

[448] EUROPEAN Union Agency for Fundamental Rights, *op. cit.*, p. 7.

[449] UNITED Kingdom. *High Court of Justice. Queen's Bench Division (Divisional Court). Case n. ° CO/4085/2018. Judgment in* 04 *sept.* 2019. Disponível em: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp--judgment-Final03-09-19-1.pdf. Acesso em: 01 jul. 2021.

[450] CARVALHO, Isabella. União Europeia discute proibir reconhecimento facial por cinco anos. StartSe, 2020. Disponível em: https://www.startse.com/noticia/nova-economia/uniao-europeia-proibicao-reconhecimento-facial. Acesso em: 26 jun. 2021.

de dados, demonstra a crescente vulnerabilidade dos titulares dos dados pessoais. Em relação aos países latino-americanos, Valentina Hernandez diz, em artigo sobre o tema, que, embora na última década tenha ocorrido impulso regulatório com forte tendência de normatização da coleta de dados biométricos – com o objetivo de identificação e verificação de identidade, especialmente para fins de vigilância pública –, voltados principalmente para procedimentos investigativos, tais normativos estão sendo realizados, em sua maioria, sem as necessárias alterações legislativas específicas.[451]

4. NOVAS TECNOLOGIAS PARA OS MESMOS SUSPEITOS?

A questão central no uso de tecnologias de reconhecimento facial na área de segurança pública, analisada após um período de experiências em diversos estados brasileiros, é que a tecnologia, além de ser ineficiente, possivelmente agravará o encarceramento em massa, principalmente de jovens e negros das periferias.[452]

Levantamento realizado pelo Laboratório de Políticas Públicas e Internet identificou cinco riscos do uso de tecnologias de reconhecimento facial: i) violação de direitos fundamentais;

[451] BAUZÁ, Valentina Hernández. *Sucesos regulatorios en materias de privacidad e internet en Latinoamérica*. Derechos Digitales América Latina, 2020, p. 13. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/tendencias-privacidad-latam.pdf. Acesso em: 29 jun. 2021.

[452] NUNES, Pablo. Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. The Intercept_Brasil, 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 26 jun. 2021.

ii) vigilância em massa; iii) racismo; iv) transfobia; e v) violação dos direitos das crianças e adolescentes.[453]

O jornalista Ricardo Moura, em artigo publicado no site A Rede de Observatórios de Segurança, monitorou os casos de prisões e abordagem com o uso de reconhecimento facial desde que eles foram implantados em março de 2019 e descobriu que, dos casos em que havia informações, 90,5% das pessoas presas flagradas pelas câmeras eram negras. A Bahia foi a campeã de abordagens e prisões com a tecnologia: 51,7% das prisões; seguida do Rio, com 37,1%; Santa Catarina, com 7,3%; Paraíba, com 3,3%; e o Ceará, com 0,7%.[454] Moura ainda ressalta que o uso da tecnologia não é neutro, haja vista que a técnica absorve muito do conteúdo ideológico e cultural de quem a opera.

Nesse ponto, cabe o seguinte questionamento: a tecnologia é de última geração, mas o controle e a vigilância são exercidos sobre os mesmos suspeitos de sempre – negro, pobre e periférico?

---

[453] REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando, *op. cit.*, p. 8-9.

[454] Nesse sentido: "Em outubro de 2019, O POVO noticiou que policiais militares poderão se valer da técnica do reconhecimento facial no policiamento das ruas por meio do aplicativo Portal do Comando Avançado (PCA), que tem como base de dados todos os RGs emitidos no Estado. A ideia, conforme a Secretaria da Segurança Pública e Defesa Social (SSPDS), é possibilitar a identificação de pessoas abordadas sem documentação e em "situação suspeita" por meio do reconhecimento não apenas biométrico (impressão digital), mas facial. Não é preciso muita imaginação para sabermos a cor e o biotipo das pessoas que serão os principais alvos desses novos equipamentos". [MOURA, Ricardo. Novas tecnologias para os suspeitos de sempre. Rede de Observatórios da Segurança, 2019. Disponível em: http://observatorioseguranca.com.br/novas-tecnologias-para-os-suspeitos-de-sempre/. Acesso em: 01 jul. 2021].

A resposta a essa indagação deve ser analisada em conjunto com os dados acima apresentados e com a pesquisa da antropóloga Simone Browne, que alerta que, desde a época da escravidão até os atuais circuitos internos de TV, os negros sempre foram objeto de vigilância ("*dark surveillance*"[455]). Basta um simples levantamento de pessoas e de comportamentos considerados como suspeitos no cotidiano para verificarmos esse viés racial que perpassa não somente o olhar do policial, mas a nossa própria visão, como no recente caso ocorrido na cidade do Rio de Janeiro, onde um jovem negro foi acusado por um casal branco de ter furtado a própria bicicleta.[456]

Para o especialista em liberdade na internet, Dave Maass, citado por Ricardo Moura, o principal problema dos sistemas de vigilância em massa é a prisão de inocentes, seja por falha na sua identificação, seja pela análise de seu padrão de comportamento. Tal constatação levou o Conselho de Ética em Tecnologia de Inteligência Artificial e Policiamento da empresa Axon a deixar de produzir tecnologias de reconhecimento facial para uso corporal. A empresa manifestou, ainda, particular preocupação com "a evidência de desempenho desigual e não confiável em raças, etnias, sexos e outros grupos de identidade".[457]

[455] MOURA, Ricardo, *op. cit.*

[456] DUTRA, Daniele. Casal branco acusa jovem negro de roubar a própria bicicleta no Leblon (RJ). UOL News, 2021. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2021/06/14/casal-branco-acusa-jovem-negro-de-roubar-a-propria-bicicleta-no-leblon.htm. Acesso em: 01 jul. 2021.

[457] MOURA, Ricardo, *op. cit.*

Tanta tecnologia seria realmente capaz de reduzir a criminalidade ou servirá apenas para agravar ainda mais os complexos problemas de segurança pública que já enfrentamos?

CONSIDERAÇÕES FINAIS

No Brasil, o que mais se vê é um encantamento com as máquinas, como se o processo de aperfeiçoamento da atividade policial ocorresse somente pelo emprego de artefatos de última geração, mas é preciso que a sociedade civil esteja atenta para que a euforia com a implementação de novas tecnologias não sirva de escudo para a prática de atos discriminatórios e abusivos.

É preciso, ainda, que haja a plena conscientização de que os "direitos humanos *on-line*" devem ter a mesma força protetiva que os "direitos humanos *off-line*". Para assegurá-los, é fundamental a implementação de processos de aperfeiçoamento da tecnologia e de *accountability*. Faz-se necessário que o tratamento dos dados coletados em sistemas de reconhecimento facial ofereça o mínimo de transparência e segurança, notadamente para que essas tecnologias não criem vieses discriminatórios.

Não se pode deixar de mencionar que o racismo estrutural não merece abrigo nos algoritmos utilizados nos sistemas de reconhecimento facial. Enquanto sociedade, devemos cobrar das autoridades públicas reposta imediata a prisões ilegais decorrentes do uso dessas tecnologias, assim como que se adotem medidas com o intuito de suspender ou evitar o uso dessas ferramentas até a sua completa regulamentação e aperfeiçoamento.

Nesse cenário repleto de incertezas, é preciso que se promova ampla conscientização da sociedade, empresas e órgãos públicos sobre o uso de algoritmos e as ameaças que as novas tecnologias de reconhecimento facial oferecem à democracia pelos resultados, muitas vezes, tendenciosos, podendo aumentar ainda mais as desigualdades socioeconômicas e a discriminação social resultante da raça e da classe social.

ADOÇÃO DA CONVENÇÃO DE BUDAPESTE PELO BRASIL: DESAFIOS E PERSPECTIVAS

Bruna Veríssimo Lima Santos[458]

INTRODUÇÃO

A presente pesquisa tem como objetivo avaliar as eventuais implicações da adoção da Convenção de Budapeste para o Estado brasileiro no âmbito da cooperação internacional. Busca-se, com isso, aferir os benefícios ou prejuízos ao país decorrentes da internalização dessa norma.

O artigo insere-se no contexto de constante aumento da complexidade não apenas do cometimento de crimes cibernéticos, mas também dos trâmites exigidos à sua efetiva persecução. De um lado, os meios para execução de delitos vão desde redes sociais ou *sites* na *Internet* até programas intrincados capazes de captar dados sensíveis dos cidadãos em pouco tempo; de outro, a natureza aberta da internet faz que dados importantes para a solução desses casos estejam em territórios diversos, gerando problemas quanto à jurisdição aplicável.

Apenas no Brasil, há cerca de 130 milhões de usuários inscritos no *Facebook*, 120 milhões com conta no *WhatsApp*, 95 milhões no *Instagram*[459], sem contar outras redes sociais como

[458] Diplomata brasileira. Bacharel em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Cursa Pós-graduação em Direito Digital promovida pela Universidade do Estado do Rio de Janeiro (UERJ), o Instituto de Tecnologia e Sociedade (ITS Rio) e o Centro de Estudos e Pesquisas no Ensino do Direito (CEPED).

[459] VOLPATO, Bruno. Ranking: as redes sociais mais usadas em 2021 no Brasil e no mundo, insights e materiais gratuitos. Resultados digitais, 2021. Disponível em: https://resultadosdigitais.com.br/blog/redes-sociais-mais-usadas-no-brasil/ . Acesso em 3 jul 2021.

Youtube, *Twitter* e *Tiktok*, que também dispõem de grande público nacional. Ainda que nem todos os usuários sejam pessoas físicas, os números corresponderiam a cerca de 60% da população brasileira[460] inserida em pelo menos uma rede social. Tal fato é ainda mais relevante se considerado que o armazenamento de dados por boa parte dessas redes ocorre fora do território nacional. Com isso, embora o Brasil já disponha de legislação sobre temas cibernéticos, não é possível ter certeza de que os agentes públicos terão acesso aos dados coletados no país, pois a efetividade da jurisdição brasileira pode ser prejudicada pela existência de normas estrangeiras com previsões em contrário. Chega-se a um cenário em que delitos são cometidos, mas as autoridades encontram obstáculos à aplicação da lei brasileira.

Ao longo da pandemia de Covid-19, houve aumento em aproximadamente 80% nas tentativas de golpes *online*, de acordo com a Federação Brasileira de Bancos (FEBRABAN)[461]. Dados divulgados pelo PROCON-SP indicam que houve aumento de 186% em golpes contra usuários de aplicativos de entrega entre janeiro e maio de 2021[462]. Esses delitos pressionam ainda mais os agentes penais brasileiros a encontrarem

[460] IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. População do Brasil. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/box_popclock.php . Acesso em 4 jul 2021.

[461] GONÇALVES, Antonio Baptista. Aumento dos crimes cibernéticos com a pandemia da Covid-19. Estadão, 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/aumento-dos-crimes-ciberneticos-com-a-pandemia-da-covid-19/ . Acesso em 3 jul 2021.

[462] GRANDI, Guilherme. Golpes por aplicativos de delivery crescem 186% em cinco meses, saiba como se proteger. Gazeta do Povo, 2021. Disponível em: https://www.gazetadopovo.com.br/bomgourmet/mercado-e-setor/golpes-aplicativos-delivery-pandemia/ . Acesso em 3 jul 2021.

soluções efetivas para os crimes cibernéticos com frequência ascendente no país. Parte dessa resposta encontra-se na busca por cooperação jurídica internacional**.**

A Convenção de Budapeste ou "Convenção sobre o Cibercrime" completa, em 2021, vinte anos de entrada em vigor para seus signatários[463]. É, até hoje, o único instrumento juridicamente vinculante (*legally binding*) sobre o assunto e, por isso, serve como parâmetro para legislações nacionais que tratem do tema[464]. O Ministério Público Federal admite que, dada a ausência de outros instrumentos multilaterais de combate a crimes cometidos internacionalmente, a Convenção de Budapeste acaba por tornar-se referência[465]. Diferentemente de outras normas sobre cooperação internacional, o decurso do tempo não tornou a Convenção obsoleta, ainda que já existam propostas de aprimoramento de seus dispositivos[466].

---

[463] CONSELHO DA EUROPA. Convention on Cybercrime, 23 de novembro de 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Acesso em 20 jun 2021.

[464] Idem. Budapest Convention, 2021. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em 20 jun 2021.

[465] Idem. Convenção de Budapeste (trad português). Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?-documentId=09000016802fa428 . Acesso em 20 jun 2021.

[466] Para algumas críticas à Convenção, cf. NGUYEN, Chat Le. GOLMAN, Wilfred. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Computer Law & Security Review (40) 2021. DOI: https://doi.org/10.1016/j.clsr.2020.105521. RODRIGUEZ, Katitza. Global Law Enforcement Convention Weakens Privacy & Human Rights. Electronic Frontier Foundation. 8 jun 2021. Disponível em: https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights . Acesso em 15 nov 2021. EILBERG, Daniela Dora et al. Os Cuidados com a Convenção de Budapeste. Jota. 8 jul 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privaci-

A Convenção tem caráter inovador em diversos aspectos. Já em seu preâmbulo, atenta para a dualidade existente entre os benefícios e os perigos provenientes das novas tecnologias, sobretudo da *Internet* e do ambiente digital[467]. Além disso, reconhece a necessidade de cooperação com os agentes privados e entre os Estados para a efetividade do processo penal relativo a crimes cibernéticos transnacionais[468]. Tais princípios permanecem atuais ainda que tenha havido mudanças nas formas de interação digital e aumento da complexidade dos delitos cometidos por essa via nas últimas duas décadas. Por sua atualidade, trata-se de documento com notável relevância e cuja adesão não pode ser desconsiderada.

Em dezembro de 2019, o Brasil foi convidado a aderir à Convenção[469]. Tal convite terá validade de três anos e acaba

dade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021. Acesso em 15 jul 2021.

[467] "Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas; Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;" Ibid. preâmbulo, p. 1.

[468] "Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;" Ibid.

[469] SECRETARIA GERAL DA PRESIDÊNCIA DA REPÚBLICA. Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. GOV.BR, 2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica . Acesso em: 25 jun 2021.

de seguir para o Senado Federal[470]. Em que pese já tenha havido debates sobre eventual participação brasileira no tratado, está-se diante do momento mais interessante para analisar a adequação daquelas normas, tendo em vista a possibilidade real de adesão do país. Nesse sentido, o presente trabalho visa a contribuir com a literatura sobre o tema.

1. A CONVENÇÃO DE BUDAPESTE

Apesar de contar com quase 20 anos de vigência, a Convenção sobre o Cibercrime continua a ser um dos instrumentos mais ambiciosos de combate a crimes cibernéticos e de cooperação jurídica internacional nesse âmbito. Trata-se de esforço de harmonização das normas dos Estados com objetivo de favorecer a persecução penal de crimes cometidos no ambiente cibernético.

De acordo com Jonathan Clough[471], a harmonização de normas é importante para (i) evitar os chamados *safe heavens*, ou

[470] BRASIL. Câmara dos Deputados. Mensagem de Acordos, convênios, tratados e atos internacionais nº 412 de 30 de julho de 2020. Texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, com fins de adesão brasileira ao instrumento. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2258985. Acesso em: 21 nov 2021. BRASIL. Senado Federal. Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais nº 255 de 15 de outubro de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258. Acesso em: 21 nov 2021.

[471] CLOUGH, Jonathan. A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonization. Clough, Jonathan, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation (2014). (2014) 40(3) Monash University Law Review, p. 701, Monash University Faculty of Law Legal Studies Research

seja, Estados que não reconhecem como crime determinadas condutas e, por essa razão, obstem a cooperação com outros países, e (ii) para gerar efetiva cooperação entre os Estados. Sem tal esforço, o diálogo entre jurisdições torna-se mais difícil e prejudica a rapidez com que as medidas no ambiente online devem ser tomadas.

A harmonização de normas em âmbito internacional, por sua vez, depende de três requisitos: abrangência (*comprehensiveness*), (ii) garantia de direitos e (iii) representatividade[472]. No que concerne à abrangência, a Convenção contém normas não apenas sobre crimes em espécie, mas também sobre aspectos procedimentais. Na seção II, título 2, tem-se a obrigação de tomar medidas para conservar dados informáticos. Interessa ressaltar que, dado o caráter internacional do tratado, a aplicação de normas como essa não se encerra na jurisdição de determinado Estado, na medida em que os demais optaram por aceitar o documento.

No que diz respeito à cooperação internacional propriamente dita, é possível que a investigação seja levada a cabo por outra parte sem que se lance mão de acordo internacional bilateral[473]. Para tanto, não se exige dupla incriminação[474], um dos obstáculos à cooperação entre Estados. Apesar de utilizar expressões mais genéricas como "auxílio mútuo mais amplo

Paper No. 2015/06, Disponível em: https://ssrn.com/abstract=2615789. Acesso em: 1 jul 2021.

[472] Ibid. p. 698.

[473] Ibid., p. 704. CONSELHO DA EUROPA. Op cit., p. 14. Capítulo III – Cooperação Internacional.

[474] CLOUGH. Op cit., p. 705.

possível"[475], que, em si, não garantem a assistência, o fato de tal previsão estar incluída no documento já induz às partes a conduta mais cooperativa.

A previsão legal de crimes cibernéticos tampouco foi negligenciada pela Convenção. Além de definir infrações penais entre os artigos 2º e 11, o tratado também estabelece que as partes deverão estabelecer jurisdição doméstica sobre tais condutas, a fim de que os responsáveis recebam sanção correspondente[476]. Há, nesse ponto, mais um esforço de dirimir a existência de *safe heavens* para o cometimento de crimes cibernéticos entre os signatários.

A Convenção também garante direitos individuais. O Conselho da Europa, mais antiga organização internacional do continente europeu, tem como prerrogativas a defesa dos direitos humanos, o desenvolvimento democrático e a estabilidade político-social da Europa[477]. O texto do tratado reflete tais preocupações e conta com arcabouço de princípios com vistas a estabelecer parâmetros mínimos de observância às garantias individuais a serem observadas pelas partes. Já no preâmbulo, faz menção direta à Convenção do Conselho da

[475] "As Partes concederão entre si o auxílio mútuo mais amplo possível para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal". CONSELHO DA EUROPA. Op cit. Artigo 25(1), p. 16.

[476] "1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação dos Artigos 2o a 11o sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade." CONSELHO DA EUROPA. Op cit. Artigo 13(1), p.16.

[477] Idem. Conselho da Europa – Quem somos, 2021. Disponível em: https://www.coe.int/pt/web/about-us . Acesso em 1 jul 2021.

Europa de 1981, para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950 e ao Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966. Além disso, a adesão à Convenção é controlada pelos Estados contratantes e pelo Comitê de Ministros do Conselho da Europa[478], a fim de que os parâmetros sejam respeitados por todas as partes.

Embora o tratado não tenha a desejável abrangência global, já foi assinado por 66 países ao redor do mundo, entre eles Argentina, Reino Unido, Israel e Estados Unidos[479]. Na medida em que é a única e mais longeva iniciativa sobre o tema dessa envergadura, a ausência de maior representatividade não é escusável, mas é compreensível. Um impeditivo ao aumento do número de partes é o filtro exercido pelo Comitê de Ministros do Conselho da Europa[480], conforme já mencionado. Outra possibilidade é a legislação doméstica, já que os Estados devem ter leis com parâmetros mínimos que permitam[481] a

[478] "Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no artigo 20o, alínea d), dos Estatutos do Conselho da Europa e por unanimidade dos representantes dos Estados contratantes com direito de voto no Comité de Ministros." Idem. Convenção de Budapeste. Artigo 37(1), p. 23.

[479] Idem. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, 2021. Disponível em: https://www.coe.int/en/web/cybercrime/parties-observers. Acesso em: 20 jun 2021.

[480] CLOUGH. Op cit., p. 724.

[481] "Cada Parte adoptará as medidas legislativas e outras que se revelem

efetivação da norma prevista no tratado. Não por acaso, o Brasil foi convidado a aderir à norma apenas quando a Lei Geral de Proteção de Dados (lei nº 13.709/2018) já tinha sido aprovada.

Apesar de o Brasil já dispor de seus próprios mecanismos para proceder extradição e cooperação internacional, a Convenção pode servir de complemento aos termos da legislação pátria. Problemas como dupla incriminação, necessidade de observância de garantias mínimas de proteção a direitos humanos e busca de relativa representatividade estatal são problemas que acometem diferentes Estados, inclusive o Brasil. Apesar de não resolver plenamente todas as questões, o tratado tenta amenizar as tensões existentes.

2. IMPLICAÇÕES E DESAFIOS

a) Legislação nacional

Atualmente, o Brasil dispõe de alguns mecanismos que buscam facilitar a persecução penal de crimes cibernéticos. Para os fins da presente pesquisa, destacam-se aqui os que se referem a procedimentos em vez da cominação de crimes em espécie.

Em que pese a inviolabilidade de comunicações dos indivíduos, a Constituição da República admite a possibilidade de quebra de sigilo mediante ordem judicial (artigo 5º, XII, CRFB[482]). De acordo com a lei de interceptações telefônicas

necessárias, para instituir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou de procedimento penal." CONSELHO DA EUROPA. Convenção de Budapeste. Artigo 14(1), p. 8.

[482] "Artigo 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no

(lei nº 9.296/96[483]), a referida quebra se estende a fluxos de comunicação telemáticos (artigo 1º, parágrafo único[484]). Os principais responsáveis por cuidar desse fluxo de informações são o Ministério Público (artigo 129, II e IV, CRFB) e a polícia judiciária, mais especificamente, o Delegado de Polícia (Lei 12.830/2013[485]).

O Marco Civil da Internet (lei nº 12.965/2014[486]), em seu artigo 10, estabelece dever de guarda de registros que contri-

último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em 30 jun 2021.

[483] BRASIL. Lei nº 9.296, de 24 de julho de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm . Acesso em 3 jul 2021.

[484] "Artigo 1º, parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática." BRASIL. Lei nº 9.296, de 24 de julho de 1996, artigo 1º, parágrafo único.

[485] BRASIL. Lei nº12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm . Acesso em 15 jun 2021.

[486] "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º." BRASIL. Lei nº 12.965, de 25 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em 20 jun 2021.

buam para a identificação dos usuários ou do terminal utilizado. Para que esse armazenamento ocorra, exige-se ordem judicial (artigo 10, §1º) e sempre preservar a intimidade, a vida privada, a honra e a imagem das partes (artigo 10, caput).

A Lei Geral de Proteção de Dados (lei nº 13.709/2018), em seu artigo 3º[487], estabelece sua aplicação a pessoas jurídicas de direito público ou privado, independentemente do país sede da empresa ou do local em que os dados estejam armazenados, desde que a operação de tratamento ou coleta tenha sido feita em território nacional ou que o serviço seja prestado em território nacional. Sendo assim, reconhece a jurisdição brasileira mesmo nos casos em que o componente internacional se apresenta na localização dos dados e/ou da pessoa física ou jurídica responsável por sua guarda.

Embora observada por diversas plataformas, a prática de interceptação e armazenamento de determinadas informações encontra dificuldades a depender da tecnologia empregada. O aplicativo *WhatsApp*, por exemplo, apenas armazena as

[487] "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;

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional". BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em 15 jun 2021.

conversas dos usuários com criptografia ponta a ponta[488], o que inviabiliza a interceptação dos diálogos. Por outro lado, há empresas que simplesmente não dispõem de personalidade jurídica no Brasil, de modo que os dados não podem ser obtidos via obrigação legal, apenas por meio de cooperação jurídica internacional.

Além disso, em que pese a extensão da aplicabilidade da lei brasileira a outros territórios, não se pode esquecer que os demais Estados também têm suas próprias normas de armazenamento e transferência de dados. Desse modo, as normas brasileiras não necessariamente serão aplicáveis. Para que sejam eficazes, sobretudo num processo judicial, o acesso a esses dados possivelmente dependerá de cooperação jurídica internacional. Nesse contexto, a Convenção de Budapeste pode servir ao auxílio dos agentes públicos brasileiros, sobretudo quando não houver acordo bilateral estabelecido ou quando esse acordo carecer de menção ao ecossistema digital.

b) Cooperação entre os Estados

O Brasil tem Acordos de Assistência Mútua em Matéria Penal (MLAT, em inglês) firmados até o momento com 21 países[489], cerca de apenas 10% das nações do mundo. Desses, apenas oito datam da última década. Isso leva a crer que, mesmo nos países com os quais o Brasil tem buscado aproximação jurídica,

[488] WHATSAPP. About end-to-end encryption. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en . Acesso em 20 jun 2021.

[489] BRASIL. Ministério da Justiça e Segurança Pública. Acordos bilaterais em matéria penal. Disponível em: https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais/acordos-bilaterais-1 . Acesso em 30 jun 2021.

os documentos estão desatualizados, dadas as transformações pelas quais as tecnologias passaram e o próprio entendimento sobre os rumos da jurisdição penal no ambiente cibernético.

O acordo firmado com os Estados Unidos[490], por exemplo, um dos países que mais abriga servidores de empresas com funcionamento no Brasil, não tem nenhum dispositivo específico sobre crimes cibernéticos ou obtenção de dados nessas condições. Tal incompletude, compreensível pela data de ratificação do acordo (2 de maio de 2001), já não é mais aceitável na atual situação do avanço tecnológico[491].

Além da natural obsolescência sofrida pelos MLATs ao longo dos últimos anos, a possibilidade de aplicação fora judicializada e segue pendente de julgamento. A Ação Direta de Constitucionalidade (ADC) 51[492] tem por objetivo confirmar a constitucionalidade de mecanismos de cooperação internacional vigentes no Brasil, em especial do Decreto no 3.810, de

[490] BRASIL. Decreto nº3.810, de 2 de maio de 2001. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm . Acesso em 29 jun 2021

[491] Sobre esse ponto, cf. GUIDI, Guilherme. B. C. REZEK, Francisco. Crimes na Internet e Cooperação Internacional em Matéria Penal entre Brasil e Estados Unidos.Guilherme Berti de Campos Guidi, Francisco Rezek. DOI: doi: 10.5102/rbpp.v8i1.5130. Acesso em 1 jul 2021.

[492] BRASIL. Supremo Tribunal Federal. Ação Direta de Constitucionalidade 51. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - ASSESPRO Nacional. Relator: Ministro Gilmar Mendes. Disponível em: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5320379. Acesso em 15 nov 2021.

2 de maio de 2001, que dispõe sobre o acordo entre Brasil e Estados Unidos. Em que pese haja relativo consenso sobre a adequação dos MLATs ao texto constitucional, o modelo adotado pelo Brasil sofre críticas[493] quanto à celeridade e adaptação às novas demandas do Poder Judiciário frente às plataformas. Faltaria, portanto, ponto de equilíbrio que reconhecesse os MLATs sem inviabilizar processos judiciais por de meses, ou mesmo anos, até o cumprimento dos acordos.

Nessa perspectiva, a Convenção de Budapeste pode ser útil. Embora o texto também seja de 2001, a possibilidade de auxílio mútuo e de informação espontânea pelas partes contribuiria para a celeridade de procedimentos de cooperação[494]. Aplicada conjuntamente aos acordos bilaterais, incrementaria as ferramentas à disposição dos Estados sem prejuízo da constitucionalidade dos MLATs. A própria Convenção prevê aplicação complementar entre Estados que já disponham de acordos bilaterais (artigo 39), facilitando a atualização necessária de diversas previsões dos MLATs em vigor.

Conforme já mencionado, o tratado pode ajudar nas tratativas do Brasil com Estados com os quais ainda não tenha acordos dessa natureza, facilitando o processo de obtenção de informações. A partir desse primeiro contato, também é possível que haja reforço positivo para que acordos em ní-

[493] SOUZA, Carlos Affonso. PERRONE, Christian. 'Fake news' e acesso a dados armazenados no exterior. Jota. 30 jun 2020. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020. Acesso em 21 nov 2021.

[494] Idem.

vel bilateral sejam firmados, o que fortaleceria o arcabouço jurídico brasileiro de cooperação.

A própria Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020) reconhece (i) como uma das ações estratégicas do Brasil o aumento da cooperação internacional do Brasil nesse âmbito (ponto 2.3.8); (ii) a necessidade de ampliar os meios de compartilhamento de informações por vias mais institucionalizadas e de forma integrada, permitindo ação estratégica do país quanto ao tema[495]. Nesse sentido, por contribuir para a efetividade dessas orientações, a adesão à Convenção também parece oportuna.

c) Ponto de partida para acordo multilateral

Em maio de 2021, a Assembleia Geral das Nações Unidas aprovou resolução com parâmetros para a negociação de tratado sobre crimes cibernéticos[496]. O fato de o Brasil começar a ter experiência em tratados multilaterais sobre o assunto pode auxiliar a que o país seja protagonista nas negociações de tratado com maior representatividade e possa apresentar suas experiências domésticas para o mundo.

Ao longo das discussões, o tema da representatividade na elaboração do texto já foi citado. Isso porque o esboço

[495] BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm . Acesso em 1 jul 2021.

[496] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations. 26 mai 2021. Disponível em: https://www.un.org/press/en/2021/ga12328.doc.htm . Acesso em 30 jun 2021.

de texto partiu de iniciativa russa e estadunidense sem expressiva participação dos representantes dos demais Estados. Nos trâmites internacionais, em que cada palavra pode ter impactos importantes na forma como as normas serão aplicadas pelos países[497], o baixo grau de interferência de outros países é notável. A participação brasileira nesse âmbito é importante para que não apenas os interesses pátrios sejam respeitados, mas também aqueles dos demais países em desenvolvimento.

Não por acaso, delegados da União Europeia, por exemplo, já manifestaram preocupação com o fato de que a tramitação não consensual dessa resolução pudesse levar, no futuro, a aumento da polarização, inviabilizando o sucesso de eventual documento final proposto pelas Nações Unidas[498]. O Brasil, nesse contexto, logrou êxito em aprovar a votação das propostas por dois terços dos membros do Comitê[499], com objetivo de não permitir o travamento das negociações.

Apesar de ter conseguido aprovar a emenda à resolução, o país não conta com representantes no Comitê Ad Hoc para elaborar a Convenção Internacional sobre uso de tecnologia da Informação e das Comunicações para fins Criminais. A expertise adotada pelo Brasil com eventual adesão à Convenção de Budapeste pode ajudar o Estado a se posicionar nas próximas vezes que o tema vier a ser discutido na Assembleia Geral ou mesmo para subsidiar as posições de países do

[497] DIPLO. Language and Diplomacy, 2021. Disponível em: https://www.diplomacy.edu/language . Acesso em 26 jun 2021.

[498] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Op cit.

[499] Ibidem.

GRULAC (*Group of Latin American and the Caribbean*) que compõem o Comitê.

d) Problema do acesso a dados armazenados fora do território permanecerá

Apesar de contemplar diversas previsões para acelerar o acesso a dados, a Convenção não elimina completamente os trâmites necessários à sua obtenção. O artigo 32 da Convenção trata do chamado *transborder access* (acesso transfronteiriço)[500]. Segundo essa previsão, os dados poderiam ser disponibilizados sem autorização do outro Estado-parte quando (i) forem acessíveis ao público ou (ii) houver consentimento voluntário de pessoa legalmente autorizada a divulgar tais informações. Em outras palavras, no caso de um processo criminal, o próprio acusado ou pessoa jurídica autorizada deveria consentir com a liberação dos dados.

As disposições interpretativas sobre o artigo 32b[501] indicam que o dispositivo tem previsão limitada e que as partes são encorajadas a buscar os recursos existentes de cooperação

[500] "Uma Parte pode, sem autorização de outra Parte:

[a)] Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou

[b)] aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático." CONSELHO DA EUROPA. Convenção de Budapeste. Artigo 32, p. 21-22.

[501] CONSELHO DA EUROPA. T-CY Guidance Note # 3 Transborder access to data (Article 32), 3 dez 2014, p.4. Disponível em: https://rm.coe.int/16802e726a . Acesso em 25 jun 2021.

internacional. O artigo seria aplicado, por exemplo[502], no acesso a e-mail pessoal armazenado em servidor fora do território por um provedor de serviços. Outra possibilidade seria de o acusado consentir que a polícia tivesse acesso a seu celular ou *tablet* mesmo que as informações de sua conta estivessem armazenadas em servidor fora do território nacional. Nas demais hipóteses de acesso a dados, o recurso ao artigo 32b deveria ser evitado. Sendo assim e em respeito às soberanias nacionais, persistirá a necessidade de tramitar o pedido perante outra jurisdição.

De todo modo, a Convenção visa a reduzir o tempo de resposta desse processo. O artigo 31 promove o recurso ao auxílio mútuo para obtenção de dados. Segundo esse dispositivo legal, as partes devem dar satisfação acerca do pedido feito pelos demais Estados. Quando houver risco de perda ou modificação dos dados, o pedido deverá ser satisfeito o mais rápido possível.

O artigo 29, por sua vez, indica que é possível requerer a conservação de dados armazenados no território da outra parte sem que se exija a dupla incriminação. Em contextos tributários, por exemplo, sabe-se que o instituto da dupla incriminação é um dos grandes obstáculos à cooperação[503]. Sendo assim, ainda que o armazenamento e a entrega dos dados não sejam obrigatórios às partes, a redação dos artigos promove esse

[502] Ibidem, p. 4.

[503] RAMOS. Samuel E.F. A Lavagem de Dinheiro Por Meio De Paraísos Fiscais Como Crime Transnacional: A Cooperação Internacional Na Recuperação De Ativos. Revista Jurídica da Escola Superior de Advocacia da OAB-PR. 4(2), out. 2019, p. 57. Disponívem em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/10/revista-esa-10-cap-06.pdf. Acesso em 25 jun 2021.

comportamento mais colaborativo entre os Estados e pode facilitar eventual negociação bilateral.

Dessa forma, a adesão ao tratado não deve ser vista como resolução de "todos os problemas" relativos a conflitos de jurisdição, mas parece ser alternativa viável a melhorar a forma como essas questões são tratadas no Brasil.

e) Tramitação do tratado em âmbito doméstico

Conforme indicado anteriormente, o convite à adesão do Brasil tem validade de três anos. Ao longo desse período, o país terá prioridade em programas de capacitação na área de segurança cibernética fornecidos pelo Conselho da Europa[504]. Trata-se de oportunidade ímpar para desenvolver o ecossistema securitário do Brasil nesse âmbito e aumentar o número de agentes capazes de lidar com as questões complexas que concernem o ambiente cibernético.

A adesão encontra, no entanto, obstáculos na burocracia brasileira. Tratados e convenções internacionais em geral adotam o modelo multifásico de internalização[505]. Sendo assim, não basta que o Presidente da República assine o tratado

[504] CONSELHO DA EUROPA. Budapest Convention: Brazil invited to acede. Disponível em: https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede. Acesso em: 20 jun 2021

[505] BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. A Internalização dos Tratados Internacionais no Brasil. In: Cooperação em pauta. ISSN 2446-9211. n. 51. Maio 2019. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiDquv-FwrjxAhVwH7kGHZKTDOcQFjAAegQIAhAD&url=https%3A%2F%2Fwww.justica.gov.br%2Fsua-protecao%2Flavagem-de-dinheiro%2Finstitucional--2%2Fpublicacoes%2Fcooperacao-em-pauta%2Fcopy3_of_CooperaoemPautaMaio2019.pdf&usg=AOvVaw2ete5Z5Hh0szyFnBD8hI-T. Acesso em 20 jun 2021

para que se configure sua validade em território nacional. Ao contrário, o documento deve ser chancelado pelas Comissões da Câmara dos Deputados, notadamente a Comissão de Constituição, Justiça e Cidadania (CCJC) e a Comissão de Relações Exteriores e Defesa Nacional (CREDN), bem como pelo próprio Plenário da referida casa legislativa. Posteriormente, deverá tramitar no Senado Federal em Comissões homólogas. Apenas após a aprovação nas duas instâncias legislativas, o projeto será levado à sanção presidencial e será publicado no Diário Oficial da União (DOU). Caso não haja nenhuma outra previsão, o tratado só terá vigência em território nacional 45 dias após a publicação no DOU.

O já complexo procedimento encontra desafios ainda maiores no contexto fático. Diversas mensagens presidenciais deixam de ser analisadas por anos nas Comissões das casas do Congresso Nacional. Além disso, mesmo após a aprovação do Decreto Legislativo, pode haver demora na publicação do texto no Diário Oficial. Exemplo disso é a Convenção de Viena sobre Sucessão de Estados em Matéria de Tratados. O texto fora aprovado em 28 de novembro de 2018 no Congresso Nacional, por meio do Decreto Legislativo n. 166/2018. Meses depois, em 7 de fevereiro de 2019, o governo brasileiro ratificou o tratado, de modo que o Brasil passou a poder ser responsabilizado internacionalmente por eventual descumprimento. A publicação no DOU ocorreu apenas em 30 de janeiro de 2020, ou seja, quase um ano depois. A Convenção de Viena sobre Direito dos Tratados, documento de vigência quase universal, por sua vez, foi levada ao Congresso Nacional em 1992 e aprovada apenas em 2009. A dilação de prazo entre aprovação pelo Congresso, ratificação e vigência em território nacional pode comprometer seja a validade do convite, caso

o Decreto Legislativo demore a ser apreciado, seja a responsabilização internacional do Brasil caso o instrumento tenha sido ratificado pelo país, mas, em razão da não publicação no DOU, as normas não sejam obrigatórias em território nacional.

O cenário, no entanto, é otimista. Em 16 de junho de 2021, a Convenção foi aprovada pela Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados[506]; em 18 de agosto, pela Comissão de Constituição e Justiça e de Cidadania (CCJC)[507]; por fim, em 6 de outubro de 2021, o Plenário da Câmara dos Deputados aprovou o texto[508], que agora segue para o Senado Federal[509]. O Ministério Público Federal tem pressionado a Casa Legislativa para aprovação célere do documento[510]. Caso a mesma presteza se confirme

[506] BRASIL. Câmara dos Deputados. Mensagem de Acordos, convênios, tratados e atos internacionais nº 412 de 30 de julho de 2020. Texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, com fins de adesão brasileira ao instrumento. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2258985. Acesso em: 21 nov 2021.

[507] BRASIL. Câmara dos Deputados. Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais nº 255 de 15 de outubro de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513&ord=1. Acesso em 21 nov 2021.

[508] Idem.

[509] BRASIL. Senado Federal. Projeto de Decreto Legislativo de Acordos, tratados ou atos internacionais nº 255 de 15 de outubro de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258. Acesso em: 21 nov 2021.

[510] CONVERGÊNCIA DIGITAL. MPF pressiona Congresso por Convenção de Budapeste e vigilância online. Convergência Digital. 19 nov 2021. Dispo-

no Senado, é possível esperar que a adoção do tratado seja deliberada em Plenário em 2022, ou seja, dentro do prazo de adesão estabelecido pelo Conselho da Europa[511].

CONSIDERAÇÕES FINAIS

A Convenção é um instrumento abrangente, garantidor de direitos e representativo. É um esforço ambicioso de harmonização legislativa que, embora já tenha mais de duas décadas de vigência, segue importante para a normativa internacional sobre crimes cibernéticos. Apresenta mecanismos que permitem investigação, cooperação internacional e extradição mesmo na ausência de acordos bilaterais sobre o assunto.

A adesão à Convenção de Budapeste pelo Brasil não é certa. Ainda há longo caminho procedimental e político a ser percorrido, seja no âmbito do Poder Legislativo, seja no âmbito do Poder Executivo. Ainda assim, aspectos jurídico-políticos internos e internacionais tornam o processo de adesão oportuno e adequado para o país. Complemento à legislação nacional, atualização dos mecanismos vigentes de cooperação com outros Estados e elevação das credenciais do país para negociar acordos sobre o assunto internacionalmente são apenas alguns dos motivos.

---

nível em: https://www.convergenciadigital.com.br/Internet/MPF-pressiona-Congresso-por-Convencao-de-Budapeste-e-vigilancia-online-58766.html?UserActiveTemplate=mobile. Acesso em 21 nov 2021.

[511] SECRETARIA GERAL DA PRESIDÊNCIA DA REPÚBLICA. Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. GOV.BR, 2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica . Acesso em: 25 jun 2021.

Não é o caso, contudo, de se considerar o referido tratado uma "tábua de salvação" para os problemas existentes no Brasil de cooperação jurídica internacional e, de forma mais ampla, da persecução penal que se relacione com o ambiente *online*. Ainda haverá necessidade não apenas de instrumentos jurídicos, como acordos bilaterais e multilaterais mais abrangentes, mas também do reforço na capacitação dos agentes públicos a fim de que estejam preparados para manejar esses novos mecanismos.

Ao longo dos próximos anos, resta saber se a adesão ocorrerá e, nesse caso, quais serão as efetivas consequências que esse instrumento trará para a realidade brasileira.

ANÁLISE DA TERRITORIALIDADE DE SERVIÇOS EM NUVEM E SUAS IMPLICAÇÕES EM NEGÓCIOS INTERNACIONAIS

Giovanna Bonach Pires Ribeiro[512]

INTRODUÇÃO

O processo de instauração e vigência de leis de proteção de dados pelo mundo é uma grande conquista para a militância de direitos digitais, por prezar pelo empoderamento de titulares de dados, resguardar princípios fundamentais para o respeito à dignidade humana (como princípios da transparência, autodeterminação informativa e controle pelos titulares)[513] e disseminar boas práticas corporativas e educação quanto à segurança da informação. Contudo, cada nação, munida de sua soberania[514], dispõe de seu próprio sistema de normas em sua própria jurisdição e, portanto, uma forma peculiar de tratar sobre o tema de legislação em privacidade.

Uma das pioneiras a abordar sobre o assunto foi a legislação europeia, primeiro com as diretrizes com recomendações em privacidade, e, posteriormente, com o Regimento Geral de Proteção de Dados (GDPR). Porém, apesar de guiar muitas das demais leis concernentes à privacidade que surgiram

[512] Advogada digitalista, com formação em Direito pela Pontifícia Universidade Católica de Goiás, Sistemas de Informação pela Universidade Federal de Goiás e com cursos de extensão em Direito Digital e Direitos Humanos pela ***Université Paris 1 Panthéon-Sorbonne*** e ***London School of Economics***. Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade (ITS Rio), em parceria com a Universidade do Estado do Rio de Janeiro (UERJ). Possui experiência profissional em ***data analytics***, ***compliance***, privacidade e proteção de dados pessoais.

[513] Princípios vistos presentes na Lei Geral de Proteção de Dados, no Brasil; na ***General Data Protection Regulation***, na Europa, e na ***California Consumer Privacy Act***, nos Estados Unidos.

[514] BONAVIDES, Paulo. Ciência política. 10 ed. São Paulo: Malheiros, 2000.

posteriormente no mundo, ainda há peculiaridades e desafios que devem ser discutidos e pacificados.

Diante de uma sociedade pós-industrial em sua fase de informação - ou seja, na qual os serviços amplamente distribuídos, baseados em conhecimento teórico e aplicação generalizada assumem posição central na estrutura econômica, a informação passa a ser eixo principal de desenvolvimento da sociedade[515]. A Cúpula Mundial sobre a Sociedade da Informação (CMSI) concluiu que a Internet seria o ponto medular da sociedade da informação, concentrando a abordagem especulativa à temática das formas possíveis de regulação e governança das redes[516]. Paralelamente (ou até mesmo consequentemente), com a popularização dos serviços em nuvem, há a facilitação um grande fluxo internacional e instantâneo de dados, viabilizando, então, a queda das barreiras entre nações e indivíduos – chega-se a estimar que, em breve, raramente lidaremos com computação chamada tradicional (com armazenamento em máquinas locais – o chamado "*on premise*")[517]. Comumente, este tipo de tratamento por serviços em nuvem é compreendido por doutrinas e jurisprudências como sendo um exemplo de processamento de transferência internacional de dados.

---

[515] BELL, Daniel. O advento da sociedade pós-industrial: uma tentativa de previsão social. São Paulo: Cultrix, 1973.

[516] LUCERO, Everton. Governança da Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: Fundação Alexandre de Gusmão, 2011.

[517] Kommerskollegium, National Board Trade. How Borderless is the Cloud? An Introduction to cloud computing and international trade. Disponível em: https://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/how_borderless_cloud_e.pdf. Acesso em 20 jun. 2021.

Com uma variedade de entendimentos legislativos e implicações de alta complexidade técnica dos serviços de nuvens, o presente artigo possui como principais objetivos, à luz da GDPR e da LGPD, conceituar i) o que seria transferência internacional de dados e ii) o que seria o *Cloud Computing*, suas máquinas virtuais e instâncias; compreender i) como os serviços de nuvem são concebidos juridicamente - se caracterizam como transferências internacionais de dados, de fato e, se forem, como poderiam ser adequados e ii) se, no momento de criação de uma máquina virtual para o servidor das aplicações forâneas, a migração para uma instância na região de destino descaracterizaria a categorização como transferência internacional de dados. Por fim, visa-se analisar as implicações práticas de tais atividades.

Para tal desenvolvimento, tendo em vista a exiguidade de literatura atualizada, a fim de alcançar uma maior familiaridade e abrir oportunidades de estudos futuros, foi estabelecida uma pesquisa exploratória aplicada[518], com revisão bibliográfica acerca dos temas de direito digital, legislações de proteção de dados e acervos técnicos de computação em nuvem.

Desta forma, almeja-se realizar uma análise crítica sobre a aplicação e impacto de leis de proteção de dados na comunicação e cooperação entre entidades estrangeiras, compreendendo se dispositivos legislativos mais protecionistas poderiam impactar negativamente o livre mercado internacional de dados ou se impactariam positivamente com a viabilidade de harmonização da matéria.

[518] GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 5a ed. São Paulo: Atlas, 1999.

1. DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Falar sobre transferência internacional de dados é tratar, também, sobre conceitos críticos e fundamentais do direito internacional. Tópicos como soberania das nações, segurança nacional, proteção aos direitos fundamentais, competitividade do mercado e até mesmo colonialismo digital devem nortear um pensamento crítico acerca do trânsito de informações no meio digital.

Por requerer, na maioria dos casos, um fluxo de dados entre sistemas não originalmente nativos e uma adequação entre requerimentos legislativos estrangeiros, a transferência internacional é uma atividade que inerentemente oferece riscos às liberdades e direitos dos titulares envolvidos no processo, havendo, portanto, de se garantir a proteção aos dados compreendidos neste tratamento.

A seguir, será possível observar uma análise comparativa entre o entendimento previsto pela Lei Geral de Proteção de Dados (LGPD), no Brasil, e a GDPR, na Europa. Insta-se apontar que, observando as mais diversas abordagens legislativas domésticas, é possível identificar que, apesar de diferentes países possuírem diferentes padrões de adequação para a possibilidade de transferência internacional, geralmente se vê um entendimento pacífico quanto a o que seria o conceito de tal prática: um processamento compartilhado de dados pessoais entre diferentes países ou entidade que integram sede baseada em país distinto à origem do dado.[519]

[519] BERRY, Renee; REISMAN, Matthew. Policy Challenges of Cross-Border Cloud Computing. Journal of International Commerce and Economics. United States Internacional Trade Commission, 2012.

1.1. TRANSFERÊNCIA INTERNACIONAL DE DADOS PELA LEI 13.709/18 (LEI GERAL DE PROTEÇÃO DE DADOS)

Apesar de a Internet estar instaurada no epicentro do cotidiano da comunicação humana e de serviços sociais tradicionais desde os anos 1990, é recente a discussão de suas implicações jurídicas: isso se confirma ao observar que as primeiras discussões com o intuito de estabelecer normas de utilização e fornecimento de serviços de Internet foram a partir de 2009, com a elaboração e posterior vigência do Marco Civil da Internet (Lei nº 12.965/2014), em 2014; mais recentemente, viu-se a aprovação e vigência da tão esperada Lei Geral de Proteção de Dados Brasileira.

Por não se tratar de um assunto tão familiar ao direito e aos operadores da matéria, a LGPD possui um notável aspecto didático, o qual pode ser compreendido logo em suas disposições preliminares, que contam com um Glossário (art. 5º). De acordo com tais preceitos, tendo em vista a aplicação da lei por uma perspectiva espacial, a existência de operações fora do Brasil é entendida como transferência internacional de dados, a qual é definida como "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro" (art. 5º, XV) e pressupõe o uso compartilhado de dados[520].

[520] BRASIL. Lei Geral de Proteção de Dados, 2018 - Art. 5º, XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Tendo em vista uma perspectiva possivelmente extraterritorial, observa-se no art. 3º, o qual dispõe as hipóteses taxativas de aplicação da Lei, que a LGPD regulará sempre que "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" (art. 3º, II) ou quando houver coleta de dados no país (art. 3º, III).

Ainda quando da aplicação, segundo o art. 4º, IV da Lei, não se aplica a LGPD em operações "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência".

Ainda, o uso compartilhado de dados com entidades estrangeiras é regido por instruções específicas da Lei, estipuladas por um capítulo inteiro exclusivamente para esta matéria. O Capítulo V, "Da Transferência Internacional de Dados", estipula que tal processamento deverá observar tais regras previstas nos artigos 33 a 36. A evidência do termo "somente" no art. 33 aponta a existência do condicionamento à legitimação de validade de alguma das bases legais elencadas pelos incisos do artigo – a não constatação de tais requerimentos, portanto, inviabilizaria a operação de transferência internacional de dados.

1.2. TRANSFERÊNCIA INTERNACIONAL DE DADOS DE ACORDO COM O REGULAMENTO GERAL EUROPEU SOBRE A PROTEÇÃO DE DADOS 2016/679

Sob a ótica do Direito Comparado, um grande cânone para a análise do direito à proteção de dados pessoais é a General

Data Protection Regulation (GDPR), instituída na Europa em 2018 e que serviu de grande valia para a estruturação de leis protetivas de dados por todo o mundo, incluindo a LGPD. De acordo com o art. 4º do regulamento europeu, há o conceito de "tratamento transfronteiriço" (o chamado "*cross-border processing*"), que determina que as regras que protegem os dados pessoais continuam a aplicar-se independentemente da localização dos dados, nas hipóteses em que "a) o tratamento de dados pessoais ocorra no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou b) O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro", nas palavras do art. 4º, 23[521].

Bem como estipula a lei brasileira, o tratamento transfronteiriço poderá ocorrer desde atendidas as condições taxativas do regimento europeu. A transferência para um organismo internacional fora da União Europeia ou para um país terceiro será viabilizado desde que garantido um nível próprio de proteção, respaldado por decisão da Comissão Europeia[522].

[521] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu. General Data Protection Regulation. Disponível em: https://gdpr-info.eu/. Acessado em 27 jun. 2021.

[522] COMISSÃO EUROPEIA. Que regras se aplicam se a minha organização transferir dados para fora da UE? Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/

Caso inexista decisão da Comissão, a transferência poderá ser realizada quando o Controlador ou Operador do tratamento dos dados propiciar devidas salvaguardas para a privacidade e segurança dos dados envolvidos, nas formas de "*corporate binding rules*" (normas corporativas vinculadoras); cláusulas contratuais padrão pré-determinadas pela Comissão Europeia ou autoridade competente; procedimento válido certificador de conformidade, nos termos do art. 42 da norma europeia; autorizações específicas (a chamada "*derrogation*"), diante de consentimento específico do titular, por exemplo, dentre outros.

No que tange especificamente a matéria de tratamentos internacionais, é possível observar uma distinção entre a normativa europeia e brasileira: a GDPR dispõe, em seu art. 49, exceções para o processamento caso não haja o devido preenchimento das demandas empenhadas nos artigos anteriores. Neste caso, a fim de conter eventuais riscos e danos envolvidos no processo, o tratamento deveria possuir características limitantes, tais como se dar de forma pontual (sem recorrência), refrear o número de titulares envolvidos, dentre outras – que deverão ser informadas à Autoridade de Proteção competente pelos foros jurisdicionais onde ocorrerão o tratamento.

Observando as similaridades de aplicação de ambas as leis, evidencia-se, também, a necessidade de cumprimento de princípios em comum. Tanto pela legislação europeia, quanto pela brasileira, para que qualquer tratamento ocorra (e aqui, inclui-se o tratamento transgeográfico), é imprescindível que se verifique finalidades legítimas, informadas, explícitas e específicas; adequação compatível com a finalidade; necessidade de

obligations/what-rules-apply-if-my-organisation-transfers-data-outside--eu_pt. Acessado em 28 jun. 2021.

limitação ao mínimo de dados necessários; livre acesso pelos titulares; qualidade dos dados, a fim de garantir fidedignidade e distinção; transparência e segurança

2. CLOUD COMPUTING E SEU ENTENDIMENTO PELO DIREITO

2.1. CONCEITOS FUNDAMENTAIS DE *CLOUD COMPUTING*

Como apontado no início do estudo, com o alcance da sociedade da informação, o poder tecnológico permite pessoas comuns e simples a terem acesso a conteúdos antes inalcançáveis. Com a expansão de negócios digitais e acesso a tais serviços e conteúdos, viu-se, também, a necessidade de extensão da capacidade de memória dos servidores, além de amplificar sua distribuição para além dos horizontes onde foram inicialmente produzidos.

Diante disso, a Computação em Nuvem (*Cloud Computing*) se tornou uma opção primordial para desenvolvimento de distribuição de serviços que envolvam tecnologia (o que, no século XXI, se torna praticamente uma regra de negócios. Para uma melhor compreensão do conceito de nuvem, nas palavras do cientista Rajkumar Buyya:

> Nuvem é um tipo de sistema distribuído e paralelo, consistindo em uma coleção de computadores interconectados e virtualizados que são dinamicamente providos e apresentados como um ou mais recursos de computação unificados, baseados no acordo de nível de serviço estabelecido

> pela negociação entre o provedor de serviço e o consumidor.[523]

Portanto, há uma otimização de fornecimento de serviços, oferecendo, portanto, um modelo de negócios cujo destaque se dá pela elasticidade, escalabilidade e liberalidade de nível de serviços. Os serviços são prestados proporcionalmente à solicitação dos seus clientes (pagamento *on-demand*) e, por ter uma possibilidade de encapsulamento como um produto abstrato, é o foco majoritário quando se pensa em economia de larga escala: os custos são bruscamente reduzidos e as configuração são altamente customizáveis, encontrando-se, pois, a tão falada Computação Utilitária[524], na qual apenas se paga pelo que se consome.

A computação em nuvem pode ser dividida em três categorias[525], sendo elas, resumidamente: *Software as a Service* (SaaS), que compreende integralmente a aplicação acessada pela nuvem como o objetivo fim, e é o tipo mais comum no mercado, tendo como exemplo os serviços do Instagram e Microsoft Office; *Platform as a Service* (PaaS), que é um serviço em nuvem que providencia acesso ao ambiente de desenvolvimento em nuvem – portanto, nesta categoria, os desen-

[523] BUYYA, R. Cloud Computing and the emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. Future Generation Computer Systems, v.25, n.6, p. 606, 2011.

[524] ARMBRUST, M. et al. Above the Clouds: A Berkeley view of Cloud Computing. EECS Department, University of California, Berkeley, Tech Rep. UCB/EECS-2009-28, 2009.

[525] RODAMILANS, Charles Boulhosa. Uma Metodologia para Caracterização de Aplicações e de Instâncias de Máquinas Virtuais no Ambiente de Computação em Nuvem. São Paulo, 2014.

volvedores possuem criatividade para customizar softwares e hospedarem seus serviços e dados, sem entrar no mérito dos servidores -, exemplos são Microsoft Azure e Amazon Web Services (AWS). Por fim, há a categoria *Infrastructure as a Service* (IaaS), que fornece funções básicas computacionais virtuais. Nesta última categoria, o usuário paga pelo uso maquinário, uso de rede e pelo tipo de sistema operacional pelo qual optou – exemplos desse serviço são Amazon EC2 e Google Compute Engine (GCE).

Como aponta a citação de Buyya, entende-se "servidor" de nuvem como o grupo de maquinário que possui configurações destinadas a um mesmo objetivo, replicando sua funcionalidade como se fosse apenas uma máquina. Tais maquinários se encontram em um espaço industrial físico, moderno e de espaço limitado para fins exclusivos de processamento de dados e fornecimento de energia para tal, os quais são chamados de *data centers*. Grandes empresas provedoras de *Cloud Services* possuem dezenas de *data centers* em todos os continentes do mundo.

Já as instâncias podem ser compreendidas como os tipos de servidores que executam alguma aplicação ou ordem de serviço. Tanto a instância, quanto o servidor, são de configurações a critério de quem contrata o serviço – a escolha da região onde estarão presentes ou a complexidade do servidor a ser contratado. É como explica Rodamilans:

> Um tipo de instância é um conjunto de recursos computacionais, tais como CPU, memória, armazenamento e rede. A grande variedade de tipos de instâncias permite que se possa escolher qual

> deles é mais adequado para uma determinada aplicação. No entanto, uma vasta possibilidade de tipos de instâncias pode dificultar a seleção precisa. Isto porque um provedor pode fornecer diversos tipos de instâncias, com interoperabilidade entre as Nuvens, e diversos provedores de Nuvem podem ser utilizados. Isto amplia a oferta dos tipos de instâncias (...).[526]

Com tais conceitos compreendidos, tendo em vista a característica essencial do serviço de nuvem de poder otimizar sua capacidade, para tal viabilidade, como citado acima, muitas vezes é necessário mover a aplicação dentre diferentes servidores, a depender do local disponível para o armazenamento. Desta forma, mesmo que o cliente tenha optado por uma região específica para a hospedagem do servidor, para uma otimização da prestação do serviço da Nuvem, o provedor poderá mover para outra localização (outro país ou até mesmo outro continente) ao longo de tal tratamento. Desta forma, corre-se o risco de, sem mesmo ter conhecimento sobre isso, o cliente da nuvem estar sujeito a responder por leis estrangeiras, independentemente de onde optou por hospedar suas informações.[527]

Além disso, a fim de reforçar a segurança das informações retidas em nuvem e se prevenir de eventuais incidentes, vê-se a redundância como uma prática comum no mercado. Para conseguir garantir que o serviço não será interrompido em caso de incidentes - como se viu, por exemplo, no incêndio

[526] RODAMILANS, Charles Boulhosa. Ibidem. 2014.

[527] Kommerskollegium, National Board Trade. Ibidem. 2013.

do maior data center da França[528] -, não basta apenas realizar backup dos arquivos e dados contidos em nuvem. É necessário duplicar os dados presentes em um data center para outro, garantindo, portanto, que o que eventualmente afetar um dos data centers, não afete o outro – mantendo a cópia da instância acessível e segura[529]. Comumente, a redundância é realizada em servidores hospedados em data centers internacionais, incorrendo novamente o risco de aplicação de leis estrangeiras.

2.2. CATEGORIZAÇÃO DE SERVIÇOS DE NUVEM PELA PERSPECTIVA JURÍDICA DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Tendo os conceitos técnicos de serviços de nuvem esclarecidos, apreende-se que é possível determinar a região na qual a instância do servidor será localizada territorialmente; contudo, como exposto no final do capítulo anterior, há o risco de ocorrer realocações extraterritoriais de instância sem a aquiescência do contratante, seja para garantia de qualidade do serviço, seja para garantia de segurança. Com isso, fica a dúvida: serviços de Cloud Computing são, como regra, transferências internacionais de dados? Como o direito os categoriza?

Em 1996, no Fórum Econômico Mundial de Davos, o ativista político cyberlibertário John Perry Barlow publicou a emble-

[528] REUTERS. Millions of websites offline after fire at French cloud services firm. Paris, 2021. Disponível em: https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU. Acesso em 18 jun. 2021.

[529] CARVALHO, Tereza Cristina M.; GONZALEZ, Nelson M.; MIERS, Charles C.; REDÍGOLO, Fernando F.; ROJAS, Marco Antônio. Segurança das Nuvens Computacionais: Uma Visão dos Principais Problemas e Soluções. Revista USP, ed. 97. São Paulo, 2013.

mática Declaração de Independência do Cyberespaço[530], o qual preza pela não-intervenção estatal e consequente liberdade e anarquia no meio digital. No mesmo sentido, um dos diferenciais dos serviços em nuvem é a sua intangibilidade e flexibilidade, exatamente por não depender de um local físico específico para a prestação de um serviço final. Logicamente, há a necessidade de instalação de data centers físicos para a hospedagem de tais atividades - porém a realocação entre diferentes servidores ficaria a critério do provedor do serviço de nuvem, com o fim de fornecer um serviço de maior qualidade e rapidez. Isso quer dizer que a transparência de localidade nem sempre é garantida para o cliente final, o contratante do serviço.

A premissa diferencial serviços de hospedagem e fornecimento de aplicações em nuvem é exatamente o que se enfocou anteriormente: um fluxo globalizado de dados que perpassa qualquer barreira territorial e nacional. Isto posto, tal modelo de negócio é usualmente um exemplo unânime de transferência internacional de dados – essa perspectiva é vislumbrada não apenas em análises de especialistas[531] do tema, mas o próprio *Information Commissioner's Office* britânico cita tal constatação em documentos oficiais[532].

---

[530] BARLOW, John Perry. MERLO, Rafael Augusto Arruda Merlo (tradução). Uma Declaração da Independência do Ciberespaço. Davos, 8 fev. 1996. Disponível em < https://bit.ly/3hd2dXB>. Acessado em 29 jun. 2021.

[531] SAHOO, Narendra. Impact of GDPR on Cloud Service Providers. The State of Security Magazine, 2021. Disponível em: https://www.tripwire.com/state-of-security/security-data-protection/cloud/impact-of-gdpr-on-cloud-service-providers/. Acessado em 29 jun. 2021.

[532] INFORMATION COMMISSIONER'S OFFICE. International Data Transfer. 2021. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-

Uma questão chave para a compreensão é a disposição, por parte dos provedores de serviços, se a realocação extra-territorial de instâncias de nuvens é compulsória, a partir do momento que se contrata o fornecimento, ou facultativa, a critério do contratante. Tal dúvida pode ser sanada por meio da leitura das Políticas de Privacidade (documentos fundamentais para a transparência da forma de oferecimento de serviços e gerenciamento de configurações de privacidade) das principais empresas de nuvem, dentre elas, Amazon Web Services, Microsoft Azure e Google Cloud:

> [Dentre as 40 políticas analisadas] Cerca de um quarto sustenta que o consumidor poderia escolher a localidade do data center onde seus dados estariam armazenados. Outras políticas, como a da Cisco, por exemplo, constatam que os dados do consumidor poderão ser armazenados globalmente ou onde quer que o provedor opere.[533]

Desta forma, visualiza-se que, dentre as ofertas de alguns provedores, há a possibilidade de escolha por parte do usuário.

Seria possível, na hipótese de que houvesse a escolha de instâncias nacionais (no país no qual o serviço está sendo contratado) e, na política de privacidade do provedor constasse

-ended/the-gdpr/international-data-transfers/. Acessado em 27 jun. 2021.

[533] TURTON, Felicy; KAMARINOU, Dimitra; MICHELS, Johan D.; MILLARD, Christopher. Privacy in the Clouds, Revisited: An Analysis of the Privacy Policies of 40 Cloud Computing Services. Queen Mary Law Research Paper No. 354/2021. Londres, 2021. Disponível em: https://bit.ly/3xgTOYZ. Acessado 27 de jun. 2021.

que a localização ficaria apenas a critério da configuração estabelecida pelo consumidor, que a transferência internacional de dados pelo serviço de nuvem estaria descaracterizada?

Voltando à interpretação pacificada já citada no primeiro artigo do presente trabalho, transferência internacional de dados seria "um processamento compartilhado de dados pessoais entre diferentes países ou entidades que integram sede baseada em país distinto à origem do dado". Na hipótese levantada acima, a sede dos provedores de serviço seria dada pelos data centers nos quais estariam hospedados os dados, não havendo, portanto, um processamento compartilhado por países distintos. Desta forma, é possível inferir que há exceções à análise da territorialidade e processamento de dados em serviços de nuvem.

Contudo, a "mera" escolha de região em configurações de nuvem implica em questões mais complexas, dentre elas, os riscos da determinação fixa de localidade. Apesar de possível, tal limitação fere o diferencial do serviço[534] e abre precedentes para possíveis insânias legislativas, as quais poderiam impedir parcerias estrangeiras e até mesmo o livre fluxo comercial internacional, como ocorre com o conceito de servidores *Europe-only*[535]: nesta conjectura, serviços prestados na Europa

[534] "Localization requirements are problematic for cloud providers, as "location independence" is a core aspect of the cloud delivery model.48 Policies that require providers to locate facilities in a given location may leave them with the choice of selecting a sub-optimal location or not serving the targeted market at all." (BERRY; REISMAN, 2012).

[535] SINGH, J.; BACON, J.; CROWCROFT, J.; MADHAVAPEDDY, A.; PASQUIER, T.; HON, W.; MILLARD, C. Regional clouds: technical considerations. Centre for Commercial Law Studies, Queen Mary University of London. Londres, 2014. Disponível em: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-863.pdf. Acessado em 30 jun. 2021.

poderiam apenas estar hospedados em servidores europeus, sem comunicação estrangeira. Tal ideia, além de contradizer a legislação europeia (haja vista que a GDPR estabelece condições para que dados pessoais sejam transferidos para fora da EEA, e não requer obrigatoriamente o armazenamento físico nacional de tais dados), não necessariamente reforçará a segurança e proteção dos dados objetos do produto, além de criar potenciais barreiras econômicas e legislativas[536].

Um exemplo complexo, mas mais palpável da discussão de configuração de instâncias e limitação transfronteiriça é a utilização do Research Electronic Data Capture (REDCap) por instituições estrangeiras. Tal sistema é uma aplicação online, desenvolvida pela Universidade Vanderbilt (EUA) voltada para a captura de dados para a pesquisa clínica e criação de bases de dados para estruturação de projetos[537]. Diante do êxito em desenvolvimento de pesquisas, o sistema passou a ser utilizado por grande parte das pesquisas clínicas em instituições de ensino e pesquisa em saúde pelo mundo – mas encontra grandes empecilhos técnicos e comunicacionais.

Por ter sido desenvolvido nos Estados Unidos, o servidor de nuvem do sistema se encontra em território estadunidense: isso significa que, quando uma universidade brasileira for utilizar, por exemplo, por ter como objetivo o oferecimento de serviço

[536] HON, Kuan W.; MILLARD, Christopher; REED, Chris; SINGH, Jatinder; WALDEN, Ian; CROWCROFT, Jon. Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Legal Studies Research Paper 191/2015. Queen Mary University of London. Londres, 2015.

[537] PATRIDGE, Emily; BARDYN, Tania. Research electronic data capture (REDCap). Journal of the Medical Library Association. 106. 10.5195/JMLA.2018.319. Nashville, 2018. Disponível em: https://cutt.ly/ymlbW5h. Acessado em 30 jun. 2021.

de pesquisa para brasileiros, a LGPD se aplicaria e, portanto, seria realizada uma transferência internacional de dados. Até então, não haveria dificuldades, haja vista que o processo para tal tratamento já é regulado pela lei e, portanto, factível.

Contudo, é indiscutível a necessidade e importância de colaboração internacional para o desenvolvimento de soluções em saúde e fortalecimento da ciência, como aponta o relatório atual da UNESCO[538]. Tendo em vista o tratamento de dados sensíveis pelo sistema (de acordo com o art. 5º, II, da LGPD e art. 9º, I, da GDPR, por serem relativos à saúde), o servidor estar fisicamente no território estadunidense e a pesquisa ser realizada em outra universidade estrangeira, há obstáculos técnicos para pesquisas que envolvam pacientes europeus, por exemplo, de forma que garantisse o *compliance* das leis aplicáveis aos processos. Desta forma, muitas universidades acabam recomendando pesquisas com dados anonimizados ou até mesmo alertas de alinhamento com a GDPR, de forma a evitar infrações às normas de proteção de dados estrangeiras (principalmente a europeia) – como se vê pelo posicionamento, por exemplo, das diretrizes da Universidade de Melbourne[539], Cambridge[540] e do Instituto de Pesquisa Clínica de Oregon[541].

---

[538] UNESCO. Science Report: the race against time for smarter development. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000377250. Acessado em 30 jun.2021.

[539] MELBOURNE UNIVERSITY. REDCap at the University of Melbourne. Disponível em: https://clinicalresearch.mdhs.unimelb.edu.au/about/health-informatics/redcap. Acesso em 30 jun. 2021

[540] UNIVERSITY OF CAMBRIDGE. The Cambridge Integrated Data Environment. Disponível em: https://www.ide-cam.org.uk/ethics-grants-submission-help/. Acesso em 26 jun. 2021.

[541] OREGON CLINICAL AND TRANSLATIONAL RESEARCH INSTITUTE. REDCap: Your Complete Solution for Online Databases and Surveys for Research.

Assim, vê-se evidentes restrições em cooperações acadêmicas internacionais.

CONSIDERAÇÕES FINAIS

A tecnologia de nuvem permite o crescimento sustentável, flexível, livre e autônomo por permitir interação mundializada entre entidades governamentais, empresas, consumidores e provedores do serviço. O que hoje é investido e desenvolvido nesta matéria poderá ter grandes consequências – positivas ou negativas – no futuro da diplomacia, comércio exterior e da economia global. Para compreender a percepção jurídica da territorialidade da tecnologia de nuvem, o presente estudo primeiramente procurou conceituar o que seria a transferência internacional de dados pessoais pelo direito brasileiro e pelo direito europeu, elencando pontos em comum e discrepantes de tais entendimentos.

Viu-se que há uma definição similar com relação ao tratamento internacional, que se dá com o manuseio compartilhado de dados entre países distintos; contudo, cada sistema jurídico possui requerimentos específicos para que tal processo seja viabilizado. As disparidades entre a LGPD e a GDPR são quanto às hipóteses em que as leis são aplicadas e exigências de conformidade para a execução da transferência. Ainda, foi possível observar similaridades entre as leis no que tange aos princípios a serem obrigatoriamente seguidos.

Em segundo lugar, observou-se que *cloud computing* é um serviço de amplitude global, que se dá de forma virtualizada,

Disponível em: https://www.ohsu.edu/octri/redcap-your-complete-solution-online-databases-and-surveys-research. Acesso em 26 jun. 2021.

elástica e paralela, por meio de máquinas virtuais distribuídas por instâncias em data centers físicos – mas a comunicação entre tais espaços se dá de forma fluida e global. Tais serviços de nuvem são, na generalidade, entendidos como transferências internacionais de dados; mas, com a configuração fixa de localidade no momento da criação da máquina virtual, é possível descaracterizar tal procedimento, tornando a operação sujeita apenas à lei doméstica de proteção de dados (se houver).

Por fim, foi possível observar que, por mais que tanto os serviços de nuvem, quanto as leis de garantia de segurança de dados sejam positivas para o desenvolvimento de tecnologias em larga escala de forma sustentável e que assegure direitos humanos, as implicações práticas da regionalidade em configurações de nuvens e legislações excessivamente protetivas a nível local podem ser negativas. Para exemplificar tal colocação, citou-se as complicações na interação estrangeira no uso do principal software de pesquisa clínica, o REDCAP.

Sem entrar em méritos mais específicos que se relacionam com comunicações de conteúdos estrangeiros, como censura de internet, matérias de propriedade intelectual ou comércio internacional, observando as implicações que a técnica da computação em nuvem levanta, uma possibilidade para a viabilização do uso de tais serviços a nível global seria a harmonização de orientações e padronização de fornecimento de nuvens, por meio de acordos globais. Um modelo de orientação é visto na ISO (*International Organization for Standardization*), organização responsável por normalização de pautas técnicas, a qual chegou a estabelecer um comitê

de estudos para a padronização do Cloud Computing[542] – o objetivo, nesta oportunidade, era dialogar quanto aos desafios enfrentados pela matéria.

Além disso, o diálogo para a pacificação de desafios e legislações não deveria partir apenas entre nações, mas também entre empresas que ofereçam esse tipo de serviço, a fim de que se garanta um compartilhamento estruturado de boas práticas. A interação estruturada, transparente e colaborativa entre agentes de poder poderá garantir um mundo interconectado mais equilibrado e sustentável.

[542] ISO/IEC JTC 1/SC 38. Cloud computing and distributed platforms. Disponível em: https://www.iso.org/committee/601355.html. Acesso em 01 jul. 2021.

A DESINFORMAÇÃO DOS IDOSOS NA INTERNET E O DEVER DE ATUAÇÃO ESTATAL

Victor Hugo Lameira da Silva[543]

INTRODUÇÃO

Vivenciamos um momento único, em que a sociedade se expõe e recorre de forma exponencial ao uso da internet. Esta, notoriamente após chegar aos celulares, se tornou o principal meio de informação de grande parte da sociedade. Contudo, se antes tínhamos meios de informações minimamente regulados com níveis de confiabilidade razoáveis, com o advento da internet, toda e qualquer pessoa, física ou jurídica, pode tornar-se uma fonte primária de informação. Nos tempos atuais, para transmitir ou divulgar uma notícia, basta acessar uma conta em uma rede social ou um aplicativo de celular e postá-la para atingir outros usuários da rede, restando quase impossível definir de imediato o alcance que tal notícia terá.

A ampliação das liberdades de expressão e de informação presentes na internet é apenas uma das faces que a facilidade de comunicação nas redes trouxe para nossa sociedade. Em outro viés, a internet facilitou também a disseminação de fatos e notícias falsas, que não refletem a verdade ou mesmo tiradas de contexto, de modo a dissimular situações inexistentes. Este grupo de comunicações e informações falsas, não verdadeiras

[543] Victor Hugo Lameira da Silva é Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ) e pós-graduando em Direito Digital no Instituto de Tecnologia e Sociedade do Rio de Janeiro da UERJ. O presente artigo foi apresentado ao Instituto de Tecnologia e Sociedade do Rio de Janeiro e à Faculdade de Direito da Universidade do Estado do Rio de Janeiro como requisito para conclusão do Módulo I: Direito Digital e Inovação no Setor Público no âmbito de avaliação da pós-graduação em Direito Digital.

e incompatíveis com a realidade fática estão inseridas no que se chama de "desinformação".

Segundo a definição do Grupo de Peritos de Alto Nível sobre Notícias Falsas e Desinformação instaurado pela Comissão Europeia, apresentada em um relatório de 2018, o conceito de desinformação abrange "as informações falsas, inexatas ou deturpadas concebidas, apresentadas e promovidas para obter lucro ou para causar um prejuízo público intencional".[544]

Ao contrário do que muitos podem deduzir, a desinformação não é compatível com as liberdades de informação e de expressão; pelo contrário, seu cerne reside justamente em deturpar ambas, visto que o conteúdo da desinformação não corresponde à realidade, ocasionando a supressão do seu conhecimento por aqueles que a consomem. Da mesma forma, o fenômeno da desinformação manipula conclusões, opiniões e entendimentos de seus consumidores, gerando liberdades de expressões viciadas, pautadas em inverdades, com implicação direta quanto aos direitos fundamentais, e afetando o livre trânsito de ideias da sociedade, pondo em risco preceitos fundamentais do regime democrático de direito.

Nas palavras do ministro do Supremo Tribunal Federal Dias Toffoli:

[544] EUROPEAN COMMISSION. Final report of the High Level Expert Group on Fake News and Online Disinformation. Luxemburgo, Serviço das Publicações da União Europeia, Mar. 2018. Disponível em: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation. Acesso em: 9 nov. 2021.

> O regime democrático pressupõe um ambiente de livre trânsito de ideias, no qual todos tenham direito a voz. A liberdade de expressão está amplamente protegida em nossa ordem constitucional. As liberdades de expressão intelectual, artística, científica, de crença religiosa, de convicção filosófica e de comunicação são direitos fundamentais (art. 5º, incisos IX e XIV) e essenciais à concretização dos objetivos da República Federativa do Brasil, notadamente o pluralismo político e a construção de uma sociedade livre, justa, solidária e sem preconceitos de origem, raça, sexo, cor, idade ou quaisquer outras formas de discriminação (art. 3º, incisos I e IV).[545]

Acrescenta-se ainda o fato de que o fenômeno da desinformação não se limita à atuação meramente humana: a coleta de dados de forma instantânea por computadores e dispositivos ligados à rede, associados à atuação dos algoritmos, é um dos grandes propulsores deste fenômeno. Os algoritmos são capazes de manipular e conduzir quais informações chegam até determinada pessoa, sem qualquer discernimento crítico, atuando de forma automática, pautando-se somente nas informações disponíveis sobre cada usuário, como suas preferências, hábitos, localização e círculos sociais. Dentro desta dinâmica, uma vez que um usuário comece a consumir conteúdos de desinformação, como teorias da conspiração, instruções falsas de automedicação, entre outros, os algoritmos,

[545] TOFFOLI, José Antonio Dias. ***Fake news***, Desinformação e Liberdade de Expressão, p. 13, julho/set. 2019. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/bitstream/handle/bdtse/7624/2019_toffoli_fake_news _desinformacao.pdf?sequence=1&isAllowed=y. Acesso em: 11 jun. 2021.

por meio de filtragem de sugestões, condução de publicações em redes sociais, promoção de determinados comerciais em sites, todos de conteúdos semelhantes, acabam por estimular um maior consumo de informações falsas por esse usuário e potencializam seu contato com conteúdo de desinformação.

Por conseguinte, informações que, por sua vez, correspondem a notícias e fatos verdadeiros passam a estar cada vez mais distanciadas das pessoas que consomem desinformações, resultando em uma verdadeira violação ao direito de livre acesso à informação destas pessoas, de seus poderes de disposição sobre suas vontades e de sua autodeterminação informativa. Além disso, não se pode perder de vista que a internet carrega consigo o preceito fundamental de liberdade para seus usuários, sendo o panorama da manipulação e filtragem de informações violador não só de preceitos fundamentais de um Estado Democrático de Direito, mas também violador de preceitos fundamentais da própria internet.

É junto às pessoas idosas que o fenômeno da desinformação apresenta seu mais alto grau de risco. Pesquisas realizadas na Coréia do Sul e na Austrália mostram que a maioria dos idosos utiliza a internet para fins informativos, e uma parte a utiliza como sua fonte primária de informação[546], enquanto no Brasil um estudo realizado pelo Instituto Brasileiro de Geografia e

[546] MOON, Grace. South Korea 's elderly conservatives turn to YouTube, and conspiracy theories. Seul, 26 May 2021. Disponível em: https://restofworld.org/2021/elderly-conservatives-in-south-korea-turn-to-youtube-and-conspiracy-theories/. Acesso em: 9 nov. 2021.

YIANNAKIS, Michael. Health alert: elderly at risk from social media misinformation. Sydney, 4 Nov. 2020. Disponível em: https://lighthouse.mq.edu.au/article/october-2020/Health-alert-elderly-at-risk-from-social-media-misinformation. Acesso em: 9 nov. 2021.

Estatística (IBGE) em 2017 demonstrou que pessoas que estão na terceira idade estão cada vez mais conectadas na internet[547]; isto sem considerarmos ainda as consequências do isolamento na pandemia da Covid-19, que obrigou a sociedade como um todo a lidar ainda mais com a internet.[548]

Uma pesquisa publicada pela revista científica *Science Advances* e realizada no período eleitoral americano em 2016 indicava que pessoas acima de 65 anos compartilharam sete vezes mais notícias falsas do que o grupo etário mais jovem.[549] Outros estudos apontam que as pessoas idosas tendem a confiar mais nas informações a que têm acesso, comumente deixando de realizar juízo sobre a veracidade dos fatos ou sobre a confiabilidade da fonte da notícia, sejam provenientes de sites ou de perfis de suas redes sociais.

Ao ser inserida no mundo da internet em idade mais tardia, a pessoa idosa recebe as informações de forma totalmente desequilibrada, uma vez que essa introdução ocorre já num estágio mais avançado da vida, ao contrário do que ocorreu com a maioria dos usuários da rede. Essas pessoas possuem pouco ou quase nenhum poder de discernir se informações

---

[547] PORTAL FOLHAPE. Como e por que fazer a inclusão digital dos idosos. Pernambuco, 27 set. 2019. Disponível em https://www.folhape.com.br/economia/como-e-por-que-fazer-a-inclusao-digital-dos-idosos/117496/. Acesso em: 9 nov. 2021.

[548] MOTA, Lara. Quarentena acelera inclusão digital de idosos. São Paulo, 13 mai. 2020. Disponível em: https://www.cnnbrasil.com.br/nacional/2020/05/14/quarentena-acelera-inclusao-digital-de-idosos. Acesso em: 9 nov. 2021.

[549] GRINBERG, Nir. JOSEPH, Kenneth. FRIEDLAND, Lisa. SWIRE-THOMPSON, Briony. LAZER, David. Fake news on Twitter during the 2016 U.S. presidential election. [*S. l.*], 25 Jan. 2019. Disponível em: https://science.sciencemag.org/content/363/6425/374.full. Acesso em: 9 nov. 2021.

ou mesmo ações com as quais têm contato pela primeira vez são verdadeiras, ou se são artifícios de outros agentes, como empresas, hackers ou usuários mal-intencionados, que teriam por objetivo disseminar informações ou situações não correspondentes à realidade.

Apesar de permitir maior independência, amplificação do exercício do direito de livre expressão, do direito de acesso à informação, uma maior plenitude social e muitas vezes emocional da pessoa idosa, a internet também é responsável por acentuar muitas das fragilidades inerentes a este grupo, sendo a relação entre idosos e desinformação um dos maiores exemplos da ampliação destas fragilidades. A privacidade, a liberdade, a segurança e outras garantias legais e constitucionais da pessoa idosa adquirem um grau de exposição e risco que reforçam ainda mais o dever de todos os agentes sociais de tutelar este grupo de pessoas, sem eximir o Estado de tal papel.

1. A PROTEÇÃO À PESSOA IDOSA

O envelhecimento humano está associado a um aumento da vulnerabilidade e da fragilidade da pessoa humana, não apenas física, mas também mental e emocional. Estas características são fatores de desigualdade que servem de fundamento para que o ordenamento jurídico brasileiro tenha previsto e estabelecido a proteção da pessoa idosa, com a exigência de seu respeito e de sua promoção por todos os agentes sociais.

O ordenamento jurídico brasileiro reconhece expressamente o idoso como pessoa mais vulnerável do que outras de diferentes faixas etárias, cabendo-lhe tratamento distinto das demais. A atenção especialmente dada aos idosos pela Constituição da

República Federativa do Brasil decorre diretamente do Princípio Constitucional da Dignidade da Pessoa Humana, que faz com que o ordenamento jurídico seja um instrumento para dirimir as diferenças e garantir a igualdade de todos, possibilitando a convivência de diversos grupos heterogêneos ao passo em que preserva a pessoa como indivíduo único.

O caput do art. 230[550] consagra o princípio da solidariedade social ao impor à família, à sociedade e ao Estado o dever de amparar o idoso. Ao redigir o texto do artigo, na tentativa de evitar eventuais prejuízos sociais aos idosos, o constituinte buscou a proteção deste grupo da forma mais abrangente possível, atribuindo o dever de proteção dos idosos a todos os agentes sociais. Neste mesmo sentido, o dispositivo deve ser interpretado sempre da maneira mais ampla, a fim de conferir maior proteção àqueles de idade igual ou superior a 60 anos.

O Estatuto do Idoso, Lei 10.741/03, por sua vez, foi responsável por conceituar positivamente o que era idoso. Pautando-se exclusivamente no critério etário, o ordenamento brasileiro passou a adotar a concepção de idosos como pessoa com idade igual ou superior a 60 (sessenta) anos, de modo a abranger a universalidade de pessoas nessa faixa etária, independentemente de outras características, como sexo ou condições econômicas.

O Estatuto é, no ordenamento jurídico brasileiro, a norma que concretiza de forma mais efetiva as ações afirmativas, com o objetivo de diminuir as discrepâncias existentes entre

[550] Constituição da República Federativa do Brasil de 1988, art. 230: "A família, a sociedade e o Estado têm o dever de amparar as pessoas idosas, assegurando sua participação na comunidade, defendendo sua dignidade e bem-estar e garantindo-lhes o direito à vida."

os idosos e o restante da sociedade. O regulamento garante aos idosos o direito de serem protegidos de qualquer forma de discriminação, negligência, opressão ou crueldade.

Ademais, a legislação traz a já mencionada doutrina da "proteção integral", que preceitua no reconhecimento do idoso como titular de direitos fundamentais e sociais que devem ser assegurados por todos, seja a família, a sociedade ou o Estado. O princípio da proteção integral do idoso pode ser coletado ainda na interpretação dos arts. 2º e 9º do Estatuto, que assim dispõem:

> Art. 2º O idoso goza de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-lhe, por lei, ou por outros meios, todas as oportunidades e facilidades, para preservação da sua saúde física e mental e seu aperfeiçoamento moral, intelectual, espiritual e social, em condições de liberdade e dignidade.
>
> Art. 9º É obrigação do Estado garantir à pessoa idosa a proteção à vida e à saúde, mediante efetivação de políticas sociais públicas que permitam um envelhecimento saudável e em condições de dignidade.

Conforme estabelecido no Estatuto do Idoso, a pessoa idosa deve ter não apenas oportunidades, mas também facilidades para preservar sua saúde psicológica, física e mental, para se aperfeiçoar e gozar da totalidade de seus direitos. O direito à vida, à liberdade, ao respeito e à dignidade, o direito à saúde,

à cultura, à educação, ao esporte e ao lazer, o direito de acesso ao mercado e ao trabalho, à previdência ou à assistência social, à habitação e à locomoção são garantias inerentes à pessoa humana, e quando relacionados aos idosos devem ser preservados e efetivados, não podendo o Estado, a família ou a sociedade permitirem ativa ou passivamente que esse grupo não usufrua o que lhes é essencial.

2. O ESTADO E A PROTEÇÃO DO IDOSO FRENTE À DESINFORMAÇÃO

O preâmbulo da Constituição Federal estabelece os preceitos do Estado Democrático de Direito nos seguintes ditames:

> Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, [...]

No contexto de um Estado democrático de direito, o Estado como instituição ocupa um papel de protagonismo na defesa, promoção e efetivação dos direitos fundamentais constitucionalmente previstos, contando com a implementação de

políticas públicas como um de seus principais artifícios para o exercício efetivo de seu papel.[551]

A Constituição da República brasileira tem como princípio o entendimento da pessoa humana como fundamento e fim do Estado. O modelo de Estado estabelecido é aquele em que o Estado deve se utilizar de seus poderes e meios para a maior eficiência e garantia dos direitos fundamentais, o que inclui o esforço por colocar todas as pessoas humanas em pé de igualdade, cumprindo o papel fundamental de compensar desequilíbrios, combater desigualdades e promover políticas para alçar os mais vulneráveis a patamares de menor desvantagem perante os demais.

Neste mesmo sentido, no Estado Democrático de Direito estabelecido no Brasil, as políticas públicas devem cumprir um papel de efetuação de previsões, medidas e objetivos, principalmente na proteção de direitos essenciais, não se limitando a uma função normativa geral e abstrata.

Os idosos despontam como um dos principais grupos de pessoas que contam com proteção especial por parte da Constituição Federal e do ordenamento jurídico brasileiro como um todo. Desta forma, a atuação do Estado na proteção desse grupo contra as violações presentes no fenômeno da desinformação possui máxima importância e urgência, devendo-se buscar a efetivação e a promoção de políticas públicas para a proteção de seus direitos da forma mais célere e eficiente possível.

[551] CASTRO, Josiana Dourado. O Estado como garantidor dos Direitos Humanos. Dez. 2014. Disponível em: https://science.sciencemag.org/content/363/6425/374.full. Acesso em: 13 nov. 2021.

As políticas públicas cabíveis ao Estado para a busca de uma solução da problemática da desinformação na internet posta às pessoas idosas podem ter as mais variadas naturezas e formas de execução, englobando medidas de áreas diversas, como a regulação da desinformação na internet, a promoção de educação digital, o fomento da inclusão social da pessoa idosa na internet e a adoção de medidas de assistência.

Apesar de o ordenamento jurídico brasileiro estar ampliando as previsões legislativas acerca do uso da internet, tendo como principais normas legislativas o Marco Civil da Internet, Lei 12.965/2014, e a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, ainda não é possível abarcar de forma absoluta as necessidades legislativas necessárias ao combate à desinformação, ou mesmo à promoção da proteção integral de grupos mais vulneráveis, partindo majoritariamente de uma perspectiva de que os usuários da internet compartilham igualmente das mesmas condições, o que não ocorre com os idosos.

A LGPD estabelece em seu art. 9º o direito de acesso a informações sobre tratamento de dados pessoais, mas também estabelece que cabe à Agência Nacional de Proteção de Dados (ANPD), órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil, garantir que o tratamento de dados de idosos seja feito de maneira simples, clara, adequada e acessível ao seu entendimento. Em tal sentido:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados,

que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

[...]

Art. 55-J. Compete à ANPD:

[...]XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso)[...][552]

[552] 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: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 nov. 2021.

Contudo, apesar de esses dispositivos compartilharem de princípios e adotarem fins que em muito dialogam com o combate à desinformação e com a proteção de grupos vulneráveis, incluindo a proteção da privacidade, da liberdade de expressão e de direitos fundamentais dos usuários da internet, o processo da desinformação e a proteção específica para os direitos da pessoa idosa na internet contam com um tratamento aquém ao necessário para a proteção de direitos essenciais.

Cabe mencionar que não só a questão da disseminação da desinformação, sob o viés de um ato ilícito, mas também o funcionamento dos algoritmos e sua capacidade de criar verdadeiras bolhas de desinformação, com processamento quase ilimitado de dados dos usuários da internet, ainda não encontra tratamento próprio em nossa legislação para assegurar a garantia dos direitos de liberdade de informação e de expressão dos usuários da rede, em especial da pessoa idosa.

2.1 MEDIDAS ESTATAIS PARA O ENFRENTAMENTO DA DESINFORMAÇÃO POR PESSOAS IDOSAS

2.1.1 A REGULAÇÃO DA DESINFORMAÇÃO

Apesar de ser um tema que ainda divide opiniões, a regulação do combate à desinformação na internet se apresenta como uma das principais soluções para o enfrentamento da desinformação pelas pessoas idosas, uma vez que é capaz de abarcar pontos diversos sobre o assunto.

Questões como o limite de processamento de dados por algoritmos, a responsabilização de agentes por promoção à desinformação e a previsão de formas e ferramentas de informação a usuários podem ser tratadas e definidas de ma-

neira específica pelo Estado a partir da regulação, de modo a estabelecer meios apropriados e específicos para o enfrentamento do fenômeno da desinformação por pessoas idosas, compatibilizando parâmetros e mecanismos da rede com a proteção de direitos dos usuários idosos e com os fins de promoção dos direitos e garantias fundamentais inerentes ao Estado Democrático de Direito.

A regulação também se mostra como uma resposta eficiente ao combate à desinformação, uma vez que, ao serem estabelecidos os limites de atuação nas redes, com previsões e sanções específicas para a garantia de direitos dos idosos, haveria uma maior dificuldade e um desestímulo à manipulação de informações e à promoção da desinformação para estes grupos, seja por meio de sanções pecuniárias, restritivas de direitos ou mesmo com implicações penais.

Dentre as ações de caráter restritivo possíveis pela regulação da desinformação na internet, destaca-se a limitação à atuação dos algoritmos para usuários idosos. Imposições de restrições e limitação à extensão dos algoritmos perante essas pessoas configuram medidas capazes de reduzir o fenômeno da desinformação, representando verdadeira contenção do contínuo estímulo propagado pelos algoritmos ao consumo de conteúdos de desinformação por aqueles que já o tenham acessado, principalmente quando se trata de pessoas idosas.

Ademais, a regulação estatal é medida capaz de estabelecer um dever de maior transparência por parte dos agentes responsáveis pelo funcionamento dos algoritmos e de outras ações automatizadas, bem como incentivar e estimular esses agentes a disponibilizarem ferramentas de controle de conteúdo de forma mais clara e direta para os usuários da rede,

principalmente aqueles que estão em desequilíbrio perante os demais. A título de exemplo, a possibilidade de definição das preferências de configurações no processamento de informações pelo usuário desde seu primeiro acesso à internet, e não só como uma opção de alteração de determinada configuração pré-estabelecida.

A regulação permitiria não só a promoção de medidas meramente restritivas, mas também a promoção de medidas positivas que incentivem a atuação dos agentes sociais na direção do respeito e da garantia aos direitos fundamentais da pessoa idosa como internauta. Deveres específicos de informação aos usuários, viabilização de mecanismo de checagem sobre a veracidade de fatos e notícias, classificações e avisos sobre o grau de confiabilidade de notícias a partir daqueles que a estão divulgando, promoção da adoção de medidas de design thinking, além da adaptação de linguagens para compatibilizar com o vocabulário dos idosos, estão entre as medidas passíveis de serem estimuladas por incentivos fiscais do Estado aos agentes sociais por meio da regulação do combate à desinformação, combinando interesses públicos e privados.

Não há dúvida de que a busca pela adequação da internet para o estabelecimento de canais de comunicação próprios para as pessoas idosas deve se apresentar como um dos principais e mais urgentes pontos ao tratar da regulação da desinformação. Faz-se imprescindível que a parcela de idosos da sociedade seja colocada em igualdade com os demais usuários, ampliando sua aptidão para compreensão das informações presentes na internet, seja de forma direta ou indireta, devendo o Estado mobilizar seu aparato nesse sentido.

2.1.2 APLICAÇÃO DA EDUCAÇÃO DIGITAL

Conforme disposto no art. 205 da Constituição Federal, cabe ao Estado o dever de educar, promovendo o pleno desenvolvimento da pessoa, não se excetuando a educação digital desta previsão, uma vez que atualmente seu aprendizado está intrinsecamente associado a um saber inerente à nossa sociedade.

Ao contrário do que costuma ocorrer em grupos mais jovens, os idosos possuem uma maior necessidade de serem educados digitalmente para atingirem uma plena capacidade de utilização das ferramentas da rede. A desvantagem técnica deste grupo de pessoas no uso da internet representa verdadeiro combustível para a promoção da desinformação, uma vez que estas pessoas tendem a confiar nas informações que consomem sem questionarem de imediato a confiabilidade de suas fontes.

Cabe aqui mencionar que, uma vez que os atuais idosos tiveram seu desenvolvimento informativo a partir de meios de comunicação como rádio, televisão e jornais, essa geração criou um alto grau de confiabilidade nos canais responsáveis por transmitirem informações, canais estes que eram ainda minimamente regulamentados e positivados, o que não ocorre em muitas das fontes de notícias presentes na internet.

A educação digital surge como uma necessidade para a autodeterminação plena da pessoa idosa no uso da internet, não só para o uso dos seus meios físicos ou de suas funções básicas, como digitação e utilização de máquinas, mas também para que os idosos atinjam um nível mais apropriado de compreensão sobre a forma o funcionamento da internet, por via de um estímulo educacional ao desenvolvimento de

um pensamento mais crítico por este grupo, capacitando-os para compreender o alcance da internet, reconhecer fontes confiáveis de informação, averiguar procedência de notícias e entender os mecanismos virtuais e o processamento de suas informações.

A implementação da educação digital da pessoa idosa pelo Estado inclui ainda a adoção de programas próprios de capacitação e desenvolvimento de profissionais da educação, tendo por fim uma educação digital adequada para as pessoas idosas, visto que este grupo apresenta necessidades próprias frente à internet e aos meios digitais. A promoção da educação digital pelo Estado deve entender os idosos não como agentes inativos, mas como agentes plenamente ativos e capazes, que precisam estar inseridos na sociedade atual de forma plena, absoluta e devidamente educada.

2.1.3 INCLUSÃO SOCIAL

Em sentido afim, a inclusão social pode representar um desdobramento tanto da regulação da desinformação na internet como da implementação da educação digital para as pessoas idosas, mas importa destacar que sua abrangência não se resume a estes pontos.

O conceito de pessoa idosa engloba o direito de envelhecimento pleno, capaz e integrado; logo, a inclusão social da pessoa idosa na internet tem um importante papel na defesa dos direitos dos idosos. A manipulação da informação por terceiros, as *fake news* e a falta de medidas próprias para esse grupo pelos diversos agentes sociais, associadas às restrições próprias dessa parcela de indivíduos, ameaçam excluir siste-

maticamente os idosos de plena inclusão na sociedade, o que inclui o uso da internet.

A ausência de políticas de inclusão social das pessoas idosas na internet é um fator que reforça o fenômeno da desinformação. Estando os idosos sistematicamente excluídos da integração online de forma plenamente capaz, aqueles que promovem e se beneficiam da desinformação manterão milhares de pessoas suscetíveis às suas manipulações, trazendo consequências sociais de grande prejuízo não só aos direitos destas pessoas, mas também ao Estado Democrático de Direito.

A inclusão social engloba a adoção de políticas públicas voltadas a promover a integração da pessoa idosa com a internet, incluindo o estímulo à integração entre agentes privados atuantes na internet, principalmente aqueles com maior controle sobre os meios de informação online, e os idosos, por intermédio do Estado, para que esse grupo de pessoas não esteja mais à margem da socialização virtual. Suas necessidades devem ser ouvidas e assimiladas por todos os agentes sociais atuantes, tendo o Estado um papel primordial na integração da sociedade.

Medidas de ensino e diálogo social, associadas a uma abertura para que os agentes da internet adaptem suas atuações, ou mesmo a promoção de programas assistenciais para idosos na internet representam formas de alcançar a plena inclusão social da pessoa idosa no mundo digital, resultando em uma utilização da rede mais segura e com menor risco aos direitos de liberdade e de informação da pessoa idosa.

A inclusão social não deve colocar os idosos somente como sujeitos a serem protegidos, mas como agentes capazes que devem ser alçados à atuação e autodeterminação plena, que

devem ter suas necessidades atendidas e facilitadas para estarem em iguais condições com os demais usuários da internet. A capacidade de aprendizado e integração da pessoa idosa deve ser promovida e jamais subestimada ou colocada de forma secundária.

O Estado possui verdadeiro dever de implementar políticas efetivas para equilibrar as situações de exclusão e as limitações impostas aos idosos na internet. A ausência de atuação estatal para a efetivação de políticas próprias aos idosos no combate à desinformação é um empecilho ao envelhecimento pleno, colocando em segundo plano direitos que deveriam ser tutelados e promovidos pelo Estado.

CONSIDERAÇÕES FINAIS

Ainda que a desinformação na internet seja um fenômeno considerado recente em nossa sociedade, seu alcance e suas consequências se apresentam como justificativas suficientes para a atuação imediata pelo Estado ao seu combate. O dever de assegurar os direitos fundamentais da pessoa humana e os preceitos do regime democrático de direito, principalmente quando tratando de grupos que merecem tutela especial por parte do Estado, não é compatível com a inércia dos entes estatais frente a esse fenômeno.

Por outro lado, a atuação estatal não pode ser exacerbada e precipitada a ponto de permitir que outros direitos sejam colocados em risco. Apesar de a regulamentação da desinformação se mostrar como uma das principais formas de o Estado solucionar a questão, sua implementação requer cautela, cabendo mencionar aqui o exemplo do Projeto de

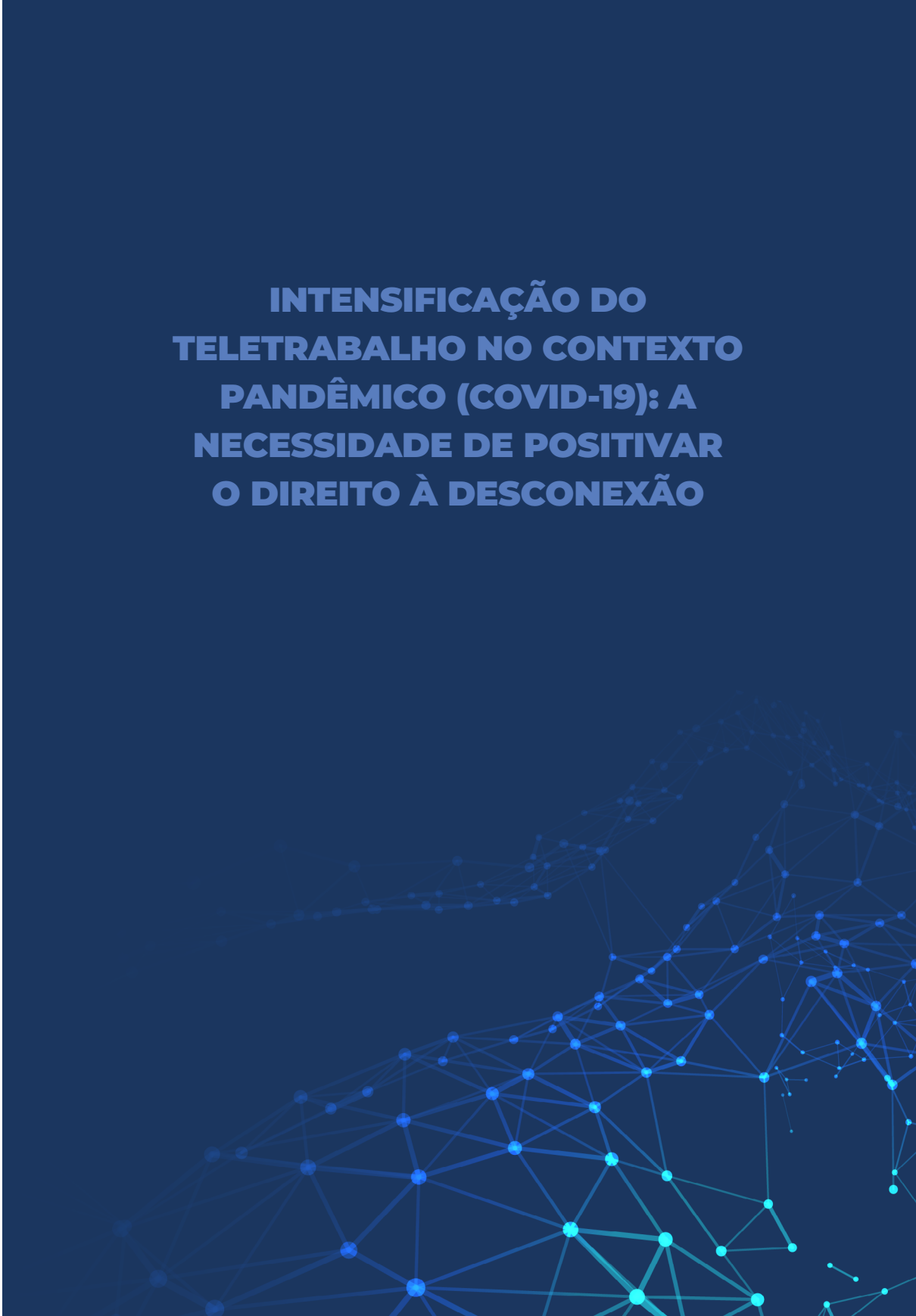
Lei 2.630/2020, conhecido como "PL das *Fake News*"[553], pois suas medidas podem acabar por criar formas de censura e restrição da comunicação pelos usuários da internet, violando preceitos fundamentais da Constituição Federal.

Simultaneamente, a simples regulamentação da desinformação na internet não necessariamente significa que os idosos receberão tratamento específico e adequado pelo Estado. A implementação da regulamentação da desinformação na internet deve cuidar especialmente de grupos que estão em condições desiguais de uso da internet, conferindo tratamento específico para idosos, menores de idade, pessoas de baixa renda e pessoas com necessidades especiais.

Todavia, conforme apontado, o Estado possui aparato suficiente para o combate à desinformação que atinge pessoas idosas na internet de forma imediata, não representando a regulamentação da questão o único caminho. Medidas de educação digital e inclusão social da pessoa idosa se mostram como suficientes para que o fenômeno perca força e para que os direitos de liberdade de expressão, livre informação, autodeterminação e igualdade da pessoa idosa sejam, através da atuação estatal e implementação de políticas públicas, resguardados no mundo da internet.

[553] URUPÁ, Marcos. Especialistas defendem transparência contra *fake news* e criticam PL 2.630. Disponível em: [*S. l.*], 22 jun. 2021. Acesso em: 9 nov. 2021.

INTENSIFICAÇÃO DO TELETRABALHO NO CONTEXTO PANDÊMICO (COVID-19): A NECESSIDADE DE POSITIVAR O DIREITO À DESCONEXÃO



Silvia Helena von Calmbach[554]

INTRODUÇÃO

A pandemia de coronavírus (Covid-19), cujo primeiro caso no Brasil, foi confirmado em 26/02/2020, em São Paulo, fez com que várias empresas e empregados tivessem a necessidade de adotar o teletrabalho, de forma repentina e sem muito planejamento, a fim de evitar a disseminação da doença. Aquilo que seria, a princípio, uma solução temporária, vem se prolongando a mais de um ano, o que tem feito as empresas deliberarem a respeito da possibilidade de tornar o teletrabalho uma prática consolidada.

Adotado, inicialmente, com o objetivo de evitar a propagação do vírus e proporcionar condições para a continuidade do serviço nas empresas e para a manutenção dos empregos, o teletrabalho está se tornando um modelo que poderá ser utilizado de forma definitiva no Brasil, como demonstram algumas reportagens veiculadas pela mídia.[555] [556] [557]

---

[554] Graduada em Direito pela Universidade Estácio de Sá (2019). Pós-graduanda em Direito Digital pela UERJ/ITS.

[555] CAMPOS, S.; BIGARELLI, B. Companhias já aderem ao home office permanente. Valor Econômico. São Paulo: Globo, 08 jun. 2020. Disponível em: https://valor.globo.com/carreira/noticia/2020/06/08/companhias-ja-aderem-ao-home-office-permanente.ghtml. Acesso em: 28 out. 2021.

[556] PINHO, M. Empresas aderem ao home office permanente e mudarão escritórios. R7, 20 jun. 2020. Disponível em: https://noticias.r7.com/economia/empresas-aderem-ao-home-office-permanente-e-mudarao-escritorios-22062020. Acesso em: 29 out. 2021.

[557] GANDRA, A. Trabalho em *home office* tende a continuar após fim da pandemia. Agência Brasil, 01 maio 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-04/trabalho-em-home-office-tende-

Segundo a pesquisa "*Home Office* 2020" realizada pela SAP Consultoria em Recursos Humanos em parceria com a Sociedade Brasileira de Teletrabalho e Teleatividades – SOBRATT, 46% das 554 empresas participantes da pesquisa adotam o teletrabalho/home-office de maneira estruturada, 52% das empresas passaram a praticar a modalidade em função da pandemia e, destas últimas, 72% planejam manter a prática. A pesquisa demonstrou que muitas empresas brasileiras cogitam adotar o teletrabalho, mesmo após o fim da pandemia, em modelo permanente ou híbrido, isto é, quando parte da prestação de serviço é realizada dentro da empresa, em alguns dias por semana, de forma habitual[558].

Por ser uma modalidade que cada vez mais será adotada no país e por possuir uma dinâmica recente para as relações trabalhistas, o teletrabalho deverá trazer questões que ainda não estão consolidadas na legislação vigente brasileira. Uma dessas questões que estão vindo à tona – principalmente com a intensificação do teletrabalho na pandemia – é a do direito ao tempo disponível para lazer e descanso, também conhecido como direito à desconexão, que será aprofundado neste artigo.

1. DO TELETRABALHO

A prática do trabalho remoto não é uma novidade no Brasil. Já vinha sendo implantada, há algum tempo, em diversas

-continuar-apos-fim-da-pandemia. Acesso em: 30 out. 2021.

[558] SAP CONSULTORIA EM RECURSOS HUMANOS; SOCIEDADE BRASILEIRA DE TELETRABALHO E TELEATIVIDADES. Pesquisa Home Office Brasil 2020. Dez./2020. Disponível em: https://sapconsultoria.com.br/pesquisa-home--office-brasil-2020/. Acesso em: 30 out. 2021.

empresas e por muitos profissionais. Verifica-se que, desde 2011, já havia na CLT disposição acerca de trabalho realizado fora das dependências do empregador, conforme redação do art. 6º incluído pela Lei nº 12.551[559]:

> Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego.
>
> Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio.

Mesmo com a alteração realizada na CLT em 2011, a normatização em relação ao teletrabalho ainda deixou muitas lacunas sem tratamento adequado. Somente após 11 de novembro de 2017, com a entrada em vigor da Lei nº 13.467[560], mais conhecida como Lei da Reforma Trabalhista, foram dispostos novos regramentos e definições relacionados ao trabalho realizado à distância, longe do espaço físico da empresa. A Reforma

[559] BRASIL. Lei nº 12.551, de 15 de dezembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm. Acesso em: 29 out. 2021.

[560] BRASIL. Lei nº 13.467, de 13 de julho de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13467.htm. Acesso em: 29 out. 2021.

trouxe um capítulo específico para tratar desta modalidade: o capítulo II-A, "do teletrabalho".

A partir de então o teletrabalho passou a ser conceituado como a "prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo."[561]. Vale enfatizar, no entanto, que o regime do teletrabalho não é descaracterizado quando da presença do empregado nas dependências do empregador.

Para que uma atividade laborativa possa ser caracterizada como teletrabalho, alguns elementos, que estão previstos na legislação, devem estar presentes:

> A lei exige, para sua validade, que o contrato seja escrito e que expressamente conste a modalidade de prestação de serviços como sendo de teletrabalho, e eventual alteração do contrato deve também obedecer a forma escrita, que deve prever quem será responsável pela aquisição, manutenção e fornecimento da infraestrutura necessária e adequada para a prestação do trabalho e reembolso de despesas, que não possuem natureza salarial. Foi permitido, também, a alteração dos contratos vigentes para o regim

Os autores Cavalcante e Jorge Neto indicam como elementos que caracterizam o teletrabalho:

[561] BRASIL. Lei nº 13.467, de 13 de julho de 2017, cit., art. 75-B.

> (a) atividade realizada a distância, ou seja, fora dos limites de onde os seus resultados são almejados; (b) as ordens são dadas por quem não tem condições de controlá-las fisicamente. O controle é ocasionado pelos resultados das tarefas executadas; (c) as tarefas são executadas por intermédio de computadores ou de outros equipamentos de informática e telecomunicações.[562]

Do mesmo modo, Fincato apresenta como elementos caracterizadores do teletrabalho sistematizados pela lei e pela doutrina: o elemento geográfico ou topográfico no qual "o teletrabalhador desempenha suas atividades fora do espaço tradicional (físico) da empregadora"; o elemento tecnológico, no qual o "teletrabalhador desenvolve suas tarefas mediante o emprego de tecnologia da informação e comunicação que poderá, ainda, ser identificada como a mediadora da relação ou como o próprio espaço de trabalho" e o elemento organizativo, no qual "o empregador deverá estar organizado, em sua estrutura produtiva e de recursos humanos, para o teletrabalho, visualizando o trabalhador remoto como integrante de sua rede de empregados em todas as ações e estratégias (ambiência laboral, medicina do trabalho, capacitações e promoções, etc)."[563]

---

[562] CAVALCANTE, J. Q. P.; JORGE NETO, F. F. A tecnológica, o teletrabalho e a reforma trabalhista. Revista eletrônica Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 8, n. 75, p. 116, fev. 2019. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/152291. Acesso em: 30 out. 2021.

[563] FINCATO, D. Teletrabalho na reforma trabalhista brasileira. Revista eletrônica Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 8,

Importante enfatizar que o teletrabalho não descaracteriza o trabalho subordinado, uma vez que "a Lei n. 13.467/2017 ressalta a ideia de subordinação estrutural através de uma nova interpretação do art. 3º da CLT, de forma a considerar empregado (e não um autônomo) o trabalhador que presta serviços em local diverso das dependências da empresa, concedendo toda proteção inerente ao contrato de emprego."[564]

As atividades do teletrabalhador podem ser, facilmente, controladas pelo empregador, que pode utilizar, para isso, diversos mecanismos tecnológicos e informáticos. Conforme salientam Rocha e Muniz,

> (...) o empregador não renuncia o controle sobre as atividades do teletrabalhador, apenas o realiza pelos meios informatizados e/ou telemáticos ou até mesmo pelos resultados produzidos por estes. Salienta-se ainda que, atualmente, com as recentes invenções, o empregador possui pleno (ou o devido) controle sobre o empregado que se encontra a distância, sabendo inclusive quando este está trabalhando ou não.[565]

n. 75, p. 64, fev. 2019. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/152290. Acesso em: 30 out 2021.

[564] MACHADO, A. C. C. (Org.); ZAINAGHI, D. S. (Coord.). CLT interpretada: artigo por artigo, parágrafo por parágrafo, cit., p. 100.

[565] ROCHA, C. J. da; MUNIZ, M. K. de C. B. O teletrabalho à luz do artigo 6º da CLT: o acompanhamento do direito do trabalho às mudanças do mundo pós-moderno. Revista Tribunal Regional do Trabalho da 3ª Região, Belo Horizonte, v. 57, n. 87/88, p. 108, jan./dez. 2013. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/74935v. Acesso em: 30 out. 2021.

Tais autores explicam, ainda, que "o poder diretivo e a subordinação não desaparecem no teletrabalho, apenas mudam de forma, para atender aos parâmetros estabelecidos e à operacionalização técnica da prestação de serviços. Altera-se a forma, mas a essência continua a mesma, podendo inclusive estar mais incisiva e camuflada, até porque quanto maior a liberdade maior também a responsabilidade."[566]

Em relação à duração do trabalho, a Reforma Trabalhista definiu que o trabalhador que se encontra em teletrabalho não faz jus às horas extras, intervalos para repouso e alimentação, adicional noturno e descanso semanal remunerado, uma vez que foi disposto no artigo 62, inciso III da CLT, que os empregados em regime de teletrabalho não são abrangidos pelas normas que regulamentam a jornada de trabalho.

Pode-se dizer, entretanto, que essa medida é questionável, visto que o empregador tem condições de controlar a jornada de trabalho e fiscalizar a produtividade do empregado, por meio de modernos equipamentos eletrônicos, que podem, por vezes, realizar o monitoramento em tempo real. Segundo Oliveira e Tourinho,

> A justificativa legal para tal inovação legislativa foi a dificuldade do empregador manter a fiscalização e o controle estrito da jornada de trabalho, ante a ampla liberdade que o teletrabalhador ostenta no serviço remoto, longe das lentes de inspeção. Contudo, transferir o ônus dessa dificuldade para o trabalhador, que em muitos casos é coagido a migrar ou ingressar no teletrabalho, revela o verda-

[566] Ibid., p.109-110.

> deiro estado de exceção aos direitos fundamentais dos obreiros imbuídos do movimento neoliberal.[567]

A adoção do teletrabalho pode trazer muitas vantagens para o trabalhador: a economia no tempo de deslocamento para empresas, a diminuição de estresse e dos gastos com transporte e com alimentação, além disso, a flexibilidade de horário, a maior autonomia, a possibilidade de convívio com a família, a maior inclusão no mercado de trabalho de pessoas com dificuldade para se deslocar para o ambiente da empresa (ex. pessoas com deficiência; pais e mães solteiros). Para o empregador algumas das vantagens são: a redução de custos fixos operacionais, a diminuição do absenteísmo, pois os trabalhadores ficam menos doentes; o aumento da produtividade e da satisfação dos empregados; a viabilização de novos contratos; a possibilidade de retenção de talentos; a oportunidade de a empresa operar por 24 horas por dia, sete dias por semana, considerando a flexibilidade horária e geográfica que o teletrabalho proporciona.

Como bem observam os autores Dutra e Villatore, o teletrabalho traz benefícios tanto ao trabalhador como ao empregador:

[567] OLIVEIRA, L. P. F. de; TOURINHO, L. de O. S. Síndrome de Burnout, teletrabalho e revolução tecnológica: um estudo do adoecimento profissional em tempos de Covid-19. Revista Jurídica Trabalho e Desenvolvimento Humano, v. 3, p.12-13, 2020. Disponível em: https://doi.org/10.33239/rjtdh.v3.83. Acesso em: 30 out. 2021.

> O teletrabalho tornou-se uma opção mais econômica para o empregador, e mais cômoda ao empregado, vez que, para o empregador, são inúmeras vantagens, dentre elas, a ausência de custo com espaço físico, como sala para o escritório, estacionamentos, combustível para veículos de frota quando são utilizados, secretária, horários de entrada e saída seus empregados, bem como intervalos, vale-transporte, dentre outras. Já para os empregados, as vantagens também podem ser inúmeras, como maior aproveitamento do tempo com o lazer, com a família, com atividade física, posto que ausentes o tempo de deslocamento para o trabalho e do trabalho para a sua residência, além de que o trabalho poderá ser executado de acordo com a vontade e disponibilidade do trabalhador, desde que cumpra o prazo estabelecido para o desenvolvimento daquela tarefa específica.[568]

Apesar dos inúmeros pontos positivos já observados, o teletrabalho, contudo, é cercado de controvérsias. Nas ponderações de Rocha e Muniz[569], uma questão de muita relevância envolvendo o teletrabalho é sua ambiguidade, pois ao mesmo tempo que pode oferecer benefícios para o trabalhador realizar suas atividades em casa, pode trazer desvantagens, haja vista que o trabalho acaba adentrando

[568] DUTRA, S. R. B; VILLATORE, M. A. C. Teletrabalho e o direito à desconexão. Revista eletrônica Tribunal Regional do Trabalho da 9ª Região, Curitiba, v. 3, n. 33, p. 144, set. 2014. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/93957. Acesso em: 30 out. 2021.

[569] ROCHA, C. J. da; MUNIZ, M. K. de C. B. O teletrabalho à luz do artigo 6º da CLT: o acompanhamento do direito do trabalho às mudanças do mundo pós-moderno. cit., p. 109.

no lar do empregado, gerando interferência na sua vida pessoal e familiar.

Assim, podem ser mencionados como desvantagens para o teletrabalhador, o isolamento social, a menor chance de desenvolvimento profissional e de promoção, decorrente da perda de contato direto com colegas e superiores, a indefinição do tempo de trabalho e de lazer e descanso, a falta de equilíbrio entre as esferas laboral e familiar, o aumento da carga de trabalho e o enfraquecimento de representação coletiva, devido à dificuldade de organização sindical, decorrente da descentralização dos ambientes de trabalho.

Martinez e Possídio apontam que "o teletrabalho, como qualquer modalidade de serviço em domicílio, é um fenômeno de isolamento do obreiro. Por não encontrar outros trabalhadores submetidos às mesmas condições laborais, ele tende a evitar o associativismo. Por consequência, há um natural enfraquecimento da luta de classes e da atuação sindical."[570] Há também o risco de possíveis problemas ergonômicos devidos à exposição do trabalhador em frente ao computador por longos períodos e, em muitos casos, em condições inadequadas. Como desvantagens para o empregador, estão os custos com a implantação e manutenção de equipamentos, os perigos quanto à segurança de dados e a dependência da tecnologia.

[570] MARTINEZ, L.; POSSÍDIO, C. O trabalho nos tempos do coronavírus. São Paulo: Saraiva, 2020. E-book, p. 254.

2. DO TELETRABALHO NO CONTEXTO DA PANDEMIA DE COVID-19

A pandemia e as políticas sanitárias de isolamento e de restrição da mobilidade forçaram, de forma repentina e urgente, a adoção de medidas de isolamento social entre as pessoas para limitar a transmissão do vírus. A fim de garantir a manutenção das atividades econômicas e dos empregos, as empresas precisaram implementar planos para incentivar o trabalho remoto. De uma hora para a outra, o teletrabalho – que antes era uma exceção – tornou-se regra.

> Os Estados tiveram que implantar novas regras pertinentes ao isolamento social durante a eclosão do novo vírus e, com isso, as empresas precisaram fechar suas portas para o público externo e dispensar o trabalho presencial. O serviço remoto, então, foi a solução apresentada pelas autoridades estatais para manutenção das atividades empresariais.[571]

Conforme aponta Rodrigues[572], se forem observados, cronologicamente, os fatos decorrentes da pandemia do novo coronavírus, percebe-se o quanto avassalador foi este fenômeno que se sobrepôs, de modo inesperado e imprevisto, à

[571] OLIVEIRA, L. P. F. de; TOURINHO, L. de O. S. Síndrome de Burnout, teletrabalho e revolução tecnológica: um estudo do adoecimento profissional em tempos de Covid-19. cit., p. 30.

[572] RODRIGUES, I. C. COVID-19: um exemplo literal de força maior no direito do trabalho. In: LIMA, F. R. de S. (Coord.) [et al.]. COVID-19 e os impactos no Direito: mercado, Estado, trabalho, família, contratos e cidadania. São Paulo: Almedina Brasil, 2020. E-book. p. 192.

vontade de empregados e empregadores, ainda mais se considerarmos que, em 20/03/2020, o Governo Federal editou do Decreto nº. 10.282/2020[573], definindo quais seriam os serviços públicos e as atividades consideradas essenciais que poderiam permanecer em funcionamento e obrigando todas as demais atividades não-essenciais a serem realizadas virtualmente ou a interromperem seus trabalhos.

Como medida de enfrentamento da crise nas relações de trabalho decorrentes do estado de calamidade pública produzido pela pandemia, foram editadas Medidas Provisórias com o objetivo de evitar a extinção de vários postos de trabalho e flexibilizando várias regras para os empregadores: a MP 927 de 22/03/2020[574], com prazo de vigência encerrado em 19/07/2020; a MP 936 de 01/04/2020[575], convertida em Lei nº 14.020, de 06/07/2020[576] e a MP 1.046, de 27/04/2021[577], com vigência de 120 dias, podendo ser prorrogada por igual período por ato do Governo Federal. Vale ressaltar que nenhuma dessas Medidas Provisórias tem o poder de alterar o

[573] BRASIL. Decreto nº. 10.282, de 20 de março de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10282.htm. Acesso em: 01 nov. 2021.

[574] BRASIL. Medida Provisória nº 927, de 22 de março de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv927.htm. Acesso em 01 nov. 2021.

[575] BRASIL. Medida Provisória nº 936, de 01 de abril de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv936.htm. Acesso em: 01 nov. 2021.

[576] BRASIL. Lei nº 14.020, de 06 de julho de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14020.htm. Acesso em: 01 nov. 2021.

[577] BRASIL. Medida Provisória nº 1.046, de 27 de abril de 2021. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Mpv/mpv1046.htm. Acesso em: 01 nov. 2021.

disposto na CLT e que só possuem vigência durante o período excepcional de calamidade provocado pela pandemia.

De acordo com Rodrigues,

> O "espírito" da MP n. 927/2020, basicamente, foi o de eleger algumas das previsões contidas na CLT – aptas à sustentação econômica das relações trabalhistas e passíveis de alteração por negociação coletiva (arts. 134 a 145 e 611-A, CLT) – e criar procedimentos mais céleres para suas implementações, em especial pela atribuição de validade jurídica a acordos individuais firmados diretamente entre empregados e patrões, sem a necessidade de intervenção dos sindicatos, o que, em tese, contraria os princípios da autonomia da vontade coletiva e da hipossuficiente dos trabalhadores, ressalvada a hipótese do art. 444, § único, CLT[578].

As modificações advindas das Medidas Provisórias 927/2020 e, posteriormente, da MP 1.046/2021, tiveram como objetivo flexibilizar algumas exigências previstas na CLT em relação ao teletrabalho e instituir especificidades para o contexto de pandemia, tornando mais célere a alteração da modalidade presencial para o regime de teletrabalho. Algumas delas encontram-se aqui elencadas: a) a não necessidade de acordos coletivos ou individuais para alterar o regime de trabalho; b) a dispensa de registro prévio da alteração no contrato individual de trabalho; c) prazo mínimo 48 horas de antecedência para

[578] RODRIGUES, I. C. COVID-19: um exemplo literal de força maior no direito do trabalho. cit., p. 195-196

comunicar ao empregado a alteração de regime de trabalho; d) a não necessidade de acordo do empregado para o regime de teletrabalho; e) a permissão de extensão do teletrabalho para estagiários e aprendizes; f) a disposição sobre a responsabilidade pela aquisição e custeio dos equipamentos e da infraestrutura para teletrabalho, previstos em contrato escrito firmado previamente ou no prazo de 30 dias, contados da data de mudança do regime de trabalho.

É fato que a crise de saúde pública instalada pela pandemia ocasionou mudanças drásticas e repentinas na rotina dos trabalhadores. Por conta do novo cenário dela decorrente e diante da implantação urgente do regime de trabalho remoto, os funcionários, de uma hora para outra, foram obrigados a inserir o espaço de trabalho em sua casa e no seu círculo familiar. Muitos trabalhadores e gestores não estavam preparados para o trabalho remoto e foram instados a procurar uma forma adequada de distribuir e executar metas e prazos, que passaram a se imiscuir nas tarefas domésticas, no tempo do convívio familiar, nas atividades escolares etc. A casa, de certo modo, tornou-se a extensão da empresa. Dada a falta de preparo e estruturação para o ambiente de teletrabalho, os empregados começaram a se ver às voltas com longas jornadas de trabalho, altamente desgastantes, com um maior número de reuniões e com curtos prazos a serem cumpridos. Tais práticas passaram a ameaçar o equilíbrio entre a vida e o trabalho, ocasionando, a muitos trabalhadores, uma série de dificuldades e riscos físicos e emocionais. "Os trabalhadores foram colocados em uma nova rotina de trabalho, acentuadamente mais estressante do ponto de vista da produtividade, haja vista que o ambiente de trabalho – em casa – sofre com

interferências de familiares e amigos, assim como não há limitação de jornada."[579]

É sabido que o excesso de tempo trabalhado pode desencadear doenças relacionadas à saúde mental, doenças osteomoleculares, adoecimento emocional, estresse, depressão, ansiedade e síndrome de *Burnout*. Inclusive, em maio de 2021, a Organização Mundial da Saúde (OMS) e a Organização Internacional do Trabalho (OIT) divulgaram um estudo informando que trabalhar mais de 55 horas por semana eleva as chances de morte por motivo de doenças cardíacas e acidentes vasculares cerebrais (AVC).[580]

3. DO DIREITO À DESCONEXÃO

Por conta da pandemia, o mundo corporativo foi obrigado a modificar as suas atividades, intensificando o trabalho remoto com o intuito de manter a produtividade elevada e a busca de melhores resultados. Com a invasão do trabalho no ambiente doméstico das pessoas, passou a ocorrer, em muitos casos, um desequilíbrio entre o tempo destinado ao trabalho e o tempo para o descanso do trabalhador. Percebeu-se, assim, que as horas trabalhadas aumentaram a despeito da diminuição das horas destinadas ao repouso, à convivência familiar e ao lazer do empregado. Mendonça, Almeida e Valério[581]

[579] OLIVEIRA, L. P. F. de; TOURINHO, L. de O. S. Síndrome de Burnout, teletrabalho e revolução tecnológica: um estudo do adoecimento profissional em tempos de Covid-19. cit., p. 30.

[580] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. Longas jornadas de trabalho podem aumentar as mortes por doenças cardíacas e derrames, de acordo com a OIT e a OMS. 17 maio 2021. Disponível em: https://www.ilo.org/brasilia/noticias/WCMS_792828. Acesso em 01 nov. 2021.

[581] MENDONÇA, A. L. P.; ALMEIDA, C. V. G.; VALÉRIO, M. M. Direito à desco-

apontam dois fatores que potencializaram a intromissão do trabalho no ambiente familiar: a tecnologia e a pandemia de Covid-19. A tecnologia, com o uso praticamente constante dos meios telemáticos como e-mails, *laptops* e telefones celulares e a utilização dos aplicativos de conversas e reuniões *on-line,* passou a manter o empregado conectado ao trabalho, independentemente da hora ou do local em que estivesse. Já o segundo fator, a pandemia de Covid-19, fez com que o funcionário se sentisse isolado dentro de sua casa e acabou por levá-lo a substituir suas horas de saúde e lazer por jornadas de trabalho muito mais extensas do que as realizadas antes da pandemia.

O teletrabalho, adotado de modo repentino e não planejado por significativa parcela da população, fez com que emergissem, de forma muito expressiva, alguns problemas do trabalho remoto que talvez demorassem mais tempo para se tornarem significativos e que, neste momento, tornam-se pontos importantes e merecedores de definição, pois têm o poder de ameaçar o equilíbrio entre a vida pessoal e profissional do teletrabalhador. Necessário se faz o debate sobre os prejuízos causados pela acentuada conexão ao trabalho (ou hiperconexão do teletrabalhador), que o uso das tecnologias de comunicação e informação proporcionou e sobre horas de trabalho mais intensivas, mais longas e imprevisíveis, que invadiram a esfera privada do indivíduo. Neste sentido, exprimem Oliveira e Tourinho,

---

nexão: uma avaliação do teletrabalho em tempo de covid-19: da exceção à regra. Revista Científica do UniRios, v. 1, p. 309, 2021. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2021/29/direito_a_desconexao.pdf. Acesso em: 30 out. 2021.

> O desafio enfrentado pelo trabalhador em teletrabalho é justamente estabelecer uma rotina de trabalho uniforme, com limites bem determinados da jornada laboral. E a ausência disso coloca em risco a saúde mental e física do trabalhador, que pode extrapolar a jornada sem a devida remuneração das horas suplementares. Esse obstáculo é provocado ainda mais pelo empregador, que exige do funcionário tempo totalmente a disposição do trabalho, o que retira os momentos de descanso e lazer do obreiro.[582]

A pandemia e o uso de tecnologias de comunicação e informação exacerbaram algumas tensões laborais, criando diversas formas de esgotamento para o teletrabalhador em seu ambiente de trabalho. Muitas vezes, devido ao medo de perder o emprego (ainda mais escasso nos tempos de pandemia) e por conta do uso das tecnologias digitais que permitem a conexão a qualquer momento do dia, os empregados se sentem obrigados a responder imediatamente a toda e qualquer solicitação de seu empregador. Esta "obrigação" de estarem constantemente disponíveis para trabalhar, a fim de se mostrarem comprometidos com o trabalho, pode resultar em ambientes laborais tóxicos, nocivos e geradores de doenças ocupacionais, pois um empregado que trabalha em demasia, pode gerar uma espécie de pressão sobre os outros colegas. O medo de serem penalizados por não se fazerem presentes, estando sempre conectados, pode causar picos de estresse e de ansiedade, afetando diretamente o psicológico

[582] OLIVEIRA, L. P. F. de; TOURINHO, L. de O. S. Síndrome de Burnout, teletrabalho e revolução tecnológica: um estudo do adoecimento profissional em tempos de Covid-19. cit., p. 31.

dos trabalhadores. Assim, as pessoas estão trabalhando mais tempo do que nunca, respondendo a e-mails e mensagens em quaisquer dias da semana, fora do horário de expediente, no intuito de mostrar seu comprometimento com a empresa, o que pode ocasionar uma nova forma de escravidão do empregado, como declara Lopes e Santos,

> O uso abusivo e excessivo dos meios telemáticos e a ausência de controle de jornada prevista no inciso III do art. 62 da CLT, acrescido pela Lei nº 13.467 (BRASIL, 2017), podem levar a uma nova forma de escravidão do empregado. Por isso a importância do direito à desconexão, que é decorrência lógica do direito à limitação da jornada de trabalho, ao lazer e à convivência familiar, mas que ainda não é regulamentado pela ordem jurídica interna.[583]

O Ministério Público do Trabalho (MPT) atento a esses problemas e visando a auxiliar as empresas e trabalhadores no contexto de pandemia, emitiu Nota Técnica 17/2020[584], com diretrizes a serem observadas nas relações de trabalho por empresas, sindicatos e órgãos da Administração Pública, com a

[583] LOPES, A. M. S.; SANTOS, S. B. dos. O teletrabalho e a limitação da exploração do trabalho sem fim: a utilização das legislações portuguesa e francesa para colmatar as lacunas normativas e ontológicas da CLT. Revista da Escola Judicial do TRT4, v. 2, n. 3, p. 262, 4 out. 2020. Disponível em: https://rejtrt4.emnuvens.com.br/revistaejud4/article/view/61/52. Acesso em: 30 out. 2021.

[584] BRASIL. Ministério Público do Trabalho. Nota técnica 17/2020 do GT nacional Covid-19 e do GT nanotecnologia/2020, de 11 de setembro de 2020. Disponível em: https://mpt.mp.br/pgt/noticias/coronavirus-veja-aqui-as-notas-tecnicas-do-mpt. Acesso em: 30 out. 2021.

finalidade de garantir a proteção de trabalhadores no trabalho remoto ou *home office*. A nota orienta os empregadores a respeitarem a jornada contratual na modalidade de teletrabalho e em plataformas virtuais e defende medidas para assegurar as pausas legais e o direito à desconexão, além disso, traz um modelo de etiqueta digital, que especifica os horários de atendimento virtual de demanda e que assegura os repousos legais, permitindo o direito à desconexão. Observa-se que as orientações da nota técnica não possuem caráter vinculativo, uma vez que não estão dispostas em lei, mas que podem ser utilizadas para fundamentar decisões e fiscalizações do MPT.

Apesar de o ordenamento jurídico brasileiro não tratar objetivamente do direito à desconexão, há dispositivos e normas que servem para coibir a intensa conexão do trabalhador, limitar a jornada de trabalho e proteger o seu direito ao descanso. Conforme resume, Goldschmidt e Graminho,

> É necessário [...] tutelar o direito à desconexão que, [...] trata-se de um direito fundamental implícito dos trabalhadores, decorrente de outros direitos, igualmente fundamentais expressos na Constituição Federal e em tratados internacionais. Nesse passo, entende-se que o direito à desconexão pode ser deduzido de normas constitucionais que estabelecem o direito à privacidade (art. 5º, X), ao lazer (art. 6º), à limitação da jornada de trabalho (art. 7º, XIII e XIV), ao repouso semanal remunerado (art. 7º, XV) e ao gozo de férias anuais remuneradas (art. 7º, XVII), todos intimamente relacionados ao

> princípio da dignidade humana, valor central do ordenamento jurídico brasileiro.[585]

Entende-se, assim, que o direito à desconexão é um direito fundamental implícito, uma vez que decorre de direitos fundamentais expressos na Constituição Federal, que permite que os sujeitos se desconectem de suas atividades laborais, nos períodos de repouso e férias, destinados por lei ao não trabalho. Nas palavras de Dutra e Villatore,

> Tem-se por desconexão, o direito que todo e qualquer trabalhador possui de usufruir descansos de seu trabalho diário, seja ele dentro da jornada laboral ou ao término, de estar totalmente desvinculado do cargo ou função que exerce, servindo a restabelecer as energias, a suprir suas necessidades biológicas e fisiológicas, ao sono, restando, disposto para o próximo período laboral.[586]

O aumento do uso de tecnologias, como o *smartphones*, *tablets*, *laptops*, aplicativos, redes sociais, *e-mails*, entre outros, tem aumentado gradativamente o tempo de trabalho e de prestação de serviços. O trabalhador encontra-se constantemente conectado ou hiperconectado, o que impossibilita o descanso efetivo entre as jornadas de trabalho e, invaria-

[585] GOLDSCHMIDT, R.; GRAMINHO, V. M. C. Desconexão: um direito fundamental do trabalhador. Rio de Janeiro, Lumen Juris, 2020, p. 132.

[586] DUTRA, S. R. B; VILLATORE, M. A. C. Teletrabalho e o direito à desconexão. cit., p. 144.

velmente, afeta os direitos fundamentais, como o direito ao lazer, à saúde, ao descanso, à vida privada, entre outros. Nas palavras de Tenório:

> Num mundo extremamente interligado, 24 horas do dia conectado pelo celular ou por dispositivos semelhantes, se não houver controle e prudência, a linha divisória entre o trabalho e a vida privada do empregado; entre suas funções na empresa e seu lar; entre seu espaço de lazer e descanso e seu espaço de trabalho, será extinta.[587]

Defende-se que positivar o direito à desconexão é uma forma de garantir a efetividade de outros direitos fundamentais, como o direito à privacidade, à saúde, ao descanso, ao lazer, à vida privada, às férias remuneradas, à limitação à jornada de trabalho e ao princípio da dignidade humana,

> [...] o direito à desconexão apresenta-se como uma forma de garantia do cumprimento do preceito constitucional a partir dos novos paradigmas trazidos pela tecnologia. Em razão do limite imaginário que distinguia o tempo utilizado para lazer e para o cumprimento de atividades profissionais encontrar-se mitigado no teletrabalho, é necessário que o empregado seja acobertado por um direito que

[587] TENÓRIO, R. J. M. A saúde mental e ergonômica no trabalho remoto no pós-pandemia. Revista Espaço Acadêmico, edição especial, v. 20, p. 99. abril. 2021. Disponível em: https://periodicos.uem.br/ojs/index.php/EspacoAcademico/article/view/58092. Acesso em: 30 out. 2021.

> lhe garanta a revitalização desta divisão e o respeito do seu período de descanso[588].

Neste sentido, com vistas a sanar essa lacuna legislativa, tramita, no Senado Federal, o Projeto de Lei nº 4.044/2020 de 03/08/2020[589], de autoria do Senador Fabiano Contarato (REDE/ES), que objetiva alterar o parágrafo 2º do art. 244 e inserir o parágrafo 7º ao art. 59 e os artigos 65-A, 72-A e 133-A à CLT, com a finalidade de tutelar o direito à desconexão dos trabalhadores. Se aprovado, o empregador não poderá acionar o empregado durante o período de descanso, por meio de qualquer ferramenta telemática, sejam elas serviços de telefonia, *e-mail*, aplicativos de mensagens como por exemplo *WhatsApp*, *Telegram*, aplicativos de internet, entre outros. Cabe exceção apenas nos casos de extrema necessidade: motivo de força maior ou caso fortuito, atender à realização de serviços inadiáveis ou cuja inexecução possa acarretar prejuízo manifesto. Nessas hipóteses, que devem estar previstas em acordo coletivo ou convenção coletiva, o projeto de lei define que serão aplicadas as disposições relativas à hora extraordinária. Ressalta ainda, que não será considerada falta funcional a ausência de resposta do empregado à solicitação feita pelo empregador durante os períodos

[588] RESEDÁ, S. O direito à desconexão: uma realidade no teletrabalho. Revista de direito do trabalho, São Paulo, v. 33, n. 126, p. 157-175, abr./jun. 2007. Disponível em: https://egov.ufsc.br/portal/conteudo/o-direito--%C3%A0-desconex%C3%A3o-uma-realidade-no-teletrabalho. Acesso em: 30 out. 2021.

[589] BRASIL. Senado Federal. Projeto de Lei nº 4.044/2020, de 03 de agosto de 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/143754. Acesso em: 30 out. 2021.

destinados ao descanso. Além disso, o projeto define que durante o período de férias, o empregado será excluído dos grupos de trabalho existentes nos serviços de mensageria do empregador e das aplicações de internet exclusivas do trabalho. O projeto de lei define, ainda, que será considerado como tempo de sobreaviso a favor do empregado que for submetido ao controle patronal, à distância, por instrumentos telemáticos ou informatizados durante o período de descanso.

CONCLUSÃO

Apesar de a prática do trabalho remoto já ter sido implantada há algum tempo em empresas do Brasil, o cenário de pandemia conseguiu acelerar, de forma urgente e não muito planejada, o processo de migração do trabalho presencial para o teletrabalho.

As empresas precisaram se adaptar com mais velocidade a esse novo cenário e implementar, rapidamente, transformações digitais, para proporcionar condições à continuidade dos serviços das empresas e para manter os empregos de seus funcionários. No contexto da pandemia, o distanciamento social é uma das armas mais eficazes contra a disseminação do vírus. Por este motivo, uma parte dos trabalhadores, cujos serviços foram considerados como não essenciais, viram-se compelidos a inserir o espaço de trabalho dentro de suas casas e em seu círculo pessoal e familiar.

Com tais mudanças nas relações de trabalho, percebeu-se a importância de levantar uma questão que já vinha sendo observada e que emergiu de forma mais efetiva neste pe-

ríodo, por conta da intensificação do teletrabalho: o direito à desconexão do trabalhador.

O uso das novas tecnologias da informação e de comunicação pode fazer com que o indivíduo seja incomodado nos momentos de sua vida particular – de modo muitas vezes imperceptível – e passe a resolver questões laborais em seu momento de descanso (férias, finais de semana, feriados) interferindo na esfera privada do sujeito. A realidade do teletrabalho, exacerbada no contexto de pandemia, mostrou o quanto ainda é necessário que as leis evoluam para garantir os direitos do empregado.

O direito à desconexão é um direito fundamental implícito ao trabalhador que, portanto, ainda não está consolidado na legislação vigente. Torna-se, assim, muito importante um trabalho consistente no sentido de que a legislação o proteja de forma eficiente. Entende-se que tecnologia evolui de forma mais célere que as leis, mas cabe ao legislador acompanhar as tecnologias e amparar os trabalhadores buscando assegurar seus direitos. Sendo assim, e considerando os fatos já mencionados, entende-se como mister que o Estado positive o direto à desconexão do trabalho, visto que se trata de instrumento de garantia para outros direitos fundamentais do trabalhador, como o direito à privacidade, à saúde, à limitação à jornada de trabalho, ao descanso, ao lazer, à vida privada, e, sobretudo, ao princípio da dignidade humana.

Cabe ao Direito do Trabalho, portanto, a preocupação em acompanhar as tendências do mundo atual, observando a forma como o empregador trata a rotina dos empregados e, neste mundo cada vez mais conectado, assegurar ao tra-

balhador o direito à desconexão. A delimitação dos tempos dedicados ao trabalho e ao descanso é crucial, pois propicia ao trabalhador o gozo dos períodos de lazer e assegura seus direitos fundamentais a um trabalho digno e à qualidade de vida. Além disso, o direito à desconexão é essencial tanto para a empresa quanto para o funcionário, pois um empregado descansado, com suas forças restauradas, certamente terá um desempenho produtivo muito melhor do que um empregado exausto, estressado e adoentado.

GATEKEEPERING: CONCORRÊNCIA NOS MERCADOS DIGITAIS E A EXPERIÊNCIA EUROPEIA

Fábio Pimentel de Carvalho[590]

INTRODUÇÃO

Os efeitos da transformação digital, isto é, dos fenômenos do mundo virtual na vida real são já de tamanha ordem que o *The New York Times* publicou, em outubro de 2019, a informação de que, diariamente, são entregues em Nova Iorque mais de 1.5 milhão de encomendas oriundas do comércio online, sendo certo que a cidade já começa a experimentar severas complicações no trânsito por conta das entregas[591]. Este número, pré-pandêmico, certamente deve ser muito superior atualmente.

Como leciona Brito[592], a vertiginosa evolução das tecnologias digitais trouxe novas soluções, hábitos, preferências e, sobretudo, oportunidades. O consumidor dessa nova era possui, portanto, acesso instantâneo à informação sobre produtos e serviços, uma enorme gama de escolha e a possibilidade de comparar preços em tempo real. A isso, soma-se ainda a mobilidade, tanto em sua dimensão física, que permite ao consumidor, no exato momento em que está considerando a compra, saber onde comprar, como em sua dimensão virtual, que permite a ele transacionar numa infinidade de estabeleci-

[590] Advogado. Bacharel em direito e Especialista em Propriedade Intelectual pela PUC-Rio. Mestre em Economia e Gestão da Inovação pela Faculdade de Economia da Universidade do Porto. Ex-Trainee da Diretoria-Geral da Concorrência na Comissão Europeia. Sócio sênior de J Amaral Advogados e Chief Innovation Officer na Voice of the Oceans (Família Schurmann).

[591] Disponível em https://www.nytimes.com/2019/10/27/nyregion/nyc-amazon-delivery.html, acessado em 30/6/2021.

[592] BRITO, Pedro Q. *Promoção de vendas e comunicação de preços*. Coimbra: Almedina, 2019, p. 43.

mentos virtuais ou, em última análise, fazer uma comparação de preços na internet dentro de um estabelecimento físico[593], para aferir a vantajosidade de um preço praticado por aquele determinado comércio.

O crescimento do comércio eletrônico e das interações online de maneira geral, catalisados como efeitos da pandemia de COVID-19, coincide com um esforço da União Europeia, que vem apostando fortemente na noção de um Mercado Único Digital, emergido como interesse público primário pelos agentes públicos[594] e que traz a reboque a preocupações imperativas ao bom desenvolvimento do comércio em ambiente digital.

Uma destas preocupações reside justamente na atuação de certos *stakeholders* que, em razão de seu tamanho, comportamento, impacto e posicionamento no mercado, acabam por se consubstanciarem em verdadeiros porteiros (*gatekeepers*) do comércio eletrônico, isto é, portas de entrada rigorosamente controladas e quase inevitáveis para quem deseja vender pela internet.

O presente trabalho tem por objetivo examinar a experiência europeia com o crescimento das plataformas digitais de intermediação e os possíveis reflexos para a concorrência no âmbito digital.

---

[593] Nesse sentido, basta dizer que já no terceiro trimestre de 2018, os smartphones representavam 61% das visitas a sites do retalho no mundo. Ainda, segundo dados da KPMG, 65% dos consumidores fazem comparações de preços em dispositivos móveis enquanto compram em lojas físicas. (Informações disponível em https://sleeknote.com/pt- pt/blog/estatisticas-de-e-commerce, acessado em 30/6/2021).

[594] ABREU, Joana. O desígnio da justiça eletrónica europeia de 2019 a 2023 à luz do contencioso da União – Reflexões antecipatórias. *Direito e Pessoa no Mundo Digital – Algumas questões*, v. 1, jun 2019, p. 30.

1. COMÉRCIO ELETRÔNICO E O MERCADO ÚNICO DIGITAL EUROPEU

A digitalização do comércio é um processo que se iniciou de forma aparentemente invisível para o consumidor, com a introdução de tecnologias como códigos de barras, software de análise de transações em pontos de venda, meios de pagamento eletrônicos e integração com sistemas dos diversos agentes da cadeia produtiva[595]. A criação desse ecossistema, aliada ao desenvolvimento da internet e dos smartphones, permitiu que, de forma decisiva e definitiva, as figuras do empresário e do estabelecimento físico ganhassem independência, chegando-se até ao ponto em que vendedores e compradores podem confundir-se, alternando esses papéis sistematicamente nas plataformas de intermediação.

Este processo vem alterando, ainda, de maneira significativa, a estrutura de custos dos negócios, sendo certo que sistemas de informação e comunicação, custos de distribuição e investimentos em marketing digital ocupam lugares cada vez mais vultosos nas planilhas de orçamento das empresas.

Eventos como a pandemia do COVID-19 também são capazes de impulsionar sobremaneira o comércio eletrônico. Pesquisas indicam que o impacto do Coronavírus no tráfego online de determinadas indústrias, como os supermercados e o varejo de tecnologia, ultrapassou os 125% de

[595] HAGBER, John; SUNDSTROM, Michael; EGELS-ZANDÉN, N. The digitalization of retailing: an exploratory framework. *International Journal of Retail & Distribution Management*, v. 44, n. 7, 2016, pp. 694-712.

aumento no fim de abril de 2020.[596] É possível que mesmo após o regresso ao estágio de normalidade, muitas pessoas que começaram a comprar online em razão da situação de emergência acabem por incorporar esse novo hábito às suas rotinas.

Aliás, estima-se que até 2040 cerca de 95% das compras serão feitas online[597]. Para que se tenha ideia da dimensão dessa forma de comércio, basta dizer que em 2018 as vendas online representaram 11,9% de todas as transações do retalho ao redor do mundo, sendo certo que até o final de 2021 este número deverá ser de 17,5% das vendas globais. Em 2017, o comércio eletrônico foi responsável por 2,3 trilhões de dólares em vendas e o número esperado para 2021 ultrapassa os 4,5 trilhões. Somente nos Estados Unidos, as compras online entre empresas e consumidores finais (B2C), já respondem por 10% de toda a venda do varejo nacional. No entanto, é interessante notar que à medida que o comércio eletrônico se expande em âmbito global, o *market share* americano vem diminuindo, o que é explicado, sem dúvidas, pelo crescimento das plataformas que atuam mundo afora. A figura abaixo ilustra essa redução do mercado americano[598].

Nesse sentido, dados da Comissão Europeia estimam que a economia digital, já em 2019, representava algo entre

[596] Disponível em https://www.statista.com/study/71767/coronavirus-impact-on-the-global-retail-industry/,

[597] Disponível em https://www.nasdaq.com/articles/uk-online-shopping--and-e-commerce-statistics-2017-2017-03- 14, acessado em 25/6/2021.

[598] Disponível em https://sleeknote.com/pt-pt/blog/estatisticas-de-e-commerce, acessado em 25/6/2021.

4,5% e 15,5% do PIB mundial[599]. Portanto, a preocupação e a importância com o desenvolvimento do comércio eletrônico e com a formação de um efetivo mercado único digital são de tal ordem que a União Europeia vem, desde 2015, ampliando os esforços para derrubar barreiras e permitir a integração comercial online do Bloco. O marco inicial para a transformação digital na União Europeia (UE) apoiou-se na criação de um Mercado Único Digital (Digital Single Market – DGS), emergido como interesse público primário apontado tanto pelos agentes públicos europeus, como pelos nacionais[600].

Incutida na noção de um DGS está uma dimensão econômica fundamental: plataformas digitais podem ter um papel crucial para os governos e mercados, em uma sociedade onde estão já presentes em diversos setores, desde transportes até a produção cultural. Dessa forma, é razoável pensar que os setores desprovidos dessas tecnologias onde ainda se privilegiam os meios presenciais para negócios tenderão a ocupar um espaço cada vez mais diminuto na atividade econômica. O objetivo precípuo era, portanto, derrubar barreiras regulatórias para permitir que os até

[599] EUROPEIA, Comissão. Proposta de regulamento do Parlamento Europeu e do Conselho relativo à disputabilidade e equidade dos mercados no setor digital (Regulamento de mercadosdigitais), 2020. Disponívelem https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349 , acessado em 10/7/2021.

[600] Abreu, Joana. O desígnio da justiça eletrónica europeia de 2019 a 2023 à luz do contencioso da União – Reflexões antecipatórias. *Direito e Pessoa no Mundo Digital – Algumas questões*, v. 1, jun 2019, p. 23.

então 28 mercados nacionais existentes desse lugar a um verdadeiramente único mercado digital.

Em 2015, quando da intensificação dos debates, a Comissão Europeia (CE) afirmava que em razão das barreiras online para o comércio virtual – limitação de meios de pagamento e entregas, por exemplo – apenas 15% dos europeus faziam compras online em outros países da UE, sendo certo também que apenas 7% das pequenas e médias empresas (PME) comercializavam para além de suas fronteiras geográficas. A perda pela inexistência de um DGS efetivo era estimada em 415 bilhões euros por ano, sem considerar a criação de centenas de milhares de novos postos de trabalho[601].

Estabeleceu-se, então, uma estratégia baseada em três pilares: (i) melhor acesso de consumidores e empresas a bens e serviços digitais em toda a Europa; (ii) criação de condições adequadas e equitativas para fomento às redes digitais e serviços inovadores; (iii) maximização do potencial de crescimento da economia digital.

Para cada um desses pilares, a CE definiu um conjunto de ações principais, que deveriam ser desenvolvidas até o fim de 2016. A tabela abaixo resume e organiza essas iniciativas.

[601] Disponível em https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4919, acessado em 30/6/2021.

Tabela 1. Detalhamento dos pilares da estratégia europeia para um Mercado Único Digital.

Pilar	Ações principais
1. Melhor acesso de consumidores e empresas a bens e serviços digitais em toda a Europa	(i) Criar regras para facilitar o comércio eletrónico transfronteiriço, com a harmonização de regras sobre contratos e proteção do consumidor online; (ii) Fazer cumprir as regras já existentes de maneira mais rápida e consistente; (iii) Tornar as entregas de encomendas mais eficientes e acessíveis, partindo-se da premissa de que, àquela altura, 62% das empresas que tentavam vender pela internet afirmavam que os custos de entrega inviabilizavam a comercialização de seus produtos; (iv) Acabar com o bloqueio geográfico injustificado, isto é, uma prática discriminatória que impede o acesso ou redireciona o consumidor para outro site em razão de sua localização, permitindo que se pratiquem preços diferentes para áreas geográficas distintas; (v) identificar possíveis problemas concorrenciais que afetem os mercados europeus de comércio eletrónico, através de inquéritos; (vi) Modernização da legislação em matéria de direitos autorais, permitindo o livre acesso a conteúdo em toda a UE; (vii) Revisão da *Satellite and Cable Directive*, para avaliar a necessidade de ampliação de seu escopo, fortalecendo o acesso transfronteiriço aos serviços de emissoras na Europa; (viii) Reduzir a carga administrativa que as empresas enfrentam de diferentes regimes de IVA.

Pilar	Ações principais
2. Criação de condições adequadas e equitativas para fomento às redes digitais e serviços inovadores	(i) Apresentar uma revisão profunda nas regras de telecomunicações da UE, com a criação de incentivos ao investimento em banda larga, com a garantia de condições equitativas para todos os participantes do mercado, inclusive os entrantes; (ii) Revisão do quadro de mídia audiovisual, concentrando-se no papel dos diferentes agentes do mercado (emissoras de TV, On-demand, etc); (iii) Analisar abrangentemente o papel das plataformas online (mecanismos de busca, mídias sociais, lojas de aplicações) no mercado, incluindo questões como a não transparência dos resultados de pesquisas e políticas de preços; (iv) Reforçar a confiança e segurança nos serviços digitais, especialmente no que se refere à proteção de dados pessoais e (v) Propor parceria com a indústria de segurança cibernética para reforçar essa confiança.
3. Maximização do potencial de crescimento da economia digital	(i) Propor uma iniciativa europeia de livre fluxo de dados, posto que novos serviços são muitas vezes dificultados por restrições sobre onde os dados estão localizados ou sobre o acesso, restrições essas que nada tem a ver com proteção de dados; (ii) Definir padrões e interoperabilidade em áreas críticas do mercado único digital, como saúde eletrónica e planejamento de transportes, dentre outros e (iii) apoiar uma sociedade digital inclusiva, na qual todos tenham as competências necessárias para tirar o melhor proveitos de oportunidades no ambiente virtual, seja para comprar ou para conseguirem oportunidades de trabalho. Nesse sentido, um novo plano de ação de governo eletrónico também permitirá a conexão entre departamentos de registo de negócios em toda a EU, garantindo que diferentes sistemas nacionais possam conversar entre si e permitindo a aplicação do princípio do ***once only***, isto é, assegurando que os cidadãos não tenham que informar seus dados mais de uma vez para as administrações públicas. Essa medida em particular, aliada à implementação de assinaturas eletrónicas interoperáveis tem o potencial de gerar cerca de 5 mil milhões de euros de economia por ano.

Fonte: Autoria própria.

Importa ressaltar que a atuação da UE nesse particular ocorre ao abrigo do que dispõe o artigo 4.º, n.º 2, a) do Tratado sobre o Funcionamento da União Europeia (TFUE), no sentido de que é competência partilhada entre os Estados-Membros e a União atuar no que diz respeito ao Mercado Interno, isto é, todos os entes podem legislar e adotar atos juridicamente vinculativos nessa seara, sendo certo que os Estados-Membros devem exercer sua competência na medida em que a UE não tenha exercido a sua e tornam a exercer competência a partir do momento em que a UE tenha optado por deixar de fazê-lo, nos termos do artigo 2º, n° 2 do TFUE.

Nesse particular, deve-se recordar que, inicialmente, a União acreditou na capacidade dos Estados-Membros em promover as mudanças necessárias no sentido de implementar o Mercado Único. Contudo, em 2015, percebeu que era necessário estabelecer uma governança centralizada dos recursos digitais, com vistas a garantir a interoperabilidade e a harmonia do conjunto, pressupostos do modelo idealizado pela União, tendo em conta também que a construção de um mercado único digital pressupunha a necessidade de que o Estado também estivesse estruturado no ambiente virtual, a partir da oferta de serviços eletrônicos uniformes que contribuíssem para a criação de um contexto favorável ao desenvolvimento da economia digital.

O chamado "Plano de Ação europeu (2016-2020) para a administração pública em linha"[8] marcou um esforço organizado da Comissão para modernizar os serviços públicos, ampliando a eficiência interna do setor, sob a premissa de que a digitalização dos serviços redundaria na redução de encargos administrativos para empresas as e cidadãos, tornando suas interações com a gestão pública mais eficientes,

céleres e transparentes. Ainda, o Plano reconhecia o papel central da transformação digital da administração pública para o sucesso do DGS, atribuindo a si próprio a missão de atuar como catalisador para coordenação de esforços e recursos de modernização do setor público. É interessante notar uma ressalva salutar que é feita no documento, no sentido de que o Plano não disporá de orçamento específico, tampouco de instrumentos de financiamento; ou seja, trata-se de um modelo absolutamente programático, isto é, voltado para a assistência aos Estados-Membros na coordenação e acompanhamento das medidas colocadas à disposição deles pela UE através dos diversos programas já então existentes.

Dessa forma, restou traduzida da seguinte maneira a visão do Plano 2016-2020: *"Até 2020, as administrações públicas e as instituições públicas da União Europeia deverão ser abertas, eficientes e inclusivas, prestando serviços públicos em linha integrais, sem fronteiras, personalizados e de fácil utilização a todos os cidadãos e empresas na UE. São utilizadas abordagens inovadoras na conceção e prestação de serviços melhores de acordo com as necessidades e exigências dos cidadãos e das empresas. As administrações públicas utilizam as oportunidades oferecidas pelo novo ambiente digital para facilitar a sua interação entre si e com as partes interessadas."*.

Logo, é correto afirmar que a União Europeia vem executando uma agenda minuciosamente voltada para um continente digital, sendo certo, nesse sentido, que tal propósito aparece claramente também na Estratégia Europa 2020[602], quando se

[602] Conforme o disponível em https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market, acessado em 10/6/2021.

menciona o objetivo de potencializar o crescimento econômico e os benefícios sociais através do DGS.

Toda essa estratégia passa, portanto, pela persecução, enquanto interesse público, dos objetivos estabelecidos nos diversos documentos de trabalho da União. Ou seja, as administrações públicas devem, necessariamente, sentirem-se parte do processo, de maneira a promoverem as políticas inerentes ao estabelecimento de um DGS[603], contribuindo para a formação de um ambiente econômico promissor.

2. OS GATEKEEPERS E O DIGITAL SINGLE MARKET ACT

O descolamento entre a figura do empresário e a dimensão espacial do estabelecimento, com endereço físico, revelam as potencialidades de uma nova forma de interação socioeconómica que só é possível graças aos recursos tecnológicos existentes, notadamente os *smartphones*. Nesse contexto, destacam-se os mercados de dois lados (*two sided markets*) ou M2L, assim entendidos como aqueles em que há uma plataforma tecnológica cujo objetivo é justamente aproximar agentes económicos que possuem uma forte dependência e um papel central no próprio equilíbrio do mercado, na medida em que a utilidade de um dos lados aumenta quando a quantidade de utilizadores do outro também aumenta[604].

[603] ANDRADE, Francisco; ABREU, Joana. Da interoperabilidade à mediação eletrónica: um novo desafio para a Administração Pública. *A Mediação Administrativa: contributos sobre as (im)possibilidades*. Almedina, 2019, p. 45.

[604] FRAJHOT, Nicholas. *Mercado de Dois Lados: O Mercado de Cartões de Pagamento no Brasil. Pontifícia Universidade Católica do Rio de Janeiro – PUC/RJ. Departamento de Economia.* Monografia. Retirado de http://www.econ.puc- rio.br/uploads/adm/trabalhos/files/Nicolas_Frajhof.pdf. Acessado em 30/6/2021.

Logo, segundo Rochet e Tirole[605], autores de um trabalho que é referência para o tema, a mola principal dos M2L é o esforço para reunir ambos os lados em um modelo de negócio com forma de cobrança apropriada e que maximiza os lucros à proporção em que a interação entre os lados aumenta, diminuindo os custos de transição e custos duplicados[606], a partir da ideia de *matchmaking*, isto é, de encontro e interação entre as partes[607].

Nesse contexto, é notório o surgimento de grandes plataformas de intermediação, que se beneficiam de aspectos inerentes ao modelo econômico, como os efeitos de rede, agregando por vezes serviços de seu próprio ecossistema. Dessa forma, dado seu tamanho e projeção mercadológicos, estas grandes plataformas tem se tornado elementos estruturantes da economia digital, intermediando boa parte das transações entre usuários profissionais (vendedores) e usuários finais (compradores). No entanto, algumas dessas plataformas acabam por atuar como verdadeiras portas de acesso ao mercado digital, fazendo o papel *porteiros* deste acesso (*gatekeepers*), valendo-se de uma posição arraigada no mercado que é construída, geralmente, a partir da aglutinação de serviços essenciais à plataforma, como meios de pagamento e logística,

[605] ROCHET, Jean-Charles; TIROLE, Jean. Platform Competition in Two-Sided Markets. *Journal of the European Economic Association*, 1 (4), 990-1029, 2003, p. 78.

[606] EVANS, David.; SCHMALENSEE, Richard. Markets with Two-Sided Platforms: *Issues in competition law And Policy*, Vol. 1, Chapter 28, 2008, p. 54.

[607] HOLZMANN, Thomaz; SAILER K. & KATZY. B. R. Matchmaking as multi-sided market for open innovation. *Technology Analysis & Strategic Management*, 26:6, 601-615, 2014.

por exemplo, estabelecendo uma sensível dependência para os participantes da relação de intermediação.

Esta realidade acaba por produzir efeitos negativos na concorrência e, em última análise, podem levar à fragmentação do mercado interno, jogando por terra todos os esforços da Comissão Europeia no sentido da construção de um mercado único digital, como já referido anteriormente. Nesse particular, releva exemplificar que a falta de concorrência pode levar a resultados absolutamente ineficientes, que vão desde preços mais altos, queda na qualidade, menor opção de escolha para o consumidor e, ainda, redução na inovação neste meio, posto que a ausência de competitividade e de regulação podem acabar inibindo a produção de resultados inovativos[608].

Muito embora a falta de concorrência e outros problemas não sejam exclusivos do ambiente digital, o desenvolvimento destas mazelas acaba sendo proporcional à velocidade de crescimento destes ambientes. Estudos da Comissão Europeia na aplicação das regras em matéria concorrencial demonstram a existência de um grupo de serviços digitais que reúnem três características em comum. A figura abaixo descreve essas características.

[608] BLIND, Knut. The impact of regulation on innovation. ***Handbook of innovation policy impact***. Oxford: Oxford, 2016, pp. 450.

Figura 2. Características comuns de certos modelos de negócio digitais, segundo a CE.

Fonte: Autoria própria (Texto adaptado do texto da CE)

Dentro destes modelos de negócio, há um conjunto de serviços que podem ou não ser atividade preponderante de determinadas plataformas, mas que acabam por atrair com maior intensidade a incidência das características danosas reveladas acima. Tais serviços, ditos essenciais em razão de sua relevância para o ambiente de negócios digitais são, para a Comissão Europeia, aqueles que se dedicam às seguintes atividades: (i) plataforma de intermediação de comércio de bens/serviços online; (ii) motores de busca online; (iii) redes sociais; (iv) plataformas de compartilhamento de vídeo; (v) sistemas operacionais; (vi) serviços de *cloud computing*; (vii) serviços de publicidade online, dentre outros.

É importante observar, no entanto, que o simples fato de um serviço digital ser reputado essencial não significará, necessariamente, que ele representará uma ameaça à concorrência,

por evidente. Isso se dá, mais frequentemente, quando algum destes serviços essenciais são prestados por controladores de acesso (*gatekeepers*). Nesse sentido, a Comissão Europeia elencou três características para definir um *gatekeeper*, explicadas na tabela abaixo.

Tabela 2. Características que definem um *gatekeeper*. Fonte: Autoria própria.

Característica 1	Característica 2	Característica 3
Impacto significativo no mercado interno. (Assim definido como empresas que possuem um volume de negócios anual de pelo menos 6,5 bilhões de euros)	Operação de uma ou várias portas de acesso relevantes para os clientes. (Base de usuários maior que 45 milhões de utilizadores finais mensais e 10 mil utilizadores comerciais anualmente).	Gozo ou suscetibilidade a figurar em uma posição arraigada e duradoura em suas operações. (Atende ao primeiro e segundo critérios por 3 anos consecutivos).

Sendo a regulação um esforço para orientação de condutas de agentes econômicos no mercado, cujo critério legitimador encontra abrigo na obtenção de resultados eficientes pelo e para o mercado, tratando-se, portanto, de uma função ativa, ou seja, que trás em si a intenção e, portanto, envolve decisões voltadas à orientação dessas condutas[609], a Comissão Europeia optou por divulgar, em 15 de dezembro de 2020 uma propos-

[609] MORENO, Nathalia. de A. Regulatory Decision-Making: parameters of good regulation (mimeo). *1st 2018 Politics Postgraduate Research Seminar, College of Social Sciences and International Studies*, University of Exeter, 2018.

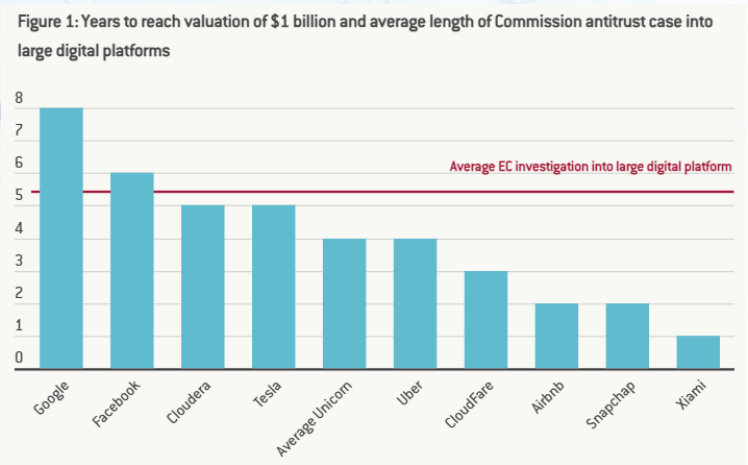
ta para regular os mercados digitais, como parte do esforço para criar um ambiente que garanta a livre concorrência e potencialize o crescimento sustentável da economia digital.

Essa iniciativa recebeu o nome de *Digital Markets Act* (DMA)[610] e teve como principal meta permitir, tanto para usuários finais, como para usuários profissionais, o aproveitamento máximo do que a economia de plataformas possa oferecer, a partir da adoção de uma estratégia de regulação *ex-ante*, assim entendida como aquela que se antecipa aos fenômenos de mercado, buscando prever os atos lesivos à concorrência, prevenindo-os.

A regulação *ex-ante* acabou, portanto, por adotar uma abordagem bastante diferente daquela que pressupõe a aplicação da legislação antitruste em geral, que tende a ser utilizada após o cometimento de uma infração. Nesse sentido, importa ter em conta que em se tratando de negócios digitais, as fiscalizações empreendidas após a suspeita dos fatos ilícitos terem ocorrido pode não ser eficaz, na medida em que seu desenvolvimento geralmente tem velocidade bastante inferior à do próprio crescimento dos negócios em âmbito digital. Quanto a isso, para que se tenha uma ideia desta velocidade, enquanto uma investigação antitruste pode levar, média, 5 anos, *startups* bem-sucedidas podem atingir o *valuation* de US$ 1 bilhão em muito menos tempo. A figura abaixo ilustra essa relação entre o tempo médio de uma investigação promovida pela Comissão Europeia e o número de anos que as empresas levaram para atingirem a avaliação acima referida.

[610] Disponível em https://eur-lex.europa.eu/legal- content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN , acessado em 10/7/2021.

Figura 2. Relação entre tempo médio de investigação na CE e crescimento de negócios de base tecnológica.



Fonte: Extraído de Anderson, J. *et al*, 2021.

A estratégia de atuação *ex-ante*, portanto, apresenta uma vantagem significativa, posto conseguir alcançar os objetivos regulatórios de maneira mais célere do que tendencialmente faria a regulação *ex-post*. No entanto, como se pode imaginar, ela não está indene de limitações. Como lecionam Anderson *et al*[611], é correto afirmar que a regulação *ex-ante* estaria mais suscetível de ser capturada pela indústria, isto é, tornada inútil em razão de contramedidas adotadas pelo regulado para driblá-la. Da mesma forma, sua aplicação em caráter excessivo pode redundar no efeito contrário, já que nem todo o comportamento anticompetitivo é necessariamente ruim para o consumidor. Ademais, tratando-se de um ambiente

[611] ANDERSON, Julia.; MARINELLO, Mario. ***Regulating big tech: the Digital Markets Act***. Disponível em https://bit.ly/3eiUchV , acessado em 20/6/2021.

extremamente dinâmico, é possível ainda que a regulação se torne rapidamente obsoleta.

Para construir sua estrutura e abordagem, portanto, o DMA levou em consideração um conjunto de supostas práticas desleais perpetradas por grandes plataformas digitais que foram ou estão sendo investigadas no âmbito regional, pela Comissão Europeia, ou mesmo pelas autoridades nacionais da concorrência europeia. A tabela abaixo sintetiza as práticas, os acusados, a natureza da preocupação e o âmbito em que estão sendo investigados.

Tabela 3. Práticas/casos que basearam a elaboração do DMA.

Prática	Plataforma	Natureza da preocupação	Ações legais adotadas
	Apple	Práticas desleais na App Store (Caso Epic Games).	Ação judicial individual (2020)
	Booking.com	Cláusulas para beneficiar certos países.	Investigação pela autoridade da concorrência (AC) alemã.

Prática	Plataforma	Natureza da preocupação	Ações legais adotadas
Termos contratuais desleais	Amazon	Vinculação indevida entre acessos, rankings e condições avulsas.	Investigações pelas ACs da Alemanha e Áustria.
	Google	Cláusulas de exclusividade (Google Adsense)	Decisão sancionatória da Comissão Europeia, pendente de apreciação pela Corte de Justiça Europeia.
Uso anticoncorrencial de dados de terceiros	Amazon	Má utilização dos dados do marketplaces para beneficiar seus próprios serviços.	Investigação da Comissão Europeia (2019).
	Google	Má utilização de dados de terceiros para fomentar a publicidade online	Investigação da AC italiana.
	Apple	Preocupação com uso de dados na App Store para favorecer o desenvolvimento de produtos musicais próprios.	Estudo da AC holandesa (2019).
	Facebook	Má utilização de dados de terceiros.	Julgamento da AC alemã aguardando revisão (2019).

Prática	Plataforma	Natureza da preocupação	Ações legais adotadas
Autofavorecimento em rankings e listagens	Google	Direcionamento de listas (Google Shopping)	Decisão sancionatória da Comissão Europeia (2010-2017), pendente de apreciação pela Corte de Justiça Europeia.
	Google	Pré-instalação do Chrome no Android.	Decisão sancionatória da Comissão Europeia (2015-2018), pendente de apreciação pela Corte de Justiça Europeia.
	Google	Recusa em listar aplicativos concorrentes.	Investigação da AC italiana.
	Amazon	Influência do preenchimento e listagens de fornecedores usando um recurso automatizado.	Investigaçãoda AC italiana.
"Amarração e empacotamento"	Microsoft	Embarque do Media Player no sistema operacional.	Decisão sancionatória da Comissão Europeia (2000-2004).
	Apple	Pré-instalação do Apple Music nos dispositivos Apple.	Estudo da AC holandesa (2019).

Prática	Plataforma	Natureza da preocupação	Ações legais adotadas
Falta de acesso a funcionalidades-chave	Apple	Falha de acesso ao chip de pagamento.	Estudo da AC holandesa (2019).
	Amazon	Acesso exclusivo a um sistema de rating (Vine)	Investigações pelas ACs da Alemanha e Áustria.
Outros tipos de auto- preferências	Apple	Pagamento de comissões de até 30% para derrubar concorrentes.	InvestigaçãoCE aberta (2020).

Fonte: Adaptado de Argentesi, E.*et al*[612].

Em linhas gerais, o DMA está estruturado em seis grandes capítulos, que vêm precedidos por uma exposição de motivos composta por 79 parágrafos que contextualizam a pertinência temática e material da iniciativa, apresentando os contornos nocivos da atuação dos *gatekeepers* e uma perspectiva de solução a partir da aplicação do direito da União, consubstanciada na proposta do DMA.

O capítulo I, por sua vez, define o âmbito de aplicação, bem como estabelece os principais conceitos necessários à sua harmonização com a legislação e atuação de cada estado-membro na matéria.

[612] ARGENTESI, Elena.; BUCCIROSSI, Paolo; CALVANO, Emilo; DUSO, Tomaso; MARRAZO, Alessia; NAVA, Salvatore. ***Ex-post Assessment of Merger Control Decisions in Digital Markets***. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/803576/CMA_past_digital_mergers_GOV.UK_version.pdf , acessado em 5/7/2021.

Já o capítulo II trata das questões relativas à conceituação dos controladores de acesso (*gatekeepers*), estabelecendo os critérios já mencionados anteriormente, que caracterizam um agente econômico, qualificando-o como um controlador. É interessante observar que a Comissão Europeia acabou por reservar para si a possibilidade de enquadrar um agente econômico como *gatekeeper* sem a necessidade de preencher os critérios objetivos anteriormente fixados, abrindo certa margem de discricionaridade nesse sentido.

O capítulo III cuida de estabelecer que práticas dos controladores de acesso limitariam a concorrência, tornando-se, portanto, desleais. Ainda, dispõe sobre as obrigações impostas aos *gatekeepers* e a flexibilidade para revisão destas obrigações à luz do caso concreto.

O capítulo IV preceitua regras para a realização de investigações de mercado, notadamente o estabelecimento de requisitos para se desencadearem tais investigações, seja para a designação de um agente econômico como *gatekeeper*, seja para apurar eventuais descumprimentos de obrigações impostas ou mesmo para averiguar a existência de novos serviços essenciais capazes de contribuir para a formação de controladores de acesso.

Já o capítulo V estabelece regras para o controle do cumprimento do DMA e procedimentalização dos processos fiscalizatórios, bem como prevê as sanções possíveis no caso da identificação de irregularidades.

O capítulo VI prevê disposições gerais e reafirma a competência do Tribunal de Justiça da União Europeia para apreciar questões relativas ao DMA.

Do ponto de vista de marcha do processo legislativo, o DMA ainda será debatido no Parlamento Europeu e no Conselho da União Europeia, onde passará pela análise de diversos comitês temáticos. No Parlamento, por exemplo, está prevista a avaliação do Comitê Econômico, da Indústria e da Justiça.

Em termos de prazo para a adoção do DMA, portanto, estima-se que o mesmo leve algo em torno de 2,5 anos para ser aprovado, muito embora se tenha notícias[11] de que a França pretende conduzir essa apreciação com maior celeridade, quando assumir a Presidência do Conselho da EU, a partir do primeiro semestre de 2022. No entanto, mesmo assim, muito são ainda céticos quanto à sua efetividade depois de um processo legislativo ainda tão longo.

CONCLUSÃO: UMA POSSÍVEL INSPIRAÇÃO PARA O MERCADO BRASILEIRO

A análise da experiência europeia na condução do estabelecimento de uma estratégia de mercado único digital revela sua preocupação em assegurar que neste mercado estejam incluídas as melhores condições possíveis para a concorrência em âmbito digital. Se, de um lado, o desenvolvimento da economia digital revelou a obsolescência de muitos instrumentos empregados pela autoridade da concorrência europeia[12], por outro abriu uma enorme oportunidade de melhoria e atualização dos controles.

Dados do comércio eletrônico no Brasil indicam que mais de 20 milhões de pessoas passaram a fazer compras online no ano de 2020. Da mesma forma, estima-se que o número de

lojas na internet aumentou cerca de 40%, atingindo a incrível marca de 1,3 milhão de estabelecimentos[613].

Este crescimento tende a, naturalmente, potencializar a performance de plataformas de intermediação que atuam no país. Algumas delas, por exemplo, já oferecem serviços integrados como meios de pagamento e logística, tornando-se verdadeiras referências tanto para consumidores finais, como para vendedores profissionais. Por um lado, é absolutamente justificável que estes grandes agentes econômicos busquem a oferta destes serviços complementares, na medida em que não só garantem maior lucratividade, como também conseguem solucionar diversas dores do empreendedor, especialmente do pequeno e médio empresário. Basta pensar, por exemplo, na logística. Se, por um lado, a triagem e despacho de mercadorias dê sinais de evolução a passos largos, com os armazéns automatizados da Amazon[614][615] – muito embora se saiba que esta ainda não seja a realidade para a maior parte dos *e-sellers*, naturalmente – por outro, a logística de entrega e devolução ainda precisam de saltos evolutivos mais significativos, que dificilmente serão dados por pequenos e médios empresários.

---

[613] Dados disponíveis em https://resultadosdigitais.com.br/blog/dados-de-ecommerce-no-brasil/ , acessado em 10/7/2021.

[614] Para mais,ver "Inside Amazon's robot warehouses", disponível em https://www.youtube.com/watch?v=a77XyUI-zXo, acedido em 26/6/2021.

[615] É interessante relevar que, mesmo diante do quadro de avanços significativos, a automação integral dos processos de ***storage*** e ***shipping*** ainda está distante de ocorrer, como se depreende do artigo disponível em https://www.theverge.com/2019/5/1/18526092/amazon-warehouse-robotics-automation-ai-10-years-away, acessado em 26/6/2021. Interessante também a análise sobre a automação dos armazéns da Amazon disponível em https://www.vox.com/recode/2019/12/11/20982652/robots-amazon-warehouse-jobs-automation, acessado em 26/6/2021.

No entanto, é absolutamente salutar que estes movimentos de consolidação sejam observados com cautela, para que um ambiente de dependência econômica e, portanto, pobreza concorrencial, não se instale no país. É necessário, dessa forma, zelar para que o desenvolvimento dos mercados da economia digital permita a ampliação da concorrência, de maneira que consumidores finais e utilizadores profissionais possam tirar máximo proveito dos potenciais que estes novos modelos econômicos podem proporcionar.

Nesse sentido, e observando as lições da experiência da União Europeia, é chegado o tempo de o Brasil debruçar-se sobre esta questão, à exemplo do que vem fazendo o Conselho Administrativo de Defesa Econômica[616]. Em se tratando de uma área em que políticas públicas estão em mudança frequente, trata-se, portanto, de uma discussão urgente, sob pena de que quaisquer produtos regulatórios tardiamente idealizados já nasçam obsoletos.

[616] O CADE vem estudando a concorrência nos mercados digitais. Nesse sentido, há um valioso estudo em https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2020/documento-de-trabalho-n05-2020-concorrencia-em-mercados-digitais-uma-revisao-dos-relatorios- especializados.pdf , acessado em 10/7/2021.

O ITCMD NA HERANÇA DIGITAL

Rafaela Monteiro Montenegro[617]

INTRODUÇÃO

Diz a célebre frase atribuída a Benjamin Franklin que existem dois assuntos que, embora os seres humanos evitem, são inescapáveis: a morte e os tributos. Se os tributos já causam calafrios a nossos ancestrais há séculos, o acréscimo da tecnologia a essa equação é desafio que merece destaque. A relevância do tema ora enfrentado está justificada, na medida em que não há consenso sobre as normas gerais atinentes à matéria tributária no Brasil. Até mesmo os mais experientes precisam de prodigiosa memória para, ao analisar determinado caso concreto, considerar todas as leis, resoluções, instruções normativas, portarias e precedentes administrativos e judiciais. Por sua vez, a herança, que pressupõe a transferência de ativos pela via da *causa mortis*, é tópico igualmente complexo e que interessa à sociedade moderna, inclusive, diante do crescente mercado de bens e direitos no mundo virtual.

Como se sabe, no Brasil a competência para exigir o pagamento do imposto denominado ITCMD (transmissão *causa mortis* e doação), é dos Estados e do Distrito Federal,[618] que possuem, cada qual, a sua própria legislação. O problema é que,

[617] Rafaela Monteiro Montenegro é advogada sênior no Escritório Bichara Advogados. Graduada pela Escola de Direito da Fundação Getúlio Vargas FGV-RJ Pós-graduanda em Direito Digital pela UERJ/ITS

Membro da Comissão Especial de Defesa do Contribuinte e Política Fiscal OAB-RJ.

[618] CRFB/88. "Art. 155. Compete aos Estados e ao Distrito Federal instituir impostos sobre: I - transmissão causa mortis e doação, de quaisquer bens ou direitos."

inobstante o considerável tempo decorrido desde promulgação da Carta Magna de 1988, o Congresso Nacional não editou lei – ordinária ou complementar -, para disciplinar o tributo, sequer para dispor sobre critérios mínimos como os fatos geradores, base de cálculo, contribuintes e os responsáveis, o que abre espaço para disputas e insegurança.

A Constituição Federal, ao tratar sobre a competência para exigir o imposto,[619] estabelece regras que variam conforme a natureza do bem ou direito transmitido. No entanto, fato é que o ITCMD não estava previsto nas Constituições anteriores a 1988, de modo que o Código Tributário Nacional – CTN (Lei nº 5.172/1966), que deveria estabelecer as normas gerais relativas a esse tributo, na prática é silente sobre o tema. Como resultado, a legislação ordinária editada por cada um dos entes federativos preenche apenas em parte as lacunas interpretativas existentes, e que podem vir a surgir no futuro, a fim de dirimir assimetrias da era digital.

Recentemente, o Supremo Tribunal Federal – STF tratou a respeito do ITCMD e, em sede de repercussão geral (Tema nº 825), concluiu, no julgamento do Recurso Extraordinário nº 851.108/SP,[620] ao analisar o disposto no art. 155, §1º, inciso III,

[619] CRFB/88. "Art. 155. [...] I - relativamente a bens imóveis e respectivos direitos, compete ao Estado da situação do bem, ou ao Distrito Federal; II - relativamente a bens móveis, títulos e créditos, compete ao Estado onde se processar o inventário ou arrolamento, ou tiver domicílio o doador, ou ao Distrito Federal; III - terá competência para sua instituição regulada por lei complementar: a) se o doador tiver domicílio ou residência no exterior; b) se o de cujus possuía bens, era residente ou domiciliado ou teve o seu inventário processado no exterior."

[620] Para o Tema nº 825 da repercussão geral, o STF fixou a seguinte tese: "É vedado aos estados e ao Distrito Federal instituir o ITCMD nas hipóteses referidas no art. 155, § 1º, III, da Constituição Federal sem a intervenção da

que é necessária a edição de lei complementar, pela União, para que os Estados e o Distrito Federal possam, por sua vez, legislar supletivamente acerca do tributo incidente sobre bens e direitos no exterior. Portanto, enquanto isso não acontecer, há outros efeitos a serem destacados, decorrentes da referida previsão constitucional específica.

Nesse contexto, o que se pretende analisar é o escopo e os limites da herança digital, e se há possibilidade de o resultado do julgamento, pelo STF, para o ITCMD sobre bens e direitos no exterior (exigência de lei complementar), ter a sua conclusão estendida para os bens incorpóreos disponibilizados ao usuário através de tecnologia. Ademais, não parece constitucional, ou mesmo razoável, os Estados e o Distrito Federal afastarem regra eventualmente definida em Termos de Uso de plataformas, com o objetivo de proceder à cobrança do imposto nos casos envolvendo bens localizados no exterior, notadamente quando o doador ou *de cujus* houver adquirido o ativo objeto de doação ou sucessão através da *internet*, de provedores e prestadores de serviço domiciliados no exterior.

1. SOBRE O CONSENTIMENTO DO FALECIDO

A ilegal revisão dos termos de uso para fins fiscais

De acordo com o art. 5º, incisos XXII e XXX, da Constituição Federal de 1988,[621] a propriedade privada é pilar das garantias

lei complementar exigida pelo referido dispositivo constitucional"

[621] TEPEDINO, Gustavo e OLIVEIRA, Camila Helena Melchior Batista. "Streaming e Herança Digital". In Herança Digital: controvérsias e alternativas. Aline de Miranda Valverde Terra ... [et al] ; coordenado por Ana Carolina Brochado Teixeira, Lívia Teixeira Leal. – Indaiatuba: Editora Foco, 2021.

fundamentais e, por isso, norteadora do direito à herança, a ser resguardada sempre que há repercussão patrimonial no falecimento de pessoa física. É o que se infere do art. 91 do Código Civil, ao estabelecer que "constitui universalidade de direito o complexo de relações jurídicas, de uma pessoa, dotadas de valor econômico". Vale dizer, nas palavras de Gustavo Tepedino e Camila de Oliveira, que "(...) o objeto da sucessão, em última análise, consiste em bens e direitos suscetíveis de avaliação pecuniária e que, como tal, integram o patrimônio do de cujus".

Nesse contexto, o inventário é o procedimento por meio do qual serão listados todos os bens pertencentes ao *de cujus*, objetivando a sucessão hereditária, devendo haver um único inventário atrelado ao falecido, ainda que diversos sejam os bens deixados e independentemente das suas localizações (ou ente competente para exigir tributo), em respeito ao princípio da unidade da herança.[622] Contudo, há relevantes limitações no ordenamento jurídico com repercussões em matéria tributária.

Em primeiro lugar, ainda no âmbito do direito sucessório, nota-se que é inexistente previsão normativa que delimite o conteúdo da herança digital no Brasil ou que discrimine quais são os bens e os direitos passíveis de transmissão pela via sucessória, tampouco norma disciplinando o valor e a transmissibilidade dos dados pertencentes ao *de cujus*.[623] O Código

[622] TEPEDINO, Gustavo; NEVARES, Ana Luiza Maia; MEIRELLES, Rose Melo Vencelau. Fundamentos do Direito Civil. Rio de Janeiro: Forense, 2020. v.7. Direito das Sucessões, p. 229.

[623] O Projeto de Lei nº 5.820/2019, de autoria do Deputado Elias Vaz (PSB/GO), aguarda apreciação e propõe alterar o art. 1.881 do Código Civil, inserindo, em seu §4º, que a herança digital seria constituída por "vídeos, fotos, livros, senhas de redes sociais, e outros elementos armazenados

Civil de 2002, assim como a legislação tributária em vigor, está pautado em economia tangível e, embora sempre aplicável, no que couber, aos intangíveis, essas normas se apresentam ainda insuficientes. A Lei Geral de Proteção de Dados - LGPD, instituída pela Lei nº 13.709/2018, deixou de fora o regramento atinente à proteção de dados de pessoas que já faleceram.[624] Também resta ausente previsão nesse sentido no Marco Civil da Internet (Lei nº 12.965/2014).

Dito isso, ainda que seja superado o óbice relacionado à possibilidade, ou não, de transmitir bens digitais, surge um segundo problema, na medida em que, para a sucessão se tornar relevante para fins fiscais, é necessário que se atribua valor ao ativo, de acordo com o mercado. No entanto, tal tarefa pode se revelar inviável na prática, a depender da natureza do ativo transmitido.

Ultrapassado esse segundo e relevante obstáculo, é de se notar que os entes competentes, quais sejam os Estados e o Distrito Federal, não possuem os meios para conseguir fiscalizar o pagamento do imposto em determinadas situações.

Por exemplo, de acordo com a Receita Federal do Brasil – RFB, os residentes fiscais no país têm o dever de informar, na Ficha denominada "Bens e Direitos" da Declaração de Ajuste Anual (DAA), os criptoativos enquadrados nas especificações

---

exclusivamente na rede mundial de computadores, em nuvem" podendo ser provada por meio de codicilo em vídeo.

[624] Regulamento Geral de Proteção de Dados da União Europeia (***General Data Protection Regulation***, ou GDPR). Item 27 "o presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas."

da Instrução Normativa nº 1.888/2019, sendo certo que, na hipótese de falecimento, tudo aquilo que é, em tese, pertencente ao falecido deverá ser objeto de divisão entre os seus herdeiros, e consequentemente oferecido à tributação. Mas o fato de o ativo constar na DAA não significa que o bem pode ser transmitido aos herdeiros.

Não seria inusitado, porém, cogitar de hipótese em que o falecido não tenha deixado para nenhum dos herdeiros os seus *tokens* e outras chaves necessárias para efetivamente garantir o acesso aos criptoativos, hipótese em que a integração desse bem ao patrimônio dos sucessores pode se revelar deveras problemática.

Posto isso, repita-se que, antes de incluir qualquer bem ou direito no inventário, para a transmissão *causa mortis*, é preciso verificar se existe algum óbice de natureza fática ou contratual que impeça os sucessores de assumirem o domínio dos bens digitais detidos pelo *de cujus*. Por exemplo, sabe-se que muitas plataformas de serviços digitais impedem a sucessão das contas de usuários falecidos por seus herdeiros, exigindo que haja um consentimento do titular originário nesse sentido.

Aliás, no que toca ao aceite aos Termos de Uso, cabe salientar que pesquisas desenvolvidas no campo da psicologia comportamental, nas últimas quatro décadas, levantam dúvidas sobre a racionalidade de decisões humanas, demonstrando que, em geral, as pessoas priorizam prazeres imediatos, ainda que frívolos, como mero passatempos, em detrimento de seu bem-estar, o que abre portas para interpretar as disposições desses contratos sob o ponto de vista da abusividade.[625]

[625] Merece destaque a contribuição dos psicólogos israelenses Daniel Kah-

Ainda sobre os Termos de Uso, destaca-se decisão do Tribunal alemão – *Bundesgerichtshof* – , equivalente ao Superior Tribunal de Justiça no Brasil, que reconheceu a transmissibilidade da herança aos herdeiros de usuários de redes sociais, e definiu que caberia ao titular decidir o destino do conteúdo mantido na *internet*.[626] De todo modo, é razoável supor que, em grande parte dos casos, apenas a intervenção do Poder Judiciário seria capaz – em alguns nem mesmo isso – de equacionar conflitos e garantir aos sucessores o direito de acessar a herança consistente em bens digitais.

Outra questão relevante reside em saber se, nos casos em que autorizada a transmissibilidade dos ativos pelas plataformas que mantém os bens digitais deixados pelo *de cujus*, se os usuários poderiam dispor livremente sobre o patrimônio que será deixado em vida, ao arrepio da Lei ou da Constituição Federal. Os residentes fiscais no Brasil não podem violar a legítima, atribuindo acesso a terceiros, impedindo herdeiros legais a parte do patrimônio que lhes cabe, na forma do art. 1.845 do Código Civil.[627]

A despeito de existir reflexo econômico, então, as partes encontram limites, assim como o Fisco também está limitado

---

neman e Amos Tversky, cujos estudos demonstraram algumas categorias de vícios sistemáticos na capacidade de julgamento dos seres humanos, lançando as bases sobre as quais surgiria o campo da economia comportamental, levando o primeiro a ser agraciado com um prêmio Nobel de Economia. Ver, por exemplo, KAHNEMAN, Daniel; TVERSKY, Amos. Choices, Values, and Frames. *American Psychologist*, nº 39, 1984. p. 341-350.

[626] Nesse sentido, ver MENDES, Laura Schertel Ferreira e FRITZ, Karina "Case Report: Corte Alemã Reconhece a Transmissibilidade da Herança Digital". RDU, Porto Alegre, Volume 15, n. 85, 2019, 188-211, jan-fev 2019

[627] Código Civil. "Art. 1.845. São herdeiros necessários os descendentes, os ascendentes e o cônjuge."

para interpretar o destino dos bens após a morte ou doação efetuada pelo usuário, não podendo desconsiderar, para fins da tributação pelo ITCMD, ou quaisquer outros tributos, as limitações jurídicas e/ou fáticas à efetiva transmissibilidade dos bens.

Fato é que, no mundo real, as pessoas não dispõem de informações completas sobre as suas escolhas, tampouco possuem habilidades cognitivas ou força de vontade ilimitadas, o que nos leva – com frequência maior do que gostaríamos de admitir – a tomar decisões que acabam por sacrificar nosso próprio bem-estar. Não é diferente no domínio da *internet*, sobretudo no das redes sociais. O prazer imediato gerado pelas interações, para as quais somos arrastados por sofisticados algoritmos desenvolvidos para influir em nosso comportamento, nos leva a abdicar, de forma supostamente consciente e voluntária, de bens cujo valor ainda não somos, de modo geral, capazes de perceber.

Os provedores e prestadores de serviço, que atuam no Brasil, devem prestar informação clara ao consumidor (usuário) sobre o produto e/ou serviço ofertado, o que deve sempre incluir, em tese, o detalhamento sobre o que ocorrerá com os dados e com os ativos digitais após a sua morte. Afinal, o art. 6º da Lei nº 8.078/1990 – Código de Defesa do Consumidor, há de ser observado independentemente do meio utilizado.

> "Art. 6º São direitos básicos do consumidor:
>
> [...]
>
> III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação

> correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; [...]
>
> IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;
>
> V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas."

Nesse sentido, a LGPD também prevê que a autodeterminação informativa é fundamento para a disciplina da proteção de dados no Brasil, relevante parâmetro para que cada indivíduo possa controlar (e proteger) o seu patrimônio. Portanto, o cenário é amplo e o que se discute, no fim do dia, envolve criar mecanismos que sejam capazes de incentivar o mercado, de um lado, e de outro lado dar tratamento responsável à relação jurídica, bem como aos dados na Era Digital, que são os ativos mais relevantes.

Para que não haja vício de consentimento a ser suscitado, o usuário deve estar ciente de forma clara sobre o destino de sua conta/ativo, nos termos do CDC e LGPD, em especial sobre aquilo que optou por comprar ou comprometer o patrimônio. Mesmo assim, independentemente das iniciativas dos próprios provedores, de regular até a manifestação de luto para com os usuários, e de vir a proibir a utilização indevida dos dados através dos seus Termos de Uso, a questão é complexa e vai além do que se consegue levar a registro em documento, como a DAA entregue perante o Fisco Federal. De forma ou

de outra, o tema da abusividade das cláusulas de Termos de Uso não escapará de apreciação pelo Poder Judiciário.

Em geral, os gigantes digitais se utilizam de licenças outorgadas (direito de uso), e negam a transmissão aos herdeiros. É o que se verifica nos contratos por adesão com a *Netflix* e a *Amazon*, e nos Termos de Uso para manter conta junto ao *Facebook* e *Instagram*.[628] Há aqueles que mantêm conta que não é ligada a um indivíduo (CPF/CNPJ) propriamente dito, mas de caráter jornalístico, artístico, comercial, controlado por terceiros, e que geram receita, junto a patrocinadores e até mesmo remuneração paga pela própria plataforma, como oferece o *YouTube*, que remunera os influenciadores com significativa movimentação de seguidores.

Na cláusula 4.2 dos Termos de Uso, a *Netflix*[629] se limitou a indicar como os familiares e amigos devem proceder para o cancelamento de conta de assinante falecido. Já o *Spotify* proíbe a utilização de *login* e senha de outra pessoa.[630] Já

[628] Código Civil. "Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau.

[629] A cláusula 4.2 dos Termos de Uso da Netflix "4.2. O serviço Netflix e todo o conteúdo visualizado por intermédio do serviço Netflix destinam-se exclusivamente para uso pessoal e não comercial, não podendo ser compartilhados com pessoas de fora da sua família. Durante sua assinatura Netflix, a Netflix concede a você um direito limitado, não exclusivo e intransferível para acessar o serviço Netflix e assistir ao conteúdo da Netflix. Exceto pelo descrito acima, nenhum outro direito, titularidade ou participação lhe é concedido. Você concorda em não utilizar o serviço em exibições públicas".

[630] Cláusula 9 dos Termos de Uso do Spotify – Diretrizes de usuário. "11.

nos Termos de Uso do *Kindle Unlimited*, e da *Amazon Prime Video*,[631] é possível ler que se concede "uma licença não exclusiva, intransferível, não sublicenciável e limitada durante o Período de Visualização aplicável, para acessar e visualizar o Conteúdo Digital em conformidade com as Regras de Uso, para uso pessoal, não comercial e privado. Podemos remover automaticamente Conteúdo Digital do seu Dispositivo Compatível após o final de seu Período de Visualização".

Conclui-se que a plataforma e o usuário estão vinculados à Lei, e à governança corporativa e às políticas de privacidade estabelecidas, e tais parâmetros devem ser respeitados pelos donatários, herdeiros e *de cujus*. Os Tribunais Superiores, STF e STJ, ainda não se debruçaram sobre a transmissibilidade na herança digital, tampouco há notícia de litígios administrativos ou judiciais tratando do ITCMD sobre ativos incorpóreos, como os objetos adquiridos para melhorar a performance em jogos eletrônicos, por exemplo, e outros intangíveis.

Em algum momento haverá caso concreto envolvendo valor econômico agregado à administração de contas de pessoa pública falecida que figura como celebridade,[632] e o Fisco. A administração do perfil é atividade lucrativa, não sendo raro que ocorra incremento de seguidores e de publicidade após o

fornecer sua senha para qualquer outra pessoa ou usar o nome de usuário e senha de qualquer outra pessoa". Disponível em https://www.spotify.com/br/legal/end-user-agreement/. Acesso em 10/07/21.

[631] Termos de Uso da Amazon Prime Video disponível em https://www.primevideo.com/help/ref=atv_hp_nd_nav?nodeId=G202095490. Acesso em 22/11/21.

[632] LEAL, Lívia Teixeira. Internet e morte do usuário: a necessária superação do paradigma da herança digital. Revista Brasileira de Direito Civil, v. 16, abr./jun. 2018.

falecimento. No entanto, embora haja manifestação de riqueza passível de sofrer com a voraz pretensão do Fisco, poder-se-ia argumentar a inocorrência de fato gerador do ITCMD, pois a cobrança não recairia sobre a herança digital, mas sobre a renda auferida, que já estará sujeita à tributação pelo Imposto de Renda. Todavia, seria igualmente plausível a alegação de que um perfil em rede social capaz de gerar receitas de modo consistente possui valor econômico passível de ser aferido por diversos métodos utilizados na avaliação de negócios, hipótese em que a cobrança do ITCMD seria defensável.

Há de ser respeitada a escolha que é externalizada, em vida, pelo usuário quando do aceite aos Termos de Uso das plataformas digitais, sendo a decisão definitiva e que não comporta controle pelo Fisco, almejando tributar a transferência de ativos, pois o consentimento representa ato de vontade. Verdade seja dita, o alcance da tecnologia é imprevisível. Contudo, uma vez existente Termos de Uso dispondo que o direito é restrito, limitado e intransferível, a princípio não poderiam os herdeiros, ou o Estado, interessado no patrimônio do *de cujus*, interpretar ou questionar a declaração manifestada em vida, com o objetivo de proceder à cobrança de ITCMD, ou outro tributo, incidente sobre bens e direitos digitais, ensejando a perpetuação das informações no ambiente digital à revelia de qualquer escolha do seu detentor originário.

Assim, superado que o consentimento manifestado pelo *de cujus*, no que tange à transmissão *causa mortis*, ou mesmo na doação, é condição indispensável para que se possa incluir bens e direitos no inventário, e que não caberia à Fazenda Pública ponderar sobre a aplicação dos Termos de Uso celebrado entre o falecido e a plataforma, mas apenas respeitá-lo quando em consonância com a legislação vigente, é preciso

avaliar de que forma a competência tributária deve se aplicar na prática.

2. SOBRE OS BENS E DIREITOS DIGITAIS

Os conflitos de competência para o itcmd – o re nº 851.108 e a posição do STF quanto à reserva de lei complementar

O STF já reconheceu que a aquisição de bens e de direitos vai além de uma simples compra efetuada presencialmente pelo consumidor na loja, ou encomenda de produto com suporte físico, e que transcende o lastro material (RE nº 176.626/SP). Desde então, muita coisa mudou, e o desenvolvimento da engenharia computacional está permitindo que os usuários utilizem (e desenvolvam) número cada vez maior de facilidades, para as mais diversas finalidades. É exemplo a aquisição de imóveis digitais, que existem apenas no universo virtual, utilizados para replicar a realidade em outro ambiente. A *Republic Realm*, empresa dos Estados Unidos, investiu quase 1 milhão de dólares em propriedade no *Decentraland*, espécie de jogo baseado em *blockchain* e que usa criptomoedas e *NFTs* nas negociações.[633]

Como dito, o Brasil optou por tributar a transmissão *causa mortis* através do ITCMD, imposto de competência estadual, e do Distrito Federal, e que envolve também o fato gerador sobre a doação efetuada a terceiros. O problema surge quando confrontada tal prerrogativa para além dos bens e ativos tangíveis. A Economia Digital envolve desafios maiores, como

[633] Nesse sentido, https://exame.com/future-of-money/dinheiro-tendencias/empresa-compra-imovel-virtual-de-jogo-em-blockchain-por-r-5-milhoes/. Acesso em 22/11/21.

identificar a natureza de *tokens* fungíveis, a localização deles no ambiente cibernético, definir a base de cálculo sobre a qual deverá recair a alíquota do imposto, e efetivamente fiscalizar o contribuinte.

É exemplo disso a Instrução Normativa RFB nº 1.888/2019, que disciplina, no âmbito da Receita Federal do Brasil, a obrigatoriedade de as pessoas físicas e jurídicas prestarem informações relativas às operações com criptoativos, ao passo que se sabe que as autoridades fiscais não têm como conferir a veracidade daquilo que é inserido pelo detentor do ativo – e o fato de que existem, perante o Poder Legislativo, propostas em tramitação que pretendem modificar o ordenamento jurídico vigente, como o Projeto de Lei nº 67/2021, que enumera não exaustivamente quais seriam as espécies de bens e direitos cuja transmissão *causa mortis* – e por doação – e seria passível de incidência do ITCMD , destacando dentre eles as "*criptomoedas, derivações ou assemelhados*", e o Projeto de Lei que pretende alterar o art. 1.788 do Código Civil,[634] para normatizar, na esfera cível, a herança digital.

A despeito de tais pretensões, e de diversas outras,[635] a celeuma pode ir além dos criptoativos, livros digitais e milhas aéreas, no que se refere às heranças digitais. Essa expectativa é relevante para fins tributários, pois a tecnologia é capaz de gerar uma verdadeira confusão quanto ao sujeito ativo da obrigação (Estado, *lato sensu*, competente para tributar a

[634] Código Civil. "Art. 1.788. Morrendo a pessoa sem testamento, transmite a herança aos herdeiros legítimos; o mesmo ocorrerá quanto aos bens que não forem compreendidos no testamento; e subsiste a sucessão legítima se o testamento caducar, ou for julgado nulo."

[635] Hoje em tramitação, o PL nº 5.820/19, PL nº 6468/19, PL nº 3050/20 – igual PL nº 6468, PL nº 3.051/20 – com redação similar ao PL nº 7.742/17

atividade), o sujeito passivo (quem deve figurar como devedor do tributo), ou mesmo o local de incidência, o que torna questionável a atuação da Fazenda Pública. De qualquer forma, não há regramento suficiente para o ITCMD.

A herança digital não é matéria simples. E por isso não é razoável que os contribuintes domiciliados no Brasil tenham que se submeter a insegurança jurídica, ou o setor de tecnologia sofrer qualquer limitação indevida, ainda que sob a justificativa tributária. É claro que não se pretende defender neste artigo que herdeiros não devam pagar tributos, seja o ITCMD ou mesmo Imposto de Renda da Pessoa Física, mas tão somente alertar para a complexidade da situação relativamente a bens e direitos digitais.

Sob essa perspectiva, é relevante o fato de as transferências patrimoniais digitais envolverem majoritariamente partes (provedores, prestadores do serviço, intermediários, usuário, dentre outros) localizadas em países distintos, além do Brasil, o que traz à tona a necessidade de se avaliar a aplicabilidade – ou não – de regra específica da Constituição Federal de 1988, para dispor sobre a competência dos Estados e Distrito Federal para as situações envolvendo residência e bens mantidos no exterior.

> Art. 155. Compete aos Estados e ao Distrito Federal instituir impostos sobre:
>
> I - transmissão causa mortis e doação, de quaisquer bens ou direitos; [...]
>
> § 1º O imposto previsto no inciso I:
>
> [...]

> III - terá competência para sua instituição regulada por lei complementar:
>
> a) se o doador tiver domicílio ou residência no exterior;
>
> b) se o de cujus possuía bens, era residente ou domiciliado ou teve o seu inventário processado no exterior.

No caso do ITCMD, o mecanismo para evitar potencial conflito de competência entre os entes da federação foi determinado pelo legislador constituinte, ao exigir expressamente a edição de lei complementar quando o doador tiver domicílio ou residência no exterior ou o *de cujus* possuir bens, tiver sido residente ou domiciliado ou tiver seu inventário processado no exterior. Nessas hipóteses, é a lei complementar que, "desempenhando a função que lhe foi atribuída pelo art. 146, I, da Magna Carta, vai disciplinar o assunto, dando critérios para que se saiba, com exatidão, a qual unidade federativa compete o imposto em tela"[636] Em comentário ao disposto no art. 155, §1º, da Constituição Federal de 1988, o Professor Luis Eduardo Schoueri é assertivo,[637]

> Claro que nem sempre caberá a lei complementar, se os incisos anteriores já resolverem o tema do conflito de competência. Por exemplo, considere-se

[636] CARRAZA, Roque Antonio. Curso de Direito Constitucional Tributário. 27ª ed., São Paulo, Malheiros, p. 1049

[637] SHOUERI, Luis Eduardo. Direito Tributário – sistema tributário e discriminação de competências tributárias, 6ª. ed. Saraiva. p. 281.

> o caso de uma sucessão envolvendo dois bens – um imóvel, situado em Pernambuco e uma conta bancária, na Suíça. Admita-se que o inventário foi processado em Alagoas, onde residia o de cujus. Será necessária lei complementar? A resposta é negativa, já que as normas dos dois primeiros incisos do § 1º do artigo 155 do texto constitucional já resolvem, por completo, o conflito, assegurando a Pernambuco a tributação da transmissão do imóvel e a Alagoas a da conta corrente no exterior. Diversa seria a situação no exemplo inverso: sucessão envolvendo imóvel na Suíça e conta bancária em Alagoas; de cujos residia na Suíça, onde se processou seu inventário. Neste caso, vê-se que as duas primeiras normas não resolvem a competência, fazendo-se necessária a lei complementar.

Contudo, a despeito de existir previsão expressa na Constituição Federal de 1988 quanto ao ITCMD sobre bens no exterior, alguns Estados, diante da inexistência de lei complementar, ou mesmo ordinária, passaram a dispor sobre a matéria, optando por instituir normas internas, e exigir o pagamento do imposto de forma ampla. Ainda que o doador estivesse no exterior, e o falecido mantivesse bens fora do país, o herdeiro e o donatário (quem recebe a doação), nos territórios com Lei Estadual, se viam obrigados a ter que arcar com o imposto.[638]

É o caso de São Paulo. Com amparo no art. 24, inciso I, §3º, da CRFB/88, que prevê que "inexistindo lei federal sobre

[638] Vide, por exemplo, no Estado do Rio de Janeiro, as Leis n.º 7.174/15 e 1.427/89; no Estado de Minas Gerais, a Lei nº 14.941/03; e no Distrito Federal, a Lei nº 3.804/06.

normas gerais, os Estados exercerão a competência legislativa plena, para atender a suas peculiaridades", e no art. 34, §3º, do ADCT,[639] o Fisco paulista defendeu perante o Supremo Tribunal Federal, no RE nº 851.108/SP, a constitucionalidade da Lei nº 10.750/00,[640] que estabelecia a sua prerrogativa para tanto.

Na origem, o caso versava sobre Mandado de Segurança impetrado em face de ato de autoridade fiscal do Estado de São Paulo, com vistas à cobrança do ITCMD relativamente a bens recebidos no exterior, a título de herança. O contribuinte recebeu doação testamentária, consistente em imóvel localizado na Itália e determinada quantia em Euros, de cidadão italiano domiciliado naquele país. A herança foi declarada pelo herdeiro perante a Receita Federal do Brasil, por meio da Declaração de Ajuste Anual da Pessoa Física. Contudo, a despeito do recolhimento de tributos à Itália, a autoridade fiscal no Estado de São Paulo promoveu notificação para o pagamento do imposto sobre a herança recebida. Considerando as decisões

[639] CRFB/88. ADCT. "Art. 34. O sistema tributário nacional entrará em vigor a partir do primeiro dia do quinto mês seguinte ao da promulgação da Constituição, mantido, até então, o da Constituição de 1967, com a redação dada pela Emenda nº 1, de 1969, e pelas posteriores. [...] § 3º Promulgada a Constituição, a União, os Estados, o Distrito Federal e os Municípios poderão editar as leis necessárias à aplicação do sistema tributário nacional nela previsto."

[640] A Lei paulista dispunha o seguinte: "Artigo 4º – O imposto devido nas hipóteses abaixo especificadas, sempre que o doador residir ou tiver domicílio no exterior, e, no caso de morte, se o 'de cujus' possuía bens, era residente ou teve seu inventário processado fora do país : I – sendo corpóreo o bem transmitido: a) quando se encontrar no território do Estado; b) quando se encontrar no exterior e o herdeiro, legatário ou donatário tiver domicílio neste Estado; II – sendo incorpóreo o bem transmitido: a) quando o ato de sua transferência ou liquidação ocorrer neste Estado; b) quando o ato referido na alínea anterior ocorrer no exterior e o herdeiro, legatário ou donatário tiver domicílio neste Estado."

favoráveis obtidas pelo contribuinte em tese devedor, nas instâncias ordinárias, o Fisco interpôs Recurso Extraordinário, este que também teve o seu provimento negado no STF, à maioria de votos.

Ocorre que as disputas atualmente objeto de julgamento pelos Tribunais no Brasil não envolvem a exigência de tributos sobre a herança digital. Os Tribunais vem sendo instados a se manifestar sobre o acesso de herdeiros a bens e direitos digitais de pessoa física falecida. No entanto, tais decisões têm em comum o fato de dizerem respeito à esfera cível, e estarem fora do espectro da Fazenda Pública. É o que se infere das demandas envolvendo pedido de familiar para a apresentação em juízo de conteúdo de e-mail de cônjuge falecido[641] e/ou o acesso a *login* para uso de dispositivo móvel (celular),[642] bem como para prestadores de serviço procederem à exclusão de conta mantida em rede social.[643] Há variada gama de possibilidades sobre o que pode surgir nas próximas décadas. Porém, é de natural expectativa que, diante do potencial do mercado tecnológico, e do rápido crescimento da sua importância, o assunto chame atenção do Fisco e chegue aos Tribunais para avaliarem a riqueza digital gerada em favor do herdeiro.

Diante disso, não se pretende esgotar o assunto, mas trazer à baila reflexão sobre em que medida o direito tributário tem legitimidade para adentrar nesse campo.

---

[641] TJ-SP. 10ª Vara Cível, Processo nº 1036531-51.2018.8.26.0224, j. 28/02/20.

[642] TJ-MG. Vara Única da Comarca de Pompeu, Processo nº 0023375-92.2017.8.13.0520, j. 08/06/18.

[643] TJ-SP. 31ª Câmara de Direito Privado, Apelação Cível nº 1119688-66.2019.8.26.0100, j. 09/03/21.

CONCLUSÃO

As regras de tributação, tanto no Brasil como no mundo, foram concebidas originalmente para ativos tangíveis e é cada vez mais comum, diante do avanço tecnológico, que os contribuintes e as autoridades fiscais tenham dificuldade de equacionar interesses, quando o assunto envolve definir a tributação de operações no mundo digital, e o *quantum* a ser pago e a quem. Outrossim, o cenário em termos de arrecadação tributária para ITCMD e para o desenvolvimento de tecnologias é amplo.

O fluxo de bens físicos, como joias, dinheiro e imóveis é rastreável, e assim conta com fiscalização passível de ser implementada através de terceiros, mediante a atribuição do dever de colaboração daqueles que mantém a custódia do ativo e estão sujeitos a intensa regulamentação, como as instituições financeiras, ao passo que, na economia digital, nem sempre existe a figura do intermediário apto a desempenhar a mesma atividade, o que dificulta o exercício de poder de polícia pelo Estado, a fim de concretizar a arrecadação tributária legítima sobre os ativos digitais.

É natural existirem conflitos em decorrência do evento morte, por questões federativas e de políticas públicas, quando se escolhe garantir ao herdeiro a prerrogativa de suceder o patrimônio do *de cujus*, e ao Estado o dever de tributar essa transferência. Mas o problema maior para aqueles que investem em ativos digitais é o tempo que se leva, no Brasil, para se decidir algo de maneira definitiva. Tal como a edição de uma simples lei para dispor sobre o ITCMD, o que pende desde 1988, como descrito, ou de decisão transitada em julgado do Plenário do STF. Quando do RE nº 851.108/SP, a Corte

poderia ter ido materialmente além das suas já longas mais de 80 páginas de acórdão, que sequer guiam o intérprete no campo de incidência dos bens digitais e disponibilizados por empresas com residência fora do território nacional.

Não parece adequado que eventual regramento tributário para o ITCMD restrinja inadvertidamente o surgimento de novas tecnologias, com combinações possíveis de produtos disponíveis para além do que a mente humana consegue alcançar hoje. E o mercado dos games (jogos eletrônicos) é apenas um dos setores no mundo digital, capaz de suscitar essa variedade de premissas. Contudo, com o avanço tecnológico, a indústria dos jogos eletrônicos vem ocupando lugar de destaque, com milhares de dólares envolvidos. Diante disso, não seria de se admirar, embora fosse absurdo, que os Estados passassem a exigir dos herdeiros o pagamento de ITCMD quando, dentro da realidade virtual, herdassem objetos como uma espada, imóvel, carro etc.

Em 2017, a Newzoo, especializada em pesquisas sobre a indústria de jogos eletrônicos, classificou o Brasil em 13º lugar no *ranking* de países consumidores desse mercado. Os brasileiros gastaram, nesse período, em torno de 1.3 bilhão de dólares, ao passo que os chineses, líderes do *ranking*, consumiram 32.5 bilhões de dólares em jogos, seguidos dos americanos, com gastos na ordem de 25.4 bilhões de dólares.[644] Não há dúvida da lucratividade do mercado, que está em ascensão. A Newzoo prevê aumento de participação do segmento *games* para *smartphones* de 36%, em 2017, e

[644] https://newzoo.com/insights/rankings/top-100-countries-by-game-revenues/. Acesso em 22/11/21.

para 49% em 2021.[645] Sendo assim, basta olhar ao redor para concluir que a realidade mudou.

[645] https://newzoo.com/key-numbers/. Acesso realizado em 22/11/21.