UNIVERSIDADE FEDERAL DE ALAGOAS
CAMPUS A. C. SIMÕES
FACULDADE DE DIREITO DE ALAGOAS

LGPD E *USER EXPERIENCE* (*UX*): ABORDAGEM DAS PRÁTICAS DE CONSENTIMENTO NA UTILIZAÇÃO DE *COOKIES* DE NAVEGADOR

MACEIÓ
2023

JOSÉ WAGNER RODRIGUES DOS SANTOS

LGPD E *USER EXPERIENCE* (*UX*)): ABORDAGEM DAS PRÁTICAS DE CONSENTIMENTO NA UTILIZAÇÃO DE *COOKIES* DE NAVEGADOR

Trabalho de Conclusão de Curso apresentado ao de Direito da Universidade Federal de Alagoas – UFAL, como requisito parcial à obtenção do título de Bacharelado em Direito.

Orientador: Prof. Dr. Filipe Lôbo Gomes

MACEIÓ

2023

Catalogação na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

S237l Santos, José Wagner Rodrigues dos.
LGPD e User Experience (UX): abordagem das práticas de consentimento na utilização de cookies de navegador / José Wagner Rodrigues dos Santos. – 2023.
103 f. : il.

Orientador: Filipe Lôbo Gomes.
Monografia (Trabalho de Conclusão de Curso em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Maceió, 2023.

Bibliografia: f. 94-103.

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. Consentimento. 3. *Cookies* (Computação). Experiência de usuário. I. Título.

CDU: 34:004.6

Dedico
Aos meus pais, José (in memoriam) e Margarida, aos meus afilhados, Cícero e Alícia, ao meu amigo Marcos e às minhas irmãs Josineide, Patrícia, Eliane, Adriana e seus filhos.

AGRADECIMENTOS

Aos meus pais, pelo amor, base e sustento.

À minha família, pelo convívio.

Aos meus afilhados, pelo afeto.

Ao meu amigo Marcos Lucas, pelo apoio.

Ao Prof. Dr. Filipe Lôbo Gomes, pela orientação.

Aos professores do curso, pela formação.

Ao corpo técnico-administrativo, pela disponibilidade.

Ao sistema de educação pública do país, pelas oportunidades.

RESUMO

Trata-se de estudo sobre a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) –, a área do *design* de *interface* homem-máquina, voltada à *User Experience* (*UX*) – Experiência de Usuário –, e seus impactos sobre as políticas de obtenção de consentimento na utilização de *cookies* de navegador, dos usuários titulares dos dados pessoais. A pesquisa busca responder as seguintes hipóteses: (H1) *UX Design* tem alguma implicação sobre os modelos de obtenção do consentimento na utilização de *cookies* por parte dos controladores dos dados pessoais dos titulares? (H2) as técnicas de obtenção do consentimento utilizadas estão alinhadas com as diretrizes assentadas na LGPD? (H3) existem abordagens alternativas às ferramentas de obtenção do consentimento mais comumente utilizadas para a utilização de *cookies* dos titulares dos dados pessoais, que melhor se adequam às exigências da LGPD? Discorrendo acerca da construção histórica do arcabouço jurídico internacional que resultou na instauração da LGPD; das legislações já existentes no sistema jurídico brasileiro acerca da proteção de dados pessoais; dos conceitos referentes à Ciência da Computação ligados ao objeto da pesquisa; e aos julgados dos Tribunais Superiores pátrios, intenta-se trazer à reflexão indagações que colaborem para o aperfeiçoamento das práticas de obtenção do consentimento de uso dos *cookies* de navegador dos titulares dos dados, em consonância com os requisitos adstritos ao consentimento, enquanto base legal estipulada pela norma: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Palavras-chave: LGPD. Consentimento. *Cookies.* Experiência de Usuário.

ABSTRACT

This is a study on Law nº 13.709/2018 – General Data Protection Law (LGPD) –, User Experience (UX), and their impacts on policies for obtaining consent in the use of browser cookies, of the users who hold the personal data. The research seeks to answer the following hypotheses: (H1) does the UX Design have any implications on the models for obtaining consent in the use of cookies by the controllers of the holders' personal data? (H2) Are the techniques for obtaining consent used in line with the guidelines established in the LGPD? (H3) are there alternative approaches to the most used tools for obtaining consent for the use of cookies by the holders of personal data, which best suit the requirements of the LGPD? Discussing the historical construction of the international legal framework that resulted in the establishment of the LGPD; the existing legislation in the Brazilian legal system regarding the protection of personal data; the concepts related to Computer Science linked to the research object; and the judgments of the national Superior Courts, it is intended to bring to the reflection questions that collaborate to improve the practices of obtaining consent for the use of browser cookies from data subjects, in line with the requirements attached to consent, as a legal basis stipulated by the norm: free, informed and unequivocal expression by which the holder agrees to the processing of his personal data for a specific purpose.

Keywords: LGPD. Consent. Cookies. User Experience.

SUMÁRIO

1 INTRODUÇÃO

Em sua atual fase pós-moderna, a sociedade vem passando por transformações radicais e disruptivas no modo como seres humanos estão vivendo, trabalhando, se relacionando e produzindo conhecimento, como oportunamente apontou Schwab (2016), fundador do Fórum Econômico Mundial. O autor vaticinou mudanças profundas na nossa perspectiva histórica, com consequências ao mesmo tempo promissoras e perigosas nunca vistas. Sua principal preocupação recai sobre o pensamento linear, sem predição de rupturas por parte dos tomadores de decisão, cuja praxe costuma ser voltar a atenção para as preocupações imediatas, tornando o pensamento estratégico nebuloso, quando se trata da escolha, regulação e aprimoramento das inovações que moldam o futuro.

Nesta sociedade hiper conectada, onde qualquer informação está a um clique, ou um toque, as transformações que sempre impactaram o Direito – por sua própria natureza mutante, em tentar adaptar-se às variadas demandas das sociedades e seus agrupamentos humanos em constante ebulição –, merecem acurada atenção no que tange à tutela de dados pessoais. Essa emergente era da informação digital trouxe, junto com todas as benesses prometidas, desafios deveras perturbadores em várias frentes do nosso mundo contemporâneo, seja na esfera das liberdades individuais, sociais, dos meios de produção e até mesmo do futuro das democracias.

Zuboff (2021) analisou as imbricadas relações por trás de uma engenhosa força conduzida por novos imperativos econômicos que desconsideram normas sociais e anulam direitos básicos associados à autonomia individual – essenciais para a própria possibilidade de uma sociedade democrática –, por meio de um sistema econômico emergente, cunhado pela autora, nos termos Capitalismo de Vigilância.

Nesse novo modelo de capitalismo, a experiência humana se tornou a matéria-prima gratuita, utilizada para a tradução em dados comportamentais, reivindicada unilateralmente pelos principais atores do próprio capitalismo de vigilância. Trata-se do uso e manipulação de dados que, embora sejam aplicados para o aprimoramento de produtos e serviços, acabam por tornar-se "supéravit comportamental" do proprietário.

O tratamento realizado junto aos dados dos usuários acaba por alimentar processos conhecidos como "inteligência de máquina", manufaturando "produtos de predição" que antecipam as ações dos indivíduos no momento presente, no momento seguinte e no momento

futuro. Comercializados num novo tipo de "mercado de comportamentos futuros", esses produtos de predições têm gerado acúmulo vertiginoso de riqueza aos capitalistas de vigilância, por meio da exploração da cobiça das companhias no nosso comportamento futuro.

Na esteira dessa nova lógica em vigor nas operações de mercado global, o Brasil estreou no rol dos países da América Latina que possuíam leis gerais para a proteção dos dados pessoais dos titulares, com a aprovação da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD). Os oito anos que separaram a publicação da primeira consulta pública até a aprovação da LGPD – entre os anos de 2010 e 2018 –, marcados por intensos debates, atestam o valor atribuído ao processo democrático, na busca da elaboração de uma estrutura normativa que harmonizasse e ampliasse o direito à proteção de dados pessoais no contexto regulatório brasileiro.

Salientamos que o trabalho objetiva analisar a interseção entre a Lei Geral de Proteção de Dados Pessoais (LGPD), o uso de *cookies* e o consentimento circunscritos ao âmbito do Direito Civil. A entrada em vigor da LGPD em setembro de 2020 trouxe significativas mudanças na forma como os dados pessoais são tratados e protegidos no Brasil. Dentre os aspectos abrangidos pela Lei, destaca-se a necessidade de obtenção de consentimento válido dos usuários para o uso de *cookies*, que são amplamente utilizados na coleta de informações online. Assim, torna-se essencial compreender como o consentimento se enquadra no contexto civil, considerando as implicações jurídicas relacionadas à proteção de dados.

A utilização de *cookies*, que são pequenos arquivos de texto armazenados nos dispositivos dos usuários, desempenha um papel fundamental na coleta e processamento de dados pessoais. No entanto, essa prática levanta questões relacionadas à privacidade e à proteção de dados, especialmente à luz da LGPD. Nesse sentido, é relevante investigar como o consentimento é abordado no Direito Civil no contexto do uso de *cookies*. Compreender as bases legais para a obtenção de consentimento, bem como as condições para sua validade, torna-se crucial para garantir a conformidade com a legislação de proteção de dados.

Diante do panorama legal atual, é fundamental examinar as implicações e os desafios que surgem na obtenção do consentimento para o uso de *cookies* no contexto da LGPD. Questões como a transparência na coleta de dados, a possibilidade de consentimento tácito e a necessidade de consentimento específico para diferentes finalidades tornam-se centrais para uma análise aprofundada. Ademais, a presente pesquisa também buscará identificar eventuais lacunas ou contradições entre as normas de proteção de dados e os princípios do direito civil,

visando a propor soluções que harmonizem essas áreas e assegurem a proteção efetiva dos direitos individuais no ambiente digital.

Como já mencionado, os limites da pesquisa estão restritos à seara civilista, não abarcando análises de cunho criminal. Quando muito – pela escolha metodológica essencialmente descritiva dos elementos –, faremos citações a artigos do Códex Penal, apenas a título de exemplificação de norma que abrange questões ligadas à privacidade. Da mesma forma, artigos do Código de Defesa do Consumidor (CDC), também serão citados paralelamente aos da LGPD, como comparação da técnica legislativa percorrida na elaboração de ambas as normas. Finalmente, no item 4.2 – Comentários ao texto da Lei nº 13.079/2018 (LGPD) –, a pesquisa se limita à análise de caráter panorâmico do texto da Lei. O intuito não foi o de encerrar, pormenorizadamente, os tópicos alcançados pela Lei, mas elucidar os pontos preponderantes ao tema e objetivos do trabalho.

O norte teórico da análise do nosso objeto de estudo é composto pelas quatro modalidades de intervenção no comportamento humano (leis, normas sociais, mercado e arquitetura) estabelecidas por Lessig (2006), para se debruçar sobre a origem, alcance e perspectivas da Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD) –, acerca das políticas de consentimento e coleta de dados adotados pelos controladores de dados, assim como a implementação das ferramentas e técnicas envolvidas no processo de autorização do uso de *cookies* de navegador pode impactar a liberdade de escolha dos titulares dos dados, a partir do *design* de Experiência do Usuário (*UX*), no compartilhamento dos seus dados pessoais com terceiros e sua privacidade, sob a perspectiva do novo arcabouço jurídico instaurado pela LGPD.

A estratégia metodológica empregada é a da análise qualitativa dos elementos, para interpretá-los por meio do método descritivo, em busca de respostas às hipóteses teóricas levantadas, e diagnosticar os novos contornos do direito à privacidade na rede, ante o fenômeno da prática do consentimento de uso dos *cookies* de navegador. Serão analisadas obras interdisciplinares a fim de se verificar a interseção entre Direito e tecnologia, como a relação entre *cookies* de navegador, *UX Design*, técnicas de obtenção do consentimento e as consequências práticas sobre a livre manifestação e a privacidade dos dados dos usuários. A pesquisa consiste, basicamente, na análise de instrumentos indiretos, como obras bibliográficas sobre Direito e tecnologia. O método adotado é o dedutivo, embasado a partir de consultas sobre a literatura disponível: bibliografia, doutrinas, jurisprudências, artigos acadêmicos e legislações nacionais e internacionais.

No capítulo 2, abordaremos a evolução histórica, conceitos e espécies do direito à privacidade. No capítulo 3, discorreremos sobre o estado da arte da proteção de dados no mundo, o papel dos Estados na era da informação, e os antecedentes da Lei n° 13.079/2018 – Lei Geral de Proteção de Dados (LGPD). No capítulo 4, analisaremos a dialética entre a CF/88 e as normas setoriais já existentes, assim como teceremos comentários ao texto da LGPD, nos pontos que consideramos mais significativos ao desenvolvimento da pesquisa. No capítulo 5, faremos considerações atinentes ao campo da Responsabilidade Civil, analisaremos o regime jurídico da responsabilidade dos agentes de tratamento de dados e os desafios da Agência Nacional de Proteção de Dados (ANPD) na fiscalização e aplicação das sanções previstas na LGPD. Por fim, no capítulo 6, elucidaremos conceitos da Ciência da Computação, trataremos sobre o *design* de *User Experience* (*UX*) e *cookies* de navegador, assim como as técnicas de obtenção do consentimento de uso dos *cookies* de navegador.

2 CONSIDERAÇÕES SOBRE O DIREITO À PRIVACIDADE

2.1 Evolução histórica

A evolução histórica do direito à privacidade é um tema complexo que tem sido objeto de discussão ao longo dos séculos. Desde a antiguidade, o ser humano tem buscado proteger sua intimidade e sua individualidade de ingerências indevidas, seja na esfera pública ou privada. Com o passar do tempo, a proteção à privacidade foi sendo ampliada e incorporada nos sistemas jurídicos de diversos países. No entanto, a evolução tecnológica e das comunicações tem trazido novos desafios para a proteção da privacidade, exigindo a constante adaptação das leis e dos sistemas jurídicos. Por isso, compreender a evolução histórica do direito à privacidade é fundamental para entender como esse direito tem sido moldado e como ele pode ser aprimorado para atender às necessidades da sociedade atual.

Flaherty (1991, pp. 832-833) aponta que, historicamente, enquanto conceito sem previsão legal, a preservação da privacidade esteve a cargo de cada indivíduo, ora em caráter mais amplo, ora mais restrito e que, a despeito da drástica transformação desta concepção, favorecida pelo início da industrialização no século XIX – embora muitos esforços tenham sido engendrados na manutenção da privacidade –, a instituição de autoridades e a edição de leis foi imprescindível no intento de sua preservação.

Cancelier (2017, p. 214), fazendo referência aos pontos de origem das categorias público e privado, leciona que na antiguidade clássica grega – posteriormente transmitidas à cultura romana – havia a esfera da *polis* e a esfera do *oikos*, sendo aquela comum aos cidadãos livres, e esta particularizada aos indivíduos. A vida pública não estava necessariamente ligada a um local; existia no diálogo (léxis), sendo que a inserção dos cidadãos nesse ambiente baseava-se na sua posição no *oikos*.

Na sociedade grega, família e política demarcavam a distinção entre as esferas pública e privada, pela forma assimétrica da organização de ambas. Ao adentrar na esfera pública o cidadão recebia uma segunda vida *(bio politikos),* que implicaria na distinção do seu próprio modo de existir – findava o relacionamento com o que lhe era próprio *(idion)*, para dar lugar ao que lhe era comum *(konion)*. Havia autonomia do espaço privado em relação à *polis*, cujos

limites se sustentavam devido ao fato de que não seria possível que o cidadão participasse dos "negócios do mundo" sem ser dono de sua casa, sem ter um "lugar que lhe pertencesse".

O autor ainda indica a Idade Média como o período da história onde já se denota uma maior necessidade de isolamento, da mesma forma como aquele momento em que o espaço público fez certa concessão ao espaço privado, erigindo-o à verdadeira condição de *status*. Contudo,

> [...] ainda não é possível reconhecer um sistemático anseio das pessoas pela privacidade ou isolamento; pode-se ao máximo constatar que alguns poucos podiam isolar-se dos demais, como os senhores feudais que o desejassem, ou então pessoas que optassem pela solidão em detrimento da vida pública, como alguns religiosos, místicos ou mesmo banidos. Ao fim da Idade Média, entretanto, podemos identificar entre os senhores feudais bem colocados na sociedade manifestações que podem ser entendidas como indícios do surgimento de uma esfera privada em moldes vagamente similares aos atuais; [...] (DONETE, 2006, p. 91).

Datam deste período histórico, alterações de hábitos e comportamentos considerados, hodiernamente, como essencialmente privados, tais quais os atos sexuais e as necessidades fisiológicas, a despeito da possibilidade de isolamento ter continuado como privilégio de poucos. E, vale ressaltar, a importante mudança na relevância que as questões do ambiente do lar passaram a ocupar na comunidade, iniciando uma nova configuração de espaço público. Como o espaço da casa permitia um ambiente de separação entre o espaço comum e o privado, o ambiente ganhou maior relevância, de tal forma que, conforme destaca Agostini (2011), a casa não fosse mais vista como um espaço em que eram discutidas questões de pouca importância, mas sim o centro de representação do poder político. Daí porque algumas casas passaram a ser ligadas a grandes dinastias.

A ascensão da burguesia fez emergir ainda mais o caráter da individualidade, notadamente, por meio da busca da apropriação de espaços particulares dentro da sociedade, caracterizada pelo afastamento propiciado pelo soerguimento de barreiras, que comprovam essa necessidade de uma nova forma de individualidade. É importante mencionar que essa nova configuração entre o público e o privado extrapola as dimensões políticas e econômicas da época, cimentando uma percepção que se reflete no âmbito interno dos sujeitos, como forma de expressão da personalidade.

Neste sentido, Schreiber (2013, p. 135), assenta que, sendo pobreza e privacidade contraditórias, esta acabaria identificada como um direito da "era de ouro" da burguesia,

limitada aos detentores de poder econômico e fama, cuja preocupação voltava-se a resguardar sua vida íntima da curiosidade e interesse alheio. Cancelier (2017, p. 216) esclarece que a "[...] alteração fundamental tem origem numa conceituada emancipação psicológica [...] do sujeito perante a sociedade e, com isso, [...] aquilo que é privado em contraposição ao que é público deixa de ser identificado por um enfoque político para ganhar força na oposição entre o social e o íntimo".

Vieira (2007, p. 32) afirma que os indícios do que viria a se constituir em direito à privacidade, remontam ao século XVI, na Inglaterra, por meio do princípio da inviolabilidade do domicílio, popularmente vocalizado no adágio *a man's house is his castle.* Entretanto, restrito à privacidade do lar, não abrangendo outras espécies como a física, das comunicações, decisional e informacional, haja vista a necessidade de um lapso temporal de cerca de dois séculos, para que essas outras formas de privacidade se constituíssem em direito autônomo, a partir do século XIX.

Na Alemanha, em 1846, David Augusto Röder publicou o trabalho intitulado *Grundzüge des Naturrechts oder der Rechtsphilosophie* – Fundamentos da Lei Natural ou Filosofia da Lei, em tradução livre –, onde considera como atos violadores ao direito natural à vida privada, incomodar alguém com perguntas indiscretas, ou adentrar um aposento sem prévio anúncio. Contudo, seria na França, no ano de 1858, que o direito à privacidade viria a ganhar contornos legais, ainda que em sede jurisprudencial, mediante o caso *Affaire Rachel*, no qual o Tribunal de Séné reconheceu o direito a não publicação de imagem no leito de morte, à família de uma famosa atriz.

Não obstante, toma-se como marco doutrinário, o ano de 1890, nos Estados Unidos,

> [...] quando Samuel Dennis Warren e Louis Demitz Brandeis publicaram um artigo em *Harvard Law Review* intitulado *Right to privacy.* Analisando-se alguns precedentes judiciais da Suprema Corte dos EUA referentes à propriedade, direitos autorais e difamação, os autores concluíram que se poderia extrair das decisões até então proferidas o estatuto de um direito geral à privacidade. Defenderam a necessidade de reconhecimento pelas Cortes do denominado *Right to privacy:* o direito de o indivíduo estar só com seus pensamentos, emoções e sentimentos, independentemente da forma de expressão (manifesto em cartas, diálogos, livros, desenhos, pinturas ou composições musicais) (VIEIRA, 2007, p. 33).

Doutrinariamente, os autores prestaram duas importantes contribuições. Primeiramente, a distinção entre o *right to privacy* da proteção da honra, uma vez que a proteção desta última

se concretiza pela busca em manter o indivíduo preservado contra a divulgação de fatos inverídicos e maliciosos, e aquele busca garantir proteção até contra fatos verdadeiros quando o autor não autoriza a divulgação de tais fatos ao público. Em segundo plano, pelos apontamentos de que o direito de estar só não seria absoluto, podendo ser paliado em determinados casos, como na publicação de matéria de interesse público; autorização legal; e com a permissão de divulgação do próprio indivíduo.

Por sua vez, Cancelier (2017, p. 217), aponta o trabalho de Warren e Brandeis, como aquele que inaugurou o direito à privacidade enquanto figura jurídica autônoma. Embora já se pudesse encontrar contornos daquilo que futuramente se veria consolidado, "[...] foi Thomas MacIntyre Cooley (1824-1898), jurista norte-americano e Presidente da Suprema Corte de Michigan, quem cunhou, em 1888, a expressão o direto de estar só (*the right to be let alone*)[1]".

> A ideia do direito à privacidade surge no final do século XIX, com a obra do juiz norte-americano Thomas M. Cooley intitulada A Treatise on the Law of Torts or the Wrongs Which Arise Independence of Contracts (em tradução livre, Um Tratado sobre a Lei de Danos ou de Injustiças que Surgem Independentemente de Contratos), de 1879. O referido livro trouxe a ideia do "right to be let alone", que é, basicamente, o direito de ser deixado sozinho, em uma espécie de completa imunidade, de forma que deve ser remediado, não só o dano, mas também a tentativa de causar dano a outrem. (ARAÚJO; SILVA; D'ÁVILA, 2021, pp. 07-08)

Após avanços de cunho doutrinário e jurisprudencial, o direito à privacidade alcançou relevo internacional, mediante diversos tratados e normativas, conforme esquematizado no seguinte quadro:

Figura 1 – Evolução cronológica dos Tratados Internacionais

ANO	NORMA	DESTAQUES
1948	Declaração Universal dos Direitos Humanos	Art. XII: "Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua

[1] Em 1880, Thomas M. Cooley cunhou a frase "o direito de ser deixado em paz" em seu tratado sobre a lei de responsabilidade civil, cujo conceito foi expandido por Samuel Warren e Louis Brandeis em um artigo da Harvard Law Review de 1890, no qual os dois sugeriram um "direito de privacidade". O artigo deles foi uma resposta a vários ataques da imprensa à família de Warren. Essa primeira noção de privacidade mais tarde se desenvolveu na causa de ação delito por invasão de privacidade, definida como "uma exploração injustificada da personalidade de alguém ou intrusão em sua atividade pessoal."

		correspondência, nem de ataques à sua honra ou à sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques.”
1950	Convenção Europeia dos Direitos do Homem	Art. 8º: “Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito pela vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício desse direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.”
1966	Pacto Internacional dos Direitos Civis e Políticos	Art. 17: “§ 1º Ninguém poderá ser objeto de ingerências arbitrárias ou

		ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. § 2º Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.”
1967	Conferência Nórdica sobre o Direito à Intimidade	Principais ofensas ao direito à intimidade: (a) penetração no direito à solidão da pessoa, incluindo-se espreitá-la pelo seguimento, pela espionagem ou pelo chamamento constante ao telefone; (b) gravação de conversas e tomadas de cenas fotográficas e cinematográficas das pessoas em seu círculo privado ou em circunstâncias íntimas ou penosas à sua moral; (c) audição de conversas privadas por interferências mecânicas em telefone e em microfilmes dissimulados deliberadamente; (d) exploração de nome, de identidade ou de semelhanças de uma pessoa sem o seu consentimento; (e)

		utilização de falsas declarações, revelação de fatos íntimos, e crítica da vida das pessoas.
1969	Pacto de São José da Costa Rica (Convenção Americana sobre Direitos Humanos)	Reproduziu a redação da Declaração Universal dos Direitos do Homem, prevendo o direito à privacidade em seu art. 11.

Fonte: Elaborado pelos organizadores (2023)

A despeito de toda evolução conceitual que se deu em âmbito internacional, favorecida pela promulgação dos diplomas legais supracitados, autores como Vieira, (2007, pp. 34-36) defendem que para se alcançar a efetiva defesa do direito à privacidade, seria preciso ir além dos apontamentos dos diversos documentos que até então haviam se consolidado. Assim, ganhou força a recomendação para que fossem aprovadas legislações internas ao arcabouço legal de cada nação, que facilitassem sua aplicação pelo poder judiciário.

Foi com base nessa recomendação internacional, que países como Alemanha, em 1957, e Itália, em 1962, organizaram o 42º Congresso Jurídico de Düsseldorf e o Simpósio Internacional de Trento, respectivamente, para tratar dos temas relativos à privacidade e intimidade. Logo, outros países deram seguimento às recomendações, implementando suas próprias leis correlatas, a exemplo de Áustria, Dinamarca, Suíça e Portugal, que passaram a introduzir normas em sede penal para proteger a privacidade de seus cidadãos. Somente após um passo adiante, em direção à esfera civil – enquanto *status* de direito de personalidade –, o direito à privacidade ganhou guarida sob o prisma constitucional.

Em meados do século XX, o direito à privacidade foi abandonando o reduto de seu berço burguês e suas conotações originárias, para moldar-se às feições mais contundentes da compreensão que viria a adquirir.

> Tal cenário começa a alterar-se de forma mais contundente no decorrer da década de 1960 motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da tecnologia de coleta e sensoriamento, resultando em uma capacidade técnica cada vez maior de recolher, processar e utilizar a informação. (CANCELIER, 2017, p. 219).

O século XX foi, portanto, o grande marco temporal da transformação do direito à privacidade. Devido à expansão de suas fronteiras; a relação de novos sujeitos; e à complexidade cada vez maior de símbolos, objetos, locais e redes que até então não o abarcavam, alcançou a democratização do interesse pela sua tutela e exercício, em decorrência das mudanças significativas ocorridas nos vínculos entre sujeito e sociedade, e nos mais variados espaços da vida pública e privada.

2.2 Conceitos e espécies

O direito à privacidade é um dos direitos fundamentais mais importantes na sociedade moderna, garantindo ao indivíduo o controle sobre suas informações pessoais, proteção contra a intromissão indevida em sua vida privada e a possibilidade de tomar decisões quanto à divulgação e compartilhamento dessas informações.

Lima (2021, p. 18), sustenta que "tradicionalmente centrado na ideia de inviolabilidade da esfera privada, [o direito à privacidade] revela nítida concepção liberal. [...] a noção de um 'direito a ser deixado em paz' (*right to be let alone*) é um traço característico da proteção jurídica do direito à privacidade no Direito ocidental a partir do final do século XIX e por todo o século XX".

Atendo-se a um recorte da legislação pátria, ao se referir às escolhas tanto do nosso Constituinte, quanto do Legislador Ordinário, Cancelier (2017, pp. 219-220), ressalta a omissão conceitual para as expressões vida privada e intimidade, ao substituírem o termo privacidade na legislação nacional. Da mesma forma, sublinha que, em que pese as menções da Carta de 1988 aos termos sigilo e inviolabilidade, o faz inferindo a possibilidade de uso de qualquer um dos termos em referência a ambas as situações. Assim,

> [...] fala-se em vida privada ou vida íntima para tratar do mesmo espaço da vida para qual se fala. Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. Ao mesmo tempo, cada um deles poderá assumir – de forma bastante subjetiva – a depender do sujeito da fala, um significado específico. Assim, nem sempre o íntimo será secreto, ou o assunto sigiloso será privado. (CANCELIER, 2017, p. 220).

Convém ressaltar a oportuna observação que Doneda (2006) sustenta, ao mencionar a profusão dos termos dos quais a doutrina brasileira se utiliza – apropriadamente, ou não –, para se referir ao que seja privacidade. Assim como a contribuição da doutrina estrangeira, ao apontar para várias alternativas que certamente induz, validamente, os juristas do nosso país. Dessarte,

> A verdade é que a falta de uma definição "âncora", que reflita uma consolidação do seu tratamento semântico, não é um problema localizado da doutrina brasileira; tome-se por exemplo a doutrina norte-americana, que conta com um vocábulo consolidado (privacy, fortalecido com o reconhecimento do right to privacy) que, no entanto, faz referência a um vasto número de situações, muitas das quais o jurista brasileiro (ou outro da tradição de civil law) não relacionaria com a privacidade. Uma eventual contraposição entre o modelo de common law e o de civil law não basta para justificar esta discrepância: as concepções do right to privacy variam consideravelmente entre os EUA e o Reino Unido, por exemplo; enquanto os países com tradição de civil law percorreram caminhos razoavelmente particulares neste sentido, antes de considerar uma tendência à unificação de seu conteúdo, que é recente. (DONEDA, 2006, p. 91).

Não obstante a opção terminológica da legislação brasileira, independentemente do termo utilizado, os sujeitos que a eles recorram podem estar se referindo a uma mesma situação fática. Ainda, o significado do discurso está diretamente imbricado ao caráter subjetivo de cada sujeito. Ademais, o nosso arcabouço jurídico consente com essa possibilidade. Para o autor, privacidade "deve ser vista antes de tudo como exercício de uma liberdade da pessoa, uma necessidade humana", sem a qual fica prejudicada toda possibilidade de assunção dos anseios pessoais, haja vista partilharem da construção desse espaço íntimo que necessariamente os precede.

Autores como Lafer, Malta, Machado, Zanon, Ardenghi (*apud* Cancelier, 2017, p. 221), elaboraram diversas noções acerca do conceito de intimidade, tais quais: (i) o direito do indivíduo de estar só e possibilidade de exclusão do conhecimento de terceiros daquilo que só diz respeito ao âmbito da vida privada; (ii) enquanto proteção dos pensamentos e emoções mais restritos; (iii) o núcleo essencial da pessoa; (iv) o local exclusivo que cada sujeito reserva para si; e (v) aquele poder conferido a cada pessoa para se resguardar de intromissões ao espaço reservado de sua existência, bem como a possibilidade de fazer concessões quanto a isso.

Denota-se, portanto, que o conceito abarca desde um local, enquanto espaço reservado da interferência pública, até elementos de ordem psicológica e subjetiva, como emoções e pensamentos, mas se apresenta sob variadas vertentes, embora se ancore no aspecto primordial do espaço individual – físico ou psíquico –, dos sujeitos.

No Direito brasileiro, Júnior (2004, p. 28), fazendo distinção entre a proteção da honra e a proteção da privacidade, considera a existência de duas esferas: a esfera individual e a esfera privada. Segundo Jabur (2000, p. 260), na esfera individual o cidadão [...] acha-se relacionado com seus semelhantes; na esfera privada [...] o cidadão se situa na intimidade ou no recato, em seu isolamento moral, convivendo com a própria individualidade. Portanto, a despeito de ambas as formas de proteção – o direito à honra e o direito à privacidade –, encontrarem albergue sob o mesmo dispositivo constitucional (art. 5º, inciso X, da CF/88), possuem caráter diversos, no que tange o quesito da proteção.

Almeida e Lugati (2022), mencionando a perspectiva doutrinária de Viktor Mayer-Schönberger, propõem que a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas. Segundo as autoras, o caminho percorrido partiu de um cerne mais técnico e restrito, até alcançar disposições e técnicas que abarcassem as tecnologias modernas.

A primeira geração surgiu dentro do contexto do Estado Moderno, onde o governo se utilizando de grandes bancos de dados, exercia controle sobre a população, por meio da obtenção massiva de informações sobre os indivíduos. O Estado era o destinatário centralizador desses regulamentos, voltados diretamente à própria tecnologia. Como exemplo das leis de primeira geração, a literatura cita o *Privacy Act,* norte-americano de 1974. A primeira geração se estende até o implemento da Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.

Uma vez que a primeira geração de leis se tornou obsoleta, frente ao avanço tecnológico, devido ao fato de ser baseada somente em autorizações o tratamento de dados ultrapassou o domínio governamental, chegando também aos entes privados. Neste novo cenário, que ensejou a segunda geração de leis, o usuário ganhou poder, e o seu consentimento elevou seu status como participante ativo do processo de tratamento de dados, a partir da coleta, uso e compartilhamento dos seus dados pessoais.

Dando um passo adiante, a terceira geração de leis vai além do exercício da liberdade do titular em consentir ou não com a cessão dos seus dados. Voltando a atenção mais para a tutela do direito à privacidade, as leis dessa geração buscavam a efetividade deste direito. É

neste momento que se amplia a participação do indivíduo para todas as fases, num recrudescimento regulamentar que atinge o conceito central de "autodeterminação informativa".

Abarcando apenas uma parcela de indivíduos, a terceira geração se tornou insuficiente, pavimentando o caminho para a quarta geração, que prevalece até os dias atuais. Hodiernamente, com base no aprendizado conferido pelas gerações anteriores, cujas desvantagens eram reflexo no enfoque pessoal, as leis de quarta geração priorizam os titulares dos dados frente a terceiros que possam manipular suas informações pessoais.

Como o objeto de estudo desta pesquisa busca lançar luz sobre os aspectos condizente ao direito à privacidade, renunciaremos aos pormenores acerca do direito à honra, e passaremos à análise dos conceitos sobre o direito à privacidade defendidos por alguns autores.

Bastos e Martins (1989, p. 63), sustentam que privacidade "é a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano". Chamando a atenção para aquilo que considera um dos atributos da privacidade, Jabur (2000, p. 254), aponta que se trata da "faculdade de se excluir do conhecimento de terceiros as informações que o titular quer preservar para si próprio, o direito de viver em isolamento sem ser submetido a uma publicidade que não desejou". Por sua vez, Pereira (2004, p. 140), ao conceituar sobre o direito à privacidade, afirma que "o direito à intimidade seria [...] o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada dos mesmos, possam revelar aspectos da sua personalidade". Ainda, para Rodotà (1995, p. 122), seria "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".

Em síntese, aos conceitos até aqui apresentados, contudo, elaborado em compreensão mais abrangente,

> [...] o direito à privacidade consistiria em um direito subjetivo de toda pessoa – brasileira ou estrangeira, residente ou transeunte, física ou jurídica – não apenas de constranger os outros, a respeitarem sua esfera privada, **mas também de controlar suas informações de caráter pessoal – sejam estas sensíveis ou não – resistindo às intromissões indevidas provenientes de terceiros.** [...] traduz-se na faculdade que tem cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, **assim como na prerrogativa de controlar suas informações pessoais, evitando acesso e divulgações não autorizados.** Tem, intrinsicamente, natureza negativa ao proteger o titular das intromissões de terceiros; [...] **e natureza positiva ao permitir**

> **que o próprio indivíduo controle o que deve ser conhecido e o que não deve ser conhecido pelos demais,** pela liberdade que lhe é ínsita. (VIEIRA, 2007, p. 23, grifo nosso).

Seguindo a reflexão da autora, convém destacar a classificação da privacidade em quatro espécies ou categorias, de acordo com seu âmbito de proteção: física, do domicílio, das comunicações, decisional e informacional.

A primeira espécie, da privacidade física, visa proteger o corpo do indivíduo contra procedimentos invasivos não autorizados pelo próprio, assim como a realização forçada de testes de drogas ou exames genéticos. Há exemplos dogmáticos tanto dos tribunais nacionais quanto internacionais nesse sentido. O Supremo Tribunal Federal já decidiu a favor do réu, no sentido de não ser obrigado à realização forçada de exame de DNA.

> INVESTIGAÇÃO DE PATERNIDADE - EXAME DNA - CONDUÇÃO DO RÉU "DEBAIXO DE VARA". Discrepa, a mais não poder, de garantias constitucionais implícitas e explícitas - preservação da dignidade humana, da intimidade, da intangibilidade do corpo humano, do império da lei e da inexecução específica e direta de obrigação de fazer - provimento judicial que, em ação civil de investigação de paternidade, implique determinação no sentido de o réu ser conduzido ao laboratório, "debaixo de vara", para coleta do material indispensável à feitura do exame DNA. A recusa resolve-se no plano jurídico-instrumental, consideradas a dogmática, a doutrina e a jurisprudência, no que voltadas ao deslinde das questões ligadas à prova dos fatos. (STF, HC 71373, 1994).

Da mesma forma, o Tribunal Federal Constitucional alemão, em decisão de 10 de junho de 1963, julgou procedente a reclamação constitucional impetrada pelo réu, para que não fosse obrigado a ser submetido a uma intervenção cirúrgica para retirada de líquido cefalorraquiano, a fim de provar sua imputabilidade.

A segunda espécie, do direito à privacidade do domicílio, encontra guarida no próprio texto da Carta de 1988, mais precisamente em seu art. 5º, inciso XI, dispondo que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial".

A terceira espécie, do direito à privacidade das comunicações, assim como a segunda espécie, também encontra respaldo no texto constitucional, por meio do mesmo art. 5º, inciso XII, garantindo como "inviolável o sigilo das correspondências 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".

A quarta espécie diz respeito à privacidade decisional, aquela reconhecida como atributo inato do indivíduo humano de decidir o próprio destino, tomar as próprias decisões, de buscar a felicidade naquilo que lhe reserva o foro íntimo. Também nomeada direito à autodeterminação, enquanto direito decisional, já foi assentada pela jurisprudência norte americana em casos envolvendo o uso de anticoncepcionais e aborto, preservando ao casal o direito de decidir sobre o curso de suas vidas livre da interferência estatal. Dessarte, enquanto autodeterminação, o Tribunal Constitucional Superior alemão, também já consentiu com o direito de o indivíduo determinar autonomamente sua vida no que diz respeito ao casamento, procriação, orientação sexual, exposição pública da imagem, voz e honra pessoal.

Por fim, a quinta espécie, a da privacidade informacional, configura-se no âmbito de proteção das informações sobre determinada pessoa, relacionadas tanto à sua esfera mais íntima, quanto a dados pessoais que possam levar à identificação do seu titular. A primeira referência a essa categoria de privacidade reside na jurisprudência do já mencionado Tribunal Constitucional Federal alemão, no caso que ficou conhecido como Lei do Censo, de 25 de março de 1982. No caso, ordenou-se o recenseamento geral da população, coletando-se dados sobre profissão, moradia, domicílio e renda.

Ainda, havia previsão para a comparação dos dados levantados com registros públicos e a respectiva transmissão das informações recolhidas a repartições públicas dos três níveis: federais, estatais e municipais. Em decisão de 15 de dezembro de 1983, a Corte julgou nulos os dispositivos relacionados à comparação e à transmissão de dados para repartições públicas, por entender como pressuposto do direito à autodeterminação informativa, caber a cada indivíduo o controle e proteção dos próprios dados pessoais.

Nesse ínterim, importante destacar que os conceitos supra são de primordial relevância para compreendermos a problemática suscitada por este estudo, quanto à implementação de boas práticas de consentimento, por meio da autorização de uso dos *cookies*, considerando-se que tais conceitos vão ao encontro dos principais pontos de omissões ou abusos, por parte dos controladores de dados, conforme detalharemos mais adiante, no capítulo 4.

3 PROTEÇÃO DE DADOS NO MUNDO

3.1 Estado, pós-modernidade e os desafios na era da informação

A sociedade da informação caracteriza-se pelo acesso e uso generalizado da tecnologia, da *internet* e dos serviços digitais, que se tornaram parte integrante das vidas das pessoas em todo o mundo. Esses avanços tecnológicos têm provocado uma disrupção no modo de vida das pessoas, alterando as formas como elas interagem e se relacionam umas com as outras, como consomem bens e serviços e como se envolvem em atividades de negócios.

Essas mudanças representam tanto um desafio para os Estados quanto uma oportunidade para criar formas de servir à população. Por outro lado, essas tecnologias também têm sido usadas para monitorar e controlar as pessoas, onde os dados pessoais são usados para fins de lucro. Por consequência, cabe aos Estados da pós-modernidade, o papel ativo para garantir que as pessoas mantenham o controle de suas informações e que os dados sejam utilizados de forma segura e responsável.

Burch (2005) convida à reflexão, acerca do atual cenário de mudanças pelas quais passam as sociedades modernas, por meio da seguinte provocação:

> Estamos vivendo numa época de mudanças ou numa mudança de época? Como caracterizar as profundas transformações que acompanham a acelerada introdução na sociedade da inteligência artificial e as novas tecnologias da informação e da comunicação (TIC)? Trata-se de uma nova etapa da sociedade industrial ou estamos entrando numa nova era? “Aldeia global”, “era tecnotrônica”, “sociedade pós-industrial”, “era - ou sociedade - da informação” e “sociedade do conhecimento” são alguns dos termos cunhados com a intenção de identificar e entender o alcance destas mudanças. Mas, enquanto o debate continua no âmbito teórico, a realidade se adianta e os meios de comunicação escolhem os nomes que temos de usar. (BURCH, 2005, p. 01)

Diante dos variados termos suscitados pela autora para o fenômeno – seja ele atual ou futuro –, que designam as sociedades modernas, ela mesma sugere que, independentemente de qual seja escolhido para fazer referência ao estado da arte, ele não define, por si só, um conteúdo. Tal objeto se encontra imbricado aos contextos sociais que influenciam nas percepções e expectativas de cada comunidade global, fazendo com que cada termo traga consigo uma bagagem ideológica do passado, carregada de sentido ou de sentidos.

Tomando como ponto de inflexão o contexto da Cúpula Mundial da Sociedade da Informação (CMSI), dois termos despontaram com proeminência: sociedade da informação e sociedade do conhecimento. E, embora o primeiro tenha alcançado destaque no meio acadêmico, ainda não há consenso sobre as delimitações conceituais que cada um abarca.

Schwab (2016), fundador do Fórum Econômico Mundial, apontou uma mudança radical e disruptiva no modo como seres humanos têm vivido, trabalhado, se relacionado e produzido conhecimento, até então – muito embora os efeitos dos avanços tecnológicos já tenham implacável influência sobre o nosso modo de vida, desde muito antes. O autor vaticinou:

> As mudanças são tão profundas que, na perspectiva da história humana, nunca houve um momento tão potencialmente promissor ou perigoso. A minha preocupação, no entanto, é que os tomadores de decisão costumam ser levados pelo pensamento tradicional linear (e sem ruptura) ou costumam estar muito absorvidos por preocupações imediatas; e, portanto, não conseguem pensar de forma estratégica sobre as forças de ruptura e inovação que moldam nosso futuro. (SCHWAB, 2016, p. 16).

Baseado em pesquisa feita pelo Fórum Econômico Mundial e no trabalho de vários Conselhos da Agenda Global do Fórum, o autor identificou o que nominou de megatendências: "todas as inovações e tecnologias [que] têm uma característica em comum: elas aproveitam a capacidade de disseminação da digitalização e da tecnologia da informação" (SCHWAB, 2016, p. 26).

Para tanto, o autor organizou uma lista dividida em três categorias, indicadoras dessas megatendências: a categoria física, a digital e a biológica. Nos cingindo, exclusivamente, à categoria digital – graças à maior pertinência ao objeto de estudo desta pesquisa –, constatamos que todas as tecnologias impulsionadoras da quarta revolução industrial, categorizadas pelo autor, já fazem parte do nosso cotidiano:

- *internet of things* (IoT) – *Internet* das Coisas, em tradução literal –, "descrita como a relação entre as coisas (produtos, serviços, lugares etc.) e as pessoas que se torna possível por meio de diversas plataformas e tecnologias conectadas". (SCHWAB, 2016, p. 29);
- *blockchain,* "descrito como 'um livro-razão distribuído, [...] um protocolo seguro no qual uma rede de computadores verifica de forma coletiva uma transação antes de

registrá-la e aprová-la", cujo exemplo mais conhecido é o *bitcoin.* (SCHWAB, 2016, p. 30);

- e, em maior escala, a economia sob demanda ou economia compartilhada, "plataformas fáceis de usar em um *smartphone*, [que] reúnem pessoas, ativos e dados, criando formas inteiramente novas de consumir bens e serviços", com inúmeros exemplos na atual economia global, como *Uber, Facebook, Alibaba, Airbnb*, dentre tantos outros. (SCHWAB, 2016, p. 31).

Utilizando apenas estes três exemplos de tecnologias, como pressupostos disruptivos do que se convencionou chamar sociedade da informação, notamos que, inexoravelmente, a *internet* é o elo em comum que permitiu o surgimento e expansão de todos eles.

É inegável que, desde sua criação e constante expansão, a *internet* revolucionou as relações sociais e os meios de comunicação das sociedades modernas. Ocupando lugar de relevância em níveis exponenciais, hodiernamente, já há quem conceba o seu acesso como um direito fundamental. Assim, na defesa desta ideia, Neto (2020, p. 05), corrobora que "não obstante o direito ao acesso à *internet* não esteja consagrado no rol de direitos fundamentais constantes na Constituição Federal, sua latente importância e necessidade na vida das pessoas já per se são capazes de assim o legitimar como tal".

Como o processo de expansão da *internet* ocorreu com mais vigor somente a partir da década de 1990, o legislador constituinte de 1988 não aferiu a importância que a ferramenta teria na vida dos cidadãos. Entretanto, o que viria a se constituir em verdadeira demanda social, ganhou a atenção do legislador ordinário ao editar o Marco Civil da *Internet* (Lei nº 12.965/2014), estatuindo, em seu art. 3º, inciso I, que "a disciplina do uso da *internet* no Brasil tem como base, dentre outros, os princípios da 'garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos a Constituição Federal'. Igualmente, em seu art. 4º, inciso I, "que a regulamentação da *internet* tem como finalidade, dentre outras, promover o direito de acesso à *internet* a todos". (NETO, 2020, p. 06).

Gradativamente, o *ciberespaço* vem substituindo os meios tradicionais de comunicação em massa que, durante muito tempo, foram os responsáveis por assegurar a liberdade de expressão e acesso à informação. O uso da rede mundial de computadores democratizou o alcance aos mais diversos conteúdos midiáticos – jornalísticos, artísticos, científicos, políticos –, bem como a participação e controle do cidadão nas atividades da Administração Pública. Nesse contexto, facilitando a concretização do que fora preconizado pela Carta Constitucional,

por meio de princípios como a publicidade, por exemplo. Ademais, uma grande parcela do mercado de consumo migrou para a *web*, devido à redução dos custos e às novas técnicas de publicidade peculiares ao ambiente das redes.

A despeito do inconteste poder de catalização que a *internet* tem exercido, criando condições favoráveis para que os sujeitos possam fazer valer seus direitos fundamentais, tal fenômeno não se dá de modo inteiramente pacífico e equilibrado. Sendo o acesso à rede mundial aberto a todos aqueles que disponham de condições mínimas de acesso a dispositivos tecnológicos, a *internet* conta com uma gama de *stakeholders* [2] da sociedade global extremamente diversificada – governos, empresas, universidades e sociedade civil –, tornando o ambiente propício para a prática de condutas abusivas e ilícitas.

O processo de mercantilização da *web* fez surgir o que Bioni (2015) denominou "Economia de Vigilância", fenômeno caracterizado pelo "desprezo ao direito da privacidade dos usuários para maximizar o lucro das empresas [...] por meio da violação aos dados pessoais, [...] utilizados indevidamente para fomentar a indústria da publicidade" (NETO, 2020, p. 07). Ainda, versando sobre o mesmo tema, Zuboff (2019, p. 29), utilizando-se do termo "Capitalismo de Vigilância", disseca em pormenores, este que ela considera "um ator novo na história, ao mesmo tempo original e *sui generis"*.

O trabalho da autora foi o resultado de um amplo estudo sobre as práticas capitalistas de vigilância dentre as maiores empresas de tecnologia no mundo: *Google, Facebook, Microsoft, Amazon* e *Apple*, incluindo outras corporações. A autora faz uma ressalva quanto às políticas capitalistas da *Apple*, embora afirme que as cinco empresas pratiquem capitalismo, por evidente, não são todas 100% capitalistas de vigilância, até o momento.

Para elucidar como agem os principais atores nesse cenário, estabelecido a partir dessas novas práticas, a autora recorre à distinção entre Capitalismo e Capitalismo de Vigilância, já que "[...] essa linha é definida em parte pelos propósitos e métodos de coleta de dados. Quando uma empresa coleta dados comportamentais com a permissão do usuário somente como um meio de melhorar seu produto ou serviço, está praticando capitalismo, mas não capitalismo de vigilância [...]" (ZUBOFF, 2019. p. 39).

---

[2] Embora o termo *stakeholder* tenha sido cunhado pela primeira vez no ano de 1963, pelo filósofo norte-americano Robert Edward Freeman, em um memorando do *Stanford Research Institute* – inaugurando o que viria a ficar conhecido nos estudos de Administração, como os grupos de interesse de uma organização –, tomamos emprestado o termo da obra de Klaus Schwab: A quarta revolução industrial, para fazer referência à heterogeneidade dos variados setores das modernas sociedades globais, inseridos no contexto da Revolução 4.0.

Retomando ideias apresentadas na introdução desta pesquisa, reforçamos que o Capitalismo de Vigilância fez da experiencia humana a matéria-prima gratuita, traduzindo-a em dados comportamentais. Se por um lado parte desses dados possa ser utilizada no aprimoramento de produtos e serviços, o restante automaticamente se transforma em superávit comportamental do proprietário, servindo de base para avançados processos de "inteligência de máquina", manufaturado em produtos de predição das ações dos indivíduos nas redes. Posteriormente, os produtos de predição são comercializados num novo tipo de "mercado de comportamento futuro".

Com o aprimoramento das práticas do Capitalismo de Vigilância, as empresas perceberam que os comportamentos mais preditivos são resultado da intervenção nessa cadeia de informações, de maneira que passaram a incentivar, persuadir, sintonizar e arrebanhar comportamentos em busca de resultados lucrativos. Graças à natureza competitiva dos mercados, se deu a mudança na qual processos de máquina automatizados não só conhecem nosso comportamento, como também o moldam em escala. Nessa nova perspectiva, a meta passou da automatização do fluxo de informações sobre nós, para a nossa própria automatização.

Segundo Zuboff (2019, p. 23), o Capitalismo de Vigilância conseguiu subordinar os meios de produção a "meios de modificação comportamental de tal forma, que gerou uma nova espécie de poder, o qual ela chamou de "instrumentarismo", capaz de conhecer e moldar o comportamento humano em prol das finalidades de terceiros. A partir do uso do poder instrumentário, a autora faz um alerta aterrador acerca do futuro das democracias pós-modernas.

Como o principal objetivo do instrumentarismo é organizar, arrebanhar e sintonizar a sociedade de maneira a adquirir confluência social semelhante, a pressão do grupo e a certeza computacional substituem a política e a democracia, pondo em risco a continuidade da realidade tal qual percebemos e a função social da existência dos indivíduos. Ainda, o risco ao fim do "direito de santuário", enquanto espaço de refúgio inviolável resguardado desde tempos antigos e por todas as sociedades civilizadas, agora sob ataque, na medida em que o capital de vigilância impele profundas implicações para o futuro das sociedades e suas fronteiras de poder.

Como alerta, a autora lista algumas frentes ameaçadoras à democracia, engendradas a partir da lógica do novo modelo de capitalismo.

> Entre os muitos insultos à democracia e às instituições democráticas impostos por esse *coup des gens,* ressalto a expropriação não autorizada da experiência humana; o

> sequestro da divisão de aprendizagem na sociedade; a independência estrutural em relação às pessoas; a imposição furtiva do coletivo de colmeia; a ascensão do poder instrumentário e a indiferença radical que sustém sua lógica extrativista; a construção, a propriedade e a operação dos meios de modificação de comportamento que constituem o Grande Outro; a revogação do direito elementar ao tempo futuro e do direito elementar a santuário; a degradação do indivíduo autodeterminante como fulcro da vida democrática; e a insistência no entorpecimento psíquico como resposta à sua compensação ilegítima. (ZUBOFF, 2021, p. 609).

É de suma importância levantar as reflexões suscitadas pela autora, para evitar que se caia nas armadilhas do senso comum, acerca das inferências que geralmente costuma-se chegar, sobre o papel que as pessoas ocupam numa sociedade permeada pelo Capitalismo de Vigilância.

O primeiro ponto é que não se trata de uma tecnologia, mas de uma lógica que a permeia e a direciona: uma forma de mercado impossível fora do meio digital, mas que com ele não se iguala. Em segundo lugar, os usuários não são os clientes nem o produto desse modelo de mercado, mas as suas fontes de superávit, como objetos de uma operação de extração de matéria-prima tecnologicamente avançada, cada vez mais difícil de se escapar: os verdadeiros clientes, na verdade, são as empresas que negociam nos mercados de comportamento futuro.

O pleno exercício do direito à privacidade e à liberdade de expressão está ligado, direta e proporcionalmente, aos procedimentos adotados pelas plataformas digitais, na direção do que determinam as normas avezadas ao tema do tratamento de dados pessoais de cada país, no caso brasileiro, a LGPD. E a observação empírica da experiência de qualquer usuário com a rede mundial de computadores corrobora essa assertiva, pois, muitas das vezes,

> A sensação de liberdade na rede pode esconder um oculto processo de violação à privacidade, com a finalidade de manipular o usuário por meio do impulsionamento estratégico de conteúdos. [...] É preciso que o usuário saiba como é feito o direcionamento dos conteúdos que a ele são disponibilizados em rede, para que, a partir do acesso a esses conteúdos, possa ele fazer uso pleno do direito de informação verídica e, posteriormente, exercer o direito de expressão. É igualmente necessário que o usuário consinta previamente sobre a utilização de seus dados pessoais por terceiros e saiba, de forma transparente, para qual finalidade eles serão usados e se somente serão tratados para a finalidade para a qual foram consentidos. (NETO, 2020, p. 08).

Portanto, a regulação da *internet* surge como um desafio aos Estados modernos, na busca da efetivação dos direitos fundamentais sem, contudo, que haja violação a esses mesmos direitos. Num primeiro momento, atribuiu-se ao mundo virtual um espaço neutro, livre das interferências da soberania do Estado, “isto porque esta nova ferramenta não se [limitava] às

fronteiras territoriais, de modo que seus usuários não estariam sujeitos a nenhuma jurisdição nacional, nem teriam domicílio em qualquer lugar" (NETO, 2020, p. 08). Até pouco tempo, a crença era de que não havia espaço para a atuação dos juristas naquele novo espaço. Atualmente, tal posicionamento é tachado até mesmo de utópico, haja vista a diferença abissal entre o surgimento da *internet* e seu processo de expansão, até alcançar os contornos da *World Wide Web* [3].

Assim, nenhuma nação albergada pelos princípios de um Estado Democrático de Direito vislumbra a existência da rede mundial de computadores ileso ao aparato legiferante regulamentador do Estado. Isto não significa a total impossibilidade de autorregulação, uma vez que grande parte dos serviços na *web* também são regidos por políticas e termos de uso elaborados pelas próprias plataformas. O que se tem almejado é a coexistência entre as diretrizes privadas e as competências e deveres constitucionais conferidos aos Estados.

Sob a perspectiva teórica de Lessig (2006), a construção e a consolidação do direito à privacidade necessitam de estratégias bem elaboradas para comportar as conjunturas que se apresentam. A lei não será suficiente, se as condições das normas sociais, do mercado e da arquitetura não estiverem em sintonia com determinado regramento positivado. Mesmo que os Estados modernos, em toda sua profusão positivista, estabeleçam medidas regulatórias específicas para o uso dos *cookies*, a engenhosa arquitetura tecnológica da sociedade da informação, pode recorrer a subterfúgios para burlar as preferências dos usuários e quaisquer albergues das diretrizes legais governamentais.

A estrutura da arquitetura condiciona sobremaneira a inflexão dos comportamentos humanos na rede, com impactos diretos sobre o tema específico da autorização e uso dos *cookies*. Os complexos desafios relacionados ao direito à privacidade na era pós-moderna, impõem ao Direito reflexões a par e passo das vanguardas tecnológicas. Caso haja negligentemente no tecido das estruturas tecnológicas, corre o risco de pavimentar o caminho da desconexão entre os comandos legais e os anseios reais da sociedade da informação e seus cidadãos.

---

[3] Formado pela Universidade de Oxford, Sir Tim Berners-Lee inventou a *World Wide Web* enquanto estava no CERN em 1989. Ele cunhou o nome *"World Wide Web"*, escreveu o primeiro servidor *web* – httpd –, e o primeiro programa cliente – um navegador e editor –, em outubro de 1990. Ele escreveu a primeira versão da linguagem de formatação de documentos com a capacidade de links de hipertexto, conhecida como HTML *(HyperText Markup Language)*. Suas especificações iniciais para URIs, HTTP e HTML foram refinadas e discutidas em círculos maiores à medida que a tecnologia da *web* se espalhou.

3.2 Precedentes da Lei nº 13.079/2018 (LGPD)

A princípio, comentaremos o contexto que cimentou o caminho do processo de desenvolvimento das primeiras legislações atinentes à proteção de dados no continente europeu, até a aprovação da Lei Geral de Proteção de Dados da União Europeia – *General Data Protection Regulation* (GDPR), por tratar-se de norma de importância fundamental na construção do arcabouço legal sobre proteção de dados no Brasil, a partir da LGPD.

A primeira lei de proteção de dados da qual se tem referência, data de 1970, através da instituição da lei estadual de proteção de dados no estado alemão de Hesse – *Hessisches Datenschutzgezetz.* Com o objetivo de prover tratamento adequado às informações pessoais de indivíduos armazenadas em meios eletrônicos, o Ato de Proteção de Dados de Hesse, considerada a primeira lei de proteção de dados da história. Conforme Adriano Novaes et al (2018, p. 7), "foi pioneira ao tratar da coleta e tratamento de dados de indivíduos, ainda que não o fizesse de maneira objetiva e segmentada".

Alguns anos depois, em 1973, surgiria a primeira lei nacional de proteção de dados, com a aprovação do Ato de Dados Sueco – *Sw. Datalagen.* Apresentando uma abordagem genérica, em similaridade com a lei de Hesse, não dispunha em que situações a coleta de dados poderia ou não ocorrer, tampouco apontava princípios gerais de tratamento de dados. Entretanto, inovara ao trazer o tema para a esfera pública, ao estabelecer que a coleta de dados estaria sob a autorização da agência governamental competente.

Dando sequência ao movimento normativo ligado à privacidade, outras legislações se seguiram em países como França, Alemanha e Dinamarca, a partir de 1979, preservando, contudo, o caráter genérico daquelas que as antecederam. Entretanto, é válido ressaltar a importância que o tema da privacidade passou a obter por países como Portugal, Espanha e Áustria, devido ao status de direito fundamental, alçado em suas Constituições.

No ano de 1981, o Conselho da Europa aprovou a Convenção 108, considerada, segundo Dennys Câmara et al (2018-2021, p. 7), "o primeiro marco legal transnacional sobre proteção de dados". A Convenção, que atualmente se encontra atualizada através da Convenção 108+, se propunha a "[...] alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de caráter pessoal susceptíveis de tratamento automatizado".

Foram necessárias duas décadas de expansão e inovações tecnológicas, para que as leis de proteção de dados fossem tomando contornos mais próximos aos das legislações atuais. No território europeu, a consolidação ocorreu por meio da promulgação da Diretiva 95/46/CE, após 25 anos da Lei de Hesse, em 1995. Considerada um marco da proteção de dados, a norma tinha vigência sobre todos os países membros do bloco, que agora se encontravam sob o albergue de uma única legislação, naquilo que dissesse respeito ao tratamento de dados e direitos dos usuários.

Avançando para além dos critérios de como deveria ser feita a coleta e tratamento dos dados, a Diretiva 95/46/CE inovou ao elencar os princípios que, a partir de então, deveriam amparar tais operações, dentre os quais: (i) licitude do tratamento; (ii) limitação dos propósitos; (iii) adequação; e (iv) necessidade de transparência.

A Diretiva 95/46/CE teve vigência até maio de 2018, vindo a ser substituída pelo regulamento nº 2016/679, de 27 de abril de 2016, ou a Nova Lei Geral de Proteção de Dados da União Europeia – *General Data Protection Regulation* (GDPR).

Em solo brasileiro, a gênese da Lei nº 13.079/2018 (LGPD) reside na agenda de debates sobre proteção de dados no Brasil, iniciada pelo Ministério da Justiça, autor do Anteprojeto de Lei de Proteção de Dados (APLPD). "O Anteprojeto foi disponibilizado para consulta e comentários públicos durante o ano de 2010 em um *blog* criado especificamente para esse fim, hospedado na plataforma pública Cultura Digital, por meio do *site* culturadigital.br". (CÂMARA et al, 2018-2021, p. 10)

À época, o anteprojeto esteve diretamente associado à discussão do Marco Civil da *Internet*, cujo debate estava em pleno vigor, o que levou o anteprojeto a ficar conhecido também pelo nome de Marco Legal de Proteção de Dados, em determinados momentos, contando com uma consulta que recebeu colaboração multissetorial durante 4 meses.

Em 13 de junho de 2012, portanto, dois anos após a primeira consulta pública, é apresentado o Projeto de Lei nº 4.060/2012, de autoria do Deputado Milton Monti, dispondo sobre tratamento de dados e dando outras providências, cuja fonte foi a própria consulta pública promovida pelo Ministério da Justiça. O PL 4.060/2012 não suscitou grande atenção, até a denúncia de irregularidades nas práticas de vigilância em escala global, promovidas pela Agência Nacional de Segurança (NSA), órgão vinculado ao governo norte americano, desencadeada pelo analista de sistemas Edward Snowden, no ano de 2013.

Como não obtivera avanços significativos durante o ano de 2013, a retomada da pauta ocorreu em 2015, quando o Ministério da Justiça promoveu a segunda consulta pública sobre o Anteprojeto da Lei de Proteção de Dados na mesma plataforma pública anteriormente utilizada, por meio do *site* culturadigital.br.

A proposta – elaborada pela Secretaria Nacional do Consumidor (Senacom), junto com a Secretaria de Assuntos Legislativos do Ministério da Justiça –, foi apresentada por meio da Senacom durante o seminário internacional "Anteprojeto Brasileiro de Proteção de Dados Pessoais em Perspectiva Comparada", cuja análise das contribuições contou com a colaboração do Centro de Estudos de Tecnologias *Web* (Ceweb), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e da Universidade Federal de Minas Gerais (UFMG). Desta feita, contando com um número maior de contribuições e sugestões de alteração do texto, o Ministério da Justiça finalmente protocolou o Projeto de Lei, então PL nº 5.276/16.

Apesar da robustez do texto, que contou com a colaboração da Associação Brasileira das Empresas de Tecnologia da Informação e Comunicações (Brasscom) à Comissão Especial da Câmara dos Deputados, o PL nº 5.276/16 acabou avançando com mais celeridade que os demais. Segundo Câmara et al (2018-2021, p. 11), a "completude se deu pelo volume de audiências públicas realizadas para ouvir e debater o tema com representantes de todos os setores da sociedade brasileira, bem como de atores internacionais convidados para expor sobre o tema".

Com a entrada em vigor da nova lei de proteção de dados da União Europeia (GDPR), em 25 de maio de 2018, Câmara e Senado engendraram esforços para que o texto do PL 5.276/16, por sua completude, substituísse o PL 4.060/12 que, por ter sido apresentado com 4 anos de antecedência, tinha prioridade de tramitação na Câmara. Apensados, a nova versão foi colocada em pauta e aprovada na Câmara dos Deputados, por unanimidade, em apenas 20 minutos, no dia 29 de maio de 2018, seguindo para o Senado sob a identificação de Projeto de Lei da Câmara (PLC nº 53/2018).

O texto foi colocado em pauta na Comissão de Assuntos Econômicos (CAE) do Senado Federal no dia 03 de julho de 2018, sob a relatoria do Senador Ricardo Ferraço, também relator do PLS nº 330/2013 – que tramitava em paralelo no Senado Federal –, e aprovado na mesma sessão, com requerimento de urgência para ser incluído na pauta do plenário do Senado Federal. Após forte pressão da sociedade civil e demais setores, o PLC foi pautado, votado e aprovado

por unanimidade no plenário do Senado Federal, em 10 de julho de 2018, e submetido à sanção presidencial, concretizada em 14 de agosto de 2018, com vetos. A esse respeito,

> [...] principalmente no que se refere aos artigos 55 a 59 que constituíam e organizavam a Autoridade Nacional de Proteção de Dados ("ANPD") e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, sob a justificativa de que havia vício de iniciativa, ou seja, a entidade não poderia ser criada por uma lei de iniciativa do poder legislativo, e sim teria que ser criada por iniciativa normativa oriunda do poder executivo. (CÂMARA et al, 2018-2020, p. 12)

Por último, no dia 27 de dezembro de 2018 editou-se a Medida Provisória nº 869 (MP nº 869/18), cuja publicação se deu no dia seguinte, em 28 de dezembro de 2018, trazendo alterações no texto sancionado e a criação da Autoridade Nacional de Proteção de Dados (ANPD).

4 TUTELA JURÍDICA DOS DADOS PESSOAIS NO BRASIL

4.1 A Constituição e as normas setoriais já existentes na legislação brasileira

Humberto Lima (2021, p. 18), assevera que "com o advento da LGPD pode-se afirmar que há hoje no país um verdadeiro sistema jurídico de proteção de dados pessoais do qual ela ocupa o núcleo, em que orbitam regras esparsas da legislação ordinária". E, como bem pondera o autor, diante da multiplicidade e fragmentariedade das regras que compõem esse conjunto específico de normas, despretensiosamente, passaremos a uma análise panorâmica do arcabouço normativo do sistema de proteção de dados brasileiro, a despeito das mais de 40 normas correlatas ao tema, anteriores à LGDP:

> A LGPD cria toda um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos. Importante salientar que o país já dispunha de mais de 40 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, a LGPD vem substituir e/ou complementar esse arcabouço regulatório setorial, que por vezes era conflituoso, pantanoso, trazia insegurança jurídica e tornava o país menos competitivo no contexto de uma sociedade cada vez mais movida a dados. (MONTEIRO, 2018).

Portanto, tomando como ponto de partida o nível mais alto do nosso ordenamento jurídico, citamos a Constituição Federal de 1988 como exemplo de difusão de diferentes formas de proteção de dados da pessoa, tanto mediante o rol de direitos fundamentais, quanto por meio de regras direcionadas à Administração Pública: (i) a liberdade de expressão e pensamento (art. 5º, inciso IX e art. 220); (ii) a inviolabilidade da vida privada, da honra e da imagem (art. 5º, inciso X); (iii) o sigilo das comunicações (art. 5º, inciso XII); (iv) o direito de acesso à informação (art. 5º, incisos XIV, XXXIII, LXXII, "a"; art. 37, § 3º, inciso II e art. 216, § 2º); e (v) o direito à integridade da informação (LXXII, "b".

Apesar dos auspícios motivados pelo artigo 5º, inciso X, onde, devido à grande atenção dada ao tema da proteção à privacidade, alçado à verdadeira condição de direito fundamental, Schreiber (2013, p. 141), nos lembra da grande importância do instrumento do *Habeas Data,* enquanto inovação produzida pelo Constituinte. Regulado pela Lei nº 9.507, de 12 de novembro de 1997 – enquanto figura original do nosso ordenamento jurídico, dentre os remédios

constitucionais previstos –, apresenta-se como instrumento primoroso para evitar e corrigir violações à privacidade.

Prosseguindo em nossa análise, desceremos nos níveis da nossa topologia normativa, nos deparando com as leis e decretos do nosso ordenamento jurídico que, sob algum prisma, abordam a temática desta pesquisa, tais quais: (i) Código Civil (Lei nº 10.406/2002); (ii) Código Penal (Decreto-Lei nº 2.848/1940); (iii) Lei dos Crimes Cibernéticos (Lei nº 12.737/2012); (iv) Código de Defesa do Consumidor – CDC (Lei nº 8.078/1990); (v) Lei do Cadastro Positivo (Lei nº 12.414/2011); (vi) lei que que alterou a Lei Complementar nº 105/2001 e a Lei nº 12.414/2011 (Lei nº 166/2019); (vii) Lei de Acesso à Informação (Lei nº 12.527/2011); (viii) Marco Civil da *Internet* (Lei nº 12.965/2014); (ix) decreto que regulamenta o Marco Civil da *Internet* (Decreto nº 8.771/2016); (x) lei que instituiu o Sistema Brasileiro de Inteligência (Lei nº 9.883/1999); (xi) Lei de Interceptações Telefônicas (Lei nº 9.296/1996); (xii) Lei de Propriedade Industrial (Lei nº 9.279/1996); (xiii) Lei do Sigilo Financeiro (Lei Complementar nº 105/2001) e; (xiv) Lei dos Bancos de Dados de Crédito (Lei nº 12.414/2011).

O Código Civil de 2002 nos traz, dentre os direitos da personalidade, o direito ao nome e sua proteção (arts. 16, 17, 18 e 19); a proteção contra indevida divulgação de escritos, transmissão da palavra ou utilização da imagem (art. 20); e a inviolabilidade da vida privada (art. 21).

Na esteira dos comentários ao Códex Civil, Anderson Schreiber (2013, p. 142), faz críticas ao excerto do art. 21. Para o autor, uma vez que o art. 5º, inciso X, da Carta Constitucional, versa expressamente acerca da inviolabilidade da intimidade e da vida privada, assegurando até mesmo o direito à indenização pelo dano material ou moral decorrente de sua violação, o mínimo que se poderia esperar do legislador ordinário, é que aperfeiçoasse o mando constitucional. Dessarte, minudenciando-o, poderia regular as situações triviais, oportunizando remédios para as situações usuais. Entretanto, o conteúdo do art. 21, do Códex Civil, se limitou a repisar o argumento relacionado à inviolabilidade da vida privada, como já disposto no texto constitucional, pondo em xeque a utilidade prática do enunciado. Em defesa de seu argumento:

> A norma diz muito pouco para o seu tempo. Como já se enfatizou em relação aos direitos da personalidade em geral, o desafio atual da privacidade não está na sua afirmação, mas na sua efetividade. A mera observação da vida cotidiana revela que, ao contrário da assertiva retumbante do art. 21, a vida privada da pessoa humana é violada sistematicamente. [...] Falhou, portanto, o art. 21 do Código Civil ao declarar a tão solene quanto irreal inviolabilidade da vida privada. Melhor figura faria se ocupando das múltiplas manifestações da privacidade, dos fatores relevantes para sua

> ponderação com outros interesses dignos de proteção, ou ainda dos instrumentos específicos a serem empregados na prevenção e solução dos conflitos mais frequentes nesse campo. (SCHREIBER, 2013, pp. 142-143).

Dando seguimento à nossa análise, partindo da seara civilista para a criminal, o Código Penal designa a tipificação de condutas voltadas à tutela de dados pessoais, dos quais são exemplos os crimes contra a inviolabilidade das correspondências (art. 151); os crimes contra a inviolabilidade dos segredos, como o de divulgação de segredo (art. 153); violação de segredo profissional (art. 154) e; invasão de dispositivo informático (art. 154-A) – inserido pela Lei dos Crimes Cibernéticos (Lei nº 12.737/2012).

Não obstante, o Códex Penal prediz tipos penais que tutelam a fé pública, que podem servir como meio de proteção à informação pessoal, mesmo que de forma subjacente, tais quais os crimes de falsidade de documento público (art. 297); falsificação de documento particular (art. 298); falsidade ideológica (art. 299); supressão de documento (art. 305) e; falsa identidade (art. 307).

Por último, encerrando as prospecções da área penal, citemos os crimes contra a Administração Pública, a exemplo da inserção de dados falsos em sistema de informações e modificação ou alteração não autorizada de sistema de informações (arts. 313-A e 313-B).

Autores como Câmara et al (2018-2021, p. 14) defendem como surgimento embrionário da preocupação com a privacidade e a proteção de dados no Brasil, o Código Penal, em 1940. Apesar de não tratar especificamente da proteção de dados, o artigo 151 do Códex é visto pelos autores como verdadeiro marco por prever, pela primeira vez, o direito à privacidade por meio da proibição expressa da violação de correspondência alheia:

Contudo, foi com o advento da Lei nº 8.078/1990 – Código de Defesa do Consumidor (CDC) –, que o país viu emergir a primeira lei nacional considerada como aquela que de fato veio a tratar da proteção de dados e outros direitos correlatos. Na esfera dos microssistemas, o CDC foi complementado pela Lei nº 12.414/2012 – Lei do Cadastro Positivo –, voltada à proteção de dados no contexto das relações de consumo, sobremaneira, dados de adimplência e modelagem de crédito, assim como temas sobre os princípios da finalidade, da necessidade e revisão das decisões automatizadas.

No CDC, as regras destinadas à proteção de informações estão, especificamente, delineadas ao direito de acesso do consumidor a informações pessoais e de consumo, que

estejam registradas em banco de dados (art. 43) e em órgãos públicos de defesa do consumidor (art. 44, § 1º). Em complemento a estas disposições, o CDC tipifica como crime a conduta consistente em impedir o acesso do consumidor a tais informações (art. 72); o direito à integridade da informação conferido ao consumidor, que pode exigir a correção de dados pessoais inexatos (art. 43, § 3°); a conduta omissiva do fornecedor que deixar de corrigir imediatamente informações que sabe ou deveria saber ser inexata (art. 73); e a vedação de fornecimento de informações relacionadas a débitos prescritos, por parte dos sistemas de proteção ao crédito (art. 43, § 5º).

Neste ponto, cabe destacar a importância da Lei nº 12.414/2011 que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Após duas décadas do surgimento do CDC, a lei veio para regular o banco de dados sobre bons pagadores, "como contraponto aos cadastros negativos de créditos e, [...] exigia o consentimento do consumidor para que seus dados financeiros comerciais pudessem ser analisados pelas agências a fim de pontuar e classificar o seu nível de adimplemento". (NETO, 2020, p. 34).

Salientamos, também, a Lei nº 12.527/2011 – Lei de Acesso à Informação –, que estabelece o princípio da publicidade e da transparência como regra de tratamento das informações na Administração Pública, elencando as hipóteses de sigilo no patamar das excepcionalidades, justificadas pelo interesse público (art. 3º), assim como regula o procedimento de acesso à informação perante as pessoas jurídicas de direito público (art. 10 a 20). Ainda, as circunstâncias de restrição ao acesso por meio do mecanismo de classificação de informações (art. 21 a 30).

A Lei também determina regras específicas para o tratamento de informações pessoais (art. 31), com disposições sobre o prazo de restrição ao acesso à informação sob tal atributo, com prazo de 100 (cem) anos a contar de sua produção, e hipóteses de dispensa do consentimento do titular.

A Lei nº 12.965/2014 – Marco Civil da *Internet* –, traz em seu bojo, dentre os principais pontos meritórios, expressamente, os princípios do uso da *internet* no Brasil, a garantia da liberdade de expressão, de comunicação e de manifestação de pensamento; a proteção da privacidade e a proteção dos dados pessoais (art. 3º).

Outrossim, legitima como direitos do usuário, a inviolabilidade da intimidade e da vida privada, sua indenização e proteção pelo dano material ou moral decorrente de sua violação; a

inviolabilidade e sigilo do fluxo de suas comunicações e a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (art. 7º). E ainda disciplina a coleta de dados pessoais via *internet* – incluindo a guarda de registros de conexão –, assim como as regras sobre o fornecimento do consentimento do usuário e sobre exclusão de dados (arts. 7º, 13, 14 e 15).

O Marco Civil da *Internet* foi regulamentado pelo Decreto nº 8.771/2016, que norteou o procedimento para requisição de dados cadastrais de usuários de *internet*, bem como padrões de segurança e sigilo dos seus registros, dados pessoais e comunicações privadas.

Cumpre ressaltar a importância das legislações que limitam o poder de investigação do Estado perante o particular e que, por essa razão, também figuram entre as normas de proteção às informações pessoais.

Destacamos, em primeiro plano, a Lei nº 9.883/1999, que instituiu o Sistema Brasileiro de Inteligência e criou a Agência Brasileira de Inteligência (ABIN), cujo conteúdo protetivo elenca como fundamento do Sistema Nacional de Inteligência, além da preservação da soberania nacional e a defesa do Estado Democrático, a dignidade da pessoa humana e os demais direitos e garantias individuais presentes na Constituição Federal, assim como nos tratados dos quais o Brasil seja parte (art. 1º, § 1º).

A Lei define como atividade de inteligência aquela que abarca o processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como salvaguarda da informação pelo acesso de pessoas ou órgãos não autorizados (art. 2º, § 1º). Compromisso este, reforçado pela cláusula do art. 3º e seu parágrafo único.

Ao passo, temos a Lei de Interceptações Telefônicas (Lei nº 9.296/1996), que regulamenta as contingências e expedientes para a obtenção de informações de comunicações privadas com vistas à investigação e instrução criminal.

Em paralelo a diversas disposições da LGPD que se referem à proteção dos segredos comercial e industrial, a Lei de Propriedade Industrial (Lei nº 9.279/1996) regula, ainda que parcamente, sob a tipificação de crimes de concorrência desleal, a conduta consistente em divulgar, explorar ou utilizar sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços (art. 195, inciso XI, XII, XIII e XIV).

Convém, ainda, referir a Lei Complementar nº 105/2001 – Lei do Sigilo Financeiro –, e a Lei nº 12.414/2011 – Lei dos Bancos de Dados de Crédito –, voltadas à proteção da informação pessoal atinentes às atividades econômicas e financeiras.

Por fim, não se pode olvidar da recente EC 115/2022, promulgada pelo Congresso Nacional no dia 10 de fevereiro de 2022, que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais listados no art. 5º e estabelece a competência material e legislativa da União sobre a proteção e o tratamento de dados pessoais.

A referida emenda acrescentou o inciso LXXIX ao art. 5º da Constituição, para incluir expressamente a proteção dos dados pessoais:

> LXXIX é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Recordemos que em 2020, o Supremo Tribunal Federal já tinha declarado a proteção dos dados pessoais como um direito fundamental implícito na Constituição, inserido na cláusula geral de privacidade (art. 5º, X e XII), ao analisar os limites das atividades de tratamento de dados pessoais diante do respeito à privacidade, ao julgar o pedido de tutela provisória em cinco ações diretas de inconstitucionalidade (ADI 6387, 6388, 6389, 6390 e 6393), propostas contra a Medida Provisória nº 954/2020.

A MP, que teve a sua vigência encerrada em 14 de agosto de 2020 (Ato Declaratório do Presidente da Mesa do Congresso Nacional nº 112/2020), impunha às empresas de telefonia fixa e móvel o dever de compartilhar com o IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas naturais e jurídicas (art. 2º), para permitir a manutenção da produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente da pandemia da COVID-19.

Cardoso (2022) menciona três consequências advindas da inclusão expressa da proteção de dados pessoais no texto constitucional, mais especificamente no art. 5º.

Em primeiro lugar, a proteção de dados pessoais passa a ser um direito fundamental expresso na Constituição. Consubstanciado em cláusula pétrea, que não pode ser revogada ou restringida, nem mesmo por Emenda Constitucional posterior (art. 60, § 4º, IV), ou seja, trata-se de um direito que, de agora em diante, só pode ser ampliado na Constituição. Ainda, assenta-

se a competência constitucional do STF, para, em processos de competência originária ou recursal, apreciar questões relacionadas à proteção de dados pessoais, quando houver violação direta ao novo inciso do art. 5º.

Em segundo lugar, a EC 115/2022 modificou dois dispositivos relacionados à competência material e legislativa da União. Incluiu o inciso XXVI ao art. 21 da Constituição, que contém a competência material exclusiva da União, para acrescentar que a ela incumbe "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Assim como acrescentou o inciso XXX ao art. 22 da Constituição, para inserir entre as matérias de competência legislativa privativa da União a proteção e tratamento de dados pessoais.

Desse modo, a Constituição também esclarece que a União tem o dever constitucional de adotar medidas positivas para conferir efetividade à proteção de dados pessoais e para fiscalizar as operações de tratamento – nos termos da LGPD, realizado pela Autoridade Nacional de Proteção de Dados.

Por fim, o novo texto também esclarece que o tema da proteção de dados se insere na competência legislativa privativa da União – já passível de entendimento com fundamento no art. 22, I, da Constituição, por se enquadrar na seara do Direito Civil. Estados e Municípios não podem legislar sobre a matéria. Apenas excepcionalmente, a Constituição autoriza que a União, por meio de lei complementar, permita que os Estados legislem sobre questões específicas (art. 22, parágrafo único).

4.2 Comentários ao texto da Lei nº 13.079/2018 (LGPD)

Antes de adentrarmos nas considerações acerca da definição de dado pessoal, sob o albergue da LGPD, consideramos prudente mencionar os objetivos que inspiraram sua elaboração e consequente promulgação. Conforme salienta, objetivamente, Ana Lopes (2021, posição 101), “a LGPD foi feita para proteger o usuário, o cliente ou o cliente do seu cliente, se [o] negócio é B2B *(Business to Business*)”. Logo, a lei alcança todo e qualquer trabalho de marketing digital ou vendas online, que precisam, necessariamente, se adequar a ela.

A partir dessas considerações, podemos afirmar que a LGPD intenta, prioritariamente, proteger direitos fundamentais de liberdade e privacidade das informações que as pessoas deixam ao se cadastrarem em milhões de *sites*, lojas, *blogs* etc., na *internet*, ou por quaisquer

meios digitais. É atuando diretamente sobre a proteção do indivíduo, do consumidor, no final da linha das estratégias de marketing ou de vendas que a Lei recai.

Feitas as devidas considerações em torno dos objetivos e alcance da Lei, passemos a uma análise não extensiva, mas, circunscrita aos aspectos que consideramos relevantes ao seu entendimento, que propiciem melhor base ao escopo da nossa pesquisa.

Por meio de seu art. 1º, o texto da Lei Geral de Proteção de Dados estabelece o escopo e objetivos das regras que virão a seguir. A LGPD visa preservar o direito constitucional à liberdade e à privacidade que todos os cidadãos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos. O parágrafo também destaca que as regras da LGPD valem em todo o território nacional e que prevalece sobre quaisquer outras leis municipais ou estaduais.

Finalmente, especifica que a LGPD se aplica "inclusive nos meios digitais". Quando se fala sobre a lei, a proteção de dados na *internet* e em meios eletrônicos costuma ser o foco, mas é fundamental entender que suas normas valem para todo e qualquer tratamento de dados, inclusive analógicos – fichas de cadastro no papel, verificações presenciais de documentos, dentre outros.

O art. 2º traz mais especificações sobre os embasamentos. A lei é construída sob a premissa do respeito à privacidade e à liberdade – inclusive de expressão. Enquanto isso, o conceito de autodeterminação informativa (item II) entende que o cidadão é soberano sobre suas próprias informações pessoais e deve ser o protagonista de quaisquer temas relacionados ao tratamento de seus dados.

Os itens IV e VII estabelecem que a LGPD se preocupa com a preservação da imagem do cidadão – um dos motivos por que seus dados pessoais devem ser protegidos é que o tratamento dessas informações não pode ser feito com fins de prejudicá-lo, salvo em casos específicos com finalidade noticiosa, por exemplo.

Finalmente, os itens V e VI especificam que a LGPD não se propõe a prejudicar as atividades das empresas que realizam tratamento de dados. O objetivo das regras é proteger o cidadão, e isso compreende entendê-lo como soberano de seus dados.

Ou seja, a Lei não impede o tratamento, e sim estabelece meios para que o cidadão saiba exatamente o que será feito com seus dados. Dessa forma, ele tem autonomia e capacidade de consentir, ou não, com o uso que a empresa deseja fazer de suas informações pessoais. Isso

preserva a competitividade e as estratégias das empresas, desde que elas se preocupem com a comunicação e uso transparente dos dados pessoais tratados no decorrer dessas atividades.

O art. 3º determina o escopo de atuação da Lei, que se aplica a todo e qualquer tratamento de dados realizado tanto por pessoa física quanto por pessoa jurídica.

A LGPD se aplica a qualquer tratamento de dados ocorrido – total ou parcialmente –, em solo brasileiro, ou que tenha por objetivo vender produtos e serviços nacionais. Uma pessoa estrangeira está protegida sob a LGPD dentro do Brasil, por exemplo, enquanto um brasileiro em outro país não.

Além disso, a lei é voltada para tratamentos com fins comerciais, ou seja, trocas e outros tratamentos de dados entre pessoas físicas sem objetivos de compra ou venda de produtos e serviços não se enquadram.

> 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;
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
>
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Neste ponto, mais uma vez, conforme observado por outros autores, Ana Lopes (2021, posição 155), destaca o cuidado no tratamento dos *cookies*, um dos principais objetos da nossa pesquisa, ao afirmar que "tudo que envolver dados de pessoas no meio **digital precisa ser expressamente autorizado pela pessoa ao qual o dado se refere** [...] os termos de privacidade, **os *cookies* com botão aceita ou concorda** [...] (grifo nosso).

O art. 5º, um dos mais importantes da LGPD, estabelece a definição de conceitos fundamentais para a compreensão do texto como um todo:

- Dado pessoal: qualquer informação que possa levar à identificação de uma pessoa física (nome completo, número de CPF, endereço, filiação…);
- Dado pessoal sensível: assim considerado por haver a real possibilidade de mau uso para fins discriminatórios e prejudiciais ao indivíduo, como informações relativas a raça/etnia, religião, opinião política, sexualidade e dados genéticos ou biométricos (como a biometria facial ou o DNA de um indivíduo);
- Dado anonimizado: um dado pessoal ou dado pessoal sensível passa a ser um dado anonimizado quando deixa de ser diretamente relacionado a uma pessoa. Isso acontece, por exemplo, quando um conjunto de dados sensíveis (como a autodeclaração de raça dos colaboradores de uma empresa) torna-se estatística (a porcentagem de colaboradores que se identificam com cada raça);
- Banco de dados: seja digital, seja físico, um banco de dados é qualquer conjunto de dados pessoais;
- Titular: indivíduo a quem os dados pessoais sendo tratados se referem. É o soberano de qualquer assunto relacionado ao tratamento dessas informações e tem capacidade de consentir, ou não, com o tratamento;
- Controlador: responsável pelas decisões relacionadas ao tratamento dos dados pessoais. Entre outros pontos, é o controlador quem decide que dados serão tratados, de que forma e com que fim. Ele também é o principal responsável em caso de quaisquer incidentes que envolvam dados pessoais;
- Operador: quem trata os dados em nome de outra entidade, ou seja, em nome do controlador. O operador deve sempre seguir estritamente as ordens do controlador em relação ao tratamento dos dados;
- Encarregado: a LGPD prevê que operadores e controladores tenham um encarregado, pessoa responsável por intermediar a comunicação entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados;
- Agentes de tratamento: tanto o operador quanto o controlador são agentes de tratamento; a responsabilidade final é sempre do controlador, mas o operador também tem obrigações a cumprir e pode ser responsabilizado em alguns casos, como quando não seguir as instruções do controlador;

- Tratamento: toda e qualquer ação realizada com os dados pessoais de um titular, desde a coleta e armazenamento até o compartilhamento e uso. O ciclo completo de um dado pessoal, portanto, começa na coleta e termina na exclusão ou anonimização;
- Anonimização: um dado anonimizado é um dado pessoal que se torna total e integralmente desvinculado do titular, de forma irreversível, fazendo com que seja impossível que se possa chegar ao titular por meio desse dado. A anonimização, por remover o caráter pessoal dos dados, abre espaço para que dados sejam tratados de maneiras que são proibidas quando falamos de dados pessoais;
- Consentimento: permissão dada pelo titular para que determinado(s) dado(s) pessoal(is) seja(m) tratado(s). Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado;
- Bloqueio: suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que eles se encontram;
- Eliminação: exclusão de dados pessoais;
- Transferência internacional de dados: quando os dados pessoais são transferidos para fora do Brasil. É preciso assegurar que os dados terão proteção de nível equivalente ao proporcionado pela LGPD;
- Uso compartilhado de dados: quando os dados pessoais não ficam limitados a um único ente (privado ou público). Órgãos públicos podem compartilhar dados na prática de suas obrigações legais, enquanto entes privados podem fazê-lo mediante devido consentimento do titular;
- Relatório de impacto à proteção de dados pessoais: se houver qualquer risco de que determinado tratamento de dados possa vir a causar danos ao titular, é dever do controlador manter esse relatório. Dessa forma, em caso de incidentes, é possível entender os perigos da situação e trabalhar para mitigá-los mais rapidamente. A manutenção do relatório também visa comprovar que o tratamento que gera esses riscos recebe os devidos cuidados para evitá-los;
- Órgão de pesquisa: especificados no texto da LGPD porque tais órgãos têm regras diferenciadas para o tratamento de dados e pedido de consentimento;
- Autoridade nacional: a Autoridade Nacional de Proteção de Dados (ANPD) será o órgão responsável por implementar e gerenciar as regras da LGPD, garantindo que a Lei seja cumprida. A ANPD também é responsável por realizar auditorias, assim como aplicar as devidas sanções em casos comprovados de descumprimento da Lei.

Muito embora o conceito de dado pessoal seja bastante abrangente, nossa legislação, por meio do texto insculpido na LGPD, define como a "informação relacionada à pessoa natural identificada ou identificável".

Dessarte, conforme leciona Sandro Oliveira (2018-2021, p. 13), "um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, Passaporte e Título de Eleitor) endereço residencial ou comercial, telefone, e-mail, ***cookies*** e endereço IP" (grifo nosso).

Segundo a premissa de Dennys Câmara et al (2018-2021, p. 18), isso ocorre como meio de enquadrar mais informações dentro da definição, o que ampliaria o escopo de aplicação da Lei. Ainda, dentro desta concepção, é possível identificar duas categorias de dados pessoais segundo o texto da Lei: (i) dados pessoais sensíveis e (ii) dados anonimizados.

Ao fazer uso da nomenclatura "sensíveis" buscou-se resguardar aquelas informações que porventura pudessem sujeitar os seus titulares a práticas discriminatórias, por conseguinte, o tratamento de tais dados deve observar bases legais mais restritivas e padrões de segurança mais elevados.

Por dados anonimizados, alude-se àqueles "sobre um titular que não possa ser identificado utilizando-se meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dados anonimizados não estariam sujeitos às regras da Lei caso não possam ser reidentificados, incentivando inovações, como *internet* das coisas e inteligência artificial" (CÂMARA et al, 2018-2021, p. 18).

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação 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;
>
> III - dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> [...]

A LGPD ainda prevê a possibilidade no tratamento de dados pseudonimizados, como aqueles que estão sujeitos ao tratamento que impossibilita a associação a um indivíduo, com uma exceção: para o uso de informação anteriormente mantida em separado pelo controlador. No caso da Lei brasileira, os dados pseudonimizados só podem ser utilizados na realização de pesquisas em saúde pública, em estrita observância ao art. 13 e seus parágrafos.

> Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
>
> § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.
>
> § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
>
> § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
>
> § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Em conclusão, "podemos pontuar que os dados anonimizados, caso não seja possível a sua reidentificação através de meios razoáveis, podem ser utilizados de maneira ampla, enquanto os dados pseudonimizados só podem ser utilizados para fins científicos bastante restritos" (CÂMARA et al, 2018-2021, p. 20)

Dentre as 10 hipóteses que permitem o tratamento de dados presentes na LGPD, encontra-se a possibilidade do consentimento de dados. Neste aspecto,

> toda movimentação online só será acessível com a permissão ativa do usuário, seja o e-mail que ele cadastrou, o celular (whats*app*) que ele forneceu, localização, preferências, pesquisas nas redes sociais e em buscadores. Enfim, tudo online só poderá ser capturado com a permissão do titular". Isso engloba seus anúncios, seu marketing, sua página de vendas, suas páginas de captura, o analytics, todos os meios de tracking [*cookies*] e tudo o que você tiver que coleta informações das pessoas, mesmo que seja um algoritmo ou bot, que faça isso. [...] a lei regulamenta desde a coleta, classificação, utilização, acesso, reprodução, transmissão, compartilhamento,

> transferência internacional, armazenamento e controle de dados, até o arquivamento e eliminação (LOPES, 2021, posições 118-131).

A LGPD assenta, inequivocamente, o consentimento sobre finalidade determinada, ao cogitar expressamente da possibilidade, por meio da transcrição de seu art. 5º, inciso XII, corroborado pelo art. 7º, inciso I, que reforça a necessidade e importância do consentimento.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;

Destacamos que, em caso de consentimento escrito, ele deverá constar em cláusula destacada no contrato, cujo ônus da prova cabe ao controlador. Ademais, o titular tem o direito, de forma gratuita e facilitada, à revogação do seu consentimento.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> [...]
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Impõe destacar como a LGPD, por meio de seu art. 14, trata os dados de crianças e adolescentes de maneira particularizada. A Lei assenta a firmeza em lidar com os dados que são vulneráveis diante de um tratamento. No caso específico desses usuários, além de se tratar de proteção em caráter integral, convém ressaltar o amparo do art. 227 da Constituição, reforçada pelo Estatuto da Criança e do Adolescente. A condição de desenvolvimento é vista como um período respeitado por se tratar de dados referentes a pessoas com uma faixa etária significativa de vulnerabilidades.

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de *internet* ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Para o tratamento de dados de crianças e adolescentes, a lei destaca a necessidade de tratá-los somente para o melhor interesse do titular, reforçando essa que é uma questão necessária em qualquer tratamento de dados.

É imprescindível solicitar o consentimento de um dos pais ou do responsável legal. O intuito é assegurar que uma pessoa maior de idade dará o devido consentimento pelo titular sob o qual é responsável. E essa responsabilidade, em garantir que o consentimento de fato foi fornecido pelo responsável, recai sobre o controlador, na medida do possível.

Contudo, destacam-se duas exceções em que o consentimento do titular e/ou do responsável não é exigido: quando houver a necessidade de entrar em contato com os pais ou com o responsável, ou quando tais dados forem necessários para proteger o titular menor de idade. Nesses casos, é terminantemente proibido compartilhar ou repassar os dados coletados com terceiros.

Ainda, como a Lei prevê o cuidado em garantir que dados pessoais de crianças e adolescentes não sejam coletados além do estritamente necessário, o compartilhamento de dados não-essenciais não pode ser requisito para que o titular possa utilizar *apps* e jogos.

E, mesmo que o consentimento final tenha que ser dado por um dos pais ou pelo responsável, é importante que a criança ou adolescente entenda o que está sendo pedido. Logo, as informações sobre o tratamento de dados devem ser fornecidas com uma linguagem adequada ao público-alvo do produto/serviço em questão. Inclusive, recomenda-se a utilização de áudio, vídeo e imagens para complementar as informações e facilitar o entendimento.

No dia 24 de maio de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) publicou, o Enunciado CD/ANPD nº 01/2023, no intuito de uniformizar a interpretação da Lei Geral de Proteção de Dados Pessoais (LGPD) quanto às hipóteses legais que autorizam o tratamento de dados de crianças e adolescentes.

> O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei. (DOU, 2023, p. 129).

O Enunciado propende orientar e destacar a preponderância do melhor interesse da criança e do adolescente como critério fundamental para a avaliação de operações de tratamento de dados envolvendo esses titulares. A medida representa uma primeira iniciativa da ANPD relacionada à proteção de dados pessoais de crianças e de adolescentes e fixa entendimento da Autoridade acerca das possibilidades interpretativas do artigo 14 da LGPD.

De acordo com o texto, o tratamento de dados pessoais de crianças e adolescentes pode ser realizado com base nas hipóteses legais previstas na LGPD, como nos casos de consentimento fornecido pelo titular, de cumprimento de obrigação legal, de proteção à vida ou de atendimento a interesse legítimo do controlador. Em qualquer situação, o melhor interesse da criança e do adolescente deve prevalecer, exigindo avaliação cautelosa por parte do controlador.

Noutro giro, ainda referindo a questão etária dos usuários, agora no que tange aos dados pessoais da pessoa idosa, tem-se, por meio do seu art. 55-J, XIX, o único que leva a proteção e privacidade de idosos em consideração, informando que compete a ANPD “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."

É de se depreender que o regulamento não os visualiza como vulneráveis, ainda que em alguns momentos, comprovadamente, apresentam mais dificuldades para certas tarefas. Dessa forma, o tratamento de seus dados deve ser feito de maneira comum e simples, sempre levando em consideração o consentimento e o oferecimento de informações claras, diretas e com mais facilidade.

Entretanto, impende informar que a ANPD, em Resolução de nº 2/2022, visualiza que o tratamento em alto risco incluiria crianças, adolescentes e idosos.

> Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
>
> [...]
>
> d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

E, apesar de não ter muitos detalhes na LGPD, convém considerar que outras legislações brasileiras dialogam diretamente com os direitos dos idosos, como a Lei 10.741/2003 – Estatuto do Idoso.

Anteriormente à LGPD, existiam poucas bases legais expressamente previstas em lei, no país, tais como: consentimento, interesse público e obrigação legal. Com a LGPD, esse leque aumentou, tornando o tratamento de dados, em tese, mais flexível do que os realizados com base somente nas leis nacionais até então vigentes. A lei trouxe em seu bojo 10 bases legais – hipóteses pelas quais a legislação permite que seja realizado o tratamento de dados pessoais –, para a coleta e o processamento de dados.

Para que seja considerado legítimo e lícito, no país, o tratamento dos dados pessoais precisa observar os princípios gerais e as bases legais específicas, que dependem da categoria de dados em questão. Os princípios estão inscritos no caput e nos 10 incisos do art. 6º da LGPD, consubstanciados através: (i) da boa-fé; (ii) finalidade; (iii) adequação; (iv) necessidade; (v)

livre acesso; (vi) qualidade dos dados; (vii) transparência; (viii) segurança; (ix) prevenção e não discriminação; e (x) responsabilização e prestação de contas.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> 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;
>
> 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.

Por sua vez, o conjunto de bases legais está reunido no caput e ao longo dos 10 incisos do art. 7º, encartados: (i) pelo consentimento do titular; (ii) cumprimento de obrigação legal ou regulatória pelo controlador; (iii) execução de políticas públicas; (iv) realização de estudos; (v) execução de contrato do qual seja parte o titular; (vi) exercício regular de direito em processo judicial, administrativo ou arbitral; (vii) proteção da vida; (viii) tutela da saúde; (ix) legítimo interesse; e (x) proteção ao crédito.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Como já mencionado, as regras para o tratamento dos dados pessoais sensíveis são ainda mais restritivas do que aquelas aplicadas aos dados pessoais comuns. Em se tratando do consentimento do titular, por exemplo, deve ser feito de forma específica e destacada para as finalidades de tratamento descritas. Contudo, comporta exceções para o seu tratamento sem consentimento, caso esse dado seja indispensável para a execução das atividades destacadas na Lei.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

O art. 15 trata sobre o fim do uso dos dados e, repisando a exortação do art. 7º, reforça que o dado só pode ser usado para o fim que foi determinado ou por solicitação do titular, a pessoa cujos dados se está lidando.

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II - fim do período de tratamento;
>
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

A LGPD intenta assegurar a toda pessoa natural a titularidade de seus dados pessoais, garantindo os seus direitos fundamentais de liberdade, intimidade e privacidade.

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Ademais, elenca uma série de direitos específicos ao longo dos seus arts. 18 e 20, dentre os quais, aqueles nomeados por Dennys Câmara et al (2018-2021, p. 22), como “direitos

‘ARCO’, que garantem aos titulares: (i) acesso; (ii) retificação; (iii) cancelamento [eliminação]; (iv) oposição ao processamento de seus dados pessoais (art. 18, incisos II, III, VI e § 2º)”.

Outros direitos assegurados aos titulares pela LGPD são: (v) confirmação da existência de tratamento; (vi) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; (vii) portabilidade dos dados; (viii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (ix) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (x) a revogação do consentimento (art. 18, incisos I, IV, V, VII, VIII e IX).

Além dos direitos supracitados, podemos inferir mais um, disposto no art. 20, que versa sobre (xi) revisão de decisão automatizada que, com as mudanças carreadas pela MP nº 869/18 na LGPD, não precisa ser realizada por pessoa natural.

Em seu art. 5º, inciso XIV, a Lei define o termo “eliminação” como “a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado”. Ainda, o inciso X do mesmo art. 5º prevê a “eliminação” como uma dentre as 18 modalidades de tratamento de dados encartados no texto legal.

> Art. 5º [*omissis*]:
>
> [...]
>
> 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;
>
> [...]
>
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
>
> [...]

Contudo, o direito à exclusão dos dados pessoais não é absoluto:

> A exclusão ou cancelamento dos dados, requerida pelo titular dos dados é baseada na revogação do seu consentimento [art. 15, inciso III]. Caso exista uma outra base legal, que não o consentimento, que autorize a manutenção dos dados, a empresa poderá continuar o tratamento até que a finalidade seja atingida. Ou seja, uma vez que o

> armazenamento dos dados é uma hipótese de tratamento destes, é necessário ter uma base legal para ela, seja o consentimento ou alguma outra das previstas na LGPD (grifo nosso) (CÂMARA et al, 2018-2021, p. 21).

Além de revisitar o tema da finalidade, o art. 16 também informa que os dados devem ser eliminados após o uso no que foi autorizado:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Após o término do tratamento, os dados pessoais devem, geralmente, ser eliminados. Isso não é exigido quando a permanência dos dados é necessária para que o controlador cumpra suas obrigações legais – para fins de compliance, por exemplo.

Órgãos de pesquisa estão isentos dessa regra, mas recomenda-se a anonimização dos dados sempre que possível.

Cumpridas as diretrizes da lei e/ou sob a solicitação do titular, a transferência dos dados a terceiros é permitida no lugar de sua exclusão. Além disso, caso o controlador anonimize os dados, é possível mantê-los para uso único e exclusivo – para fins estatísticos, por exemplo.

Ana Lopes (2021, posição 232), chama a atenção para a importância do art. 21, no tocante à utilização, informação adequada e finalidade no tratamento dos dados: “Se algum cliente se sentir prejudicado pela utilização das informações dele, ou se ele achar que não informou os dados dele para a finalidade que você está usando, você vai ter problemas com a justiça [...]”

> Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

O art. 42 e seus incisos dispõe sobre a responsabilidade solidária por parte dos operadores e controladores, em caso de danos devido à má utilização das informações fornecidas por um titular dos dados. Todos os envolvidos no mau uso dos dados, desde o controlador principal, até os contratados, passando pelos profissionais responsáveis pelo lançamento de e-mails, mensagens ou quaisquer conteúdos, poderá ser responsabilizado pela ilegalidade:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
>
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
>
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Passando à última análise dos parâmetros traçados pelo legislador, quanto aos percursos do tratamento de dados delimitados pela LGPD, reportamos as sanções administrativas atribuídas à ANPD:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos

> os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;

Como medida, para definição da sanção aplicável, a ANPD deverá seguir o que está arrolado no art. 52, § 1º, incisos I a XI:

> Art. 52. [*omissis*]:
>
> [...]
>
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Em 27 de dezembro de 2018, o então Presidente Michel Temer editou a MP n° 869/18, publicada no Diário Oficial da União em 28 de dezembro de 2018, que, além de promover determinadas alterações no texto sancionado da LGPD, também criou a ANPD como sendo um órgão da administração pública federal direta e vinculado diretamente à Presidência da República, conforme insculpido no texto da Lei, por meio do caput do art. 55-A.

5 PONDERAÇÕES SOB O PRISMA DA RESPONSABILIDADE CIVIL

5.1 O regime jurídico da responsabilidade dos agentes de tratamento de dados

Um dos principais eixos da LGPD gira em torno justamente das delimitações de quais são as obrigações dos agentes de tratamento de dados, fixando o regime jurídico para sua responsabilização. A esse respeito, a seção sobre responsabilidade e ressarcimento de danos – seção III, do capítulo VI –, se apresenta como exercício de desafio à dogmática jurídica.

Como a doutrina brasileira tem focado a sua atenção para responder essencialmente se o regime da responsabilidade é objetivo ou subjetivo, Bioni (2021), informa que, por mais relevante que pareça, não se trata de questão que deve pautar o debate, pois a premissa da dualidade de regimes jurídicos de responsabilidade objetiva ou subjetiva é falsa. Para o autor, mais importante é analisar os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização.

Fruto de quase dez anos de debate público, a discussão em torno da Lei deixou pistas hermenêuticas valiosas sobre como considerar os trabalhos preparatórios da lei. Houve acirrada disputa em torno da definição do modelo de regime de reponsabilidade civil, não só na seção e dispositivos diretamente dedicados ao tema, assim como em torno de outros elementos normativos que calibram o regime jurídico da reponsabilidade dos agentes de tratamento de dados.

A primeira versão do anteprojeto de lei de proteção de dados pessoais, bem como a proposta legislativa do Senado Federal adotavam um regime de reponsabilidade civil objetiva. Enquanto a primeira preceituava que “o tratamento de dados [seria] uma atividade de risco”, a segunda estabelecia que os agentes da cadeia responderiam, “independentemente da existência de culpa” pela reparação dos danos.

A partir da segunda versão do anteprojeto, ganhou força a opção por um regime de reponsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública, essa escolha foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos “independentemente de culpa” ou “atividade de risco”, que eliminariam a culpa como um dos pressupostos da responsabilidade civil.

O texto foi gradualmente se encaminhando para delimitar quais seriam as excludentes de responsabilidade civil. Até a aprovação do substitutivo, as versões anteriores eram, senão silentes, extremamente tímidas para a definição de ilicitude de uma conduta, ou com relação ao seu nexo de causalidade na responsabilização dos agentes de tratamento. Nas palavras de Bioni (2021), "[...] apenas, [...] [no] último estágio da discussão legislativa que são prescritos [os] pilares fundantes do regime jurídico da responsabilidade civil da LGPD."

> Em vez de simplesmente espelhar as excludentes do CDC, o legislador optou por eximir a responsabilização dos agentes de tratamento de dados caso comprovem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II). Da mesma forma, quando a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados, há ressalva de que tal responsabilização somente é deflagrada se não foram adotadas as "medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação". Trata-se de elementos que afasta a responsabilização do sistema de responsabilidade civil objetiva. (BIONI, 2021, p. 402).

Tem-se, pois, que os trabalhos preparatórios da LGPD apontam que sua política legislativa optou pela denegação de um regime de reponsabilidade civil objetiva. Há outros elementos normativos que, direta ou indiretamente, convergem para que se conclua por uma valoração em torno da culpa do lesante.

A LGPD estabelece dois pressupostos para a responsabilidade civil dos agentes de tratamento de dados, quando há a "violação à legislação de proteção de dados pessoais" ou a "violação da segurança dos dados". Ambas equalizadas pela noção de tratamento irregular, prevista no artigo 44, que procura sistematizar critérios para aferição da culpa dos agentes de tratamento de dados a esse respeito.

O art. 44 prevê que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado."

Contudo, o conceito de tratamento irregular apresenta divergências, já que, segundo Bioni (2021, p. 406), se a figura do tratamento irregular se conecta igualmente com ambas as hipóteses de responsabilidade – tanto por violação da legislação, quanto da segurança –, melhor

seria prever sobre a irregularidade em dispositivo autônomo, o que permitiria equilíbrio entre as duas hipóteses de violação de normas da LGPD.

Como solução possível, ao que considera má técnica legislativa, passível de explicação a partir da transposição do CDC, ao regular defeito do serviço (art. 14, § 1º), para a LGPD, o autor sugere que melhor seria "um dispositivo que previsse, no caput, que os agentes de tratamento responderiam pelos danos decorrentes de tratamento irregular de dados. E, em parágrafo, houvesse a explicação do conteúdo do tratamento irregular". (BIONI, 2021, p. 407).

Podemos concluir, pelas razões até aqui levantadas, que o critério determinante para a imputação de responsabilidade é o da irregularidade do tratamento. Critério, por sua vez, preenchido com base nas legítimas expectativas de segurança que um titular médio pode legitimamente esperar do tratamento de dados em questão, a partir da leitura do art. 44, caput,

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou **quando não fornecer a segurança que o titular dele pode esperar,** consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.
>
> [grifo nosso]

Combinado com o art. 46, caput,

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

Para realizar de maneira acurada o juízo de culpa, caso a caso, Bioni (2021) sugere analisar as circunstâncias relevantes para determinação da segurança que o titular médio pode esperar do tratamento de dados: I – o modo pelo qual o tratamento é realizado; II – o resultado

e os riscos que razoavelmente dele se esperam; e III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

A partir do uso da terminologia "entre as quais" no caput do artigo 44, o autor afirma tratar-se de elenco não exaustivo das circunstâncias para determinar a segurança que o titular pode esperar do tratamento de dados pessoais, ou a possibilidade de violação às normas de proteção de dados em sentido latu sensu. Assim, diante de importante abertura normativa, em virtude da vagueza do artigo 44, em especial dos incisos I e II, pode-se recorrer a outros elementos normativos da própria LGPD.

Um caminho possível para robustecer o teor normativo de tais incisos, seria coaduná-los ao que preceitua o art. 50, em especial os §§ 1º e 2º.

> Art. 50 *[omissis]*
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> [...]

Portanto, depreende-se que os agentes devem ajustar suas medidas de segurança para corresponder à probabilidade e gravidade de uma violação em face dos possíveis impactos nos direitos e liberdades dos titulares dos dados. Tem-se como objetivo singular, separar e estimar os riscos variados para, em seguida, aplicar medidas de segurança.

O art. 43 prevê as excludentes de responsabilidade dos agentes de tratamento. Diante de dano decorrente de tratamento de dados, presume-se: (i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; e (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento. A redação do art. 43 é cristalina.

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

> II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
>
> III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Temos, portanto, três excludentes de responsabilidade dos agentes de tratamento envolvidos em um evento danoso.

A primeira exclui a responsabilidade do agente que não realizou o tratamento de dados pessoais. Eis, que não é difícil a um titular demandar a empresa incorreta, acreditando ser ela a responsável pelo tratamento do dado pessoal, quando não o é.

A segunda hipótese de exclusão de responsabilidade é relacionada à ausência de violação da LGPD naquela atividade de tratamento de dados pessoais. Pois, tal ausência de violação afastaria a ilicitude do ato e, portanto, o dever de indenizar.

A terceira hipótese diz respeito à culpa exclusiva da vítima no evento danoso ou de terceiros. Sobre essa hipótese Santos (2021) faz um questionamento interessante. Ainda que o operador e controlador adotem as melhores técnicas de proteção, acaso haja uma invasão, como resultado de técnicas absolutamente inovadoras, mesmo comprovada a adoção de medidas de segurança eficientes e razoáveis, seria admitida a excludente de responsabilidade por fato de terceiro?

A autora apresenta a resposta para esse questionamento, admitindo que a adoção das medidas de segurança e a prova dessa adoção é a chave para a solução. Agindo de tal forma, pode ser que a responsabilidade por uma invasão seja exonerada ou mitigada, a depender do caso concreto.

Para além da presunção geral dos dois elementos supracitados da responsabilidade civil dos agentes de tratamento, a Lei também prevê a possibilidade de o juiz inverter o ônus da prova a favor do titular dos dados quando a alegação for verossímil, quando houver hipossuficiência ou quando a produção de provas for excessivamente onerosa (art. 42, § 2.º).

Em busca da compatibilização entre as previsões do arts. 42, § 2º e 43,

> [...] caso a alegação da vítima seja verossímil, ou haja hipossuficiência para produção de provas, ou a produção seja excessivamente onerosa, o juiz poderá inverter o ônus da prova em relação a esses três últimos elementos. Como resultado, a vítima não precisará provar nenhum elemento da responsabilidade, ficando a cargo dos agentes de tratamento o ônus de provar a sua não ocorrência. (BIONI, 2021, p.418).

O regime jurídico da responsabilidade civil estipulado pela LGPD pende significativamente os filtros da responsabilidade civil em favor do titular dos dados. Ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas, podendo haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil.

5.2 Os desafios da Agência Nacional de Proteção de Dados (ANPD) na fiscalização e aplicação das sanções previstas na LGPD

A LGPD foi aprovada em 14 de agosto de 2018, cuja entrada em vigor estava prevista para fevereiro de 2020. Em julho de 2019, com a aprovação da Lei n° 13.853, a data foi modificada para agosto de 2020 e, posteriormente, alterada novamente devido à instabilidade provocada pela pandemia do coronavírus (Covid-19), entrando em vigor em setembro de 2020, parcialmente.

Conforme a Lei nº 14.010, de 10 de junho e 2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET), no período da pandemia, as multas e sanção previstas na LGPD só entrariam em vigor no dia 1º de agosto de 2021, com a atuação da Autoridade Nacional de Proteção de Dados (ANPD), órgão vinculado à Casa Civil. O prazo de quase um ano foi determinado pelo Congresso para que as empresas pudessem se adequar à Lei e para que a ANPD pudesse se preparar.

A criação da Autoridade Nacional de Proteção de Dados (ANPD), que já havia sido aprovada pela Lei nº 13.853/2019, mas teve sua estrutura disciplinada somente com o Decreto nº 10.474/2020, fortaleceu o desenvolvimento da cultura de proteção de dados no país. Tomando a responsabilização dos agentes de tratamento de dados pessoais como um dos eixos da LGPD, intensas discussões têm despontado a respeito do regime de responsabilização – judicial e administrativa –, que teria sido reservado aos agentes de tratamento em caso de descumprimento da Lei nº 13.709/2018.

Schvartzman (2021) sustenta que desde a edição da LGPD, o tema da responsabilidade civil adotada – se subjetiva ou objetiva – atraiu maior atenção em comparação com o regime de responsabilização administrativa, por duas razões: (i) o Poder Judiciário seria a primeira via

para os titulares de dados reivindicarem seus direitos, ao menos enquanto a ANPD ainda não fosse operacional; (ii) e o capítulo da LGPD relativo às sanções administrativas (arts. 52 a 54) só teria vigência a partir de 1º de agosto de 2021 (art. 65, I-A), diferentemente do restante da Lei nº 13.709/2018, que já era passível de tutela judicial.

A LGPD previu um rol variado de sanções administrativas, de natureza admoestativa, pecuniária e restritiva de atividades. Conforme o art. 52 da LGPD, a ANPD pode aplicar as seguintes sanções administrativas:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o inciso II;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Caracterizada qualquer infração à LGPD, as sanções poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) aos agentes de tratamento de dados, inclusive, aos entes da administração pública.

Conforme dispõe o caput do artigo 52 da LGPD, as sanções administrativas previstas pela LGPD são passíveis de aplicação somente pela ANPD. Além disso, as competências da ANPD prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Contudo, a aplicação das sanções previstas na LGPD não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078/1990 (CDC) e em legislação específica. Assim, eventual atuação de outros órgãos públicos, como agências reguladoras ou

órgãos de defesa do consumidor, deve se dar segundo as suas próprias competências, ao abrigo de suas legislações específicas.

Independentemente da função do agente que incorreu em ilícito administrativo, a aplicação das sanções requer prévio processo, que possibilite a oportunidade do contraditório e ampla defesa, de acordo com as peculiaridades do caso concreto e considerados os parâmetros e critérios definidos no §1º do art. 52 da LGPD.

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
>
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;
>
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

O art. 53 da LGPD determina que a ANPD deverá editar regulamento próprio sobre a forma como será feita a fiscalização e os critérios para aplicação das sanções. A LGPD determina que a ANPD deverá editar regulamento próprio sobre sanções administrativas, que deverá ser objeto de consulta pública, contendo as metodologias que orientarão o cálculo do valor-base das sanções de multa.

As metodologias para as sanções pecuniárias devem ser previamente publicadas e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos na LGPD.

Nos termos da Lei, a aplicação de sanções requer criteriosa apreciação e ponderação de diversas circunstâncias, conforme aqueles já mencionados, do art. 2º, § 1º e seus incisos. Dessarte, por tais parâmetros, e em conformidade com sua Agenda Regulatória, a ANPD passou por fase de conclusão da elaboração do Regulamento de Fiscalização e Aplicação de Sanções Administrativas, mediante Consulta Pública entre 28 de maio e 28 de junho de 2021.

Em comento às sanções administrativas de cunho pecuniário, o cálculo da multa simples prevista na LGPD adotou técnica legislativa semelhante às multas do GDPR, conjugando dois limites máximos diferentes, sendo um deles em valor absoluto (R$ 50 milhões) e o outro um teto percentual (até 2% do faturamento).

A esse respeito, Schvartzman (2021), ressalta que No Brasil, o cômputo da multa simples por infração à LGPD está limitado ao percentual máximo de 2%, ainda, restrito ao subteto no valor absoluto de R$ 50 milhões – valor que corresponde à multa máxima fixada na Lei Geral de Telecomunicações (Lei nº 9.472/97, art. 179) e na Lei de Crimes Ambientais (Lei nº 9.605/98, art. 75).

Por consequência, empresas, grupos ou conglomerados com faturamento superior a R$ 2.5 bilhões ficam igualmente sujeitas ao limite máximo de R$ 50 milhões por infração, independentemente do seu faturamento.

Outra consideração pertinente, ao se levar em conta a questão do faturamento dos agentes de tratamento, como base para o cálculo das multas aplicáveis, é o fato de que para a multa simples adota-se o "faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil".

Eis que, como o conceito de agentes de tratamento de dados abrange tanto pessoas jurídicas como naturais, pergunta-se como as pessoas físicas – sem faturamento – seriam sancionadas – se não forem empresários individuais–, ou mesmo quando os agentes de tratamento forem pessoas jurídicas com receitas estranhas à noção de faturamento – doações, cotas do Fundo Partidário e demais arrecadações de partidos políticos que não são consideradas exatamente como "faturamento" na legislação eleitoral.

Ao que se depreende do texto legal, a LGPD não pretendeu ressalvar esses agentes da aplicação de sanções pecuniárias – pois somente entidades e órgãos públicos foram expressamente excepcionados no art. 52, §3º. Portanto, eventual multa imposta a pessoas

naturais ou a pessoas jurídicas sem faturamento provavelmente suscitarão questionamentos passíveis de judicialização.

Levando-se em conta os princípios da legalidade e da tipicidade em matéria de direito administrativo sancionador, a indefinição acerca da base de cálculo das multas para pessoas naturais também impede a aplicação de sanções por analogia, consoante a jurisprudência do STJ.

> PROCESSUAL CIVIL. ADMINISTRATIVO. AÇÃO POPULAR. ATO DE IMPROBIDADE. APLICAÇÃO DAS SANÇÕES IMPOSTAS PELA LEI N.º 8.429/92. IMPOSSIBILIDADE. PRINCÍPIOS DA LEGALIDADE E TIPICIDADE.
>
> 1. O direito administrativo sancionador está adstrito aos princípios da legalidade e da tipicidade, como consectários das garantias constitucionais (Fábio Medina Osório in Direito Administrativo Sancionador, RT, 2000).
>
> 2. À luz dos referidos cânones, ressalvadas as hipóteses de aplicação subsidiária textual de leis, a sanção prevista em determinado ordenamento é inaplicável a outra hipótese de incidência, por isso que inacumuláveis as sanções da ação popular com as da ação por ato de improbidade administrativa, mercê da distinção entre a legitimidade ad causam para ambas e o procedimento, fato que inviabiliza, inclusive, a cumulação de pedidos. Precedente da Corte: REsp 704570/SP, Rel. Ministro Francisco Falcão, Rel. p/ Acórdão Ministro Luiz Fux, DJ 04.06.2007.
>
> 3. A analogia na seara sancionatória encerra integração da lei in malam partem, além de promiscuir a coexistência das leis especiais, com seus respectivos tipos e sanções 4. Recurso especial desprovido.
>
> (STJ, REsp n. 879.360/SP, 2008)

O art. 52, § 4º, da LGPD reproduziu redação muito similar à do art. 37, § 2º, da Lei de Defesa da Concorrência, substituindo apenas as autoridades em questão – menção ao Cade pela ANPD.

Por conseguinte, admitiu que o cálculo da multa considere "o faturamento total da empresa ou grupo de empresas, quando não disp*user* do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea".

Entretanto, apesar da redação coincidente dos dispositivos, a lógica do Sistema Brasileiro de Defesa da Concorrência não se verifica na LGPD. Haja vista a Lei nº 12.529/2011 trazer previsão expressa de solidariedade entre a empresa infratora e o seu grupo empresarial, ao contrário da LGPD, que não contém previsão nesse sentido.

Se os legisladores, em algum momento, pretenderam estabelecer responsabilidade solidária entre pessoas jurídicas do mesmo grupo empresarial na sistemática da LGPD, é certo que essa intenção não foi refletida no texto aprovado e vigente da Lei nº 13.709/2018, que nada diz a esse respeito.

Como "[a] solidariedade não se presume; resulta da lei ou da vontade das partes", – em conformidade com o texto do Código Civil, art. 265 –, não pode haver solidariedade, na LGPD, entre pessoas jurídicas que integram o mesmo grupo empresarial.

Nos termos do § 4º do art. 52, o que se pode concluir é pela inclusão do faturamento do grupo de empresas para fins de base de cálculo da multa, observados os requisitos específicos do dispositivo em questão, mas a empresa tida como infratora, única e exclusivamente, é quem deve integrar o processo administrativo sancionador.

Finalmente, inexistindo solidariedade entre empresas do mesmo grupo empresarial na LGPD, mesmo a regra do §4º do art. 52 carrega aplicação passível de questionamento, por força do princípio da pessoalidade (CF/88, art. 5º, XLV), vez que a intranscendência subjetiva das sanções impede que uma multa supere a esfera jurídica da pessoa jurídica infratora.

Atualmente, o *site* da ANPD dispõe as formas pelas quais "Denúncias" ou "Petições do Titular" podem ser encaminhadas à Agência, por meio de formulários específicos para cada caso. Os procedimentos encontram-se regulamentados pela LGPD e pelos artigos 20, 25 e 26 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01/2021. Importa, nesse ínterim, fazer a distinção entre as duas ferramentas.

A "Petição do Titular" é uma solicitação realizada à ANPD pelo titular de dados pessoais quando não conseguir exercer seus direitos perante o controlador de dados pessoais. Possibilita exercer direitos em uma situação específica, em que uma empresa ou um órgão público, por exemplo, coleta, guarda, utiliza ou compartilha os seus dados pessoais.

O exercício de direitos deve ser solicitado, primeiro, diretamente ao controlador, responsável pelos dados pessoais. E, caso o pedido não tenha sido atendido ou a resposta dada pelo controlador reste insatisfatória, é possível comunicar à ANPD por meio de uma "Petição de Titular".

Convém frisar que os direitos do titular não são absolutos e nem sempre poderão ser atendidos pelo controlador, como no caso do pedido de exclusão de dados em que o controlador tenha a obrigação legal de guardar esses dados, por exemplo.

As “Denúncias”, por sua vez, são as comunicações feitas à ANPD por qualquer pessoa, natural ou jurídica, de suposta infração à legislação de proteção de dados pessoais brasileira, diferente da “Petição de Titular”.

As “Denúncias” de descumprimento à LGPD possuem a característica de não se relacionarem, necessariamente, a uma situação específica de um determinado titular de dados pessoais. Geralmente, são situações que atingem um conjunto de titulares de dados ou que impossibilitam o exercício de direitos por parte dos titulares.

Como exemplos de situações que podem ser denunciadas estão:

- o tratamento discriminatório dos dados pessoais;
- a coleta excessiva de dados pessoais;
- a ausência de encarregado pelo tratamento dos dados pessoais;
- a não existência de canal de comunicação para o exercício de direitos;
- a ausência de medidas de segurança adequadas;
- a ausência de política de privacidade, entre outros.

A LGPD prevê uma série de direitos ao titular de dados pessoais em relação ao tratamento dos seus dados, que incluem:

- o direito de confirmar a existência de tratamento de dados pessoais pelo controlador;
- o direito de acessar seus dados pessoais;
- o direito de pedir a correção de informações que estejam incompletas ou desatualizadas;
- o direito de solicitar a revogação do consentimento dado ao controlador dos dados pessoais;
- o direito de pedir informações acerca do compartilhamento de seus dados pessoais e, em algumas situações, o direito de solicitar a exclusão de seus dados.

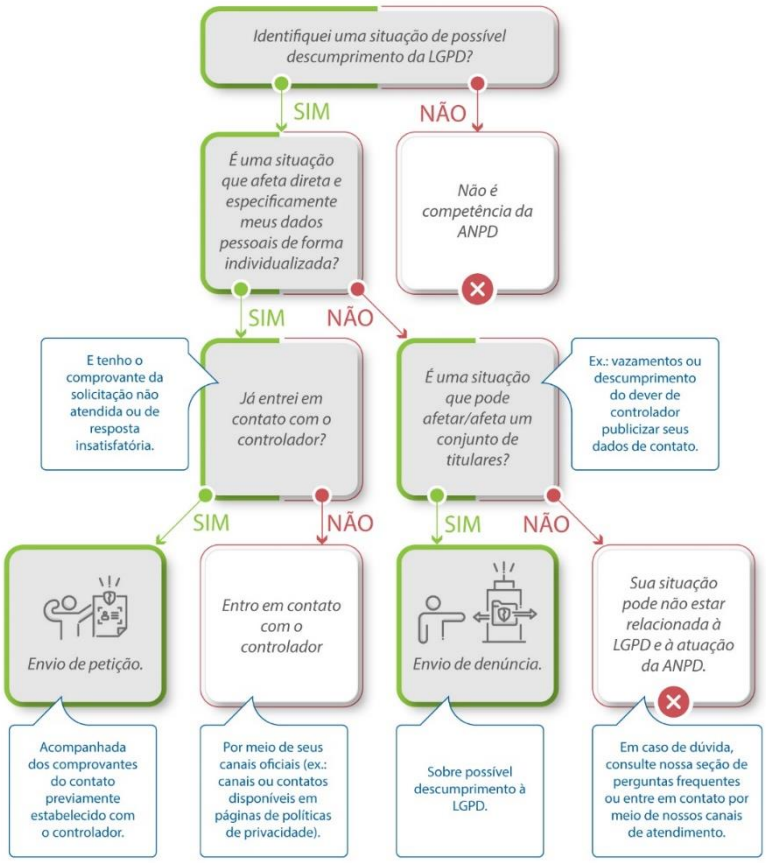
O envio de requerimentos à ANPD (Denúncias e Petições) deve ser realizado pelo preenchimento de formulário e deverá ser enviado por meio do Peticionamento Eletrônico do Sistema Único de Processo Eletrônico em Rede (SUPER.BR).

No sistema “SUPER”, deve-se selecionar o tipo de processo “ANPD – Denúncia” ou “ANPD – Petição de Titular”, a depender da demanda, juntar ao processo o formulário preenchido, preferencialmente em formato PDF e os documentos complementares, se houver.

Os requerimentos encaminhados por meio dos formulários podem ser acompanhados na plataforma de processo eletrônico da ANPD e deverão ser identificados. Não serão recebidos formulários sem identificação. As petições de titulares não poderão ser enviadas de forma anônima.

Caso se queira realizar uma denúncia anônima, elas deverão ser enviadas apenas pela Plataforma Fala.br. Não é possível realizar o acompanhamento do processo se ele for enviado como uma denúncia anônima.

Figura 2 – Fluxograma para encaminhamento de Petição do Titular contra o Controlador e Denúncias de Descumprimento da LGPD junto à ANPD



Fonte: Autoridade Nacional de Proteção de Dados (2023)

A agência informa que “Denúncias” não relacionadas à LGPD ou feitas de forma genérica não serão admitidas. É necessário que a situação apresentada à ANPD seja:

- escrita de forma clara;
- relativa a uma situação específica que envolva dados pessoais;
- relacionada a um descumprimento da legislação de proteção de dados pessoais (Lei Geral de Proteção de Dados).

Todos os requerimentos recebidos, bem como a avaliação das respostas dos controladores pelos titulares, quando for o caso, serão considerados no planejamento das ações de fiscalização, nas melhorias regulatórias e nas ações educativas propostas pela ANPD.

Os requerimentos, em regra, serão analisados de forma agregada e as eventuais providências deles decorrentes serão adotadas de forma padronizada. Desse modo, a ANPD não intervém diretamente na situação concreta e específica relacionada ao tratamento de dados pessoais ou ao exercício de direitos, mas a situação será considerada em planejamentos e ações mais abrangentes que possam alcançar, direta ou indiretamente, um conjunto de titulares com situações equivalentes ou similares.

Por fim, de modo geral, a ANPD não envia uma resposta individual e nem opina individualmente sobre os requerimentos. Entretanto, aqueles referentes a situações graves e que possam afetar muitos pessoas poderão, excepcionalmente, ser tratados individualmente.

6 CIÊNCIA DA COMPUTAÇÃO

6.1 *User Experience* (*UX*) e *cookies* de navegador

Analisaremos os conceitos de *User Experience* (*UX)*, em virtude da influência que o desenvolvimento dessa área do *design* de *interface* homem-máquina tem exercido sobre as escolhas dos controladores de dados, ao lançarem mão das ferramentas e práticas de consentimento na utilização de *cookies* de navegador da sua base de clientes ou usuários dos seus serviços.

Nesse contexto, as *Consent Manegement Plataform* (CMP), cujo principal objetivo é o de suportar as empresas na adequação de seus *sites*, costumam recorrer às ferramentas de *UX Design* para manipular a forma pela qual os titulares consentem com os termos de aceite disponibilizados por meio de *banners* ou *pop-ups*, que permitem a utilização dos *cookies* dos dispositivos dos usuários.

Numa tática que costuma variar entre o "tudo ou nada", seja pela utilização de um único botão de aceite disponibilizado junto aos termos de consentimento, ou entre um excessivo número de botões, *checkboxes* e termos que necessitam de aceite em níveis exagerados de detalhamento, as ferramentas e práticas de *User Experience* (*UX*) podem, a partir dos objetivos traçados pelas CMPs, influenciar a manifestação do titular, com relação ao que está consentindo.

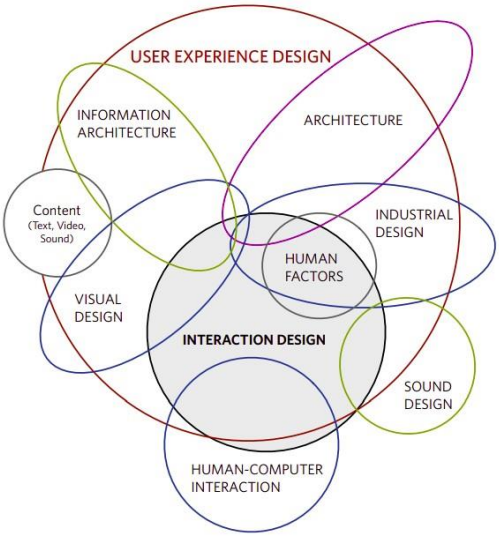
Para explicar a razão pela qual produtos ou serviços digitais similares fazem mais sucesso do que outros, recorremos ao termo "antropocentrismo digital" para referir o papel central que os usuários alcançaram na sua relação com o mundo digital: "Se ele não tem uma boa experiência com o produto digital, ele deixa de utilizá-lo e migra para *interface*s mais inteligentes, agradáveis e de fácil uso. E o diferencial do produto ou serviço digital pode residir justamente ali". (TEIXEIRA, 2014. p. 03)

O termo *User Experience* (*UX*) foi formalmente cunhado na década de 1990, pelo Dr. Donald Norman, engenheiro elétrico e cientista cognitivo da *Apple*, por meio do qual desenvolveu um *design* centrado no usuário, baseado nos objetivos e necessidades dos usuários dos produtos ou serviços. Segundo a definição apresentada por Godwin (2022, p. 11), *User Experience* (*UX*) pode ser definido como "a impressão pessoal do usuário ao usar um produto particular".

A despeito do estrangeirismo do termo que deu origem à sigla *UX*, Teixeira (2014, p. 01), sugere que sua compreensão é mais simples do que aparenta: "[...] Experiência do usuário. Experiência de quem usa." O verbete pode sugerir que se trata de algo relativamente novo, porém, como já destacamos, experiência existe desde as mais remotas atividades humanas.

Saffer (2010, p. 21), apresenta um diagrama que possibilita compreender as várias interseções e nomenclaturas com as quais a área de *UX design* dialoga. Nele, podemos visualizar que o grande círculo que representa a área de *User Experience Design* engloba diversas outras disciplinas, que vão desde Arquitetura de Informação e *Design* Industrial, até *Sound Design*.

Figura 3 – Diagrama das áreas de interseção de *UX Design*



Fonte: Saffer (2010)

Como decorrência, um dos principais objetivos almejados pelos profissionais de *UX Design*er é

> [...] construir produtos que sejam fáceis de usar (a tal usabilidade), reduzindo a fricção e permitindo que os usuários completem a tarefa desejada em menos tempo, com menos ruído e obstáculos. Ao mesmo tempo, apoiam-se em princípios da psicologia para motivar o usuário e incentivá-lo a seguir adiante. (TEIXEIRA, 2014, p. 04).

Portanto, cabe aos profissionais da área desenhar a estrutura dos produtos digitais. O que não se confunde com Direção de Arte, a quem cabe criar a identidade digital dos produtos, cuja preocupação seria com as cores e os formatos de determinado botão, por exemplo. No caso

dos *UX designers,* a tarefa recai sobre a definição de questões mais estratégicas a respeito dos tais botões, como listado por Teixeira (2014, p. 07):

- Por que o botão existe?
- Qual a importância dele naquele contexto ou página em que ele aparece?
- Ele é a ação primária ou secundária que o usuário pode tomar naquele momento?
- Para onde o usuário será levado quando clicar no botão?
- O que o texto do botão deve dizer para o usuário?
- O botão está sempre ativo, ou ele só é ativado depois que o usuário preencher determinado campo em um formulário?
- Todos os usuários, logados ou não no *site*, veem o mesmo botão?
- O tamanho do botão está adequado para ser clicado tanto com o ponteiro do mouse em um computador desktop quanto por um dedo humano em uma *interface touch* (celular, *tablet*)?
- *Ad infinitum*.

O autor destaca que, com frequência, proprietários de plataformas virtuais buscam, por meio da abordagem em *UX Design*, auxílio para a tomada de decisões mais assertivas, que respondam às seguintes dúvidas: "qual tipo de menu utilizar no *site*?", ou "como melhorar a usabilidade para aumentar as conversões de um formulário de cadastro?", por exemplo.

Atualmente, os *cookies* desempenham um importante papel na *internet*, seja aprimorando a experiência dos usuários, ou até mesmo servindo de sustentação para alguns modelos de negócios. Todos os dias, invariavelmente, quando acessamos quaisquer páginas na *internet*, recebemos um aviso de que aquele determinado *site* utiliza *cookies*.

Mediante a atual política propiciada pela legislação de proteção de dados vigente, devemos fazer escolhas relativas ao aceite, recusa ou o gerenciamento das preferências sobre o uso de *cookies*. No último caso, devemos informar, especificamente, as categorias de *cookies* e as respectivas finalidades que serão utilizadas pelo provedor do serviço.

Os *cookies* viabilizam o funcionamento das páginas eletrônicas e a prestação de serviços virtuais, que abrangem desde a medição do desempenho de determinado *site*, até a apresentação de anúncios personalizados, dentre outras finalidades. A forma de apresentação relativa ao seu uso pode variar de acordo com a página do serviço acessada e, indistintamente, os usuários

estão sujeitos a concordar ou discordar com as condições estipuladas pelos prestadores de serviços.

Dessa forma, como os usuários estão sujeitos a potenciais rastreamentos das atividades realizadas na *internet*, seja pelo controlador do *site*, ou por terceiros, "[...] assim como pode ocorrer com o uso de tecnologias similares, a utilização de *cookies* sem as devidas salvaguardas técnicas e jurídicas pode gerar impactos negativos sobre os direitos e a privacidade de titulares de dados pessoais" (LOPES et al, 2022, p. 05).

Lessig (2006, pp. 47-48) recorda que, "[...] quando um servidor da *web* recebe uma solicitação para atender a uma página da *web*, ele não sabe nada sobre o estado do solicitante antes que a solicitação seja feita". Se do ponto de vista da privacidade dos usuários, isso possa soar positivamente, não se pode afirmar o mesmo sob a perspectiva do comércio eletrônico. E não porque os *sites* comerciais queiram ou precisem saber tudo a nosso respeito, necessariamente. Mas, por motivos muito mais pragmáticos.

Se a adição e compra de vários itens ao carrinho de uma loja virtual nos parece algo deveras simples, o autor nos lembra que, como a *web* não foi originalmente construída para o comércio, a compra de alguns livros em um *site* qualquer, seria uma tarefa impossível na arquitetura da *internet* de outrora.

Digamos, por exemplo, que após adicionar cinco livros ao carrinho virtual, e clicar para encerrar a compra, o usuário seria surpreendido por um carrinho vazio. Devido à maneira como foi inicialmente projetada, a *Web* não conseguia identificar que a mesma pessoa que clicou em cinco itens diferentes, ainda que do mesmo *site,* se tratava do mesmo usuário. O servidor *web* simplesmente não tinha um protocolo para se lembrar do usuário que navegasse entre uma página e outra.

Siebecker (2003, p. 895-896) atribui a Netscape[4], o desenvolvimento da tecnologia responsável pela adaptação e aparência de um *site web* a qualquer visitante específico. Para isso, a empresa lançou mão da trilha de informações geradas por rastros eletrônicos ou marcadores, conhecidos pelos termos "dados de *clickstreaming*".

[4] Netscape – ou Netscape Communications Corporation – era uma empresa de serviços de informática mais conhecida por seu navegador da *Web*. A empresa foi fundada em 1994 por Marc Andreessen e James H. Clark como uma das primeiras e mais importantes start-ups da *internet*. O navegador *web* Netscape Navigator foi lançado em 1995 e tornou-se o navegador preferido dos usuários da época. Em novembro de 1998, foi adquirido pela AOL, que tentou, sem sucesso, reviver a popularidade do navegador da *web*. Dez anos depois, a Netscape foi totalmente fechada.

As trilhas fornecidas por esse tipo de dados costumam incluir informações básicas, como o tipo de computador, o tipo de navegador e a identificação de cada *site* ou página visitada. Inclusive, detalhes mais personalizados, como senhas, endereços de e-mail ou números de cartão de crédito.

Um dos principais problemas relacionados ao uso de *cookies* reside na falta de transparência no modo como as empresas têm utilizado a ferramenta.

> [...] a não disponibilização de informações claras, precisas e facilmente acessíveis sobre a coleta e a realização do tratamento, [...] pode inviabilizar ou restringir indevidamente o controle do titular sobre os seus dados pessoais. Os riscos à privacidade podem ser ampliados nas situações em que a falta de transparência está associada a práticas de coleta de quantidades massivas de informações pessoais para fins de identificar, rastrear e criar perfis comportamentais de usuários. (LOPES et al, 2022, p. 06).

Para esses autores, "*cookies* são arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas" (LOPES et al, 2022, p. 08).

Oliveira, (2005, p. 302), define *cookie* como um pequeno arquivo, geralmente no formato de texto, depositado pelo servidor de um *site* no disco rígido do computador que o acessa. Com propósito original de beneficiar o internauta, que pouparia tempo e poderia usufruir de visitas mais personalidades ao mesmo *site* no futuro, o autor afirma que o *cookie* é um elemento importante e quase indispensável para a comunicação com os *sites* na *internet*, de maneira que se tornaria muito difícil utilizá-la sem a sua presença.

Ressaltamos, ainda, a definição apresentada por Brain (2022, p. 01, grifo nosso), a partir do que não se encaixa na definição de *cookies*: "Os *cookies* não são programas e não podem ser executados como os programas. [...] eles não podem coletar nenhuma informação por conta própria. [...] **também não podem coletar nenhuma informação pessoal sobre você e sua máquina"**.

Convém destacar que, a despeito da informação mencionada pelo grifo acima, embora soe um tanto inofensiva à privacidade dos usuários, tal assertiva requer uma análise mais criteriosa, já que *cookies* podem representar alguma ameaça à privacidade dos titulares dos ados pessoais, a partir da venda de outras informações e políticas agressivas de marketing – cujos

riscos explanaremos ainda neste capítulo –, que resvalam nos métodos arrojados do Capitalismo de Vigilância, como já abordado.

Para o autor, a melhor definição, aquela que ele cita como uma que pode ser considerada válida, seria "um pedaço de texto que um servidor *web* pode armazenar no disco rígido de um usuário". Em complemento a este conceito, o autor esclarece que a principal função de um *cookie* é possibilitar que um *site* armazene informações na máquina de um usuário e as recupere posteriormente, utilizando-se de registros por meio de pares nome-valor.

Wojtowicz (2013), menciona famílias de *cookies* de navegador, conforme a sua finalidade. A primeira, dos *cookies* técnicos, se destina ao correto funcionamento de uma página na *internet*, subdividindo-se entre *cookie* persistente e *cookie* de sessão.

O primeiro cumpre a função de rastrear e memorizar as informações sobre a sessão do navegador do usuário, perdurando até a data programada para expirar, geralmente. O *cookie* de sessão, por sua vez, se desfaz cada vez que o navegador é fechado.

O autor ainda sugere uma outra família de *cookies* de navegador, a de perfil, cuja tarefa é traçar os padrões de navegação do usuário e coletá-los de maneira organizada, para oferecer mensagens publicitárias específicas às suas preferências.

Hoofnagle et al (2012) consentem que os *cookies* podem ser próprios, quando gerenciados pelo respectivo *site* que o usuário acessa, ou podem ser de terceiros, quando gerenciados por um *site* diferente do acessado.

Os *cookies* de terceiro fornecem os padrões de navegação dos usuários a empresas ou sujeitos que não guardam relação com seu acesso. Assim, ao acessar o "*site* A", o sujeito pode interagir com *cookies* de navegador do mesmo *site*, mas também do "*site* B", do "*site* C" e assim, consecutivamente.

Ayenson et al (2011), identificaram três tipos diferentes de técnicas de armazenamento de *cookies* nos computadores dos usuários: os *cookies* comuns HTTP, os *cookies flash* e os *cookies* de armazenamento HTML5, mais recentes.

Os três tipos se diferenciam quanto ao potencial de armazenamento, à forma de expiração e à maneira de acesso. O *cookie* padrão HTTP só consegue arquivar uma quantidade muito pequena de informação por vez, apenas 4 *Kbytes*, o *cookie flash* atinge 100 *Kbytes*, e o armazenamento por HTML5 consegue salvar em média 5 *MBytes*.

O *cookies flash* e HTML5 são permanentes, já o *cookie* padrão HTTP, geralmente é eliminado após o término da sessão online. *Cookies* dos tipos HTTP e HTML5 somente são acessíveis pelo único navegador em que foram salvos originalmente, enquanto o *cookie flash* fica disponível a todos os navegadores do usuário.

Cada *site* da *web* pode gerar um número de identificação exclusivo para cada visitante e armazenar o número de identificação no dispositivo de cada usuário, usando um arquivo de *cookie*. O local mais comum para o armazenamento dos *cookies*, em um dispositivo com sistema operacional Windows instalado, é o diretório (pasta): c:windowscookies. Neste diretório é possível encontrar os arquivos de *cookies* (arquivos de texto), que contém pares nome-valor. Há um arquivo para cada *site* visitado, que tenha registrado *cookies* no dispositivo.

Para compreendermos de maneira prática, como se dá essa troca de informações e consequente registro do *cookie* no dispositivo, suponhamos que tenhamos visitado o *site* ufal.br e ele tenha colocado um *cookie* em nosso dispositivo. Ao abrir o arquivo de *cookie* (arquivo de texto) para ufal.br, será possível visualizar as seguintes informações:

UserID A9A3BECE0563982D www.ufal.br/

O *site* ufal.br armazenou no dispositivo um único par nome-valor, no qual o nome é UserID e o valor é A9A3BECE0563982D. O processo de registro e atribuição do nome-valor se dá no primeiro acesso ao *site* ufal.br, que atribui um valor de ID exclusivo e o armazena no dispositivo. Há casos em que outros valores são armazenados no arquivo de *cookie*, além dos três exibidos no exemplo acima. Trata-se de informações de manutenção para o navegador.

Ao verificarmos o arquivo de *cookie* criado pelo *site* amazon.com, por exemplo, encontraremos as seguintes informações:

session-id-time 954242000 amazon.com/ session-id 002-4135256-7625846 amazon.com/ x-main eKQIfwnxuF7qtmX52x6VWAXh@Ih6Uo5H amazon.com/ubid-main 077-9263437-9645324 amazon.com/

Detalhando as informações contidas no *cookie* gerado pelo *site*, ao que tudo indica, a *Amazon* armazena um ID de usuário principal, um ID para cada sessão e a hora em que a sessão foi iniciada no dispositivo, e um valor x-main – que pode ser qualquer coisa. A maioria dos *sites* armazena apenas uma informação – um ID de usuário. Mas um *site* pode armazenar muitos pares nome-valor se quiser.

Segundo Brain (2022, p. 02), os dados registrados pelo arquivo de *cookie* são simplesmente pares nome-valor armazenados em seu disco rígido por um *site*. Isso é tudo que os dados de *cookies* são. O *site* armazena os dados e depois os recebe de volta. Um *site* da *web* só pode receber os dados armazenados em sua máquina. Ele não pode olhar para nenhum outro *cookie*, nem para qualquer outra coisa em sua máquina.

Os *cookies* evoluíram para permitir que um *site* armazene informações de estado de um dispositivo. Ou seja, o *site* se lembrará do estado em que nosso navegador está, devido ao ID atribuído junto ao arquivo de *cookie*, já que o ID é uma simples informação de estado.

A despeito do que já fora mencionado acerca do conceito e função dos *cookies*, especialmente, o fato de não serem capazes de coletar nenhuma informação pessoal sobre o usuário e sua máquina, como defendido por autores como Brain (2022), é de suma relevância esclarecer duas questões que têm demandado um olhar mais cauteloso de especialistas que estudam a relação entre o uso de *cookies* e privacidade.

A primeira questão gira em torno da venda de informações. Embora não se trate de uma prática necessariamente recente, haja vista tal possibilidade remeter a uma compra por catálogo tradicional de pedidos pelos correios, ao ser transportada para o ambiente virtual, ao comprarmos algo e inserirmos nome e endereço, os *sites* passaram a deter muito mais poder de informação sobre nós do que as empresas tradicionais de venda por correspondência.

Se por um lado as empresas de catálogos detinham nome, endereço e número de telefone do nosso pedido, e pudessem vender essas informações para terceiros interessados em nos ofertar seus produtos, por meio de um *site* é possível rastrear não apenas nossas compras, mas também as páginas que acessamos, os anúncios nos quais clicamos, as buscas que realizamos etc. E todas essas informações podem ser armazenadas nos arquivos de *cookies*.

Obviamente, as empresas podem fazer uso de políticas mais restritivas, que impeçam a venda ou compartilhamento de informações dos clientes e usuários, em observância,

sobremaneira, ao art. 6º, inciso I [5]; art. 7º, inciso I [6]; art. 15, incisos I, II, III [7] e art. 21 [8] da LGPD.

Trataremos sobre as políticas adotadas na obtenção do consentimento de uso dos *cookies* detalhadamente mais adiante. Afinal, trata-se de tópico central do desenvolvimento deste projeto de pesquisa.

O segundo ponto recai sobre uma prática que se tornou usual no ambiente virtual, e que tem relação mais estreita com o modo como as plataformas virtuais têm se mostrado dispostas a atuar no ambiente virtual da *internet*. Estamos falando da técnica de marketing veiculada por meio de *cookies* visíveis.

O *case* proeminente, citado pela literatura, é o da empresa *Doubleclick Inc.*[9] que ganhou notoriedade no uso desta ferramenta, e muitas empresas passaram a recorrer aos seus serviços para transmitir anúncios de *banner* [10] em seus *sites*. A grande inovação consistia na inserção de pequenos arquivos GIF [11], medindo aproximadamente (1x1 *pixel*) nos *sites*, permitindo o carregamento de *cookies* no equipamento do usuário.

---

[5] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

[6] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;

[7] Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público;

[8] Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

[9] Digamos que na última vez que você esteve online você clicou em páginas sobre viagens, ciprestes e vinhos italianos. Essas páginas, que ficam em sites Double-Click, são rapidamente baixadas para o seu PC. O software da *Doubleclick* observa que esses pacotes de dados foram para seu endereço na *internet*. Assim, a *Doubleclick* começa a criar um perfil seu e de seus interesses. Desde o início de março, diz o CEO Kevin O'Connor, "identificamos quatro milhões de indivíduos e estamos adicionando algo em torno de 100.000 todos os dias". O'Connor também usa os dados para criar listas de categorias de usuários – jardinagem, viagens, esportes e assim por diante – que os anunciantes "compram". Na próxima vez que você fizer logon em um site da Double-Click, seu software anotará seu endereço de e-mail, verificará seu perfil de usuário e carregará um anúncio personalizado para você - em milissegundos após o seu logon.

[10] O primeiro *banner* foi parte da campanha maior da AT&T, "You Will", que incluiu uma série de comerciais de televisão apresentando cenas previstas de um futuro habilitado para *internet* – em muitos casos com bastante precisão.

[11] GIF (Graphics Interchange Format ou formato de intercâmbio de gráficos) é um formato de imagem muito usado na *internet*, e que foi lançado em 1987 pela *Compuserve,* para disponibilizar um formato de imagem com cores em substituição do formato RLE, que era apenas preto e branco.

Por fim, chamamos a atenção para a constatação de Ayenson et al (2011) acerca de técnicas específicas para burlar o controle dos usuários sobre os *cookies*, ao qual chamaram de técnica de reaparecimento, ou *respawing*, de *cookies* deletados.

Por meio dessa técnica, as informações gravadas sobre as páginas visitadas pelo navegador (*cache*) são espelhadas por um identificador, chamado de ETag. Dessa forma, mesmo que o usuário opte por bloquear ou deletar os *cookies* HTTP, *flash* ou HTML5, eles ressurgirão para rastrear a navegação do usuário.

O resultado prático, é que certos *cookies* utilizam de um recurso inerente ao funcionamento do navegador para perdurarem, mesmo quando apagados. Para os autores, a única maneira de se livrar desse artifício, seria limpar o *cache* de navegação a cada *site* visitado pois, nem mesmo o modo de navegação anônimo seria capaz de blindar os dados contra o rastreamento.

Em outro estudo, os autores constataram outro modelo de reaparecimento de *cookies* HTTP deletados. No caso, mesmo se deletados pelos usuários, os valores dos *cookies* HTTP poderiam reaparecer como *cookies flash*, inclusive em outros *sites*. Dessa maneira, um *cookie* HTTP deletado de um "*Site* A", por exemplo, poderia reaparecer com valores idênticos como *cookie flash* no "*Site* B".

Tal estratégia tecnológica se mostra capaz de minar as escolhas dos usuários sobre os *cookies* em seus computadores, pois um *cookie* contendo dados pessoais, ainda que deletado, pode ser preservado entre terceiros que visem construir uma base minuciosa de perfis.

Os resultados dos estudos supracitados demonstram que as tecnologias verificadas nos *cookies* possuem capacidade de disseminação e de operação que vão além do domínio e habilidades de usuários comuns da *internet*. Ainda que o usuário opte por controlar os *cookies* de seu navegador, é possível e até mesmo provável, que ele não consiga lidar com algumas estratégias de armazenamento e de coleta de dados pessoais na rede e esteja fadado ao monitoramento perene, no plano virtual, ainda que contra a sua vontade.

Embora a jornada interativa-virtual da humanidade tenha iniciado com cliques, passando por toques, comandos de voz, até alcançar os gestos, acenos e piscadas – implicando na transformação com que as interações são pensadas –, a essência da usabilidade e da experiência não mudou. Boas, ou más, experiências de uso nos acompanham por meio de

objetos físicos, analógicos, digitais, desde que nascemos, e esse há de ser o caminho provável de evolução do *UX Design,* seja qual for a nova tecnologia.

Até aqui, buscamos nortear como o vasto campo de estudo da área de *UX Design* se desenvolveu desde seu mais remoto formato, caracterizado pelos interações da era analógica, até atingir os modernos e mais complexos contornos da esfera digital e suas multiplataformas. Adiante, de forma mais analítica, abordaremos como esta área do *design* de *interface* homem-máquina é utilizada no desenvolvimento de *banners* e *pop-ups*, para influenciar os titulares dos dados por meio das opções de consentimento na utilização dos *cookies* de navegador, consequentemente, nas finalidades específicas do uso de dados.

6.2 Técnicas de obtenção do consentimento de uso dos *cookies* de navegador

Outrora, destacamos as diretrizes impelidas ao controlador na LGPD, que deve, por força da Lei, garantir manifestação livre, informada e inequívoca ao titular, quando este concorda com o tratamento dos seus dados para uma finalidade específica. E, embora essas balizas legais indiquem o modo pelo qual se deva obter o consentimento, a Lei não logra critérios objetivos de como o controlador deve fazê-lo, dando margem, na sua liberdade de escolha, a técnicas de obtenção que nem sempre se alinham adequadamente às normas de tratamento amparadas por ela.

Como a legislação foi silente quanto a critérios mais específicos nesta senda, tornou-se comum a utilização de *banners* e *pop-ups* que falseiam a opção da livre manifestação, em descumprimento ao que prescreve o texto legal para o aceite das finalidades específicas ou, até mesmo, impossibilitam, completamente, o acesso à página ou aplicativo, se não houver qualquer manifestação positiva por parte do usuário.

Uma vez que tais práticas podem viciar o exercício do consentimento, passaremos à análise das técnicas mais empregadas pelo mercado, ponderando sobre quais consideramos as mais adequadas ao tratamento dos dados do titular, de acordo com as diretivas atribuídas pela LGPD.

No ambiente de *websites* – frisemos aqui que estamos a falar da navegação que comumente realizamos por meio de um PC ou *notebook* –, a técnica mais utilizada na obtenção do consentimento costuma ser mediante o uso de *banners* na página inicial de determinado *site*,

com opções sobre o uso de *cookies* para os mais variados fins, como: permitir análise de comportamento, publicidade direcionada, aferir desempenho do *site* etc.

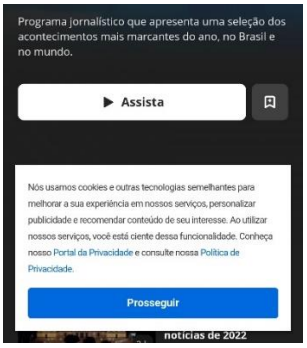
As *Consent Management Platforms* (CMP) – Plataformas de Gerenciamento de Consentimento, em tradução livre –, se incumbem da tarefa. Seu papel é apresentar o *banner* ao usuário do *site*, assim como registrar a opção que ele deve fazer sobre o tratamento dos dados.

Figura 4 – *Banner* com *checkboxes* informativos das finalidades do consentimento

Fonte: jota.info (2023)

Por outro lado, quando a navegação se dá por meio de um aparelho móvel, seja *tablet* ou *smartphone*, o recurso utilizado passa a ser um *pop-up* quando o aplicativo é acessado. A técnica costuma incluir uma descrição sobre o uso dos dados e hiperlink para a página que contém a Política de Privacidade adotada pela empresa, seguida pelo botão de aceite ou rejeite, a depender da escolha feita pelo tratador, junto ao *UX Design* disponibilizado pela CMP ao usuário.

Figura 5 – *Pop-up* de aplicativo *mobile*, sem opção de *checkboxes*, contendo um único botão de aceite, bloqueando o acesso ao conteúdo do *site*.



Fonte: globoplay.globo.com (2023)

Note-se que no exemplo da Fig. 5, o *UX Design* adotado pela CMP em sua política de obtenção do consentimento, sequer levou em conta a possibilidade de que o titular pudesse rejeitar as opções disponibilizadas para as finalidades de uso dos seus dados, haja vista a inexistência do botão de rejeição ou gerenciamento de opções. O que há é um botão único de

prosseguimento, consequentemente, viciando as escolhas do usuário quanto aos dados que gostaria de consentir e para quais finalidades específicas.

Além disso, o *pop-up*, no caso em tela, funciona como uma barreira ao conteúdo do portal, vez que não permite seu total acesso, acaso não se clique no botão prosseguir. É de se concluir, portanto, que a técnica adotada visa a obtenção do consentimento de forma tácita, ao desvirtuar a aparência de livre escolha do titular, que se vê "forçado" a aceitar as condições, caso opte por clicar na única opção disponibilizada.

Neste ponto, chamamos a atenção para uma divagação deveras importante: a possibilidade de o tratador influenciar a experiência do usuário, no intuito de obter a maior adesão possível aos termos da sua política de consentimento. Especialistas até já criaram um termo para referir esta prática:

> O termo "*dark patterns"* reflete justamente o *design* adotado pela plataforma numa tentativa de influenciar a tomada de decisão por parte do usuário de forma que nem sempre reflete a sua real intenção. Isso envolve estratégias como criar obstáculos, limitar as opções apenas a certas escolhas, induzir a interpretações equivocadas ou ainda esconder ou adiar a prestação de informações relevantes (FERNANDES; SUNDFELD, 2021).

O termo *dark pattern,* cunhado em 2010, classifica o *design* que induz os usuários a tomarem decisões que na verdade eles não gostariam de ter tomado. Bösch et al (2016) figuram entre os primeiros autores a sistematizar os *dark patterns* mais comumente adotados para a invasão de privacidade.

Tomemos como exemplo o típico caso dos usuários que não leem os avisos de privacidade completamente e frequentemente, intuitivamente, aceitam as condições apresentadas. Tal comportamento pode ser explorado por termos indesejados contidos nos avisos de privacidade.

Mathur et al (*apud* Böhme e Machuletz, 2020, p. 05) estruturaram as características mais comumente empregadas em *dark patterns* por meio de cinco dimensões: (i) assimétrica (ênfase única ou obstáculos para escolhas específicas; (ii) disfarçada (opções de *design* de *interface* escondidas); (iii) enganosa (induz à falsas percepções); (iv) informação oculta (obscurece ou atrasa a comunicação de informação relevante); e (v) restritiva (limitação das escolhas).

Os autores nomeiam, especificamente, os diálogos de consentimento de *cookies* que se utilizam de um botão de aceite em destaque, como um exemplo da dimensão assimétrica.

Buscando demonstrar como as plataformas virtuais têm se utilizado da *UX Design* para influenciar os usuários a aceitarem as finalidades de uso dos dados, de acordo com as políticas pensadas pelo controlador junto à CMP, os autores destacam que alguns estudos e pesquisas realizados chegaram a resultados que poderiam considerar previsíveis.

Em um estudo conduzido entre estudantes universitários no ano de 2020, cujo objetivo era analisar de que forma o *design* do *banner*, em particular, a presença de um botão em destaque, por padrão, e pelo número de opções disponíveis, concluiu que houve um maior índice de aceite entre aqueles participantes que visualizaram um botão destacado para tal fim, se comparados com a *UX Design* de participantes que não trazia essa opção em destaque.

Importante ressaltar que os participantes que clicaram no botão de aceite em destaque demonstraram arrependimento da decisão, em decorrência da falta de informações disponíveis.

Como resultado, os participantes que visualizaram um único botão de aceite destacado demonstraram taxas superiores de conversão em aceite, quando comparados àqueles cuja *UX* não trazia opção em destaque. Entretanto, os participantes que clicaram no botão de aceite destacado se mostraram arrependidos da decisão por falta de informações disponíveis. O estudo também demonstrou que não há implicação direta entre o maior número de opções de escolha nos *banners* e a dificuldade de manuseio.

Noutro estudo, constatou-se que o simples fato de se incluir apenas o botão de aceite resultou em um aumento de 22 a 23% na conversão de usuários (vide o exemplo da Fig. 5), se comparado a um cenário em que também havia um botão para negar o tratamento de dados disponível. No mesmo toar, a pesquisa também apontou que a inclusão de controles mais granulares na primeira página da *UX Design* levou ao decréscimo claramente perceptível de 8 a 20% no volume de aceites.

Come se depreende, as técnicas de consentimento mediante o uso de *banners* e *pop-ups* ao mesmo tempo que se tornaram praxe, também têm se apresentado como verdadeiro desafio em cumprir com o que estabelece a LGPD, haja vista a possibilidade de influenciar a experiência do usuário por meio da *UX Design*, em busca de maior adesão aos termos estipulados pela CMP.

Neste sentido, Sundfeld e Fernandes (2021) orientam que "na prática, *cookie banners* e *pop-ups* são vistos como um desafio pelo controlador do *website* ou *app*, por criar fricção na experiência do usuário. Há [...] um interesse do controlador em customizá-los de forma a influenciar o usuário a aceitar todos os usos de dados e maximizar o aceite".

Por outro lado, convém destacar que nem todas os modelos consistem em condutas desabonadoras aos quesitos elencados pelo art. 5, inciso XII, da LGPD, que buscam garantir ao usuário manifestação livre, informada e inequívoca ao aquiescer com o consentimento do tratamento dos seus dados pessoais. Por essa razão, destacaremos alguns exemplos de modelos de *UX Design* mais acurados, e que a colocam na posição de importante vetor de controle e transparência.

No campo da publicidade direcionada, encontramos a diretriz TCF 2.0, ou *Transparence and Consent Framework*, que busca demonstrar maturidade e passar confiança aos seus parceiros comerciais. Neste framework o *website* ou *app* é compelido a informar sobre todos os terceiros que podem ter acesso aos dados pessoais dos usuários do *website* ou *app*, e por quais motivos, antes mesmo da coleta dos dados. Ainda, ao titular deve ser oportunizado a possibilidade de negar ou aceitar o compartilhamento de dados com cada um dos terceiros de forma individualizada, inviabilizando o modelo "tudo ou nada" da já mencionada tática de uso de um botão único de aceite.

As diretrizes TCF 2.0 foram, até recentemente, provavelmente o framework com as regras mais bem detalhadas sobre *UX* para obtenção do consentimento. Contudo, em 25 de junho de 2021 foi publicada a ISO 29184, que trata dos avisos de privacidade online e obtenção do consentimento, trazendo recomendações semelhantes, porém, mais enxutas e atendendo a um público maior que o framework TCF 2.0.

Em que pesem as boas intenções de conferir maior confiabilidade ao processo de consentimento, a partir dos frameworks supracitados, os desafios práticos ainda se impõem. Devemos levar em consideração que opções de escolhas cada vez mais granulares, como as estabelecidas por meio do framework TFC 2.0 podem resultar em um fenômeno chamado "proliferação de escolhas":

> O termo é resultado de linhas de pesquisa da psicologia, que analisam a influência do incremento do número de escolhas alternativas no processo humano de tomada de decisão. A insatisfação é um dos efeitos negativos do fenômeno, estudado principalmente no contexto do *marketing*, às vezes referenciado também pelos termos

> "exagero de escolhas", "tirania de escolhas" ou "sobrecarga de escolhas" (BÖHME; MACHULETZ, 2020, p. 5).

A Fig. 6 nos traz um exemplo que, na contramão da experiência ofertada pelos *cookie banners* e *pop-ups* desenhados para uma política de consentimento via padrão de botão único de aceite em destaque, converge para um alternativa que busca dar maior transparência e controle sobre as informações dos dados do titular, que serão compartilhadas com terceiros, em nível de granularidade incontestavelmente superior.

E, mais uma vez, novos desafios se apresentam, em comparação com a pouca quantidade de informações disponibilizadas aos usuários, agora, em virtude do seu excesso.

Figura 6 – *Banner* com *checkboxes* informativos das finalidades do consentimento para terceiros, em maior nível de granularidade.

Fonte: elpais.com (2023)

Assim, Filho e Oliveira (2021) apontam que "ao apresentar uma chuva de botões, *checkboxes*, e termos que necessitam de aceite, tais solicitações podem ser responsáveis por fazer com que a manifestação seja falaciosa e fruto de um total desinteresse com relação aos termos que o titular está consentindo". Como resultado, surgiram novos questionamentos ligados à sobrecarga informacional durante a obtenção do consentimento, que especialistas convencionaram chamar "fadiga de cliques" ou "fadiga do consentimento".

7 CONCLUSÃO

A sociedade da informação é marcada por novos paradigmas na organização social, política e econômica, mediante o uso intensivo da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações. Neste novo modelo, a própria informação foi alçada à principal insumo do novo sistema capitalista a despontar. Nesta nova era da informação, o extraordinário avanço no setor de comunicação, especialmente após o advento da *internet*, o controle das infraestruturas, por meio de recursos computacionais, recrudesceu o interesse dos governos e da iniciativa privada sobre a privacidade dos indivíduos.

A *internet*, a despeito dos seus inúmeros benefícios, também se revelou terreno fértil para invasão à privacidade: o intercâmbio de informações pessoais entre os diversos prestadores de serviços da sociedade da informação sem a prévia autorização dos titulares dos dados; possibilidade de monitoramento eletrônico dos internautas; disseminação da cultura de auto exposição virtual; coleta de informações sobre a navegação dos usuários por meio dos *cookies* e a disseminação de programas desenvolvidos para a execução de ações maliciosas.

Neste cenário, na esteira da *General Data Protection Regulation* (GDPR), a promulgação da Lei nº 13.079/2018 – Lei Geral de Proteção de Dados (LGPD) –, trouxe novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores público e privado. A Lei veio complementar o arcabouço regulatório setorial que o país já dispunha em mais de 40 normas que, direta ou indiretamente, tratavam da proteção à privacidade e aos dados pessoais, possibilitando maior segurança jurídica neste âmbito.

A LGPD buscou dar maior controle ao titular sobre o uso que é feito dos seus dados pessoais e, a fim de assegurar a vigência do princípio da autodeterminação informativa, empoderou o titular, de forma que pudesse decidir como os seus dados seriam tratados a partir de então. A Lei estabeleceu 10 bases legais para a realização do tratamento de dados pessoais, dentre os quais destaca-se o consentimento, que deve atender a três requisitos legais pelos quais o titular consente com o tratamento de seus dados pessoais: manifestação livre, informada e inequívoca para uma finalidade determinada (art. 5º, XII).

Com exceção daquilo que possa ser considerado como segredo comercial e industrial, todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, sem o que não restará observado o requisito do consentimento informado. Na hipótese em que o

consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso, abusivo ou não tenham sido apresentados previamente com transparência, de forma clara e inequívoca (§ 1º do art. 9º).

Embora não exista hierarquia entre as 10 bases legais previstas na LGPD, criou-se certo fetiche ou uma certa cultura em torno da busca de obtenção do consentimento, como melhor caminho para possibilitar o uso dos dados dos titulares. A crença é a de que se o titular manifestar o seu aceite, isso necessariamente significa que ele aceita e concorda com as atividades de tratamento. Porém, não é o que se constata com base na observação empírica da experiência dos usuários.

A busca incessante pelo consentimento dos usuários tracionou o mercado das *Consent Manegement Plataform* (CMP), cujo principal objetivo é o de suportar as empresas na adequação de seus *sites*, a partir da utilização dos famosos *cookie banners*. As CMPs costumam recorrer às ferramentas de *UX Design* para manipular a forma pela qual os titulares consentem com os termos de aceite disponibilizados mediante o uso de *banners* ou *pop-ups*, que permitem a utilização dos *cookies* dos dispositivos dos usuários.

A tática varia ora entre o "tudo ou nada", onde um único botão de aceite é disponibilizado junto aos termos de consentimento de uso dos *cookies*, ora entre uma chuva de botões, *checkboxes* e termos que necessitam de aceite em níveis de granularidade excessiva, tornando a manifestação do titular, ambígua, falaciosa, desinteressada ou completamente desinformada com relação ao que está consentindo. Tais práticas são conhecidas pelo termo *dark partnners*, responsáveis pelo surgimento de fenômenos como a "fadiga de cliques".

Algumas iniciativas comprovam que há melhores alternativas e que a *UX Design*, quando bem utilizada a favor da privacidade, pode facilitar a entrega de um comando técnico a partir do contexto, forma e conteúdo informado ao usuário. Sob esta perspectiva, há margem para aperfeiçoar a transparência de produtos e serviços, customizar experiências, facilitar a compreensão do usuário e, de fato, dar controle sobre como seus dados são tratados, para além da discussão sobre o simples aceite a um *checkbox*.

É certo que não existe uma panaceia quanto aos tipos de proteção que devem ser incorporados a fim de promover a confiança no ambiente digital e refletir claramente as expectativas sociais e legais, estimulando também a inovação. Contudo, ao que a literatura indica, o consentimento para o tratamento de dados não é a única e nem a melhor forma de garantir o pleno exercício dos direitos à privacidade e à proteção de dados.

A sobrecarga informacional e a ignorância racional, marcas de uma economia baseada em dados, dificultam a compreensão do titular dos dados, muitas vezes tornando o seu consentimento vazio ou implicando em total falta de engajamento. Ao se pensar em modelos regulatórios de proteção de dados, é imperativo entender como as normas sociais e as limitações dos indivíduos têm importante papel na concretização de direitos.

Os esforços envidados devem caminhar rumo à eliminação de intervenções desnecessárias ou desproporcionais, fortalecendo um ecossistema no qual a tecnologia exerça papel decisivo na elaboração de soluções que beneficiem os usuários, em consonância com sua autodeterminação informativa e o arcabouço legal vigente.

REFERÊNCIAS

AGOSTINI, Leonardo Cesar de. **A intimidade e a vida privada como expressões da liberdade humana.** Porto Alegre: Núria Fabris Ed., 2011.

ALMEIDA. Juliana Evangelista de. LUGATI. Lys Nunes. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**. Viçosa. v. 12, n. 02, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597/5880. Acesso em: 26 fev. 2023.

ALVARENGA, Darlan. Novas regras do cadastro positivo entram em vigor, mas de forma incompleta. **G1.** 09 set. 2019. Disponível em: https://g1.globo.com/economia/noticia/2019/07/09/novas-regras-do-cadastro-positivo-entram-em-vigor-mas-de-forma-incompleta.ghtml. Acesso em: 31 jan. 2022.

ARAÚJO, Thiago Volpi de et al. **LGPD muito além da lei: uma análise do direito em conjunto com a segurança da informação.** [s.l.], Gvtech Soluções em Tecnologia da Informação LTDA, 2021. *E-book.*

ARUNESH. Mathur et al. **Dark patterns at scale: Findings from a crawl of 11K shopping *websites*. Proceedings of the ACM on Human-Computer Interaction.** (2019) 3, 81. 20 sep. 2019. Disponível em: https://arxiv.org/abs/1907.07032. Acesso em: 07 jul. 2022.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES (BRASSCOM). **Contribuições à Comissão Especial da Câmara dos Deputados sobre a Lei de Tratamento e Proteção de Dados Pessoais.** Jun. 2017. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/outros-documentos/Brasscom.pdf. Acesso em: 29 jan. 2022.

AYENSON, Mika D. et al. ***Flash Cookies* and Privacy II: Now with HTML5 and ETag Respawning.** SSRN. 29 jul. 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390. Acesso em: 18 jan. 2023.

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** São Paulo: GPoPAI/USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque_Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 26 fev. 2023.

BIONI, Bruno Ricardo et al. **Proteção de dados: contexto, narrativas e elementos fundantes.** Bruno Ricardo Bioni (Org.). São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BÖHME, Rainer; MACHULETZ, Dominique. **Multiple porposes, multiple problems: a *user* study of consente dialogs after GDPR.** In: Proceedings on Privacy Enhancing Technologies. Germany, 2020 (481-498). Disponível em: https://arxiv.org/pdf/1908.10048.pdf. Acesso em: 02 mai. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 01/2021.** Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Brasília, 28 de outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em: 29 mai. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 31 jan. 2022.

BRASIL. **Decreto nº 592, de 06 de julho de 1992.** Promulga o Pacto Internacional sobre Direitos Civis e Políticos. Diário Oficial da União, Brasília, DF, 07 de julho de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 28 out. 2022.

BRASIL. **Decreto nº 678, de 06 de novembro de 1992.** Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Diário Oficial da União, Brasília, DF, 09 de novembro de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 28 out. 2022.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na *internet* e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Diário Oficial da União, Brasília, DF, 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 02 fev. 2022.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940.** Código Penal**.** Diário Oficial da União, Brasília, DF, 31 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 fev. 2022.

BRASIL. **Enunciado CD/ANPD nº 01, de 22 de maio de 2023.** Diário Oficial da União, Brasília, DF, 24 de maio de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em: 24 mai. 2023.

BRASIL. **Governo Federal realiza leilão do 1º 5G da América Latina.** 04 nov. 2021. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/11/governo-federal-realiza-leilao-do-1o-5g-da-america-latina. Acesso em: 13 fev. 2022.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, DF, 11 jan. 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei Complementar nº 166, de 08 de abril de 2019.** Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 09 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Diário Oficial da União, Brasília, DF, 09 de abril de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm. Acesso em: 12 fev. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 12.414, de 09 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito**.** Diário Oficial da União, Brasília, DF, 10 de junho de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 03 de dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências**.** Diário Oficial da União, Brasília, DF, 12 de setembro de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 31 jan. 2022.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, Brasília, DF, 15 de maio de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial da União, Brasília, DF, 25 de julho de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 02 fev. 2022.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso à informações e disciplina o rito processual do *habeas data.* Diário Oficial da União, Brasília, DF, 13 de novembro de 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9507.htm. Acesso em: 31 jan. 2022.

BRASIL. **Lei nº 9.883, de 07 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências. Diário Oficial da União, Brasília, DF, 08 de dezembro de 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm. Acesso em: 02 fev. 2022.

BRASIL. **Medida Provisória nº 869, de 2018.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 30 jan. 2022.

BRASIL. **MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais.** Disponível em: https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais. Acesso em: 30 jan. 2022.

BRASIL. **Projeto de Lei da Câmara nº 53 de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www25.senado.leg.br/*web*/atividade/materias/-/materia/133486. Acesso em: 29 jan. 2022.

BRASIL. **Projeto de Lei do Senado nº 330, de 2013.** Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em: https://www25.senado.leg.br/*web*/atividade/materias/-/materia/113947. Acesso em: 30 jan. 2022.

BRASIL. **Projeto de Lei nº 4.060 de 2012.** Dispõe sobre o tratamento de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www.camara.leg.br/proposicoes*web*/fichadetramitacao?idProposicao=548066. Acesso em 27 jan. 2022.

BRASIL. **Projeto de Lei nº 5.276 de 2016.** Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: https://www.camara.leg.br/propostas-legislativas/2084378. Acesso em 30 jan. 2022.

BRASIL. Supremo Tribunal Federal. **ADI 6387 MC-Ref, Relator(a): Rosa *Web*er, Tribunal Pleno, julgado em 07/05/2020, processo eletrônico DJe-270 divulg 11-11-2020 public 12-11-2020.** Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. **HC 91867, Relator(a): Gilmar Mendes, Segunda Turma, julgado em 24/04/2012, acórdão eletrônico DJe-185 divulg 19-09-2012 public 20-09-2012.** Disponível em:

https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. **RE 673707, Relator(a): Luiz Fux, Tribunal Pleno, julgado em 17/06/2015, acórdão eletrônico repercussão geral - mérito DJe-195 divulg 29-09-2015 public 30-09-2015.** Disponível em; https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=9487405. Acesso em; 05 mar. 2023.

BRASIL. Superior Tribunal de Justiça. **REsp n. 879.360/SP, relator Ministro Luiz Fux, Primeira Turma, julgado em 17/6/2008, DJe de 11/9/2008.** Disponível em: https://scon.stj.jus.br/SCON/SearchBRS. Acesso em: 30 mai. 2023.

BRITO, Edvaldo. O que é GIF? **TechTudo.** 30 abr. 2012. Disponível em: https://www.techtudo.com.br/noticias/2012/04/o-que-e-gif.ghtml. Acesso em: 16 abr. 2023.

BURCH, Sally. **Sociedade da informação/Sociedade do conhecimento.** In: AMBROSI, Alain et al (Orgs.). Desafios de Palavras: Enfoques Multiculturais sobre as Sociedades da Informação. Paris: C & F Éditions, 2005.

C. Bösch, B. Erb, F. Kargl, H. Kopp, S. Pfattheicher. **Tales from the dark side: Privacy dark strategies and privacy dark patterns.** (De Gruyter Open, 2016), vol. 2016 237–254. 13 jul. 2016. Disponível em: https://www.sciendo.com/article/10.1515/popets-2016-0038. Acesso em: 07 jul. 2022.

CÂMARA, Dennys Eduardo Gonsales et al. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos.** São Paulo: Baptista Luz Advogados, [s.d.].

CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro.** 2017. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina. Florianópolis. 2017. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?lang=pt&format=pdf. Acesso em: 11 mar. 2021.

CARDOSO, Oscar Valente. **Proteção de dados e Emenda Constitucional 115/2022.** Disponível em: https://www.jusbrasil.com.br/artigos/protecao-de-dados-e-emenda-constitucional-115-2022/1376719634. Acesso em: 26 mai. 2023.

CASTELLANO, Ana Carolina Heringer; VENTRE, Giovanna. O dilema do consentimento e a sobrecarga informacional. **Jota.** 28 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dilema-consentimento-sobrecarga-informacional-lgpd-28072021. Acesso em: 06 nov. 2021.

CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.** Roma. 04 de novembro de 1950. Disponível em: http://gddc.ministeriopublico.pt/*sites*/default/files/convention_por.pdf. Acesso em: 26 out. 2021.

COOLEY, Thomas M. **A treatise on the law of torts or the wrongs which arise independence of contracts.** Chicago: Callaghan and Company, 1879.

CUOFANO, Gennaro. O que aconteceu com o Netscape? **FourWeekMBA.** 30 set. 2022. Disponível em: https://fourweekmba.com/pt/o-que-aconteceu-com-netscape/#:~:text=O%20navegador%20*web*%20Netscape%20Navigator%20. Acesso em: 28 jan. 2023.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais.** Rio de Janeiro: Renovar, 2006.

Doubleclick (Google): what is it and what does it do? **The Guardian.** [s.d.]. Disponível em: https://www.theguardian.com/technology/2012/apr/23/*doubleclick*-tracking-trackers-*cookies*-*web*-monitoring. Acesso em: 16 abr. 2023.

FELT, A. P. et al. How to ask for permission. **Hotsec.** Aug 07, 2012. Disponível em: https://www.usenix.org/conference/hotsec12/workshop-program/presentation/felt. Acesso em: 08 mai, 2002.

FERNANDES, Maria Luiza; SANDFELD, Philippe. LGPD e *UX*: um equilíbrio para o consentimento. **Jota.** 16 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-*ux*-um-equilibrio-para-o-consentimento-16072021. Acesso em: 06 nov. 2021.

FILHO, Paulo César Tavares; OLIVEIRA, Caio César de. A LGPD e o início do fim da cultura do consentimento: European Data Protection Board (EDPB) alerta para a "fadiga de cliques". **Jota.** 28 jun. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-e-o-inicio-do-fim-da-cultura-do-consentimento-28062021. Acesso em 06 nov. 2021.

FIUZA, Cesar. **Por uma redefinição da contratualidade.** 31 mar. 2017 In: Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direitocivil/por-uma-redefinicao-da-contratualidade/. Acesso: em 26 fev. 2023.

FLAHERTY, David H. **On the utility of constitutional rights to privacy and data protection.** Case Western Reserve Law Review, vol. 41, 1991. Disponível em: https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2048&context=caselrev. Acesso em: 22 out. 2021.

GIDDA, Mirren. **Edward Snowden and the NSA files – Timeline: What has h*app*ened to NSA whistleblower who leaked files to Guardian since he decided to reveal his identity to the *world* and began his asylum battle.** The Guardian. 21 aug. 2013. Disponível em: https://www.theguardian.com/*world*/2013/jun/23/edward-snowden-nsa-files-timeline. Acesso em 27 jan. 2022.

GOMES, Helton Simões. **Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda.** G1. 25 maio 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml. Acesso em: 29 jan. 2022.

HARDING, B.; CRISER, Mark J.; UFFERMAN, Michael R. **Right to Be Let Alone - Has the Adoption of Article I, Section 23 in the Florida Constitution, Which Explicitly Provides for a State Right of Privacy, Resulted in Greater Privacy Protection for Florida**

Citizens. 14 Notre Dame J.L. Ethics & Pub. Pol'y 945, 2000. Disponível em: https://scholarship.law.nd.edu/ndjlepp/vol14/iss2/8/. Acesso em: 29 jan. 2022.

HOOFNAGLE, Chris Jay et al. **Behavioral Advertising: The Offer You Can't Refuse.** Harvard Law & Policy Review, n 06, vol. 273, 2012. Disponível em: https://harvardlpr.com/wp-content/uploads/*sites*/20/2013/06/Behavioral-Advertising-Hoofnagle-et-al.pdf. Acesso em: 09 mar. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). ***World*** **Summit on the Information Society (WSIS).** Geneva 2003-Tunes 2005. Disponível em: https://www.itu.int/net/wsis/basic/about.html. Acesso em: 20 fev. 2022.

JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada: conflito entre direitos da personalidade.** São Paulo: RT, 2000.

JÚNIOR, Eliseu Vieira Machado. **Sinergia dos Stakeholders: Um framework de Gestão e Responsabilidade Social – Estudo de Caso em Instituição de Ensino Superior Brasileira.** 2009. 312 p. Tese (Doutorado em Engenharia da Produção. Faculdade de Engenharia, Arquitetura e Urbanismo, Programa de Pós-Graduação em Engenharia de Produção. Santa Barbara d'Oeste: Universidade Metodista de Piracicaba, 2009. p. 86-105.

JÚNIOR, Paulo José da Costa. **O direito de estar só: tutela penal da intimidade.** 3 ed. São Paulo: Siciliano Jurídico, 2004.

LAFRANCE, Adrienne. **The first-ever *banner* Ad on the *web*.** April 21, 2017. Disponível em: https://www.theatlantic.com/technology/archive/2017/04/the-first-ever-*banner*-ad-on-the-*web*/523728/. Acesso em: 26 abr. 2022.

LESSIG, Lawrence. **Code.** Nova York: Basic Books, 2006.

LIMA, Humberto A. V. **A tutela jurídica dos dados pessoais no Brasil: estudo sistemático da Lei Geral de Proteção de Dados.** 2 ed. Minas Gerais: Edição independente, 2021. *E-book*.

LOPES, Alexandra Krastins et al. **Guia orientativo: coockies e proteção de dados pessoais.** Brasília: ANPD, 2022.

LOPES, Ana Karla. **Dissecando a LGPD: entenda a Lei Geral de Proteção de Dados em uma linguagem simples e como ela interfere, na prática, em seus negócios online.** [s.l.], Edição da autora, 2021. *E-book*.

MACHULETS, Dominique; BÖHME, Rainer. **Multiple purposes, multiple problems.** Disponível em: https://arxiv.org/pdf/1908.10048.pdf. Acesso em: 02 mai. 2022.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na *Internet*: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016.** Trabalho de Conclusão de Curso (graduação) – Universidade de Brasília, Faculdade de Direito, 2017. Data da publicação: 8 jan. 2018. Disponível em: https://bdm.unb.br/bitstream/10483/18883/1/2017_LuizaFernandesMalheiro.pdf. Acesso em: 01 mar. 2023.

MARQUES, Orizzo; COLTRO, Gabrilli. **Sanções administrativas no âmbito da Lei Geral de Proteção de Dados (Lei nº 13.709/18).** 10 ago. 2021. Disponível em: https://orizzomarques.com.br/sancoes-administrativas-no-ambito-da-lei-geral-de-protecao-de-dados-lei-no-13-709-18/. Acesso em: 24 mai. 2023.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados no Brasil: análise contextual detalhada.** Jota. 16 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 13 fev. 2022.

MOREIRA, Matheus Teixeira. **Proteção de dados e Administração Pública: a utilização de dados pessoais pelo setor público em tempos de emergência sanitária.** VirtuaJus, Belo Horizonte, v. 7, n. 13, p. 27-38, 2. Sem., 2022. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/29008/20265. Acesso em: 05 mar. 2023.

NETO, José Luiz de Souza. **A proteção de dados pessoais na era da informação.** [s.l.]: Edição do autor, 2020. *E-book*.

NISSENBAUM, Helen. **A contextual *app*roach to privacy online.** Daedalus, v. 140, n. 4, p. 32-48, 2011. Disponível em: https://www.amacad.org/publication/contextual-approach-privacy-online. Acesso em: 07 jul. 2022.

NORDIC CONFERENCE OF JURISTS. **The Right of Privacy.** Estocolmo. 22-23 de maio de 1967. Disponível em: https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-1967-eng.pdf. Acesso em: 29 out. 2021.

NOUWENS, Midas et al. **Dark patterns after the GDPR: Scraping consent *pop-ups* and demonstrating their influence.** Disponível em: https://arxiv.org/pdf/2001.02479.pdf?fbclid=IwAR3T83kn_TixGxrL6SY7HYvoTR1lirBnp2UM1lSoKREWbFLQBRGA4z3P80g. Acesso em: 06 jul. 2022.

NOVAES, Manuela. **Fux explana origem da autodeterminação informativa, entenda origem do fundamento.** 27 nov. 2021. Disponível em: https://lgpdnews.com/2021/11/fux-explana-origem-da-autodeterminacao-informativa-entenda-origem-do-fundamento/. Acesso em: 02 mar. 2023.

OEA. Pacto de San Jose da Costa Rica. **Convenção Americana sobre Direitos Humanos.** 22 de novembro de 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 29 out. 2021.

OLIVEIRA, Elaine Filgueiras. **Curso de implementação: Lei Geral de Proteção de Dados. Lei de nº 13.709 de 2018.** [s.l.], [s.d.]. *E-book*.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. **Privacidade na Rede.** R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/8419. Acesso em: 21 jan. 2023.

OLIVEIRA, Sandro Lima de. **Entendendo privacidade de dados pessoais na LGPD.** [s.l.], Privacidade Guru, [s.d.]. *E-book*.

ONU. **Declaração Universal dos Direitos Humanos.** Resolução n. 217ª (III) da Assembleia Geral das Nações Unidas. 10 dez. 1948. Disponível em: https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=0BwbnJ2EXfmcDMjk2YTg2ZDAtMGZkZi00MGZhLWFmOWYtMTM2MDU2YmNjMTNi&hl=pt_BR. Acesso em: 26 out. 2021.

ONU. **Pacto Internacional de Direitos Civis e Políticos. Resolução n. 2200-A (XXI**). 16 de dezembro de 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 29 out. 2021.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na *internet*.** 2 ed. Curitiba: Juruá Editora, 2004.

PIMENTEL, José Eduardo de Souza. **Direito e ética da inteligência artificial e dos algoritmos de "caixa preta".** [s.l]. Edição do autor, 2021. *E-book*.

POHLMANN, Sérgio Antônio. **LGPD ninja: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas.** Nova Friburgo: Editora Fross, 2019. *E-book*.

RODOTÀ, Stefano. **Tecnologie e Diritti.** Itália: Il Mulino, 1995.

ROHR, Altieres. **Google começa a testar tecnologia 'FLoC' para publicidade no Chrome, mas *sites* e concorrentes desativam rastreamento.** 21 abr. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/*blog*/altieres-rohr/post/2021/04/21/google-comeca-a-testar-tecnologia-floc-para-publicidade-no-chrome-mas-*sites*-e-concorrentes-desativam-rastreamento.ghtml. Acesso em: 07 jul. 2022.

ROIG, Rafael de Asís. **Las paradojas de los derechos fundamentales como límites al poder**. Madrid: Editorial Debate, 1992.

SAFFER, Dan. ***Design*ing for interaction: creating innovative *app*lications and devices.** California: New Riders, 2010.

SANTOS, Ludmila. Governo quer mais proteção para dados na *internet*. **Consultor Jurídico.** 25 jan. 2011. Disponível em: https://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais#:~:text=De%20acordo%20com%20o%20artigo%2041%20do%20anteprojeto%2C,e%20proibi%C3%A7%C3%A3o%20de%20funcionamento%20do%20banco%20de%20dados. Acesso em: 30 jan. 2022.

SANTOS, Fernanda Cristina Soares. **A responsabilidade Civil na Lei Geral de Proteção de Dados.** 19 out. 2021. Disponível em: https://lageportilhojardim.com.br/*blog*/responsabilidade-civil-na-lgpd/. Acesso em: 30 mai. 2023.

SCHVARTZMAN, Felipe. Quatro desafios para a ANPD aplicar multas por descumprimento da LGPD. **Jota.** 03 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-

analise/artigos/quatro-desafios-para-a-anpd-aplicar-multas-por-descumprimento-da-lgpd-03022021#_ftnref7. Acesso em: 24 mai. 2023.

SCHWAB, Klaus. **A quarta revolução industrial.** São Paulo: Edipro, 2016.

SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** BVERFGE 65, 1. p. 239 e 240. Konrad-Adenauer-Stiftung, 2005. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf/view. Acesso em: 07 jul. 2022.

SIEBECKER, Michael R. ***Cookies* and the common law: are *internet* advertisers trespassing on our computers?** Southern California Law Review, vol. 76, n. 4, May, 2003. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=601921. Acesso em: 21 jan. 2023.

Sir Tim Berners-Lee, criador da *web*, recebe o Prêmio Turing Award, o Nobel da Computação. **Consórcio *World Wide Web* (W3C).** April 04, 2017. Disponível em: https://www.w3c.br/Noticias/TimBLTuringAward2017. Acesso em: 05 mar. 2022.

TEIXEIRA, Fabrício. **Introdução e boas práticas em *UX Design***. São Paulo: Casa do Código, 2014.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2007.

VOZES E DIÁLOGOS. **Dossiê comunicação e cultura.** Itajaí, v. 14, n. 01, jan-jun 2015. Disponível em: https://periodicos.univali.br/index.php/vd/issue/view/345/67. Acesso em: 16 abr. 2023.

WOJTOWICZ, Patryk. **Darknet e Deep *Web*: il Lato Oscuro del *Web* per la Privacy e la Protezione dei Dati.** Tesi di Laurea, Coso di Laurea in Ingegneria Elettronica, Informatica e Telecomunicazioni, Anno Accademico 2013, sessione II, Università di Bologna, Italia. Disponível em: https://amslaurea.unibo.it/8456/1/wojtowicz_patryk_tesi.pdf. Acesso em: 09 mar. 2023.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** Rio de Janeiro: Editora Intrínseca Ltda, 2021.