ISSN 1981-3694
(DOI): 10.46818/ v4i3.242

O ALCANCE DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS: PERSPECTIVAS SOBRE A SOCIEDADE DE VIGILÂNCIA NA ERA DA INFORMAÇÃO

THE SCOPE OF CONSENT IN PERSONAL DATA PROTECTION: PERSPECTIVES ON THE SURVEILLANCE SOCIETY IN THE INFORMATION AGE

Diego Chagas de Souza[1]
João Vitor Sangiacomo Meira Lima[2]

RESUMO: O presente trabalho tem como objetivo examinar o alcance do consentimento do titular de dados como instrumento protetivo nuclear da disciplina voltada à proteção de dados pessoais. Para tanto, analisa-se como o consentimento foi moldado no Regulamento Geral sobre a Proteção de Dados, da União Europeia, no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais e como a efetividade dessa base legal se tornou questionável para garantir a autonomia decisória do titular em meio à corrida armamentista tecnológica de vigilância. Para superar as insuficiências do paradigma do consentimento, três perspectivas apresentam-se como soluções interessantes visando adequar a proteção de dados ao mercado informacional. Conclui-se que a garantia do fundamento da autodeterminação informativa vai muito além do consentimento, como um mecanismo meramente formal. A percepção de que o titular se encontra em uma situação de vulnerabilidade nessa relação é crucial para lidar com os inúmeros desafios da proteção de dados.

PALAVRAS-CHAVE: Proteção de dados pessoais. Consentimento. Autodeterminação informativa.

ABSTRACT: The paper examines the scope of data subject's consent as a core protective instrument of personal data protection. To this end, the research analyzes how consent has been shaped under the General Data Protection Regulation, the Brazilian Civil Rights Framework for the Internet and the General Data of Protection Act. The paper also looks into how the effectiveness of this legal basis has become a questionable matter to ensure the data subject' autonomy of decision amid the technological arms race of surveillance. To overcome the insufficiencies of the consent paradigm, three perspectives are presented as interesting solutions in order to adapt data protection with the information market. Finally, it concludes that the guarantee of the fundament of informative self-determination goes far beyond consent as a

[1] Mestrando em *Public Policy* pela Hertie School of Governance, Alemanha. Mestre em Direito Constitucional e Políticas Públicas pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO). Bacharel em Direito pela Universidade Federal de Santa Catarina (UFSC). E-mail: diego.chagas.souza@gmail.com.
[2] Bacharel em Direito pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO). E-mail: joaovitorsangiacomo@gmail.com.

merely formal mechanism. The perception that the data subject is in a situation of vulnerability under this relationship is crucial to deal with the numerous challenges of data protection.

KEYWORDS: Data protection. Consent. Informational self-determination.

Introdução

Da Antiguidade Clássica à Idade Média, a concentração de riqueza e poder estava nas mãos dos proprietários de terras. Na Idade Moderna, a Revolução Industrial marca a transição de uma economia artesanal e familiar para uma economia industrial em massa, agregando valor aos produtos manufaturados. No período pós-industrial, mais especificamente após a Segunda Guerra Mundial, verifica-se uma mudança de uma economia baseada na indústria para outra focada na prestação de serviços. Mais recentemente, o mercado de capitais impõe uma nova racionalidade, pautada na captação de recursos pelas grandes companhias.

Na atualidade, o poder produtivo humano parece criar de forma ilimitada novos produtos e serviços, complexificando notavelmente as dinâmicas sociais. Arrazoa-se aqui que tais dinâmicas não possuem tradução melhor do que na Era da Informação e seus desdobramentos contemporâneos, a partir dos quais um novo ativo assume a centralidade para atividade econômica: os dados pessoais.

Talvez nem o mais otimista dos idealistas tivesse a capacidade de mensurar a proporção que a Internet um dia alcançaria, emergindo como pilar da sociedade do século XXI. Consonante a essa percepção, Alan Turing, conhecido como o pai da ciência computacional e da inteligência artificial[3], com uma concepção para além de sua realidade, asseverava que "Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer"[4].

Com o crescimento exponencial do universo digital e a disponibilização de dados na rede não somente por pessoas, mas também por algoritmos e plataformas que trocam informações entre si, formou-se um espaço de conexões cada vez mais automatizado. Constata-se, portanto, que a exploração e monetização dos dados inseridos nesse sistema, por meio, por exemplo, da criação de perfis comportamentais para o direcionamento de produtos e informações, não só interfere no livre desenvolvimento da personalidade dos indivíduos, como também na democracia que é posta em xeque.

Diante desse cenário, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), cria um novo regramento para o uso de dados pessoais no Brasil, tanto no ambiente *on-line* quanto *off-line*, nos setores privado e público. É importante ressaltar que o ordenamento jurídico brasileiro conta com normas que direta e indiretamente tratam da proteção à privacidade e aos dados pessoais, contudo a LGPD vem complementar esse arcabouço regulatório setorial, composto por esparsos comandos descentralizados e conferir segurança jurídica.

Fato é que, quando da elaboração da LGPD, houve uma notável preocupação do legislador em empoderar o titular dos dados pessoais e para tanto, atribuiu expressa notoriedade ao consentimento como uma das bases legais, que autoriza a coleta, transmissão, armazenamento e compartilhamento de dados pessoais.

Nesse sentido, é oportuno verificar qual é o alcance do consentimento na disciplina voltada à proteção de dados pessoais, para enfim tentar se alcançar um entendimento categórico desse pilar da LGPD.

A primeira seção aborda a temática do consentimento do titular para o tratamento de seus dados pessoais, sendo evidente o protagonismo a ele atribuído quando da positivação de legislações, que versam sobre o tema, algumas mesmo que de forma esparsa. Para isso, analisa-se como o consentimento foi moldado no Regulamento Europeu de Proteção de Dados,

[3] DAVIS, Nicola. The father of modern computing: Alan Turing's legacy. *The Guardian*, 15 jul. 2019. Disponível em: <https://www.theguardian.com/science/2019/jul/15/alan-turing-father-of-modern-computing-50-pound-note>. Acesso em: 20 maio 2020.

[4] Em inglês: "*We can only see a short distance ahead, but we can see plenty there that needs to be done*".

no Marco Civil da Internet e na LGPD.

A segunda seção verifica como a efetividade desse instrumento se tornou questionável para garantir a autonomia decisória do titular. Para tanto, apontam-se dois aspectos: o contraste entre *gratificações imediatas* e *prejuízos mediatos/distantes* (paradoxo da privacidade) e a assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados. Contrasta-se o quanto a autonomia decisória do indivíduo pode ser ameaçada pelo mercado informacional de dados.

A terceira e última seção investiga algumas abordagens, já adotadas por atuais legislações de proteção de dados e discutidas em trabalhos acadêmicos: (*i*) *Privacy by Design* (PbD); (*ii*) princípio da *accountability*; e (*iii*) privacidade contextual. Essas perspectivas visam adequar a proteção de dados pessoais a esse novo mercado altamente dependente da troca intensa de dados e apaziguar as insuficiências acerca do foco excessivo no consentimento.

A pesquisa tem como objetivo investigar em que medida o consentimento é capaz de concretizar o fundamento da autodeterminação informativa, verificando sua função e suas limitações.

O que impulsionou a realização deste trabalho foi conhecer e entender os obstáculos que advém da implementação de uma lei com viés protetivo ao indivíduo, em relação ao tratamento de seus dados pessoais, apresentando conceitos e reconhecendo a relevância social de uma tutela a esses dados para proteção de direitos fundamentais, com base na lei, doutrina e artigos publicados sobre a temática.

1. O consentimento do titular para o tratamento de dados pessoais na Sociedade da Informação

Uma vez direcionados a um público específico, mais inclinado a consumir determinado bem, a ciência mercadológica percebeu que o ambiente virtual poderia propiciar anúncios publicitários mais efetivos. Por meio de diversas ferramentas tecnológicas, dentre as quais se destacam os *cookies* - ferramentas de rastreamento dos hábitos dos consumidores ao longo de sua navegação na Internet[5] - tornou-se possível rastrear a navegação do usuário e, por conseguinte, inferir seus interesses, uma vez que o bem de consumo anunciado é correlacionado

[5] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 135.

cirurgicamente ao perfil deste consumidor[6].

Nessa perspectiva, o novo modelo de negócios na Internet, em um primeiro momento, atrai o usuário para que ele usufrua de um serviço e/ou produto "gratuitamente" disponibilizado, para, em um segundo momento, coletar seus dados pessoais e, então, viabilizar o direcionamento da mensagem publicitária, que é a sua fonte de rentabilização. A monetização dos dados pessoais, portanto, é uma realidade ao passo que consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada[7-8].

Ao mesmo tempo, surge uma crescente preocupação em torno do alcance do consentimento do titular para o tratamento de seus dados pessoais frente à uma sociedade cada vez mais orientada e movida por dados (*data-driven society*).

1.1 O molde do consentimento no Regulamento Europeu de Proteção de Dados

Em 1980, percebeu-se que o desenvolvimento econômico e social se tornou interdependente do processamento de dados. Nesse panorama, a OCDE emitiu as *Privacy Guidelines*, as quais cogitavam uma conciliação entre desenvolvimento econômico e a proteção da privacidade das pessoas e vieram a influenciar diversas legislações sobre proteção de dados pessoais ao redor do mundo[9].

Tais *guidelines* estabeleciam padrões normativos e princípios para a proteção de dados pessoais, com o propósito de criar um ambiente regulatório uniforme e assegurar o livre trânsito de informações entre seus países-membros. Nota-se, portanto, sua inegável excelência para o protagonismo auferido ao titular de dados pessoais.

Não por outra razão, a Convenção 108 do Conselho da Europa, de 1981[10-11], é

---

[6] Ibid., p. 16-17.
[7] Ibid., p. 22-23.
[8] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019, p. 296: "Tendo-se como exemplo as mídias sociais, sua estrutura revela a necessidade de constante inserção de dados pessoais por parte dos usuários. É essencial ao negócio a existência de uma massa substancial de usuários, os quais são estimulados a inserir de forma ininterrupta diversas informações sobre si e terceiros. Posteriormente, parte-se para a exploração e monetização dos dados inseridos no sistema, por meio, por exemplo, da venda de espaços para publicidade e anúncios, do desenvolvimento de perfis para o direcionamento de produtos e informações e da possibilidade de acesso aos dados de seus usuários por parte de parceiros comerciais".
[9] Intitulado "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*". Tradução livre: "Diretrizes da OCDE para Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais".
[10] Intitulada "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Autorizado de Dados Pessoais" (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 108/1981) ou Convenção de Strasbourg.
[11] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de

resultado desse movimento promovido pela OCDE para facilitar a harmonização das legislações que versam sobre proteção de dados pessoais, promover o livre fluxo informacional e por conseguinte, uma maior integração econômica.

Diferentemente das *guidelines* da OCDE, as quais não estabeleciam um dever de cooperação entre titular dos dados pessoais e *data controllers* - àqueles que processam os dados pessoais - a Diretiva n° 95/46/CE, do Parlamento Europeu e do Conselho[12], em 1995, documento que efetivamente padroniza a proteção de dados pessoais na União Europeia, posiciona o princípio da minimização[13] como sendo um dever de quem é responsável pela atividade de tratamento de dados.

Ademais, é notável o empoderamento atribuído ao titular dos dados pessoais pela Diretiva n ° 95/46/CE, no momento em que molda o consentimento do titular dos dados pessoais na tentativa de operacionalizá-lo. Na lição de Bruno Bioni:

> A sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno de um controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular (...)[14].

Não ao acaso, quando da elaboração do texto do *General Data Protection Regulation* (GDPR) - Regulamento Geral sobre a Proteção de Dados (RGPD), da União Europeia (UE)[15], que substitui a Diretiva n° 95/46/CE, verificou-se, mais uma vez, uma preocupação central em torno do consentimento[16], estruturando-se um artigo específico para

proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 194: "Ela também adota um prisma universalista, pois não foi estruturada como uma convenção puramente "europeia", tendo sido aberta para adesões também de países não membros do Conselho da Europa - ratificaram a Convenção 108 inclusive países latino-americanos, como Argentina, México e Uruguai".

[12] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 2 nov. 2020.

[13] Apesar de a LGPD não dispor expressamente sobre o princípio da minimização, é possível extraí-lo do princípio da necessidade, previsto no art. 6º, inciso 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".

[14] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 118.

[15] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 10 set. 2020.

[16] MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. Seis pontos para entender o Regulamento Geral de Proteção de Dados da UE. *ITS Rio*, 25 maio 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-proteção-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em: 2 nov. 2020.: "(...) O consentimento do titular de dados, por exemplo, passa a figurar como elemento principal para autorizar a coleta e tratamento de dados, devendo ser inequívoco e envolver sempre uma postura assertiva. Caso isto seja descumprido, o GDPR prevê de maneira clara a possibilidade de responsabilização daqueles que realizarem a coleta inadequadamente".

tratar das condições a ele aplicáveis[17].

Interessa, para fins do presente trabalho, notar que as adjetivações empregadas pelo GDPR ao consentimento, no considerando nº 32[18] - manifestação de vontade *livre, específica, informada e inequívoca* -, serviram de inspiração para definição dessa base legal na LGPD, como será aprofundado mais à frente.

Nessa perspectiva, é pertinente trazer à tona a condenação a multa imposta ao Google, em janeiro de 2019. A autoridade francesa de proteção de dados - Comissão Nacional de Informática e Liberdades (CNIL)[19] - fixou a multa no valor de 50 milhões de euros, por violação de regras de privacidade da UE. De acordo com a *Thomson Reuters Brasil*:

> O principal tribunal administrativo da França chancelou ontem uma multa de € 50 milhões imposta no ano passado ao Google, da Alphabet, por violar regras de privacidade on-line da União Europeia (UE). Embora seja pouco frente à receita do Google, a penalidade repercutiu no Vale do Silício e ainda é a maior multa imposta por tal violação. (...) O Google disse que avaliará possíveis alterações em sua política de privacidade. "As pessoas esperam entender e controlar como seus dados são usados", afirmou em nota. "Este caso não foi sobre se o consentimento é necessário para a publicidade personalizada, mas sobre como exatamente ele deve ser obtido. À luz dessa decisão, avaliaremos que mudanças precisam ser feitas". (...) O órgão regulador francês CNIL decidiu, em janeiro de 2019, que o Google deveria ser mais transparente ao informar usuários sobre o uso de dados pessoais e que falhou em obter consentimento adequado para anúncios personalizados. (...) A decisão se baseou no Regulamento Geral de Proteção de Dados (GDPR) da UE[20].

Outro caso de grande repercussão foi a emissão de multa em 150 mil euros à PwC (*PricewaterhouseCoopers*), em julho de 2019, pela *Hellenic Data Protection Authority* (HDPA) - autoridade grega de proteção de dados - por infrações ao GDPR, após receber uma reclamação apontando que os funcionários da empresa foram obrigados a consentir com tratamento de seus dados pessoais[21].

Em síntese, a empresa aplicou, indevidamente, o consentimento como base legal para o tratamento de dados pessoais de seus funcionários, contrariando as disposições do GDPR. Nesse sentido, é importante observar, como verifica Caio César Carvalho Lima, que atualmente

---

[17] Trata-se do art. 7º nomeado como "Condições aplicáveis ao consentimento".

[18] Considerando nº 32, do GDPR: "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral".

[19] Em francês: "*Commission Nationale de l'Informatique et des Libertés*". Disponível em: <https://www.cnil.fr/fr>. Acesso em: 19 set. 2020.

[20] Ver notícia disponível em: <https://www.reuters.com/article/tech-google-franca-idBRKBN23Q2WJ-OBRIN >. Acesso em: 5 jul. 2020.

[21] Ver notícia disponível em: COMPANY fined 150,000 euros for infringements of the GDPR. *European Data Protection Board*, 31 jul. 2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_pt>. Acesso em: 18 set. 2020.

existe um "(...) posicionamento no sentido de que o consentimento não é a base legal ideal para tornar lícito o tratamento, diante da dificuldade de sanar a assimetria existente na relação empregador-empregado"[22].

1.2 A insuficiência do Marco Civil da Internet em relação à proteção de dados

Jack Goldsmith, professor na *Harvard Law School* e Tim Wu, professor na *Columbia Law School*, doutrinadores norte-americanos e autores da obra *Who Controls the Internet?: Illusions of a Borderless World*, publicado na *Oxford University Press*[23], em 2006, defendiam que os países precisariam criar normas para regulamentar o uso da Internet, em conformidade com o contexto específico de cada Estado-nação[24].

Com efeito, a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (MCI)[25], "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Trata-se de uma tentativa de conscientização social para o uso moderado da Internet, antes encarada como uma "terra sem lei". Dentre os princípios previstos, evidenciam-se a proteção da privacidade e dos dados pessoais[26], sem, no entanto, conceituar *dados pessoais* e destinando sua regulamentação a uma legislação específica.

Fato é que, em decorrência do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos, em 2013, o MCI

---

[22] LIMA, Caio César Carvalho. Estudo prático sobre as bases legais na LGPD. *In*: OPICE BLUM, Renato. *Proteção de dados*: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020, p. 27-28: "Como exemplo de consentimento válido do empregado, podemos citar a situação em que determinada empresa resolve criar painel com fotografias dos aniversariantes do mês, os quais, se desejarem ser exibidos na imagem, deverão enviar sua imagem para o Departamento de Recursos Humanos. Nessa situação, o ato de o empregado submeter o seu retrato representará seu consentimento para o tratamento dos dados pessoais, para a única finalidade de sua utilização, no respectivo mês da celebração do seu aniversário".

[23] Tradução livre: "Quem Controla a Internet? Ilusões de um Mundo sem Fronteiras".

[24] GOLDSMITH, Jack L.; WU, Tim. Who Controls the Internet?: Illusions of a Borderless World. *Oxford University Press*, 2006. Disponível em: <http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf>. Acesso em: 12 set. 2020.

[25] MATTIETTO, Leonardo. *Developments on data protection in Brazilian Law*. *In*: Internet, Law & Politics: A decade of transformations, 2014, Barcelona. Anais… Barcelona: Universitat Oberta de Catalunya, 2014, p. 332: "The Marco Civil (Civil Rights Framework for the Internet) started as an initiative from the Ministry of Justice, in partnership with the Center for Technology and Society of Fundação Getúlio Vargas School of Law. There was developed a collaborative and multistakeholder process in which both the government and civil society could work to define the principles and rules that should guide the use of the internet in Brazil. The result was a bill of law (nr. 2.126) which was submitted to the National Congress in August 2011". Tradução livre: "O Marco Civil (Marco Civil da Internet) começou como uma iniciativa do Ministério da Justiça, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas. Foi desenvolvido um processo colaborativo e multissetorial, no qual tanto o governo quanto a sociedade civil poderiam trabalhar para definir os princípios e regras que devem nortear o uso da internet no Brasil. O resultado foi um projeto de lei (nº 2.126) que foi submetido ao Congresso Nacional, em agosto de 2011".

[26] Art. 3º, incisos II e III, da Lei nº 12.965/2014.

teve modificações substanciais em seu texto, tendo o legislador eleito o usuário como o grande protagonista para desempenhar a proteção de seus dados pessoais[27].

Em verdade, o MCI não inovou o ordenamento jurídico, atendo-se a direitos e garantias já consagrados em outras legislações, tratando de forma limitada a proteção à privacidade e aos dados pessoais. Por outro lado, expôs regras específicas dispostas a lidar com os desafios da regulamentação do uso da Internet.

Contudo, é relevante a menção à necessidade de consentimento do titular de dados pessoais em três dispositivos[28] do MCI, qualificado como "consentimento *livre, expresso e informado*". Trata-se, sobretudo, de uma orientação àquele que exerce atividade de tratamento de dados pessoais de prestar informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais do titular, utilizando-se de cláusulas contratuais destacadas.

1.3 Esmiuçando o consentimento na LGPD

De início, é de suma importância esclarecer que o consentimento não é hierarquicamente superior às demais bases legais elencadas no artigo 7º, da LGPD. Em verdade, as outras bases legais não são exceções ("dispensa") ao consentimento[29]. Como reconhece Caio César C. Lima:

> O consentimento passa a ser apenas 1 dentre 10 possibilidades trazidas na legislação, sendo que todas as outras 9 hipóteses são autônomas e não necessitam do consentimento para serem consideradas válidas. Assim, objetivamente, é possível que ocorra o tratamento de dados sem o consentimento, desde que outra base legal ampare a atividade[30].

Em contrapartida, pode-se dizer que ele é um dos elementos cardeais da lei, uma vez que a preocupação da LGPD em esmiuçar tal elemento ao longo do seu corpo normativo[31], revela o empoderamento atribuído ao titular dos dados pessoais, sobretudo, a autonomia da vontade individual[32].

Por ora, é oportuno investigar as adjetivações empregadas pelo artigo 5º, inciso XII, da LGPD ao consentimento, uma vez que a lei não especificou o que se deve entender por

[27] Veja-se, o artigo 7º que trata dos direitos e garantias dos usuários.
[28] Artigos 7º, incisos VII e IX e 16, inciso II.
[29] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 247.
[30] LIMA, op. cit., p. 26.
[31] O termo "consentimento" aparece 35 vezes no texto da LGPD.
[32] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 127-128.

"manifestação *livre*, *informada* e *inequívoca*". Ato contínuo, faz-se necessário compreender a definição de um consentimento *específico*, mencionado pela LGPD em quatro dispositivos[33].

Como ilustra Bruno Bioni "O adjetivo livre nos remete à ideia de uma ação espontânea que não é objeto de pressão, mas, pelo contrário, de livre-arbítrio caracterizado pela tomada de uma escolha em meio a tantas outras que poderiam ser feitas por alguém"[34]. Para que o consentimento seja livre, o titular dos dados deve ter a possibilidade de optar se, de fato, deseja (ou não) ter esses dados tratados, sem que haja nenhum empecilho à manifestação volitiva no momento da sua coleta[35].

O elemento central de análise do qualificador livre é o nível de assimetria de poder e revisitando, a título de exemplo, o caso da emissão de multa à PwC por aplicar, indevidamente, o consentimento como base legal para o tratamento de dados pessoais de seus funcionários, percebe-se que não há, em decorrência da vulnerabilidade do empregado, um consentimento propriamente livre.

Além disso, uma vez superada a lógica do "*take it or leave it"* enraizada nos termos de uso e nas políticas de privacidade, o consentimento torna-se *granular*[36], visto que o titular autoriza, de forma *fragmentada/fatiada* o tratamento de seus dados pessoais[37]. Nessa linha de raciocínio, Caio César C. Lima elucida que:

> (...) é importante observar o que diz respeito à granularidade, por meio da qual não se pode ter como válido o consentimento manifestado no formato de "tudo ou nada". Nesse sentido, nas situações em que houver coleta de dados para diferentes finalidades, o titular dos dados deve ter a possibilidade de escolher, uma a uma, a finalidade específica em relação à qual autoriza o tratamento de dados, sendo inválido se não houver essa opção[38].

Ato contínuo, a LGPD menciona que o consentimento deve ser informado e para tanto, o *caput* do art. 9º orienta que as informações deverão ser disponibilizadas de forma "*clara*, *adequada* e *ostensiva*" ao titular dos dados pessoais. Explicando melhor e recorrendo às relações consumeristas, a informação deve ser fornecida de forma evidente, manifesta, visível, ou seja, apresentar-se de forma *perceptível* ao consumidor[39], objetivando a diminuição da assimetria técnica e informacional existente entre as partes[40].

---

[33] Quais sejam: Artigos 7º, § 5º, 11, inciso I, 14, § 1º e 33, inciso VIII.
[34] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 185.
[35] LIMA, op. cit., p. 27.
[36] Art. 9º, §3º, da LGPD.
[37] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 185.
[38] LIMA, op. cit., p. 28.
[39] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p 180.
[40] TEPEDINO; TEFFÉ, op. cit., p. 301.

Além disso, o art. 9º elenca um rol exemplificado de informações que devem ser apresentadas ao titular dos dados pessoais. É importante mencionar que tais informações devem ser prestadas em uma quantidade suficiente para uma compreensão adequada daquela atividade de tratamento de dados.

Constata-se, portanto, uma correlação entre informação e transparência. Não ao acaso, a LGPD ao detalhar o princípio da transparência, efetiva-o por meio de "informações claras, precisas e facilmente acessíveis"[41] e prevê o consentimento *nulo* "caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"[42].

Fato é que, o consentimento dialoga fortemente com o princípio da finalidade, posto que, uma vez especificada a razão pela qual se faz uso de um dado, é possível analisar se o indivíduo foi adequadamente *informado* para tomada de uma decisão *livre*. Esta sequência de fases culmina em uma declaração de vontade *inequívoca* por parte do titular dos dados pessoais.

Quando a LGPD menciona que o consentimento deve ser inequívoco, isso significa que não pode haver dúvidas sobre a intenção do titular, no sentido de que este manifestou, de fato, a autorização para que ocorresse o tratamento de seus dados pessoais[43].

Além de livre, informado e inequívoco, quando o consentimento for a base legal que autoriza o tratamento dos dados sensíveis[44], ele deverá ser realizado de forma específica e destacada. À vista disso, Caio César C. Lima pontua que "O consentimento será entendido como específico, desde que ele seja manifestado em relação a propósitos claramente determinados pelo controlador, anteriormente ao procedimento de coleta dos dados pessoais"[45].

Como dito anteriormente, a LGPD menciona o consentimento específico em quatro dispositivos. Após a leitura dos artigos, percebe-se que os cenários expressam um risco elevado, tendo a LGPD concedido uma "camada adicional" de proteção ao titular dos dados pessoais, conferida por este consentimento especial[46].

Ao contrário da LGPD, o GDPR[47] e o MCI[48] empregaram o qualificador *expresso* em vez de específico. Bruno Bioni apresenta a seguinte crítica em relação à adjetivação inserida pelo legislador na LGPD:

---

[41] Art. 6º, inciso VI, da LGPD.
[42] Art. 9º, § 1º, da LGPD.
[43] LIMA, op. cit., p. 29.
[44] A LGPD define dado sensível em seu art. 5º, inciso II.
[45] LIMA, op. cit., p. 35.
[46] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 189.
[47] Considerando nº 51, do GDPR.
[48] Art. 7º, inciso VII, do MCI.

> Do ponto de vista de técnica legislativa, o termo específico é redundante se for considerado que o consentimento já deve ser necessariamente direcionado para propósitos "específicos e explícitos" na linha do que dispõe o princípio da finalidade. Essa significação já está contida na própria definição de uma declaração de vontade que deve ser dirigida para "finalidades determinadas"[49].

Em conclusão, as adjetivações empregadas pela LGPD ao consentimento, pretendem conceder uma carga participativa maior ao titular no fluxo de seus dados pessoais. A seguir avaliar-se-á a capacidade desse instrumento protetivo para efetivar a proteção dos titulares dos dados pessoais frente aos novos riscos e maneiras de se explorá-los.

2. Autodeterminação informativa em risco em meio à corrida armamentista tecnológica de vigilância

Sobre uma vigilância hierárquica, em *Vigiar e Punir,* Michel Foucault argui que o ato de disciplinar exige "(...) um dispositivo que obrigue pelo jogo do olhar: um aparelho onde as técnicas que permitem ver induzam a efeitos de poder, e onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplicam"[50]. Constata-se, portanto, que a produção de subjetividades dependeria da relação de olhares produzidos entre indivíduos sob o prisma da máquina disciplinar institucional.

Partindo dessa premissa, argumenta-se que, enquanto o foco da visibilidade ainda hoje permanece sobre o indivíduo, há um deslocamento contextual para a Sociedade da Informação, na qual ser vigiado é tanto imposição quanto desejo. Por um lado, herdam-se os princípios panópticos de vigilância delineados por Michel Foucault, mas, por outro, cria-se uma cultura que vai além de puro controle social, que busca "(...) prazer, sociabilidade, entretenimento, cuidado consigo e com o outro. (...) Tais heranças misturam-se e renovam-se nas atuais práticas de visibilidade, multiplicando as nuances de uma subjetividade cada vez mais alterdirigida"[51].

À vista disso, o Panóptico, originalmente concebido em 1791, por Jeremy

[49] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 189.
[50] FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014, p. 168.
[51] BRUNO, Fernanda. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013, p. 66-67.

Bentham[52] e a *teletela orwelliana*, do romance intitulado 1984, de George Orwell[53], são apenas dois modelos recorrentes de caracterização de vigilância ostensiva. Na atualidade, a figura do Grande Irmão (*Big Brother*), descrita na obra de Orwell, dilui-se pela multiplicação de Pequenos Irmãos que, aliados a crescente presença de novas tecnologias de vigilância, penetram nas vidas das pessoas para exploração econômica, por meio da observância constante de potenciais consumidores[54]: Capitalismo de Vigilância[55].

Este arcabouço social contemporâneo - de novas subjetividades aliadas a tecnologias cada vez mais avançadas de comunicação e informática - permite, então, uma reconfiguração em oportunidades comerciais dadas as marcas deixadas no espaço virtual. Daí surgem empresas especializadas em mineração e corretagem de dados (variando exemplos desde conglomerados transnacionais como Instagram até empresas públicas como API Serpro).

É por meio dessa estrutura econômica que inúmeras empresas coletam, armazenam, categorizam e, por fim, revendem o que é deixado na rede, construindo, na lição do renomado professor Stefano Rodotà, verdadeiras "redes de dados"[56] dos modos de vida capazes de perfilizar a individualidade em categorias, por meio de decisões automatizadas. Tal estrutura representa então, simultaneamente, um novo modelo de negócios de caráter decisivo dentro das complexas dinâmicas empresariais capitalistas e uma ameaça às noções jurídicas e sociais de privacidade e autonomia individual.

---

[52] LOSANO, Mario G. Trasparenza e segreto: una convivenza difficile nello Stato democratico. *Diritto pubblico*, v. 23, n. 3, 2017, p. 658: "Il suo modello architettonico è il Panopticon immaginato nel 1791 da Jeremy Bentham per tenere sotto controllo non solo carceri e manicomi, ma anche fabbriche e scuole: un edificio circolare a forma di salvagente, con finestre verso l'esterno e verso l'interno; al centro si erge una torre, dalla quale il sorvegliante vede tutti, senza però essere visto dai sorvegliati". Tradução livre: "O seu modelo arquitetônico é o Panóptico imaginado em 1791 por Jeremy Bentham para controlar não só prisões e asilos, mas também fábricas e escolas: um edifício circular em forma de salva-vidas, com janelas para fora e para dentro; no centro ergue-se uma torre, da qual o supervisor vê a todos, sem, no entanto, ser visto pelos vigiados".

[53] SCHREIBER, Anderson. *Direitos da Personalidade*. 2. ed. São Paulo: Atlas, 2013, p. 133: "Em seu célebre *1984*, o Grande Irmão é um ditador enigmático e onipresente, que tudo observa. No regime totalitário imaginado por Orwell, a privacidade é uma aspiração quase impossível. (...) Por toda parte, o partido dominante relembra aos governados que o *"Big Brother is watching you*". *1984* foi escrito no ano de 1948. A visão de Orwell sobre o futuro pareceu ao público aterrorizante, mas possível. A experiência dos regimes autoritários europeus estava ainda muito viva na memória dos leitores".

[54] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 135-137.

[55] ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, v. 30, n. 1, 2015, p. 75-76: "(...) a deeply intentional and highly consequential new logic of accumulation that I call *surveillance capitalism*. This new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control. Surveillance capitalism has gradually constituted itself during the last decade, embodying a new social relations and politics that have not yet been well delineated or theorized". Tradução livre: "(...) uma nova lógica de acumulação profundamente intencional e altamente consequente que eu chamo de *capitalismo de vigilância*. Esta nova forma de capitalismo visa prever e modificar o comportamento humano como meio de gerar receita e controle do mercado. O capitalismo de vigilância constituiu-se gradualmente durante a última década, incorporando novas relações sociais e políticas que ainda não foram bem delineadas ou teorizadas".

[56] RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

2.1 Paradoxo da privacidade: contraste entre *gratificações imediatas* e *prejuízos mediatos/distantes*

Não há como se discutir o direito à privacidade sem contextualizar o debate nas mudanças epistemológicas caracterizadas pela era digital. As crises econômicas e políticas, somadas às novas tecnologias, modificaram substancialmente as estruturas das relações de poder, produção e experiência, conduzindo, portanto, a uma remodelagem nas formas sociais de espaço e tempo, dando ensejo a uma cultura inédita de permanente mutação.

Por certo que, as novas tecnologias, de forma contínua, vêm dando vazão a novas práticas que, por sua vez, impõem tipos inéditos de modelos organizacionais. Nessa linha de raciocínio, é curioso notar que a troca contínua de dados pessoais entre os inúmeros sujeitos que integram a rede gera mais conveniência na vida dos consumidores.

Um bom exemplo é quando o usuário se cadastra em um *website* utilizando sua conta Google para ter um acesso mais dinâmico a um produto ou serviço *on-line*. Fato é que, essa troca poderá implicar em ações cooperativas, por meio do compartilhamento de informações, para que seja personalizada uma abordagem publicitária, de acordo com o perfil do potencial consumidor. Em uma conjuntura mais grave, poderá, ainda, inferir informações sensíveis sobre uma pessoa a partir do tratamento de seus dados pessoais.

Dessa forma, percebe-se que os seres humanos se concentram em recompensas imediatas, provenientes do acesso a um bem de consumo digital e minimizam os possíveis danos com relação à perda do controle sobre seus dados pessoais. Com efeito, esses possíveis danos não são imediatos, em outras palavras, os prováveis prejuízos à privacidade só são passíveis de serem vistos no futuro[57].

Deriva daí, o denominado *paradoxo da privacidade*, posto que apesar de as pessoas valorizarem a sua privacidade, elas executam atitudes contraditórias frente a tal bem apreciado. No que se refere à proteção de dados pessoais, é possível constatar uma incoerência na medida em que os titulares, ainda que prezem pela proteção de suas informações pessoais, anuem com seu trânsito contínuo, em virtude desse contraste entre *gratificações imediatas* e *prejuízos mediatos/distantes*[58].

[57] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 138-140.
[58] Ibid., p. 141-150.

2.2 Assimetria do mercado informacional: agravante de vulnerabilidade do titular dos dados pessoais

Soma-se ao paradoxo da privacidade, a descrença dos consumidores quanto à própria capacidade de controle de suas informações pessoais. Isso agrava a vulnerabilidade do titular, evidencia uma *relação assimétrica de poder* e coloca em risco a autodeterminação informativa frente à dinâmica da economia dos dados pessoais[59]. Nesse segmento, Bruno Bioni afirma que:

> Com efeito, a programada autonomia dos consumidores para controlar seus dados pessoais é sufocada por todo um mercado sedento por tal ativo econômico. A lógica da economia dos dados pessoais prevalece e impõe as suas forças sobre a parte mais vulnerável dessa relação. Os consumidores mostram-se impotentes para fazer valer o seu desejo de controlar seus dados pessoais, sendo tal *assimetria de poder* a mola propulsora de tal resignação[60].

Sem dúvida, as políticas de privacidade têm se mostrado ineficientes, corroborando com essa assimetria do mercado informacional[61]. Isso porque tal mecanismo consiste em um contrato de adesão, o qual empodera o fornecedor, que fixará unilateralmente o instrumento contratual, cabendo ao consumidor, tão somente, "concordar" ou "discordar" com essa dinâmica contratual[62]. Isto é, será delegado ao fornecedor os rumos do fluxo informacional dos usuários, eliminando a esfera de controle do titular sobre seus dados pessoais[63].

Nessa linha de raciocínio, Laura Schertel Mendes e Gabriel Campos Soares da Fonseca, concluem que:

> (...) o consentimento é meramente uma *ficção*, uma vez que o indivíduo carece de efetiva autonomia decisória para se proteger dos possíveis perigos e danos à sua personalidade. Nessas situações, a decisão individual de consentir não é livre e autônoma ou oriunda da avaliação dos ônus e dos bônus envolvidos. Ao revés, ela se

[59] Ibid., p. 155: "Na lógica da economia digital, os dados pessoais são a moeda de troca pelo bem de consumo".
[60] Ibid., p. 151.
[61] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista Estudos Institucionais*, Rio de Janeiro, v. 6, n. 2, 2020, p. 516: "Ocorre que, em não raras vezes, o titular dos dados pessoais se encontra em situação de vulnerabilidade nessa relação contratual eletrônica (...). Primeiro, pois, como já dito, os termos das políticas de privacidade podem ser demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Segundo, porque vários desses termos negociais se baseiam em uma lógica binária "*take it or leave it"*: consentir ou não consentir, sem outras opções. Porém, ao não consentir, o custo é o de não desfrutar o serviço almejado, *v.g.*, o uso de uma rede social ou de um aplicativo online (...)".
[62] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 165: "E, nesse sentido, tal ferramenta contratual está longe de ocasionar o empoderamento. Na verdade, os seus textos longos e de difícil compreensão são incapazes de sequer estabelecer uma comunicação adequada para que o titular dos dados pessoais possa racionalizar um processo de tomada de decisão".
[63] Ibid., p. 162-163.

> origina de uma verdadeira imposição estabelecida por terceiro: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital[64].

Depreende-se que não obstante o protagonismo do consentimento para o desenvolvimento da disciplina de proteção de dados, os dois aspectos apontados demonstram insuficiências do paradigma do consentimento[65]. Isto posto, verifica-se que a efetividade desse instrumento se torna questionável para garantir a *autonomia decisória* do titular.

3. Dupla atribuição sobre a autodeterminação informativa: perspectivas de efetividade do consentimento

Ante o exposto, nota-se uma desarmonia entre a autodeterminação informativa e o mercado informacional, cada vez mais sedento por dados pessoais como novo ativo econômico[66]. Essa problemática agrava-se a uma desmedida confiança na aptidão do consentimento para promoção da autodeterminação do titular dos dados[67].

Nesta seção, serão investigadas três perspectivas que visam adequar a privacidade e a proteção de dados pessoais a esse novo mercado altamente dependente da troca intensa de dados e apaziguar as insuficiências supramencionadas acerca do foco excessivo no consentimento, efetivando-o.

3.1 *Privacy by Design* (PbD): a privacidade não se trata de um serviço adicional

Como bem explicam Laura S. Mendes e Gabriel C. S. da Fonseca, se por um lado, as inovações tecnológicas têm gerado grandes riscos à personalidade dos indivíduos, por outro,

---

[64] MENDES; FONSECA, op. cit., p. 516.
[65] Esta expressão é utilizada por: MENDES; FONSECA, op. cit., p. 513.
[66] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 195.
[67] WIMMER, Miriam. Dados Pessoais - Repensando o consentimento: Resenha ao livro 'Proteção de Dados Pessoais: a função e os limites do consentimento', de Bruno R. Bioni. *Jota*, 24 dez. 2018: "Nesse contexto de assimetria de poder e de vulnerabilidade do cidadão no mercado informacional, o processo de "veneração do consentimento" observado na trajetória histórica das estratégias regulatórias voltadas à efetivação da autodeterminação informativa revela, (...), uma *contradição intrínseca*: não obstante a verdadeira proliferação de leis e arranjos normativos voltados à proteção de dados pessoais, a construção de tais estratégias ao redor do eixo central do consentimento (fartamente adjetivado como "livre", "informado", "expresso", "inequívoco", "específico") acaba por jogar sobre os ombros do cidadão a responsabilidade de gerir a proteção de seus próprios dados pessoais, sem levar em conta que tais dados - frequentemente descritos como o combustível da economia digital - se constituem também como ativo econômico em constante circulação através de uma pluralidade de agentes econômicos".

elas podem ser verdadeiras ferramentas em favor dessa proteção. Nessa linha de raciocínio, aliar direito e tecnologia:

> (...) é essencial para estruturar parâmetros regulatórios e institucionais compatíveis com os valores ético-sociais e os preceitos jurídicos de determinada sociedade. Nesse sentido, importante tarefa é, por exemplo, incentivar o desenho de sistemas tecnológicos seguros e assegurar a presença dos princípios que guiam a proteção de dados não só nas leis e/ou nos termos contratuais, mas também nos sistemas tecnológicos utilizados para tanto (...)[68].

Expressão formulada na década de 1990, por Ann Cavoukian, ex-comissária de informação e privacidade na província de Ontário, no Canadá[69], *Privacy by Design* é "a metodologia que visa resguardar a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou negócios que envolvam coleta de dados"[70]. Em outras palavras, antevendo casos de invasão à privacidade, organizações incorporam em projetos, produtos e/ou serviços, por elas desenvolvidos, medidas de prevenção e resguardo no que concerne à proteção de dados pessoais[71].

O GDPR faz menção ao PbD no art. 25 quando trata de *Data protection by design and by default*[72], aliás, o art. 46, §2º, da LGPD, também recepcionou a obrigatoriedade de observância do PbD. Laura S. Mendes e Gabriel C. S. da Fonseca elucidam que:

> Trata-se de estimular a incorporação da ideia de *autodeterminação informativa* nos sistemas, códigos, arquiteturas e procedimentos tecnológicos: aplicar o direito fundamental à proteção de dados na concepção e na aplicação das tecnologias que permeiam os serviços e produtos disponíveis aos usuários. É que, em ordem de se alcançar um consentimento material e efetivo, antes é preciso preencher diversas condições tecnológicas para tanto[73].

A inobservância do PbD ficou evidente em um caso publicado no *European Data*

---

[68] MENDES; FONSECA, op. cit., p. 520-521.

[69] CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles.* Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 27 ago. 2020.

[70] MURARO, Igor S. A importância do privacy by design e privacy by default nas aplicações: O que podemos aprender com o caso Zoom. *Jota*, 2 mai. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-importancia-do-privacy-by-design-e-privacy-by-default-nas-aplicacoes-02052020#_ftn4>. Acesso em: 4 ago. 2020.

[71] TEPEDINO; TEFFÉ, op. cit., p. 294: "Há de se obter a garantia de que os dados pessoais serão processados com a mais alta proteção da privacidade do titular (por exemplo, apenas os dados necessários devem ser tratados, o período de armazenamento deve ser curto e o acesso aos dados deve ser limitado), de forma que os dados sejam automaticamente (como padrão) protegidos em qualquer sistema de TI ou prática de negócios. A privacidade se torna componente essencial da funcionalidade principal do que está sendo entregue. Atua-se, assim, no sentido de incorporar fortes medidas de segurança ao ciclo dos dados para se garantir o gerenciamento seguro das informações do começo ao fim".

[72] Tradução livre: "Proteção de dados desde a concepção e por padrão".

[73] MENDES; FONSECA, op. cit., p. 521.

Protection Board, em dezembro de 2019[74], no qual, em síntese, uma farmácia, com sede em Londres foi multada em £275,000, pelo *Information Commissioner's Office* (ICO)[75], devido a sua atitude "descuidada" em relação à proteção de categorias especiais de dados pessoais[76] de pacientes. A *Doorstep Dispensaree Ltd*, que fornece medicamentos para clientes e casas de repouso, deixou aproximadamente 500.000 documentos em contêineres destrancados na parte dos fundos de suas instalações.

Os documentos incluíam nomes, endereços, datas de nascimento, números do registro no NHS (Serviço Nacional de Saúde), informações e prescrições médicas de seus clientes. A atuação negligente no armazenamento ocasionou deterioração destes documentos por água.

É notório que houve uma sucessão de falhas que vão desde o dever de segurança no tratamento de dados pessoais até o dano ou destruição dos documentos, o que constitui uma violação ao GDPR. Ao fixar a multa, a ICO asseverou que: "A atitude descuidada da *Doorstep Dispensaree* fica aquém do que a lei e as pessoas esperam".

À luz do caso supracitado, revela-se imprescindível o armazenamento de informações em um ambiente seguro por parte das clínicas médicas, controle de acesso a terceiros, bem como fornecimento de treinamento e capacitação aos médicos e colaboradores.

Ademais, é importante destacar que fichas cadastrais preenchidas por pacientes para realização de consultas, bem como, laudos médicos, são considerados dados pessoais sensíveis, em face de seu risco potencial em comparação a outros dados.

Por isso, a doutrina preceitua o princípio da segurança física e lógica[77], e a LGPD menciona os princípios da segurança e da prevenção, previstos no art. 6º, incisos VII e VIII, visando assegurar a efetividade da tutela dos dados pessoais dos indivíduos[78].

Por outro lado, o STAYAWAY COVID[79], aplicativo oficial de rastreio da COVID-19, em Portugal, com objetivo de prevenir e mitigar a propagação do vírus, é um exemplo

---

[74] Ver notícia disponível em: <https://edpb.europa.eu/news/national-news/2019/london-pharmacy-fined-after-careless-storage-patient-data_pt>. Acesso em: 28 maio 2020.

[75] O Gabinete do Comissário de Informação é a autoridade independente do Reino Unido criada para defender os direitos à informação de acordo com interesse público, promovendo a transparência dos órgãos públicos e a privacidade dos dados dos indivíduos. Disponível em: <https://ico.org.uk>. Acesso em: 14 jun. 2020.

[76] São categorias especiais de dados pessoais aquelas previstas no nº 1 do art. 9º, do GDPR.

[77] DONEDA, op. cit., p. 182: "Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado".

[78] MENDES; FONSECA, op. cit., p. 521: "O primeiro angariando a confiança dos indivíduos quanto aos sistemas de informação, por meio de medidas técnico-administrativas aptas a coibir acessos não autorizados aos dados pessoais, bem como efeitos adversos oriundos de situações acidentais ou ilícitas. Já o segundo incorporando, na própria tecnologia, medidas técnicas capazes de prevenir a ocorrência de danos à personalidade dos indivíduos em face de tratamentos de dados pessoais".

[79] Disponível em: <https://stayawaycovid.pt>. Acesso em: 31 out. 2020.

recente de um programa desenvolvido dentro do conceito de PbD.

Em síntese, "a principal funcionalidade da aplicação é alertar o seu utilizador de exposições, consideradas de elevado risco, a outros utilizadores da aplicação a quem foi entretanto diagnosticada a COVID-19"[80]. Em outras palavras, o sistema permite que o usuário seja informado sobre contatos com pessoas que testaram positivo para COVID-19.

Em se tratando do funcionamento do sistema, ele requer que o *Bluetooth* esteja sempre ligado, não havendo rastreio da localização do usuário, nem uso de serviços de geolocalização.

É curioso notar que o aplicativo não requer dados de identificação de seus usuários, sendo gerado apenas um código aleatório a ser inserido no aplicativo, pelo indivíduo que foi diagnosticado com COVID-19. Importante mencionar que o sistema foi alvo de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) e submetido a consulta prévia pela Comissão Nacional de Proteção de Dados (CNPD)[81].

Em suma, a proteção de dados pessoais por meio da tecnologia e da arquitetura dos sistemas informacionais[82] (*privacy by design*) apresenta-se como uma solução efetiva para melhor amparar o consentimento do titular dos dados pessoais. Por intermédio desse instrumento, a governança de dados atua sob uma dupla função: estimulando políticas de desenvolvimento ancoradas nas novas tecnologias e, ao mesmo tempo, propiciando um ecossistema onde os dados pessoais são percebidos como integrais aos direitos fundamentais.

3.2 Princípio da *accountability*: responsabilização e prestação de contas

Os professores Colin Bennett, da Universidade de Victoria e Charles Raab, da Universidade de Edimburgo, autores da obra "*Revisiting "The Governance of Privacy": Contemporary Policy Instruments in Global Perspective*[83], reconhecem que o consentimento é um importante requisito de legitimação do processamento de dados, ficando os controladores responsabilizados por aderir aos princípios da transparência e *accountability* para se estar em *compliance*[84].

[80] Disponível em: <https://stayawaycovid.pt/wp-content/uploads/STAWAWAY-COVID-doc.pdf>. Acesso em: 31 out. 2020.
[81] Disponível em: <https://stayawaycovid.pt/perguntas-frequentes/>. Acesso em: 31 out. 2020.
[82] Esta expressão é utilizada por: MENDES; FONSECA, op. cit., p. 520.
[83] Tradução livre: "Revisitando 'A Governança da Privacidade': Instrumentos da Política Contemporânea em Perspectiva Global".
[84] BENNETT, Colin; RAAB, Charles D. *Revisiting "The Governance of Privacy":* Contemporary Policy Instruments in Global Perspective. August, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086>. Acesso em: 30 out. 2020.: "The individual's

Em outras palavras, como lecionam Laura S. Mendes e Gabriel C. S. da Fonseca, a responsabilidade pela proteção de dados pessoais em um complexo ambiente digital não está restrita ao gerenciamento individual do titular por meio exclusivo do seu consentimento[85], mas também a atuação diligente dos controladores de dados.

Nesse sentido, o considerando nº 85 do GDPR incluiu expressamente o princípio da *accountability*, que é, como lecionam Ana Lara Mangeth, Beatriz Nunes e Eduardo Magrani:

> (...) o princípio segundo o qual exige-se que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas. Para tal, instituiu-se o controlador de dados, profissional responsável, por demonstrar que a organização está agindo em conformidade com os demais princípios estabelecidos pelo Regulamento[86].

Vale mencionar, também, que o considerando nº 89, do GDPR trouxe uma inovação em relação à Diretiva 95/46/CE, ao estabelecer que as notificações do tratamento de dados pessoais às autoridades de controle são necessárias somente quando se estiver diante de "operações de tratamento suscetíveis de resultar num *elevado risco* para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades".

O princípio da *accountability* também se faz presente na LGPD, sendo apresentado no inciso X do art. 6º, como o princípio da "responsabilização e prestação de contas", no qual é definido como sendo a "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".

Nota-se, portanto, que a ideia de *accountability* na proteção de dados, além de demandar maior responsabilidade e transparência, incentiva a atuação ativa dos controladores, que deverão "comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares"[87].

3.3 Privacidade contextual: uma releitura da proteção de dados pessoais

knowledge and consent were important legitimizing requirements for data processing, and data controllers had to adhere to principles of transparency and accountability for compliance with measures that gave effect to the other principles".

[85] MENDES; FONSECA, op. cit., p. 522.

[86] MANGETH; NUNES; MAGRANI, op. cit., 2018.

[87] Art. 48, da LGPD.

A *privacidade como integridade contextual*[88], elaborada pela professora Helen Nissenbaum[89], permite uma releitura da proteção dos dados pessoais[90], propondo que o trânsito das informações pessoais tem um valor social. Por meio dessa análise, a integridade do fluxo informacional será determinada quando respeitadas as legítimas expectativas do titular dos dados. Propõe-se que a proteção dos dados pessoais deve ser compreendida sob as lentes das práticas sociais e não individuais[91].

Com isso, há um *consentimento contextual*[92], que como bem traçado por Bruno Bioni "(...) não é delimitado por um propósito específico e duro - em linha com o que dispõe a expressão finalidades determinadas -, mas direcionado a uma gama de ações passíveis de serem executadas no contexto de uma relação"[93]. Explicando melhor, o titular exerce domínio sobre seus dados, ainda que sem declarar sua vontade, se estes forem tratados de acordo com as suas legítimas expectativas.

De forma complementar, como bem explicam Laura S. Mendes e Gabriel C. S. da Fonseca:

> O intuito é adequar o consentimento com a finalidade do tratamento, porém não de forma rígida, mas sim de acordo com o contexto em que inseridos. Nesse equilíbrio, a própria natureza dos dados é levada em consideração. Caso enquadrados como sensíveis, a análise do consentimento e do tratamento ocorre a partir de parâmetros mais rígidos quanto à sua forma e à sua finalidade. Enseja-se, assim, maior cautela na própria formação de bancos de dados, pretendendo garantir qualidade, exatidão, clareza e atualização dos elementos que os compõem[94].

A privacidade contextual tem como possíveis vetores de aplicação os princípios da boa-fé e da confiança, elementos estruturantes das legítimas expectativas do titular dos dados

[88] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 198: "Dessa conjunção (contexto + integridade) é que se arquiteta uma alternativa normativa em que a proteção dos dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados pessoais".
[89] NISSENBAUM, Helen. Privacy as contextual integrity. *Washington Law Review*, v. 79, p. 119-157, 2004.
[90] BIONI, Bruno. Proteção de Dados Pessoais. O que você sabe sobre o assunto?. *GEN Jurídico*, 29 nov. 2018. Disponível em: <http://genjuridico.com.br/2018/11/29/bruno-bioni/>. Acesso em: 20 out. 2020.
[91] Id., 2020, p. 197-265.
[92] BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. (ed.). *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge: Cambridge University *Press*, 2014, p. 66: "It is time to contextualize consent by bringing the landscape into focus. It is time for the background of rights, obligations, and legitimate expectations to be explored and enriched so that notice and consent can do the work for which it is best suited". Tradução livre: "Chegou a hora de contextualizar o consentimento, dando maior foco ao panorama [em que inserido]. Chegou a hora de explorar e de enriquecer o *background* dos direitos, obrigações e legítimas expectativas para que o consentimento possa cumprir com o seu papel adequado".
[93] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 225.
[94] MENDES; FONSECA, op. cit., p. 524-525.

pessoais, tendo a própria LGPD condicionado a legitimidade e legalidade do tratamento de dados à observância da boa-fé (art. 6º, *caput*)[95]. Nas palavras de Bruno Bioni:

> A privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá a sua capacidade de livre desenvolvimento da personalidade e de participação social[96].

Por fim, é curioso notar que a privacidade contextual ao limitar a carga participativa do indivíduo converte o consentimento, de um instrumento protetivo meramente formal para que passe a ser inserido no contexto fático ao qual foi manifestado. Nessa perspectiva, como lecionam Laura S. Mendes e Gabriel C. S. da Fonseca:

> A imposição de limites materiais não aponta para banir o consentimento ou inviabilizar importantes processos de tratamento de dados. Trata-se, ao revés, de revitalizar o consentimento como instrumento legítimo para o tratamento de dados, deslocando-o de um mecanismo meramente formal para um instrumento imerso no contexto real[97].

Um dos exemplos mais citados para fins de ilustração é a criação de perfis comportamentais de correntistas de bancos para combate a fraudes e incidentes de segurança. Nesse caso, não apenas o controlador é beneficiado pela prestação de um serviço mais seguro, como também o titular dos dados, pois essa prática não só reforça a proteção de seus direitos fundamentais, como está dentro das suas legítimas expectativas[98].

4. Conclusão

Em maio de 2019, em Ottawa, no Canadá, parlamentares de diferentes países, representantes de companhias tecnológicas e testemunhas especializadas reuniram-se para

[95] Ibid., p. 524.
[96] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 229.
[97] MENDES; FONSECA, op. cit., p. 525.
[98] BIONI, Bruno Ricardo. *Proteção de dados pessoais*... op. cit., p. 241: "Algo bastante comum é a criação de perfis comportamentais dos consumidores para combater fraudes e incidentes de segurança, pelos quais se diagnosticam atividades que fogem do padrão para tratá-las como suspeitas. É por esse motivo que serviços de e-mail, rede social e instituições financeiras alertam seus clientes e, em muitos casos, bloqueiam automaticamente acessos e transações financeiras. Por exemplo, se o acesso a uma conta parte de um dispositivo diferente, se a compra supera valores e é realizada em locais que não aqueles usuais. Todos esses dados informam ações de combate a fraudes e incidentes de segurança".

participar do *International Grand Committee on Big Data, Privacy and Democracy*[99]. O intuito era, entre outros, reafirmar que os direitos à privacidade e à proteção de dados pessoais devem ser fortalecidos nas plataformas de redes sociais, especialmente por meio da prestação de contas sobre os algoritmos utilizados, assim como o uso ético dos mesmos e da inteligência artificial, a fim de evitar atividades digitais que ameacem a paz social e interfiram nos processos democráticos[100].

Acrescenta-se, ainda, o mais amplo estudo já feito acerca de monitoramento *on-line* de dados, publicado pelos pesquisadores Steven Englehardt e Arvind Narayanan[101], da Universidade de Princeton, em 2016. Através do monitoramento dos cerca de 1 milhão de sites mais acessados, concluíram pela presença de, pelo menos, 81.000 *third parties* - domínios que fogem da relação usuário-*website*, representando outras empresas que podem se beneficiar das informações coletadas -, além da predominância da prática de sincronização de *cookies*, sugerindo intensa troca de dados entre corporações e/ou organizações.

À vista disso, as breves reflexões contidas nesta pesquisa permitem demonstrar que o novo mundo da proteção de dados pessoais exigirá adequação de todas as pessoas físicas e jurídicas que coletam, transmitem, armazenam e compartilham dados pessoais de terceiros. Por esse motivo, examinou-se o alcance do consentimento na disciplina voltada à proteção de dados pessoais.

O objetivo foi investigar em que medida o consentimento é capaz de concretizar o fundamento da autodeterminação informativa, verificando sua função e suas limitações.

Não obstante o engajamento das legislações de proteção de dados em conceder uma carga participativa maior ao titular no fluxo de seus dados pessoais, por meio do consentimento, a efetividade dessa base legal tornou-se questionável para garantir a autonomia decisória do indivíduo. Nesse contexto, mencionou-se o contraste entre *gratificações imediatas* e *prejuízos mediatos/distantes* (paradoxo da privacidade) e a assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados.

Na tentativa de superar essas insuficiências do paradigma do consentimento e

[99] Em português: "Grande Comissão Internacional sobre *Big Data*, Privacidade e Democracia". Disponível em: <https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10554743>. Acesso em: 23 abr. 2021.

[100] HIRSH, Jesse. What You Need to Know about the Grand Committee on Big Data, Privacy and Democracy. *CIGI Online*, 29 mai. 2019. Disponível em: <https://www.cigionline.org/articles/what-you-need-know-about-grand-committee-big-data-privacy-and-democracy>. Acesso em: 23 maio 2021.

[101] ENGLEHARDT, Steven; NARAYANAN, Arvind. "Online Tracking: A 1-million-site Measurement and Analysis" *In*: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. *ACM Digital Library,* p. 1388-1401, 2016. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/2976749.2978313>. Acesso em: 22 abr. 2021.

adequar a proteção de dados pessoais ao mercado informacional, investigaram-se perspectivas, que se apresentam como soluções interessantes, já adotadas por atuais legislações de proteção de dados e discutidas em trabalhos acadêmicos: (*i*) *Privacy by Design* (PbD); (*ii*) princípio da *accountability*; e (*iii*) privacidade contextual.

No mais, constata-se que a garantia da autodeterminação informativa vai muito além do consentimento, como um mecanismo meramente formal. Um consentimento efetivo é aquele que está imerso no contexto real. A percepção de que a capacidade do titular de controlar suas informações é limitada pela corrida armamentista tecnológica de vigilância é crucial para lidar com os inúmeros desafios da proteção de dados pessoais.

Referências

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen. (ed.). *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge: Cambridge University Press, p. 44-75, 2014. Disponível em: <https://nissenbaum.tech.cornell.edu/papers/BigDatasEndRun.pdf>. Acesso em: 20 out. 2020.

BENNETT, Colin; RAAB, Charles D. *Revisiting "The Governance of Privacy"*: Contemporary Policy Instruments in Global Perspective. August, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086>. Acesso em: 30 out. 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno. Proteção de Dados Pessoais. O que você sabe sobre o assunto?. *GEN Jurídico*, 29 nov. 2018. Disponível em: <http://genjuridico.com.br/2018/11/29/bruno-bioni/>. Acesso em: 20 out. 2020.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 set. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 16 mai. 2020.

BRUNO, Fernanda. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles.* Disponível em:

<https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 27 ago. 2020.

COMPANY fined 150,000 euros for infringements of the GDPR. *European Data Protection Board*, 31 jul. 2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_pt>. Acesso em: 18 set. 2020.

DAVIS, Nicola. The father of modern computing: Alan Turing's legacy. *The Guardian*, 15 jul. 2018. Disponível em: <https://www.theguardian.com/science/2019/jul/15/alan-turing-father-of-modern-computing-50-pound-note>. Acesso em: 21 mai. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ENGLEHARDT, Steven; NARAYANAN, Arvind. "Online Tracking: A 1-million-site Measurement and Analysis" *In*: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. *ACM Digital Library*, p. 1388-1401, 2016. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/2976749.2978313>. Acesso em: 22 abr. 2021.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014.

GOLDSMITH, Jack L.; WU, Tim. Who Controls the Internet?: Illusions of a Borderless World. *Oxford University Press*, 2006. Disponível em: <http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf>. Acesso em: 12 set. 2020.

HIRSH, Jesse. What You Need to Know about the Grand Committee on Big Data, Privacy and Democracy. *CIGI Online*, 29 maio 2019. Disponível em: <https://www.cigionline.org/articles/what-you-need-know-about-grand-committee-big-data-privacy-and-democracy>. Acesso em: 23 maio 2021.

LIMA, Caio César Carvalho. Estudo prático sobre as bases legais na LGPD. *In*: OPICE BLUM, Renato. *Proteção de dados*: desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020.

LONDON pharmacy fined after "careless" storage of patient data. *European Data Protection Board*, 20 dez. 2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/london-pharmacy-fined-after-careless-storage-patient-data_pt>. Acesso em: 28 mai. 2020.

LOSANO, Mario G. Trasparenza e segreto: una convivenza difficile nello Stato democratico. *Diritto pubblico*, v. 23, n. 3, p. 657-682, 2017.

MANGETH, Ana Lara; NUNES, Beatriz; MAGRANI, Eduardo. Seis pontos para entender o Regulamento Geral de Proteção de Dados da UE. *ITS Rio*, 25 maio 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-proteção-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em: 2 nov. 2020.

MATTIETTO, Leonardo. *Developments on data protection in Brazilian Law*. *In*: Internet, Law & Politics: a decade of transformations, 2014, Barcelona. Anais… Barcelona: Universitat

Oberta de Catalunya, 2014, p. 329-340. Disponível em: <https://www.researchgate.net/profile/Leonardo_Mattietto/publication/335210920_Developments_on_data_protection_in_Brazilian_law/links/5d573a02299bf151bad9b82a/Developments-on-data-protection-in-Brazilian-law.pdf>. Acesso em: 30 nov. 2020.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *Revista Estudos Institucionais*, Rio de Janeiro, v. 6, n. 2, p. 507-533, 2020. Disponível em: <https://estudosinstitucionais.com/REI/article/view/521>. Acesso em: 14 out. 2020.

MURARO, Igor S. A importância do privacy by design e privacy by default nas aplicações: O que podemos aprender com o caso Zoom. *Jota*, 2 mai. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-importancia-do-privacy-by-design-e-privacy-by-default-nas-aplicacoes-02052020#_ftn4>. Acesso em: 4 ago. 2020.

NISSENBAUM, Helen. Privacy as contextual integrity. *Washington Law Review*, v. 79, p. 119-157, 2004.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSEMAIN, Mathieu. Tribunal francês confirma multa de 50 mi de euros ao Google por violação de privacidade. *Thomson Reuters Brasil*, 2020. Disponível em: <https://br.reuters.com/article/internetNews/idBRKBN23Q2WJ-OBRIN>. Acesso em: 5 jul. 2020.

SCHREIBER, Anderson. *Direitos da Personalidade*. 2. ed. São Paulo: Atlas, 2013.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo (coord.). *Lei Geral de Proteção de Dados Pessoais*: e suas repercussões no Direito brasileiro. São Paulo: Revista dos Tribunais, 2019, p. 287-322. Disponível em: <https://www.academia.edu/40321216/Consentimento_e_proteção_de_dados_pessoais_na_LGPD>. Acesso em: 29 out. 2020.

WIMMER, Miriam. Dados Pessoais - Repensando o consentimento: Resenha ao livro 'Proteção de Dados Pessoais: a função e os limites do consentimento', de Bruno R. Bioni. *Jota*, 24 dez. 2018. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/dados-pessoais-repensando-o-consentimento-24122018>. Acesso em: 22 out. 2020.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, v. 30, n. 1, p. 75-89, 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 20 set. 2020.

Recebido em: 13/08/2021.
1° parecer em: 18/10/2021.
2° parecer em: 29/10/2021.