UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Rafael Scaroni Garcia

A MERCADORIA É VOCÊ: O USO SECUNDÁRIO DE DADOS PESSOAIS

Porto Alegre

2020

Rafael Scaroni Garcia

A MERCADORIA É VOCÊ: O USO SECUNDÁRIO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Orientador: Professor Doutor Fabiano Menke.

Porto Alegre

2020

Rafael Scaroni Garcia

A MERCADORIA É VOCÊ: O USO SECUNDÁRIO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Orientador: Professor Doutor Fabiano Menke.

Aprovada em 20 de novembro de 2020.

BANCA EXAMINADORA:

_____

Professor Doutor Fabiano Menke

Orientador

_____

Prof. Dr. Luis Renato Ferreira da Silva

_____

Prof. Dr. Guilherme Carneiro Monteiro Nitscke

AGRADECIMENTOS

Por muito tempo pensei eu nesta parte do meu trabalho de conclusão. Nós, muitas vezes, esquecemos de reconhecer as atitudes de quem nos quer bem, desincentivando estas pessoas a continuarem trilhando os caminhos da vida ao nosso lado.

Nós nunca deixamos de ser nós mesmos, como esclarece um dos autores citados nesta monografia. A isto, adicione-se que nós somos s soma das pessoas que em nossas vidas passaram, construindo o que nós chamamos, juridicamente, de personalidade.

Tenho eu a grande sorte de estar sempre rodeado de professores. Seria impensável começar esta parte agradecendo outras pessoas que não os mais importantes deles: meus pais, Ana Paula Romero Scaroni e Jaime Gross Garcia, de quem sempre escutei que o conhecimento é a única coisa que ninguém pode tirar de mim – nisso que eles tanto investiram, seja em tempo, carinho, dedicação e dinheiro, e que este trabalho seja, provavelmente, o ápice, até este momento, disto tudo. Junto a eles, na minha família mais próxima, pouco eu seria sem meus irmãos, Bárbara e Igor – ela com quem eu nunca deixei de brigar e de me entender e ele com quem, depois de quatorze anos, reaprendi o que é o amor de verdade. À Jessica Jung, pelo companheirismo e pelo amor de todas as horas, por me mostrar que crescer e aprender junto de quem se ama não tem preço. Ao Miguel e à Sandra, meus padrasto e madrasta, que cuidam dos meus pais e, por consequência, de mim também. À Luna e à Amora, por terem me acompanhado nas inúmeras horas de estudo durante estes cinco anos, muitas vezes dormindo em cima dos meus livros ou do meu computador, sempre pedindo atenção e carinho.

Ao Fabiano Menke, professor, orientador, mestre – qualquer adjetivação é insuficiente para expressar a grandeza deste sujeito ímpar. Muito do que sei na área jurídica, especialmente do Direito Privado, pude aprender, discutir e aperfeiçoar pelas oportunidades e portas que ele me abriu. A generosidade e o caráter impecável, com um senso de justiça e uma tecnicidade incríveis, fizeram destes anos muito melhor aproveitados. As horas de voo, digo, de estudos, são demonstradas, por ele, na prática, com tamanho afinco às ciências jurídicas. São irrestritos e enormes meus agradecimentos e minha admiração a ele, que faz questão de reconhecer na frente de todos e toma todos os cuidados para tratar das melhorias em separado.

Aos professores desta faculdade, sem os quais jamais chegaria até aqui, especialmente àqueles que tive maior contato. Ao Klaus Koplin, com quem tive o privilégio de aprender não só a respeito do processo civil, mas também quanto ao pensamento crítico necessário ao aprimoramento dos institutos jurídicos no Brasil. Um exemplo de ser humano, cujas provocações continuam a me causar dúvidas e de quem eu torcia que as aulas nunca acabassem.

À Daniela Cravo, pelo modelo de dedicação à pesquisa e à boa dogmática, além das lições sobre a necessidade da humanização do Direito. Aos professores Luis Fernando Barzotto e Luis Renato Ferreira da Silva, tanto pelas oportunidades abertas e pelos ensinamentos no tocante à historicidade dos institutos que analisamos, quanto pela importância do estudo da filosofia. Ao professor Pablo Alflen, pelo exemplar conhecimento da área penal e processual-penal, além das possibilidades a mim oferecidas em assistir aulas suas que eu originalmente não teria acesso. À professora Vanessa Chiari, modelo de seriedade e de sabedoria, que busca sempre a excelcência.

Ao Marcus Boeira e ao Filipe Speck, pessoas que eu tive a sorte em conhecer nestes cinco anos e que, hoje, são parte da família. Meu muito obrigado pelos jantares, encontros e almoços acompanhados de profundas discussões a respeito de temas que muito me atormentam.

Aos meus grandes amigos desde a época mais longínqua, Bruno Tabosa, Leonardo Facini, Lucas De Conti, Guilhermo Müller, Gustavo Gasparotto, Rodrigo Villela, Marcelo Bier e Gustavo Francisco, pela amizade, pelas conversas e pelos encontros que fazem meus dias mais leves e felizes.

A todos, meus mais sinceros agradecimentos. Eu, sem dúvidas, não teria chegado até aqui se não fosse por cada um de vocês.

Aos meus avós, Maria do Carmo Romero Scaroni e Amador Antônio Scaroni, que, mesmo sem nem mesmo completarem o ensino fundamental, eram leitores vorazes e duas das pessoas mais inteligentes que já conheci. *In memorian*.

“E assim a consciência faz todos nós covardes
E assim a cor nativa da resolução
Ganha o tom doentio do pensamento pálido
E empreitadas de grande vigor e valor,
Com tais ponderações, suas águas ficam turvas,
E perdem o nome de ação”.
(Hamlet, Ato III, Cena I, 83-88).

“Com efeito, o resultado direto e legal da consciência é a inércia”.
(Fiódor Dostoiévski, em Memórias do Subsolo)

“De fato o senhor está detido, mas não como um ladrão é detido. Quando se é detido como um ladrão, então é ruim, mas esse tipo de detenção... a mim me parece algo de sábio (...) que não entendo, mas que também não é preciso entender”.
(Franz Kafka, em O Processo).

RESUMO

O presente estudo tem, por objetivo, verificar se há compatibilidade entre a proteção de dados e o uso de dados para uma finalidade distinta daquela originalmente autorizada, especificamente no Direito Civil. Por meio do método dedutivo de abordagem, e pela pesquisa bibliográfica como método de procedimento, as duas hipóteses levantadas são, por um lado, que não há compatibilidade porque são situações mutuamente excludentes e, por outro, que a compatibilidade é possível desde que observados alguns critérios. Para responder à questão, optou-se pela divisão em dois capítulos, divididos em dois subcapítulos. O primeiro aborda a datificação da sociedade e seus impactos no Direito, fazendo um diálogo entre os autores que procuram explicar como nos organizamos socialmente a partir das informações pessoais, além de definir o que seja uso secundário de dados pessoais e analisar os princípios aplicáveis das legislações de proteção de dados pessoais. O segundo capítulo versa especificamente da maneira pela qual este assunto é tratado pelo Direito, debatendo os limites do consentimento e a necessidade de uma tutela coletiva de dados pessoais, que diminua o ônus protetivo do indivíduo. Ao final, concluiu-se pela hipótese da compatibilidade entre a proteção de dados e uso secundário de dados pessoais, estabelecendo-se critérios tanto para a proteção individual, quanto para a proteção coletiva, com especial relevo a esta última. Assim, se torna possível a conciliação entre os dois fundamentos da Lei Geral de Proteção de Dados: o desenvolvimento econômico e a proteção da privacidade.

Palavras-chave: Uso secundário de dados. Proteção de dados pessoais. Princípio da Finalidade.

ABSTRACT

This study aims to verify if there is compatibility between data protection and the use of data for a purpose other than the one originally agreed, specifically in Civil Law. Through the deductive method, and thorough bibliographic research as procedure method, two hypotheses are raised: that there is no compatibility because the situations are mutually excluding, or that the compatibility is possible since some criteria are observed. To answer this question, this study was divided in two chapters, both divided in two subchapters. The first one addresses societies datification and its impacts in law, dialoging between authors trying to explain how we socially organize in the context of personal information, besides defining what secondary use of data is and analyzing the principles being applied by the data protection laws. The second chapter addresses how do law deals with this subject, debating the limits of consenting and the necessity of a collective guardianship of personal data, that reduces the individual's protective burden. In the end, it is concluded by the hypothesis of compatibility between the use for a purpose other than the one originally agreed and personal data protection, establishing some criteria, both for individual and collective protection. Therefore, the conciliation between two of the fundaments of General Data Protection Law becomes possible: the economic development and the privacy protection.

Keywords: Secondary use of data. Personal data protection. Purpose Limitation Principle.

Sumário

Introdução

Os dados pessoais são o ativo econômico mais valioso da sociedade do século XXI. Constantemente chamados de *novo petróleo*, são extraídos diretamente de comportamentos, ações e toda a miríade i(ni)maginável de situações relacionadas a seres-humanos e a coisas – como ocorre, por exemplo, na *Internet das Coisas*.

O mercado de dados pessoais é constantemente aprimorado, e melhor azeitado quanto maior a quantidade de dados a serem tratados. O expediente de coleta massiva de dados, cristalizado na figura dos *data brokers*, tornou-se lucrativo, com o propósito de extrair o máximo possível de informações a respeito dos indivíduos, estabelecendo perfis para realizar predições mais assertivas. A característica fundamental desta nova era é a velocidade de processamento e o barateamento do armazenamento: as novas tecnologias da informação e da comunicação, munidas de um poder computacional de processamento que cresce a cada ano, tornam possíveis correlações que jamais seriam cogitadas. Isto possibilitou o surgimento do *Big Data*, ponto fulcral no processo econômico atual.

Desta maneira, as empresas são estimuladas a utilizar as informações pessoais para finalidades além daquelas que serviram de base para sua coleta – o chamado uso secundário dos dados. Vendo estes como um direito de personalidade, cabe a provocação de que a mercadoria, neste novo ambiente de negócios, somos nós, titulares dos dados. Há, neste cenário, um aparente contraste entre a proteção dos dados pessoais e o desenvolvimento econômico.

Assim, este trabalho visa responder à seguinte pergunta: é possível compatibilizar a proteção de dados pessoais e o uso de dados para uma finalidade distinta da originalmente autorizada? São duas as hipóteses possíveis: i) não há como compatibilizar, pois são situações mutuamente excludentes; ii) há como compatibilizar, devendo-se estabelecer critérios a partir do ordenamento jurídico já existente.

O objetivo desta monografia é verificar se existe compatibilização possível entre proteção de dados e uso para finalidades diversas da original, tendo em vista que este é extremamente valioso no mercado de dados. O método de abordagem a ser utilizado para solucionar o problema é o dedutivo, buscando-se a melhor maneira de tratar o uso secundário de dados nos futuros casos concretos. O método de procedimento é essencialmente a pesquisa bibliográfica, com o propósito de buscar textos doutrinários e jurisprudência que possam, com base no objetivo, responder à pergunta de pesquisa.

Este estudo tem, como escopo, o Direito Civil. Poder-se-ia tratar de uso de informações para além de sua finalidade em diversos campos do Direito, especialmente no Direito Penal[1]. Esta delimitação se justifica tanto porque a regulação da proteção de dados tem sido uma atribuição do Direito Civil[2], quanto porque é esta área do Direito que teve, com sua tradição histórico-romanística sua condição de um produto da cultura e do humanismo, capacidade para se adaptar e oferecer soluções a novos problemas[3].

Para dividir o trabalho, optou-se pelo método francês, com dois capítulos subdivididos em dois subcapítulos. Na primeira parte, explicar-se-á o fenômeno dos dados e o impacto que eles causam no Direito a partir do objetivo estabelecido pelo estudo. Para isto, o primeiro subcapítulo buscará organizar um diálogo entre os autores que procuram explicar como socialmente nos organizamos a partir das informações pessoais e os inerentes impactos que isto implica. Além disso, se analisará brevemente a jurisprudência do STJ, da Suprema Corte dos Estados Unidos da América, do STF e do Tribunal Constitucional Federal Alemão no que diz respeito a maneira de lidar com o processo formativo da sociedade da informação.

Ainda na primeira parte, o segundo subcapítulo tratará especificamente do uso secundário de dados pessoais, dos princípios da necessidade e da finalidade – elemento definidor do conceito cerne desta monografia. Com o propósito de ser possível um controle na aplicação principiológica, adotar-se-á a teoria de Humberto Ávila como vetor interpretativo desta espécie normativa, a fim de evitar seu uso indiscriminado a justificar qualquer tipo de decisão. Ademais, será feita uma pequena regressão histórica para se entender a razão da centralidade dos princípios nas legislações de proteção de dados.

Na segunda parte, buscar-se-á o enquadramento legal da problemática com vistas ao estabelecimento de critérios que possam vir a resolvê-la. Para isto, o primeiro subcapítulo trata do problema do enfoque estritamente individual da proteção de dados pessoais, especialmente no que tange ao consentimento. Para justificar a necessidade de uma proteção coletiva, se analisa as gerações de leis de proteção de dados pessoais, além dos problemas cognitivos e estruturais trazidos pelo dilema do auto-gerenciamento – dialogando com a teoria da

---

[1] Neste sentido, há, no Congresso Nacional, uma comissão de juristas elaborando proposta para o que se convencionou chamar de *LGPD Penal*, tratando de dados pessoais para segurança pública, defesa nacional e investigação de infrações penais. Vide IGNACIO, Laura. **Comissão de juristas elabora proposta para a LGPD penal**. Disponível em: <https://valor.globo.com/legislacao/noticia/2020/09/15/comissao-de-juristas-elabora-proposta-para-a-lgpd-penal.ghtml> Acesso em 10 out. 2020. O anteprojeto foi entregue ao presidente da Câmara, Rodrigo Maia, em 5 de novembro de 2020.

[2] RODRIGUES JR., Otavio Luiz. **Direito Civil Contemporâneo**: estatuto epistemológico, constituição e direitos fundamentais. Rio de Janeiro: Forense Universitária, 2019, p. 120.

[3] *Ibid*, p. 115.

integridade contextual. Por fim, investiga-se o legítimo interesse, e o teste que lhe é intrínseco, como base legal autorizativa.

O quarto, e último, subcapítulo, busca conciliar a proteção de dados e o desenvolvimento econômico por meio da estipulação de critérios que possibilitem o uso de dados pessoais para finalidades distintas da originalmente estabelecida. A abordagem será dividida entre a proteção individual, com base na ideia de obrigação como processo e norteada pela boa-fé objetiva, e a proteção coletiva, entendida como a retirada de encargos dos indivíduos, com base ou em nova base legal autorizativa distinta do consentimento do titular, ou do acolhimento, pelo ordenamento brasileiro, do teste de proporcionalidade trazido pelo GDPR.

1 O fenômeno da datificação e seus impactos no Direito

1.1 Sociedade de dados

A criação, análise e tomada de decisão a partir de dados[4] é um fenômeno tão antigo quanto a humanidade; a escrita foi desenvolvida na antiga Mesopotâmia justamente porque se desejava uma ferramenta eficiente para registro e observação de informações[5]-[6]. Há, entretanto, uma grande mudança observada no mundo em que vivemos: a transição do analógico para o digital[7]. A elevação dos dados a elemento central do desenvolvimento econômico é a ímpar consequência deste fenômeno[8].

Para se ter uma ideia, 25% das informações eram digitais no ano de 2000. Este número subiu para 93% em 2007 e chegou a mais de 98% em 2013[9]. Análises apontam que a quantidade de dados existentes em 2020 chegará a 59 zetabytes[10] (em bytes, são vinte e uma casas decimais multiplicadas por cinquenta e nove). Para tornar este número menos abstrato, estas informações se estenderiam em 230 pilhas de CD-ROMs da superfície da Terra até a da Lua – ou cobririam toda a superfície dos Estados Unidos da América, caso impressas em livros, em uma camada de 2392 páginas[11]. Aliando isto ao fato de que a quantidade de informações geradas cresce quatro vezes mais rápido que a economia mundial – e a capacidade de processamento dos

---

[4] Neste trabalho, usar-se-á os termos *dado* e *informação* como sinônimos; sobre isto, Danilo Doneda define que "o conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização". 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, p. 136. O mesmo autor distingue os conceitos: dado seria uma pré-informação, uma informação em estado potencial, enquanto a informação representa algo além do que está representado no dado, no limite da cognição. *Ibid*, p. 136.

[5] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 14.

[6] Para uma interessantíssima análise histórica a respeito da informação, vide-se: GLEICK, James. **The Information**: a history, a theory, a flood. Nova Iorque: Pantheon Books, 2011.

[7] Aqui, cabe lembrar que a LGPD se aplica *também* aos meios digitais, e não somente a eles: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, **inclusive nos meios digitais**, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

[8] Bruno Bioni faz um histórico dos componentes primários desde a sociedade agrícola: BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 3 -5.

[9] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 8 – 9.

[10] STATISA. **Volume of data/information created worldwide from 2010 to 2024**. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/> Acesso em 15 set. 2020.

[11] Os exemplos não são criações do autor; eles foram atualizados a partir dos dados trazidos em MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 9.

computadores, nove vez mais[12] -, têm-se uma preocupação cada vez maior com a proteção desses dados[13].

Tendo em vista que os humanos pensam em forma de narrativa[14] e que a narração exerce uma seleção, só admitindo determinados acontecimentos[15], diversos autores têm tentado definir esta sociedade inundada por dados: desde sociedade da informação[16]-, sociedade de redes[17], passando pela era do capitalismo da vigilância[18], pela era da psicopolítica[19], pela reinvenção do capitalismo na era do *Big Data*[20] ou mesmo pela economia do *Big Data*[21]. Todavia, todos estes

---

[12] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 9.

[13] Daniela Cravo deixa clara esta questão: "A não formulação e implementação de salvaguardas quanto ao uso dos dados pode gerar várias consequências que violam os direitos de personalidade dos indivíduos e colocam em xeque a livre concorrência e o equilíbrio do mercado". CRAVO, Daniela Copetti. **Direito à portabilidade de dados**: interface entre defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018, p. 5. Este livro deriva da Tese, por ela defendida, nesta Faculdade de Direito. A citação deste trecho na tese é a seguinte: CRAVO, Daniela Copetti. **Direito à portabilidade de dados**: necessidade de regulação ex ante e ex post. Tese (Doutorado em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2018, p. 18.

[14] HARARI, Yuval Noah. **21 lições para o Século 21**. São Paulo: Companhia das Letras, 2018, p. 21. No campo específico da narrativa jurídica, é seminal o texto de COVER, Robert M. **The Supreme Court, 1982 Term – Foreword: Nomos and Narrative**. Harvard Law Review, v. 97, n. 4, 1983 – 1984. Nele, o autor discorre sobre como o universo normativo do Direito é influenciado pelas diferentes narrativas possíveis.

[15] HAN, Byung-Chul. **Sociedade da transparência**. 4 reimp. Petrópolis: Vozes, 2019, p. 75.

[16] Também conhecida como 4ª Revolução Industrial, advinda com a internet e a digitalização da sociedade, como esclarece Otávio Luiz Rodrigues Jr. em RODRIGUES JR., Otavio Luiz**. Direito Civil Contemporâneo**: estatuto epistemológico, constituição e direitos fundamentais. Rio de Janeiro: Forense Universitária, 2019, p. 49. É o termo mais utilizado pela doutrina brasileira. Toma-se, por todos: BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 5 e ss.; 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, p. 47 e ss., DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, jul./dez. 2011, p. 92.

[17] CASTELLS, Manuel. **Ruptura**: a crise da democracia liberal. Rio de Janeiro: Zahar, 2018, e-book, posição 382. O autor também usa o termo *sociedade-rede*.

[18] *Age of surveillance capitalism*, no original, em inglês: ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019. A autora a define da seguinte maneira: "*A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction and sales; a parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; a rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; the foundational framework of a surveillance economy; as significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; the origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; a movement that aims to impose a new collective order based on total certainty; an expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty.*" *Ibid,* p. V.

[19] Enunciada pela possibilidade de decifrar modelos de comportamento a partir do Big Data. HAN, Byung-Chul**. No enxame**: perspectivas do digital. 2 reimp. Petrópolis: Vozes, 2019, p. 132.

[20] No original em inglês, *reinventing capitalism in the age of Big Data*. Os autores o defendem da seguinte maneira: "The reboot of the Market fueled by data will lead to a fundamental reconfiguration of our economy, one that will be arguably as momentous as the Industrial Revolution, reinventing capitalism as we know it". MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. Londres: John Murray, 2019, p. 4 -5.

[21] O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. Londres: Penguin Books, 2017, p. 3.

autores têm, como base comum, a constatação de que o custo para o tratamento, a coleta e o armazenamento dos dados é cada vez menor, e os limites tradicionais a estas operações – como a dificuldade de encontrar determinadas informações quando se tem uma base física - praticamente não existem mais.

É neste sentido que frequentemente se faz referência aos quatro V do *Big* Data: os computadores atuais processam dados de forma mais veloz, veraz, variada e volumosa[22]. Nisto se vislumbra uma mudança quantitativa e uma qualitativa: a primeira diz respeito à força bruta, ao poder de processar mais dados em menos tempo; a segunda, na aplicação de técnicas sofisticadas a este processamento de forma a obter resultados mais valiosos[23].

Interessante notar que a sociedade em que vivemos não *criou* novos dados; ela possibilitou que mensuremos, em números, situações antes corriqueiras[24], colocando as informações em um formato que possibilite o seu uso de diversas maneiras distintas. A este fenômeno se convencionou chamar de *datificação*[25].

Desta maneira, as formas de utilização dos dados se multiplicam em razão da capacidade de processamento e de armazenamento, trazendo maior utilidade às informações e resultando na inexistência de dados insignificantes ou que não mereçam proteção[26]. Consequentemente,

---

[22] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 25. Neste mesmo sentido: BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 34 e TSAI, Chun-Wei; LAI, Chin-Feng; CHAO, Han-Chieh; VASILAKOS, Athanasios. Big data analytics: a survey. **Journal of Big data**, n. 2, 2015, p. 2 e ss.

[23] 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, p. 151.

[24] Exemplo disto é um banco de carro que, com 360 pontos de medição e com um sistema de medição que vai de 0 a 256 em cada um destes pontos, conseguem determinar quem está sentado com 98% de precisão. MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 77.

[25] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 15 e p. 73 – 98.

[26] BVerfGE 65, 1, "Recenseamento" (*Volkszählung*). MARTINS, Leonardo. (org.) **Cinqüenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245. É o consenso a que chegou à doutrina, após a famosa decisão do censo de 1983 da Corte Constitucional alemã ter afirmado isto. Ver, por todos, FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 33. e MENDES, Laura Schertel. **A encruzilhada da proteção de dados no Brasil e o caso do IBGE**. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020> Acesso em 15 ago. 2020. A *ratio* da LGPD, ao adotar um conceito expansionista de dado pessoal em seu artigo 5º, a partir do qualitativo *identificável*, mostra preocupação com este fenômeno. Semelhante técnica legislativa já havia sido adotada no Brasil anteriormente em dois momentos: no Decreto nº 8.771/2016 (Decreto do Marco Civil da Internet) no artigo 14, I, e na Lei de Acesso à Informação, artigo 4º, I. Para explicação mais detalhada deste tema, vide BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 59 – 61.

se possibilita transformar informação dispersa em informação organizada[27], havendo uma completa reformulação da disciplina jurídica da informação em razão do desenvolvimento da informática[28].

Para o melhor proveito destes dados são necessários modelos matemáticos – algoritmos, por exemplo -, nada mais sendo que uma representação abstrata de certo processo, desde um jogo de baseball até a cadeia de fornecimento de determinada empresa[29]. Estes modelos são, necessariamente, simplificações: são escolhidos os parâmetros mais importantes para exprimir determinado fenômeno fazendo com que, inevitavelmente, informações importantes fiquem de fora, criando os pontos cegos.

Estes pontos cegos refletem a prioridade de seus criadores e podem, ou não, ser problemáticos[30]. Os exemplos de situações perigosas são vários: desde acusações realizadas por algoritmos[31], passando pela polarização a partir de um modelo de recomendação[32], até a utilização da moda e do design como uma maneira de se proteger de possíveis arbitrariedades[33]. Ainda mais grave, Mounk coloca as redes sociais e seus algoritmos como um dos três pilares para a recessão democrática[34] que vivemos, tal como Bartlett defende que uma adoção irrefletida dos modelos de *big techs* causa uma erosão paulatina da democracia[35]. Nesse mesmo sentido, Doneda afirma que a privacidade é o pressuposto de uma sociedade democrática moderna[36].

---

[27] 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, p. 137.
[28] *Ibid*, p. 149.
[29] O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. Londres: Penguin Books, 2017, p. 18.
[30] O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. Londres: Penguin Books, 2017, p. 20 – 21. Havendo problemas, opacidade e escala, a autora classifica o modelo como uma *Arma de Destruição Matemática*, ou *Weapon of Math Destruction*, em inglês.
[31] HILL, Kashmir. **Wrongfully Accused by an Algorithm**. Disponível em: <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> Acesso em 4 ago. 2020.
[32] ROOSE, Kevin. Rabbit Hole: what is the internet doing to us?. Disponível em: <https://www.nytimes.com/column/rabbit-hole> Acesso em 10 ago. 2020.
[33] SEABROOK, John. **Dressing for the Surveillance Age**. Disponível em: < https://www.newyorker.com/magazine/2020/03/16/dressing-for-the-surveillance-age> Acesso em 18 mar. 2020.
[34] Os outros dois pilares seriam a estagnação do padrão de vida e o medo da democracia multiétnica. MOUNK, Yasha. **O Povo contra a Democracia**: por que nossa liberdade corre perigo e como salvá-la. São Paulo: Companhia das Letras, 2019, p. 130. Há um pertinente artigo analisando o contexto brasileiro a partir do ponto de vista de um estrangeiro que vale menção: KEMENY, Richard. **Brazil is sliding into techno-authoritarism**. Disponível em: <www.technologyreview.com/2020/08/19/1007094/brazil-data-privacy-cadastro-base/> Acesso em 20 ago. 2020.
[35] BARTLETT, Jamie. **The people vs. tech**: how the internet is killing democracy. Londres: Ebury, 2018, p. 7 – 8. Em sentido semelhante, vide MOORE, Martin. **Democracy hacked**: political turmoil and information warfare in the digital age. Londres: Oneworld, 2018, especialmente a Parte 3, onde o autor trata de futuros alternativos: a *platform democracy*, a *surveillance democracy* e a *democracy rehacked*.
[36] 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, p. 128 – 129.

Fundamental enfatizar que os dados são os insumos destes modelos; eles são os *inputs* para que seja gerado determinado resultado (os *outputs*) – tipicamente predições comportamentais. À vista disto, quanto mais dados forem utilizados, maior será a precisão da previsão e, portanto, mais valioso o resultado e o modelo.

A quantidade de dados, além de aumentar a predictibilidade, também funciona como uma maneira de aprimoramento do próprio modelo – sendo este um exemplo de *machine learning*, definido, de maneira ampla, como métodos computacionais que utilizam da experiência para melhorar a *performance* ou para realizar previsões mais precisas[37].

Esta situação, segundo Shoshana Zuboff, é o início do capitalismo da vigilância a partir do que ela chamou de *behavioral surplus*[38] – ou excedente comportamental. O que ocorre é uma coleta de dados mais ampla do que seria necessária[39], alimentando o *machine learning* que vai trazer, como *output*, previsões a respeito do comportamento do usuário – muitas vezes em forma de um perfil[40] daquele indivíduo. Este produto, então, será vendido em mercados de comportamentos futuros, configurando uso secundário destes dados, pois distinto da finalidade originalmente aprovada. A metáfora de Dostoiévski do homem como pedal de órgão, que não mais deseja por ser completamente previsível, está muito próxima de se concretizar[41].

---

[37] MOHRI, Mehryar; ROSTAMIZADEH, Afshin; TALWALKAR, Ameet. **The Foundations of machine learning**. 2 ed. Cambridge: The MIT Press, 2018, p. 1.

[38] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019, p. 97.

[39] Violando, em termos de LGPD, o princípio da minimização, ou da necessidade, trazido no artigo 6º, III: Art. 6º, 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;

[40] Sobre o tema do *profiling*, Clarissa Fernandes de Lima defendeu, nesta faculdade, uma importante monografia sobre o tema: LIMA, Clarissa Fernandes de. **O profiling e a proteção de dados pessoais**. Trabalho de Conclusão (Graduação em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019.

[41] "Se realmente se encontrar um dia a fórmula de todas as nossas vontades e caprichos, isto é, do que eles dependem, por que leis precisamente acontecem, como se difundem, para onde anseiam dirigir-se neste ou naquele caso, etc etc, uma verdadeira fórmula matemática, então o homem será capaz de deixar de desejar, ou melhor, deixará de fazê-lo, com certeza. Ora, que prazer se pode ter em desejar segundo uma tabela? Mais ainda: no mesmo instante, o homem se transformará num pedal de órgão ou algo semelhante; pois, que é um homem sem desejos, sem vontades nem caprichos, senão um pedal de órgão? Que pensais disso? Calculemos as probabilidades: pode tal coisa acontecer ou não?". DOSTOIÉVSKI, Fiódor. **Memórias do Subsolo**. 6 ed.. São Paulo: Editora 34, 2009, p. 39 – 40. O livro foi publicado em 1864. Como já havia também profetizado Umberto Eco: "se a arte reflete a realidade, é fato que a reflete com muita antecipação. E não há antecipação – ou vaticínio – que não contribua de algum modo a provocar o que anuncia". ECO, Umberto. **Obra Aberta**. São Paulo: Perspectiva, 1969, p. 18.

É neste contexto que se estrutura a economia baseada em dados (*data-driven economy*) e que a figura dos *data brokers*[42] se mostra essencial: a lógica dos modelos preditivos e do *Big Data*, de acumular a maior quantidade possível de dados, faz com que surja este novo ator[43].

Em um importante relatório a este respeito, a *Federal Trade Commission* estado-unidense chegou a relevantes descobertas a respeito dos *data brokers*. Dentre elas, destacam-se, dentro do escopo deste trabalho[44]:

> (i) Os *data brokers* combinam dados obtidos online e off-line para atingirem consumidores online;
> (ii) Grande parte da coleta dos dados ocorre sem o consentimento dos indivíduos;
> (iii) As principais utilizações comerciais dos dados são para *marketing*, serviços de mitigação de riscos e serviços de localização de pessoas;
> (iv) A indústria de dados é complexa, com muitas camadas de *data brokers* que oferecem e trocam dados uns com os outros, sendo usual o intercâmbio e a compra e venda de informações entre eles;
> (v) Os *data brokers* coletam e armazenam bilhões de dados que, quando a pesquisa foi realizada, já cobriam praticamente todos os consumidores estado-unidenses;
> (vi) Os *data brokers* coletam mais informações do que utilizam;
> (vii) Uma das utilizações mais usual dos dados é no desenvolvimento de modelos complexos para prever comportamentos e para extrair inferências potencialmente sensíveis a respeito dos consumidores;
> (viii) As escolhas que os *data brokers* oferecem aos consumidores sobre os seus dados são invisíveis e incompletas, com grande falta de transparência.

Há, assim, um *trade-off,* uma troca: os usuários "pagam" por estes serviços com seus dados pessoais; é o que se convencionou chamar de *zero-price advertisement business model*[45] – e o que origina o título deste trabalho. Há uma imensidão de contratos de Direito Privado celebrados quotidianamente no Brasil e em todo mundo que envolve os serviços *over-the-top-content*[46].

---

[42] *Data brokers* são agentes cuja atividade única é a coleta e o processamento de dados ou a venda, a revenda ou o compartilhamento de dados, sem qualquer interação com os titulares dessas informações. Sobre o tema há um valioso episódio de *podcast*: GOULART, Guilherme; SERAFIAN, Vinicius. **Data brokers, privacidade e discriminação**. Disponível em: <https://www.segurancalegal.com/2014/06/episodio-52-databrokers-privacidade-e-discriminacao/> Acesso em 20 set. 2020.

[43] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 26.

[44] FEDERAL TRADE COMMISSION. **Data Brokers**: A call for Transparency and Accountability. 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may- 2014/140527databrokerreport.pdf.> Acesso em: 10 jul. 2020, p. 46 – 49.

[45] STRANDBURG, Katherine J.. **Free Fall: The Online Market's Consumer Preference Disconnect**. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2323961> Acesso em 5 jul. 2020, p. 96.

[46] É o que explica Otávio Luiz Rodrigues Jr: "Esse ato é associado a uma contratação de um serviço, em geral não oneroso ou com preços relativamente módicos, **posto que o utilizador remunere indiretamente a empresa com seus dados pessoais**, a cessão de informações a terceiros sobre seus hábitos de consumo ou a visualização compulsória de publicidade" (Grifei). RODRIGUES JR., Otavio Luiz**. Direito Civil Contemporâneo**: estatuto epistemológico, constituição e direitos fundamentais. Rio de Janeiro: Forense Universitária, 2019, p. 128.

Isto explica o fato de as empresas estarem se reinventando para se tornarem intermediárias de dados[47]. Este modelo de negócios é extremamente intrusivo[48], com autores defendendo que a violação da privacidade e dos dados pessoais se tornou um lucrativo negócio, baseado na extração e monetização de dados[49] a partir de modelos que se retroalimentam[50]. Neste sentido, Doneda alerta para o risco de chegarmos à *commodification* dos dados pessoais – a transformação deles em uma *commodity*[51]. Defende o autor, juntamente com Schertel Mendes, que os dados pessoais jamais poderão ser considerados como mera *res in commercium*[52].

O tratamento de dados pessoais, já caracterizado como uma atividade de risco[53] que se concretiza na utilização dos dados sem o conhecimento do titular das informações[54], se torna ainda mais perigoso[55] em virtude da opacidade destas operações. A transparência foi alicerçada pela LGPD como um dos princípios que devem ser observados nas atividades de tratamento[56] pela preocupação com o respeito à legítima expectativa do titular e com o controle deste em relação aos dados que lhe dizem respeito[57], principalmente quando inseridos em banco de dados.

---

[47] MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. Londres: John Murray, 2019, p. 149.
[48] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 27.
[49] Este tema é tratado, com foco no conceito e nas funções da *privacy* estado-unidense, em RODRIGUES JR., Otavio Luiz**. Direito Civil Contemporâneo**: estatuto epistemológico, constituição e direitos fundamentais. Rio de Janeiro: Forense Universitária, 2019, p. 119 e ss.
[50] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 29. O modelo é, justamente, a necessidade de mais dados para previsões mais assertivas, que gera um grande poder econômico e incentiva a violação da privacidade.
[51] 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, p. 297.
[52] DONEDA, Danilo; MENDES, Laura Schertel. Reflexões iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, nov./dez. 2018, p. 4.
[53] Para uma visão histórica a respeito do risco, ver BERNSTEIN, Peter L. **Against the Gods**: the remarkable story of risk. Hoboken: Wiley, 1998.
[54] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, jul./dez. 2011, p. 92.
[55] É o que defende, por exemplo, Nelson Rosenvald: ROSENVALD, Nelson. **Do risco da atividade ao "alto" risco da atividade algorítmica**. Disponível em: < https://www.nelsonrosenvald.info/single-post/2019/09/18/DO-RISCO-DA-ATIVIDADE-AO-%E2%80%9CALTO%E2%80%9D-RISCO-DA-ATIVIDADE-ALGOR%C3%8DTMICA> Acesso em 19 set. 2020.
[56] É o que determina o artigo 6º, VI: Art. 6º, 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.
[57] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. Revista dos Tribunais**, v. 1009, nov. 2019, p. 12.

Este cuidado com o conhecimento, por parte do titular, a respeito de seus dados não é novo no ordenamento brasileiro. Em um já multicitado[58] acórdão de 1995, de relatoria do Ministro Ruy Rosado, ficava clara esta preocupação:

> A **inserção de dados pessoais do cidadão em bancos de informações** tem se constituído em uma das **preocupações do Estado moderno**, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes (...) ao mesmo tempo, o **cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo**. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, **também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica**"[59]. (Grifei).

A problemática a respeito dos bancos de dados é antiga, com casos importantes tendo ocorrido já há mais de 50 anos. Se faz referência à questão do *National Data Center*, projeto de 1965, focado na construção de uma central única de armazenamento de informações pessoais, buscando unificar registros trabalhistas, fiscais e da previdência social[60]. Houve uma grande repercussão negativa por parte da sociedade com medo de uma possível centralização de poder[61] e o projeto foi encerrado. Outro projeto neste mesmo sentido foi o SAFARI (*Système Automatisé pour les Fichiers Administratifs et le Répertoire des* Individus), pensado na França, no início da década de 1970. Este consistia na transferência dos dados pessoais dos cidadãos franceses, que estavam nas mãos da administração pública, para sistemas informatizados, buscando uma maior eficiência administrativa[62]. Assim como a sociedade estado-unidense, a francesa se opôs à iniciativa e ela foi encerrada.

---

[58] Para ficar apenas em duas menções, vide: CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 88 e DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, jul./dez. 2011, p. 95.

[59] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 22.337-8/RS. Relator: Ministro Ruy Rosado de Aguiar Júnior. 20 de março de 1995. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-eletronica-1996_77_capQuartaTurma.pdf> Acesso em 15 jun. 2020.

[60] 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, p. 160.

[61] A centralização do poder é, segundo Antonin Scalia, a maior ameaça à liberdade, aqui entendida em seu sentido amplo. BAKER JR., John S; PRYOR JR., William H. Justice Scalia on federalism and separation of powers. **Regent University Law Review**, v. 30, n. 57, 2017, p. 81 – 82.

[62] 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, p. 164.

Discussão semelhante ocorreu no Brasil, durante esta década, em relação aos bancos de dados de consumo[63], em dois julgados do STJ. O primeiro[64] trata da necessidade de prévia notificação ao consumidor quando houver compartilhamento de informações de bancos de dados, sob pena de pagamento de indenização por danos morais. O segundo diz respeito ao *credit scoring*, que não constitui banco de dados, mas método estatístico de avaliação de risco a partir da utilização de dados dos usuários. A decisão[65], tomada em repercussão geral[66], dispensou o consentimento do consumidor inscrito no sistema – aplicando o modelo de *opt-out*, no qual o consumidor pode solicitar a sua retirada do banco de dados.

A Suprema Corte dos Estados Unidos[67] alterou sua jurisprudência recentemente no caso *Carpenter v. U.S.*[68], que é considerado um ponto de inflexão[69], no tratamento da *privacy*[70] naquele país, para adotar uma nova forma de interpretação: ela colocou, no centro da hermenêutica, a análise da natureza da informação para determinar se ela merece, ou não,

---

[63] Para uma discussão mais aprofundada do tema consumerista, vide BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 38 – 42.

[64] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.758.799/MG. Relatora: Ministra Nancy Andrighi. 12 de novembro de 2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019> Acesso em 25 ago. 2020.

[65] Os casos foram os REsp 1.419.697/RS e 1.457.199/RS: BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.419.697/RS. Relator: Ministro Paulo de Tarso Sanseverino. 12 de novembro de 2014. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201303862850&dt_publicacao=17/11/2014> Acesso em 25 ago. 2020. e BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.457.199/RS. Relator: Ministro Paulo de Tarso Sanseverino. 12 de novembro de 2014. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1364998&num_registro=201401261302&data=20141217&formato=PDF> Acesso em 25 ago. 2020.

[66] A decisão gerou o Tema 710 do STJ e a Súmula nº 550, do mesmo Tribunal.

[67] Cabe, aqui, uma pequena explicação: enquanto o direito brasileiro exige uma base legal para que seja permitido o tratamento de dados, o direito estado-unidense atua justamente da maneira inversa, permitindo o tratamento a não ser que haja uma situação que lhe vede. Além disto, apesar de que as legislações de proteção tendam a ser similares, buscando a adequação, a proteção de dados nos Estados Unidos é fragmentada, sem uma lei geral, como acontece no Brasil, ou um regulamento geral, como ocorre na Europa. Os casos estado-unidenses aqui mencionados devem ser, por isso, tratados com a cautela, tendo em vista a diferença no tratamento da matéria.

[68] 585 U.S. 16-402 (2018).

[69] OHM, Paul. The many revolutions of Carpenter. **Harvard Journal of Law & Technology**, v. 32, n. 2, 2019, p. 6.

[70] Optou-se por manter o vernáculo em inglês em função da diferença que existe entre o direito à privacidade e o *right to privacy*. Neste sentido, "o estudo do contexto jurídico em que se desenvolveu esse fenômeno nos coloca, de início, uma questão preliminar: a escolha do elemento a ser comparado. Sendo esses elementos o 'direito à privacidade' e o *right to privacy*, uma identidade linguística entre ambos não pode servir de base para essa comparação (...) Não é possível reconhecer, no direito norte-americano, uma unidade no *right to privacy*. Apesar da demanda pela proteção da privacidade ter surgido natural e organicamente como um aspecto evolutivo do ordenamento, essa terminologia foi utilizada para diversas funções". 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, p. 218 – 222.

proteção. Isto ocorreu pela substituição do Teste de Katz[71] pelo Teste de Carpenter[72], que buscou normatizar a equivalência tecnológica, protegendo atividades que normalmente ficariam desprotegidas mas que, na modernidade, podem acarretar violações aos titulares de dados.

A partir disto, fica claro que a ciência do usuário a respeito do tratamento de suas informações é basilar para que haja uma efetiva proteção de seus dados, sob pena de vivermos em labirintos kafkianos[73]. Há grande perigo de cristalizarmos uma *black box society*, conforme alerta Pasquale, marcada pelos *gaps* de conhecimento[74]: enquanto governos e *big techs* escondem suas ações, a vida do cidadão comum – influenciada pelos modelos utilizados por estes que ocultam – é, cada vez mais, um livro aberto. O'Neil chega a afirmar que os algoritmos são surdos: eles não escutam nem mesmo a lógica, mas apenas os dados que alimentam suas conclusões[75].

Desta maneira, os usuários perdem completamente o controle[76] de suas informações pessoais e das decisões que serão lhe impostas a partir destas invisíveis operações. Ainda mais grave, a autodeterminação informativa[77], um dos fundamentos da LGPD[78], fica seriamente

---

[71] 389 U.S. 347 (1967). O teste de *Katz*, estabelecido no voto concorrente do Justice Harlan, determinava que uma informação estava protegida quando i) houvesse uma expectativa subjetiva real de privacidade e ii) que esta expectativa fosse uma que a sociedade estivesse preparada para reconhecer como razoável. Para uma análise mais profunda, vide WINN, Peter. Katz and the Origins of the Reasonable Expectation of Privacy Test. **McGeorge Law Review**, v. 40, n. 1, 2009.

[72] O teste de Carpenter foi estabelecido para evitar a deterioração da privacidade em razão dos avanços tecnológicos (OHM, Paul. The many revolutions of Carpenter. **Harvard Journal of Law & Technology**, v. 32, n. 2, 2019, p. 56) e é constituído por quatro fatores: i) a natureza profundamente reveladora da informação, ou seja, a sensibilidade e intimidade da informação coletada, visto que ela pode conter as *privacidades da vida*; ii) profundidade, amplitude e alcance abrangente sendo estes, em ordem, a precisão da informação, a frequência e por quanto tempo foi coletada e o número de pessoas monitoradas pela base de dados; iii) coleta inevitável e automática, a partir do entendimento de que algumas coletas de dados são inevitáveis para a inclusão na sociedade moderna, afastando o elemento vontade; e iv) o ganho de eficiência.

[73] A metáfora é retratada na história de Josef K. que foi detido, em "O Processo", sem ser informado do motivo, do local onde ocorrerão as audiências em que foi citado ou ao menos do Tribunal que lhe julgará, vivendo em um verdadeiro labirinto em busca dessas informações. KAFKA, Franz. **O processo**. São Paulo: Companhia das Letras, 2005.

[74] PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, p. 1 - 3.

[75] O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. Londres: Penguin Books, 2017, p. 10 – 11.

[76] "Busca-se fortalecer a proteção da pessoa inserindo, nos poderes do titular desse direito de personalidade o controle não só sobre o acesso, mas também no que se refere ao seu tratamento, à sua utilização e à sua circulação." GEDIEL, José Antonio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito – UFPR**, Curitiba, n. 7, p. 141 – 153, 2008, p. 143.

[77] Sobre as origens do conceito, ver: MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa> Acesso em 31 out 2020.

[78] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: II - a autodeterminação informativa.

comprometida[79]: o controle é justamente sua base, e o que fundamenta a disciplina do consentimento.

A autodeterminação informativa consiste no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa. Este direito foi desenvolvido pela doutrina[80] e consolidado pela decisão da Corte Constitucional alemã no caso do censo, de 1983[81]. Esta decisão é um verdadeiro marco teórico no campo da proteção de dados pessoais, reconhecendo um direito subjetivo fundamental e alçando o indivíduo ao protagonismo no processo de tratamento de dados[82]. Nela, a Corte redefiniu os contornos do direito de proteção de dados pessoais, situando-o como verdadeira projeção de um direito geral de personalidade[83] a partir de uma leitura ampliativa do artigo 2.1[84], em conjunto com o artigo 1.1[85] da *Grundgesetz*. Atualmente, Carta de Direitos Fundamentais da União Europeia também identifica a proteção de dados como direito fundamental[86].

O Supremo Tribunal Federal recentemente também reconheceu a proteção de dados como um direito fundamental autônomo. Isto ocorreu no julgamento da ADIn 6387[87], que

---

[79] Inclusive colocando em risco o sistema democrático, como também anteriormente tratado: "Uma sociedade na qual os cidadãos não detém controle sobre as suas próprias informações **coloca em risco o seu próprio sistema democrático, em razão do estado de vigilância** permanente trazido por essa situação" (Grifei). MARTINS, Leonardo. (org.) **Cinqüenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 239 – 240.

[80] Um dos autores responsáveis por isto foi Alan Westin, em WESTIN, Alan. **Privacy and freedom**. Nova Iorque: Atheneum, 1967, especialmente nas p. 133 – 158. Esclarecendo a questão do desenvolvimento doutrinário e da posterior cristalização pelo Tribunal Constitucional Alemão, vide MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 229 e ss..

[81] *Volkszählungsurteil* (*BVerfGE*, 65, 1).

[82] MENDES, Laura Schertel. **A encruzilhada da proteção de dados no Brasil e o caso do IBGE**. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020> Acesso em 15 ago. 2020.

[83] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. **Voto do Ministro Gilmar Mendes**. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020, p. 18.

[84] Segundo Nipperdey (NIPPERDEY, Hans Carl. Livre Desenvolvimento da Personalidade. In: HECK, Luís Afonso (org.). **Direitos Fundamentais e Direito Privado**: textos clássicos. Porto Alegre: Sergio Antonio Fabris, 2011, p. 71 – 90, p. 71), aqui está em questão a proteção dinâmica da pessoa, com a famosa expressão livre desenvolvimento da personalidade: "*Artikel 2, I: Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt*".

[85] Nipperdey (*Ibid*, p. 71) entende que há, aqui, uma proteção da pessoa em sua essência: "*Artikel 1, I: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt*".

[86] "Artigo 8º Protecção de dados pessoais 1. Todas as pessoas têm direito à protecção dos dados de caracter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

[87] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020.

versava sobre o compartilhamento de dados de telefônicas com o IBGE. Cabe, aqui, fazer referência ao voto do Ministro Gilmar Mendes:

> A adequada compreensão do parâmetro de controle invocado, no entanto, perpassa o aprofundamento do inevitável debate teórico acerca da afirmação da autonomia do direito fundamental à proteção de dados pessoais como categoria dentro do rol dos direitos fundamentais, para além da mera evolução do direito ao sigilo. Nesse sentido, a análise do referendo da medida cautelar nesta ADI suscita a oportunidade e **o dever de o Supremo Tribunal Federal aprofundar a identificação, na ordem constitucional brasileira, de um direito fundamental à proteção de dados pessoais**, a fim de estabelecer de forma clara o âmbito de proteção e os limites constitucionais à intervenção estatal sobre essa garantia individual[88]. (Grifei)

O debate a respeito do enquadramento da proteção de dados como direito fundamental autônomo já ocorria tanto no âmbito doutrinário, quanto no legislativo. A respeito deste, tramita no Congresso Federal a PEC nº 17/2019, que pretende positivar na Constituição a proteção de dados entre os direitos fundamentais[89]. A Declaração de Santa Cruz de la Sierra, firmada pelo Brasil, também já o entendia como direito fundamental[90]. A doutrina[91] há muito defendia este enquadramento, entendendo ser um passo natural do direito à privacidade, que ocorreria inevitavelmente a partir das novas demandas sociais originadas na sociedade da informação[92].

---

[88] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. **Voto do Ministro Gilmar Mendes**. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020, p. 14 – 15.

[89] O projeto visa acrescentar um novo inciso no artigo 5º, XII-A, além de fixar a competência privativa da União para legislar sobre a matéria, alterando o artigo 22 da Constituição. No momento em que este trabalho é escrito, a proposta foi aprovada pelo Plenário do Senado e ainda não foi apreciada pela Câmara. BRASIL. **Proposta de Emenda à Constituição nº 17 de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594> Acesso em 10 set. 2020.

[90] A previsão estava contida no Item 45, que assim determina: "Item 45: **Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas** e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade" (Grifei). DECLARAÇÃO de Santa Cruz de la Sierra. In: CUMBRE IBEROAMERICANA DE JEFES DE ESTADO Y DE GOBIERNO, 13., Santa Cruz de la Sierra, 2003. **Anais**. Disponível em: <https://www.segib.org/wp- content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf.> Acesso em: 5 ago 2020.

[91] Vide, por exemplo: MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-81, jul./set. 2011.; DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91 – 108, jul./dez. 2011; MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014; SARLET, Ingo Wolfgang. **Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF?**. Disponível em: < https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf> Acesso em 21 out 2020.

[92] MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-81, jul./set. 2011, p. 31.

1.2 Uso Secundário e Finalidade

Neste novo contexto social, ficou evidente o risco de tornar anacrônico o Direito caso não houvesse regras adaptáveis a um mundo que se acostumou a rápidas transformações[93]. Uma das maneiras mais eficientes de oxigenar as leis, mantendo-as aplicáveis a situações anteriormente desconhecidas, é por meio da abertura do texto à construção do intérprete, seja por cláusulas gerais[94], seja por princípios jurídicos[95].

O uso secundário de dados tem sua definição atrelada justamente a um princípio, o da finalidade:

> **O sistema vale-se da informação obtida para uma finalidade e a reutiliza para uma finalidade distinta – em outras palavras, o dado *se move* do uso primário para o uso secundário**. Isto o faz *muito mais valioso* ao longo do tempo. (...) O conjunto de dados encontra usos secundários – e novo valor – quando é utilizado para uma finalidade completamente diferente. (...) Em síntese, o valor dos dados precisa ser considerado em termos de todas as possíveis maneiras que poderá ser empregado no futuro[96]. (Grifei).

Daniel Solove[97] traz um conceito semelhante:

> Uso secundário é o uso de dados para propósitos não relacionados aos propósitos para os quais o dado foi inicialmente coletado e sem o consentimento do titular dos dados.

---

[93] 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, p. 49.

[94] Sobre isto, ver: MENKE, Fabiano. A interpretação das cláusulas gerais: a subsunção e a concreção de conceitos. **Doutrinas Essenciais de Direito do Consumidor**, v. 4, p. 107 – 136, abr. 2011.

[95] Há, na doutrina, autores que equiparam os dois termos, como é o caso de Ruy Rosado de Aguiar Jr em AGUIAR JÚNIOR, Ruy Rosado de. Interpretação. **Revista da Ajuris**, ano XVI, n. 45, mar. 1989, p. 19 e ss.. Outros, no entanto, entendem ser institutos diversos, como é o caso de Judith Martins-Costa em MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2 ed. São Paulo: Saraiva, 2018, p. 161.

[96] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. First Mariner Books: New York, 2014, p. 103. No original: "*The system takes information generated for one purpose and reuses it for another – in other words, the data moves from primary to secondary uses. This makes it much more valuable over time. (...) [The] sets of data find secondary uses – and new value – when they're applied to a completely different purpose. (...) In short, data's value needs to be considered in terms of all the possible ways it can be employed in the future*".

[97] SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560, p. 519. O título do texto estabelece exatamente o que o autor tentou fazer: uma taxonomia da privacidade. A divisão que ele fez foi a seguinte: a) coleta de informações – i) vigilância; ii) interrogatório; b) processamento de informações – i) agregação; ii) identificação; iii) inseguridade; iv) **uso secundário**; v) exclusão; c) disseminação de informações – i) violação de confidencialidade; ii) divulgação; iii) exposição; iv) aumento na acessibilidade; v) chantagem; vi) apropriação; vii) distorção; d) invasão – i) intrusão; ii) interferência decisional. (Grifei).

Disto se vislumbra uma diferença primordial entre os dados e o petróleo: as informações pessoais passam a ser mais valiosas quando *reutilizadas* para além da finalidade primeiramente autorizada. Esta situação, viola a LGPD, pois ela proíbe o processamento para finalidades distintas em seu artigo 6º, I[98], e, conforme a teoria de Ávila, viola também o dever de adotar o comportamento necessário para atingir o estado ideal de coisas que, neste caso, seria de tratar os dados de acordo com a finalidade consentida.

Para que a análise principiológica, cerne deste ponto do trabalho, seja possível, é necessário que seja feito um acordo semântico com vistas a delimitar o âmbito de alcance destas normas, a fim de evitar sua utilização casuística e diminuir a subjetividade.

Levando isto em consideração, optou-se por basear esta hermenêutica na teoria elaborada por Humberto Ávila em seu *Teoria dos Princípios*[99]. Para o autor, as espécies normativas são três, a depender da dimensão imediata que experimentam: se comportamental, se está diante de uma regra; se finalística, de um princípio; se metódica, de um postulado[100].

Dentro dos postulados, Ávila os divide entre inespecíficos, sendo meras ideias gerais, despidas de critérios orientadores a aplicação[101], e específicos, nas hipóteses em que exigem o relacionamento entre elementos específicos[102]. Para diferenciar regras e princípios, o autor afasta os critérios hipotético-condicional[103], de modo final de aplicação[104] e do conflito normativo[105], para trazer três novas formas de dissociação: a natureza do comportamento prescrito, a natureza da justificação exigida, a medida de contribuição para a decisão.

A partir disto, esquematiza os princípios a partir do dever imediato de promoção de um estado ideal de coisas, com o dever mediato de adoção da conduta necessária. Sua justificação

---

[98] 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**. (Grifei).

[99] A edição utilizada foi esta: ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 18 ed., rev. e atual. São Paulo: Malheiros, 2018.

[100] *Ibid*, p. 43 – 47.

[101] *Ibid,* p. 185. São exemplos a ponderação, a concordância prática e a proibição do excesso.

[102] *Idem*. São exemplos a igualdade, a razoabilidade e a proporcionalidade.

[103] Por esta teoria, "as regras possuem uma hipótese e uma consequência que predeterminam a decisão, sendo aplicadas do modo *se*, *então*; os princípios apenas indicam o fundamento a ser utilizado pelo aplicador para, futuramente, encontrar a regra aplicável ao caso concreto" *Ibid*, p. 60. São exemplos de autores desta corrente Josef Esser e Karl Larenz.

[104] Para esta teoria, "as regras são aplicadas de modo absoluto *tudo ou nada*, ao passo que os princípios de modo gradual *mais ou menos*" *Ibid*, p. 65. São autores que defendem esta diferenciação Robert Alexy e Ronald Dworkin.

[105] Para esta teoria "os princípios poderiam ser distinguidos das regras pelo modo como funcionam em caso de *conflito normativo*, pois, para eles, a antinomia entre as regras consubstancia verdadeiro conflito, a ser solucionado com a declaração de invalidade de uma das regras ou com a criação de uma exceção, ao passo que o relacionamento entre princípios consiste em um imbricamento, a ser decidido mediante uma ponderação que atribui uma dimensão de peso a cada um deles". ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 18 ed., rev. e atual. São Paulo: Malheiros, 2018, p. 73.

se encontra na correlação entre efeitos da conduta e o estado ideal de coisas, e sua pretensão de decidibilidade está na concorrência e na parcialidade[106]. A definição de princípio trazida por Ávila, e adotada para a análise deste trabalho, é a seguinte:

> Princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementaridade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção[107]

Assim, os princípios têm, como âmago, a finalidade, que possui uma dupla-face: como motivo ou como objetivo, a partir das normas geradas[108]. Os motivos geram razões substanciais, definindo-se os fins como as razões para ser adotado determinado comportamento. Por outro lado, os objetivos geram razões finalísticas, entendidos como o estado de coisas[109] a ser promovido – no tratamento de dados, por exemplo, aquele autorizado por uma base legal. É este estado de coisas, e não a norma em si (princípio, regra ou postulado), que pode ser aplicado na fórmula *mais ou menos*: ele pode ser mais ou menos aproximado, a depender se a situação almejada foi realizada ou não. Desta forma, os princípios possuem um âmbito maior de apreciação ao possuírem um caráter primariamente prospectivo, em razão de determinarem um estado de coisas a ser construído[110].

Em suma, os princípios determinam a adoção de um comportamento a partir do estabelecimento de um estado de coisas indicado por um fim juridicamente relevante. O aplicador deve verificar, no caso concreto, a adequação do comportamento tomado em relação ao fim pretendido[111]. Isto posto, princípios possuem um caráter deôntico-teleológico:

> Deôntico porque estipulam razões para a existência de obrigações, permissões ou proibições. Teleológico porque as obrigações, permissões e proibições decorrem dos efeitos advindos de determinado comportamento que preservam ou promovem determinado estado de coisas[112].

---

[106] *Ibid*, p. 102.
[107] *Ibid*, p. 102.
[108] *Ibid*, p. 70.
[109] Ávila o define da seguinte maneira: "*Estado de coisas* pode ser definido como uma situação qualificada por determinadas qualidades. O estado de coisas transforma-se em *fim* quando alguém aspira conseguir, gozar ou possuir as qualidades presentes naquela situação". *Ibid.*, p. 95.
[110] *Ibid.*, p. 99.
[111] "Os princípios, ao estabelecerem fins a serem atingidos, exigem a promoção de um estado de coisas – bens jurídicos – que impõe condutas necessárias à sua preservação ou realização". *Ibid*., p. 95.
[112] *Ibid*, p. 95.

Consequentemente, o estado ideal de coisas só é alcançado se o comportamento for realizado. Os princípios, desta forma, estabelecem uma necessidade prática: o dever de adotar o comportamento necessário para alcançar o estado ideal de coisas[113].

Especificamente na seara da proteção de dados pessoais, foi a partir de 1973, na série de discussões relativas ao *National Data Center*, que se estabeleceram regras de controle sobre as informações pessoais[114]. Elas foram enunciadas no Relatório do Comitê Consultivo da Secretaria de Saúde, Educação e Bem-Estar dos EUA em relação a sistemas automatizados de dados pessoais[115], que já delineava alguns dos princípios que hoje conhecemos:

Os *Fair Information Privacy Princples (FIPP)*[116], como ficou conhecida a parte principiológica do relatório, serviram de inspiração para as *Guidelines* da OCDE[117], de 1980, que buscam estabelecer padrões normativos para a proteção de dados pessoais a fim de assegurar o livre fluxo de informações entre seus países-membros[118]. Estes parâmetros foram enunciados por meio de oito princípios sobre os quais a atividade de processamento deveria se basear[119]: limitação da coleta, qualidade dos dados, especificação de propósitos, limitação de uso, padrões de mecanismos de segurança, abertura, participação individual e *accountability*. As *Guidelines* sofreram um processo de revisão em 2013, tendo sido mantida sua espinha dorsal[120] - as maiores modificações tratam do procedimento de implementação do documento.

---

[113] *Ibid*., p. 96.

[114] Interessante notar, como refere Danilo Doneda, o fato de ser emblemático que a moderna discussão sobre a *privacy* ter surgido em território estado-unidense, "sendo uma das primeiras ocasiões em que um grande tema da *western legal tradition* ganhou impulso decisivo a partir de temas surgidos na América" (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, p. 123 – 124). O autor se refere, neste trecho, ao seminal artigo *The Right to Privacy* (BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, dez./ 1890, p. 193 – 220). A lógica do pensamento, entretanto, pode ser expandida à questão dos princípios, tendo em vista que o relatório influenciou a construção das *Guidelines* da OCDE e da Convenção 108 (atualmente 108+) do Conselho da Europa.

[115]UNITED STATES OF AMERICA. **Records, computers, and the rights of citizens**: report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm/> Acesso em 16 jun 2020, p. 41 – 42.

[116] Bruno Bioni defende que os princípios ensaiados como resultado do trabalho do Comitê somente ganharam escala ao serem transportadas para a OCDE. Vide BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 115, nota de rodapé nº 44.

[117] OECD. **Guidelines on the protection of privacy and transborder flows of personal data**. Disponível em: <
https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em 10 ago 2020.

[118] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 114.

[119] 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, p. 193.

[120] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 116.

Outra decorrência dos FIPP foi a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais[121] (Conhecida como Convenção 108 ou Convenção de Strasburg). Ela é resultado do movimento produzido pela OCDE para facilitar a harmonização das legislações de proteção de dados pessoais[122], e sua importância fundamental advém de que o Conselho da Europa passou a tratar a proteção de dados como um tema de direitos humanos[123].

Esta convenção incita os estados-membros e os signatários a adotarem normas específicas para o tratamento de dados pessoais[124] e está aberta para adesão também de países não-membros[125], facilitando o reconhecimento da adequação dos ordenamentos nacionais, prevista tanto na LGPD[126] quanto no GDPR[127]-[128]. Sua abordagem regulatória está focada em dois atores: o titular das informações pessoais e quem as processa[129]. Em 2018, com a adoção de um Protocolo de Emenda[130], a convenção foi modernizada, passando a ser conhecida como Convenção 108+.

---

[121] CONSELHO DA EUROPA. **Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (ETS nº 108)**. Disponível em: < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Acesso em 22 jun 2020.

[122] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 117.

[123] 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, p. 194.

[124] *Ibidem*.

[125] O Uruguai foi, em 2013, o primeiro país não-europeu a ser signatário. Atualmente, Argentina e México também fazem parte da Convenção.

[126] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem **grau de proteção de dados pessoais adequado ao previsto nesta Le**i; (Grifei).

[127] Por precaução, esclarece-se aqui que foi utilizada a versão em português do Regulamento Europeu, visto que há diferenças no tratamento de conceitos nos diferentes idiomas do texto. Sobre isto, ver MALGIERI, Gianclaudio. **The concept of Fairness in the GDPR**: a linguistic and contextual interpretation. Proceedings of FAT, jan. 2020.

[128] A adequação é prevista expressamente no artigo 45 do Regulamento: Artigo 45.o Transferências com base numa decisão de adequação 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica. 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos: (…) c) **Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais**" (Grifei). Para uma análise comparativa entre o RGPD e a LGPD, vide MENDES, Laura Schertel; BIONI, Bruno. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 797 – 820.

[129] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 118.

[130] CONSELHO DA EUROPA. Protocolo de Emenda à Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (CETS nº 223). Disponível em: < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em 22 jun 2020.

Sendo os princípios normas que definem um estado de coisas a ser alcançado a partir de um fim, pode-se considerar a finalidade o corolário principiológico das leis de proteção de dados. Junto dela, os princípios da necessidade – ou minimização – e da transparência, tratado na seção anterior, são fundamentais para entendermos as questões trazidas pelo uso secundário de dados pessoais.

O papel central da finalidade se explica pelo fato de que o consentimento, base autorizativa legal por excelência, tem este princípio como requisito – o titular, quando consente, o faz para fins certos e determinados, de maneira expressa[131]. Assim sendo, o controlador e o operador devem explicitar *todas* as finalidades pelas quais os dados serão tratados, vinculando-se aos termos desta sua manifestação pré-negocial[132]. A LGPD trouxe esta norma no artigo 6º, I[133], enquanto o GDPR a trouxe como princípio *da limitação* de propósitos, em seu artigo 5º, I, *b*[134].

O princípio da limitação de propósitos é compreendido por dois elementos[135]. O primeiro é a finalidade específica, composta pela especificidade, pela explicitude e pela legitimidade. O segundo é a compatibilidade, entendida como o processamento de forma compatível com a finalidade pela qual os dados foram originariamente coletados.

A legislação brasileira optou por desmembrar estes elementos, assentando a compatibilidade no princípio da adequação[136]. Assim, a finalidade de que trata a LGPD deve ser para propósitos legítimos, específicos explícitos, assim como o GDPR, e informados ao titular – tem-se, aqui, uma preocupação específica com a transparência, também um princípio autônomo.

---

[131] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019, p. 6.

[132] *Ibid*., p. 6. Existe discussão doutrinária a respeito da natureza negocial; sobre isto, vide 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, p. 297 e ss..

[133] 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;

[134] Também conhecido pelo seu termo em inglês, *purpose limitation principle*. Art. 5º - Princípios relativos ao tratamento de dados pessoais: 1. Os dados pessoais são: b)Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º nº 1 («limitação das finalidades»);

[135] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2013 on Purpose Limitation**. Bruxelas, 2013. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> Acesso em 12 jul 2020, p. 15 – 36.

[136] Art. 6º, II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Mesmo com a lei em vigor apenas parcialmente no momento de produção deste trabalho, houve uma decisão, da Comarca de São Paulo, condenando uma empresa de empreendimentos imobiliários por violar a finalidade ao transferir dados indevidamente a terceiros:

> Patente que os dados independentemente de sensíveis ou pessoais (art. 5º, I e II, LGPD) **foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD)**. O contrato firmado entre as partes prescreveu apenas a possibilidade de inclusão de dados do requerente para fins de inserção em banco de dados ("Cadastro Positivo"), sem que tenha sido efetivamente informado acerca da utilização dos dados para outros fins que não os relativos à relação jurídica firmada entre as partes. Entretanto, consoante prova documental, **houve a utilização para finalidade diversa e sem que o autor tivesse informação adequada** (art. 6º, II, LGPD)[137]. (Grifei).

Interessante notar que a informação a respeito da finalidade do tratamento de dados pessoais é possibilitada, na Argentina[138] e no Paraguai[139], pelo *Habeas Data Finalista*. Mesmo tendo sido um instrumento originariamente previsto pelo legislador brasileiro[140], não se previu esta hipótese no ordenamento pátrio.

O princípio da necessidade se relaciona diretamente ao postulado da proporcionalidade[141], sobretudo na adequação entre meios e fins[142]. Por se tratar de um direito fundamental e de um direito da personalidade, o tratamento de dados deve se estender ao mínimo necessário para atender as finalidades previstas.

Fica evidente, no tocante à minimização, o árduo equilíbrio quando cotejado com o *Big Data*, tendo em vista que a lógica fundante de cada um é antagônica: enquanto o princípio busca

---

[137] SÃO PAULO. Sentença nº 1080233-94.2019.8.26.0100. 13ª Vara Cível do Foro Central de São Paulo. Juíza de Direito: Tonia Yuka Koroku. 29 de setembro de 2020. Disponível em: < https://migalhas.uol.com.br/arquivos/2020/9/B05F37C296A643_decisaoLGPD.pdf> Acesso em 01 out 2020.

[138] Artículo 43.- Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. (…) **Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad**, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística. (Grifei)

[139] Artículo 135. Del Hábeas Data. Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, **así como conocer el uso que se haga de los mismos y de su finalidad**. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos. (Grifei).

[140] 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, p. 267.

[141] Especificamente sobre ele, ver ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 18 ed., rev. e atual. São Paulo: Malheiros, 2018, p. 205 – 222.

[142] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019, p. 10.

apenas a coleta de dados imprescindíveis, a ferramenta intenta colher o maior número de informações possíveis.

A preocupação com o uso secundário de dados anda de mãos dadas com o desenvolvimento principiológico das leis de proteção. Já em 1973 os *FPPI* previam que o indivíduo teria direito a evitar que isto ocorresse[143]:

> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma elas são utilizadas;
> - Deve existir um meio para um **indivíduo evitar que a informação a seu respeito coletada para um determinado propósito não seja utilizada ou disponibilizada para outros propósitos sem o seu consentimento**. (Grifei)

Em 1977, o governo estado-unidense passou a cruzar dados de registros de seus empregados com dados de benefícios federais, buscando capturar possíveis fraudes[144]. Em 1988, o Congresso deste mesmo país aprovou o *Computer Matching and Privacy Protection Act*[145], justamente para regular estes cruzamentos de bancos de dados. Ademais, o *Health Insurance Portability and Accountability Act*[146], de 1996, regulou situações nas quais poderia haver um uso secundário de dados médicos – considerados dados sensíveis - além daqueles estritamente necessários para operações de tratamento, pagamento e cuidados de saúde. Por fim, o *Gramm-Leach-Billey Act*[147], de 1999, estabeleceu limites na reutilização de dados pessoais quando uma empresa transferisse as informações a outra.

Verifica-se, assim, que a variedade de possíveis usos secundários é virtualmente infinita[148], podendo ser benéfica em algumas situações e maléfica em outras. A grande questão, aqui, é como compatibilizar a proteção de dados pessoais, o desenvolvimento econômico e a confiança do titular na relação com o controlador e com o operador, tendo em vista os limites impostos, principalmente, pela finalidade.

---

[143] UNITED STATES OF AMERICA. **Records, computers, and the rights of citizens**: report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm/> Acesso em 16 jun 2020, p. 42.
[144] SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560, p. 518.
[145] UNITED STATES OF AMERICA. **Computer Matching and Privacy Protection Act (1988)**. Disponível em: < https://www.congress.gov/bill/100th-congress/senate-bill/496> Acesso em 13 ago 2020. Além desta lei, houve outras que expressamente mandavam o estabelecimento de finalidades
[146] UNITED STATES OF AMERICA. **Health Insurance Portability and Accountability Act (1996)**. Disponível em: < https://www.cdc.gov/phlp/publications/topic/hipaa.html> Acesso em 13 ago 2020.
[147] UNITED STATES OF AMERICA. **Gramm-Leach-Billey Act (1999)**. Disponível em: < https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf> Acesso em 13 ago 2020.
[148] SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560, p. 519.

O grande problema que o uso secundário pode causar é a utilização dos dados coletados de maneiras que o titular dos dados não entenda, no mínimo, desejável[149]. Ele frustra as expectativas legítimas do usuário, indo, muitas vezes, contra a boa-fé esperada. O argumento usualmente usado em contrário é que o titular não possui uma legítima expectativa de proteção quando consente no tratamento de seus dados.

Esta corrente ficou conhecida como *Third-Party Doctrine*[150] e foi cristalizada por sucessivas decisões da Suprema Corte dos Estados Unidos. A primeira dela foi o caso *United States v. Miller*[151], de 1976, onde a Corte definiu que não há proibição na obtenção de informações reveladas a uma terceira parte, mesmo que a informação seja revelada assumindo que ela será utilizada apenas para uma finalidade específica[152]. A segunda foi o caso *Smith v. Maryland*[153], de 1979, onde a Corte enfrentou a questão da voluntariedade da entrega dos dados: ao entender que eles são transferidos voluntariamente pelos titulares, decidiu que não há uma expectativa legítima de *privacy* sobre eles.

Nas Cortes inferiores também foi aplicada esta corrente. Exemplo disto é o caso *Dwyer v. American Express Co.*[154], de 1995, onde se decidiu que o uso da lista de compras feitas por uma pessoa com o seu cartão de crédito pela companhia administradora do cartão, para finalidades secundárias, não constitui uma violação de sua *privacy*[155]. Esta corrente começou a perder força em outros dois casos, *Kyllo v. U.S.*[156], de 2001, e *Riley v. California*[157], de 2014, sendo abandonada com o caso *Carpenter v. U.S.*, tratado na seção anterior.

---

[149] *Ibid*., p. 520.

[150] Sobre o tema, ver: ALDRICH, Rick. Privacy's Third-Party Doctrine: Initial Developments in the Wake of Carpenter. **SciTech Lawyer**, v. 15, n. 3, 2019; HENDERSON, Stephen E. After United States v. Jones, after the Fourth Amendment Third Party Doctrine. **North Carolina Journal of Law & Technology**, v. 14, n. 2, 2013; HENDERSON, Stephen E. Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too. **Pepperdine Law Review**, v. 34, n. 4, 2007.

[151] 425 U.S. 435 (1976). A Corte entendeu que não há direito à *privacy* sobre registros bancários por estes estarem mantidos por uma terceira parte, o banco, e serem registros de negócios.

[152] 425 U.S. 435 (1976), p. 443.

[153] 442 U.S. 735 (1979). Aqui, decidiu o Tribunal que não há uma expectativa legítima de *privacy* nos números que são discados por eles serem voluntariamente entregues à companhia telefônica.

[154] ILLINOIS. **Dwyer v. American Express Co. (1995)**. 273 Ill. App. 3d 742 (1995). Disponível em: <https://www.quimbee.com/cases/dwyer-v-american-express-co> Acesso em 20 ago 2020.

[155] Esta decisão é mencionada por Danilo Doneda em 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, p. 236.

[156] 533 U.S. 27 (2001). Neste processo, a Corte reconheceu que os direitos à *privacy* foram afetados pelo avanço tecnológico: o caso concreto tratava do uso de imagens térmicas para verificar se um suspeito estava plantando maconha em sua casa. Os policiais ficaram fora da residência com a câmera e, pelo calor irradiado, conseguiram verificar que havia, possivelmente, uma plantação de drogas naquele local.

[157] 573 U.S. 13-132 (2014). Por fim, a Corte definiu que celulares são considerados mini-computadores que contém alguns itens extras, como câmeras, calendários, diários, jornais etc, fazendo com que eles sejam diferentes tanto qualitativamente, quanto quantitativamente, de outros itens que as pessoas normalmente carregam consigo. No voto concorrente, Justice Sotomayor frisou que talvez fosse necessário reconsiderar

Outra situação em que ocorreu um potencial dano aos titulares dos dados foi no âmbito do exército dos EUA. Lá, assim como no Brasil, são coletadas as impressões digitais[158] dos recrutas no âmbito do serviço militar obrigatório. Ocorre que estes dados foram enviados ao FBI e incorporados ao banco de dados da instituição para identificação de criminosos – um uso que ficou conhecido apenas tempos depois e que os titulares não esperavam que ocorresse[159].

Dentre os malefícios, provavelmente o mais comum diz respeito à venda de dados pessoais[160]. A prática ganhou relevo, no Brasil, com o caso da agência Yacows:

> A página da plataforma anunciava como chamariz para a clientela "240 milhões de linhas de celular com perfil atrelado"; "100 milhões de títulos de eleitores"; "cruzamento de dados cadastrais com eleitorais"; "campanhas segmentadas por zona eleitoral"; "dados georreferenciados: por estado, cidade e bairros"[161].

Não há dúvidas que o livre desenvolvimento da personalidade e a autodeterminação informativa são fortemente diminuídas em razão de modelos de negócios como estes, além de poder acarretar grandes riscos à democracia[162]. Ademais, a legislação eleitoral traz vedações expressas à doação, venda ou cessão de banco de dados, tanto na Lei das Eleições[163], como na Resolução nº 23.610 do TSE[164].

---

alguns aspectos da razoável expectativa de *privacy* dos indivíduos na era digital em razão de as pessoas revelarem grandes quantidades de informações a terceiros em *tarefas mundanas*.

[158] Que, sendo dados biométricos, s ão caracterizados como dados sensíveis e, por isto, possuem um nível maior de proteção.

[159] SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560, p. 520.

[160] Como vimos, existem atores, como os *data brokers*, especializados na coleta de dados pessoais para, posteriormente, vende-los a empresas que os tratarão com finalidades distintas.

[161] MELLO, Patrícia Campos. **A máquina do ódio**. São Paulo: Companhia das Letras, 2020, p. 46. Neste mesmo sentido: RODRIGUES, Artur. **Agência vendia em site cadastro para envio ilegal de Whatsapp na eleição de 2018**. Disponível em: <https://www1.folha.uol.com.br/poder/2020/03/agencia-vendia-em-site-cadastro-para-envio-ilegal-de-whatsapp-na-eleicao-de-2018.shtml> Acesso em 10 set. 2020.

[162] Neste sentido, recomenda-se a leitura de MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. **Proteção de Dados nas Eleições:** democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

[163] Art. 57-E. São vedadas às pessoas relacionadas no art. 24 a utilização, doação ou cessão de cadastro eletrônico de seus clientes, em favor de candidatos, partidos ou coligações. § 1º É proibida a venda de cadastro de endereços eletrônicos. § 2º A violação do disposto neste artigo sujeita o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais).

[164] Art. 31. É vedada às pessoas relacionadas no art. 24 da Lei nº 9.504/1997, bem como às pessoas jurídicas de direito privado, a utilização, doação ou cessão de dados pessoais de seus clientes, em favor de candidatos, de partidos políticos ou de coligações (Lei nº 9.504/1997, art. 24 e art. 57-E, caput; ADI nº 4650; e Lei nº 13.709/2018, art. 1º e art. 5º, I). § 1º É proibida às pessoas jurídicas e às pessoas naturais a venda de cadastro de endereços eletrônicos, nos termos do art. 57- E, § 1º, da Lei nº 9.504/1997. § 2º A violação do disposto neste artigo sujeita o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais).

Outro interessante caso ocorrido em solo brasileiro foi o da venda de dados de localização, supostamente anonimizados, pela operadora de celular Vivo[165]. Um dos usos que estes dados tiveram foi a utilização[166], pelo governo do estado do Espírito Santo, para medir a demanda e o fluxo turístico – justamente por meio de sinal de telefonia móvel. Outro uso foi feito pela administração do estádio Aliianz Parque, em São Paulo, para comparar o perfil e o fluxo de turistas que assistiram à final da Copa do Brasil de 2015 ao público do show de David Gilmour, na semana seguinte[167]. O Departamento de Proteção e Defesa do Consumidor da Secretaria Nacional do Consumidor chegou a notificar, em 2015, a empresa, em razão do fornecimento deste "serviço":

> A empresa anunciou no fim de 2012 que estava prestes a lançar um serviço que, a partir dos dados referentes à localização dos seus clientes da rede de celular, forneceria a terceiros relatórios sobre a afluência de pedestres em determinadas zonas, ruas, etc. Esta informação pode ser útil para fins mercadológicos, de planejamento urbano e tantos outros. O serviço seria lançado no Brasil, Reino Unido e Alemanha. Dados sobre a localização de consumidores do serviço de celular da empresa seriam utilizados, sem aviso prévio e sem que lhes fosse dada a opção de não ter os seus dados recolhidos - isto é, sem o seu conhecimento ou autorização. Esta situação agrava-se pelo fato dos dados em questão serem dados de localização - dados que podem afetar não somente a privacidade do consumidor, mas também sua própria segurança pessoal e liberdade[168].

Além dos dados de localização, eram vendidos dados como o gênero do titular, a idade e a classe econômica estimada. A comercialização destes dados também ocorria fora do Brasil[169]; nos Estados Unidos, o Google foi acusado de coletar ilegalmente semelhantes[170].

---

[165] DIAS, Tatiana. **Vigiar e lucrar**: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. Disponível em: < https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/> Acesso em 3 out 2020.

[166] ESPÍRITO SANTO. **Pesquisa de demanda e fluxo turístico por meio de sinal de telefonia móvel no estado do Espírito Santo**. Vila Velha, 2017. Disponível em: < https://observatoriodoturismo.es.gov.br/Media/observatorio/Pesquisas/Telefonia%20M%C3%B3vel/Descritivo%20Metodol%C3%B3gico.pdf> Acesso em 3 out. 2020.

[167] DIAS, Tatiana. **Vigiar e lucrar**: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. Disponível em: < https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/> Acesso em 3 out 2020.

[168] BRASIL. Secretaria Nacional do Consumidor. **Ministério da Justiça notifica telefônica-vivo por serviço Smart Steps**. Disponível em: < https://www.justica.gov.br/news/ministerio-da-justica-notifica-telefonica-vivo-por-servico-smart-steps> Acesso em 3 out 2020.

[169] CABRAL, Ernesto. **Telefónica del Perú vende ubicación de clientes y pone en riesgo su privacidad.** Disponível em: < https://ojo-publico.com/1393/telefonica-vende-ubicacion-de-clientes-y-amenaza-seguridad> Acesso em 3 out 2020.

[170] ROMM, Tony. **Arizona sues Google over allegations it illegally tracked Andoid smartphone users' locations**. Disponível em: <https://www.washingtonpost.com/technology/2020/05/27/google-android-privacy-lawsuit/> Acesso em 3 out 2020.

Neste país há, inclusive, uma empresa com a finalidade de que os próprios usuários monetizem seus "valiosos dados"[171].

Em abril de 2020, mais de 500 mil dados de usuários do aplicativo de vídeo-chamadas Zoom foram vendidos após uma falha no sistema de segurança, por menos de um centavo cada[172]. Em outro caso brasileiro, de maio de 2020, o Ministério Público de Brasília abriu um Inquérito Civil Público para apurar a venda de dados pessoais por parte da empresa Procob[173].

Grande parte destes dados é utilizado para melhor direcionamento de publicidade[174], nos denominados *ad-based businesses* (ou negócios baseados em publicidade). Em razão disto, a Apple adicionou, em outubro de 2020, um recurso em seu sistema operacional que obriga os desenvolvedores a consultar os usuários antes de rastreá-los na internet, gerando uma reclamação, por parte das empresas, de que seus modelos de negócios estariam sob ataque[175].

Malgradas as utilizações prejudiciais ao titular, existem, também, situações que são benéficas tanto a ele, quanto à sociedade em geral. Começemos pela segunda: Solove traz exemplos gerais de uso para prevenir um crime ou para salvar uma vida[176] – poderíamos pensar em situações que o *iter criminis* é mais longo, com etapas de preparação, no primeiro caso, e para prevenção de suicídio, no segundo.

A pandemia também nos trouxe uma situação neste sentido: o uso de dados de geolocalização tanto para prevenir a disseminação do vírus, quanto para alertar pessoas potencialmente infectadas, que possam ter tido contato com sujeitos doentes. Este tema está sendo objeto de debate neste período pandêmico, com institutos publicando artigos[177] a respeito da melhor maneira de tratar do tema, e governos, como o do estado do Rio Grande do Sul[178],

---

[171] "Earn cash, discounts, or cryptocurrency for connecting and exchanging your valuable data. Keep earning through ongoing data sales". A empresa é denominada Data Coup. DATA COUP. **The Personal Data Revolution**. Disponível em: < https://datacoup.com/#> Acesso em 3 out 2020.
[172] LIBERATORE, Stacy. **More than 500,000 zoom user credentials have been stolen and sold on the dark web for less than a penny each**. Disponível em: < https://www.dailymail.co.uk/sciencetech/article-8218723/More-500-000-Zoom-user-credentials-sold-dark-web-PENNY-each.html> Acesso em 10 ago 2020.
[173] CONVERGÊNCIA DIGITAL. **MP de Brasília abre inquérito para apurar venda de dados pessoais**. Disponível em: < https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=53773&sid=4> Acesso em 3 out 2020.
[174] Sobre isto, vide a primorosa explicação de Bruno Bioni em BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 14 – 31.
[175] ESPÓSITO, Filipe. **Facebook exec says ad-based businesses are 'under assault' by Apple's privacy changes**. Disponível em: < https://9to5mac.com/2020/10/06/facebook-exec-says-ad-based-businesses-are-under-assault-by-apples-privacy-changes/> Acesso em 10 out 2020.
[176] SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560, p. 519.
[177] SCHREMS, Max. ***Ad hoc* Paper (v 0.3) SARS-CoV-2 tracking under GDPR**. Disponível em: < https://noyb.eu/sites/default/files/2020-04/ad_hoc_paper_corona_tracking_v0.3.pdf> Acesso em 5 mai 2020.
[178] RIO GRANDE DO SUL. Comitê Científico de apoio ao enfrentamento à pandemia COVID-19. **Nota técnica sobre o rastreamento digital de contatos com smartphones, de 16 de maio de 2020**. Disponível em: <

tornando públicas orientações para o uso de dados nessas situações. Diversas cidades, como foi o caso de Porto Alegre[179], utilizaram estas informações para estabelecer a porcentagem de cidadãos que estavam seguindo o distanciamento social. A própria empresa que tratava estes dados publicou um estudo a respeito do cuidado com a privacidade[180].

Quanto aos benefícios ao próprio indivíduo, a situação mais importante é a criação de perfis dos usuários para combater fraudes e incidentes de segurança:

> 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[181].

Além deste, Bioni traz outro relevante exemplo de uso secundário: a verificação de grave vício de fabricação por uma montadora de veículos:

> Por obrigação legal, ela deve contatar os consumidores para sanar tais vícios. No entanto, ela não comercializa tais bens de consumo, de modo que ela deve ter acesso aos dados pessoais dos consumidores por meio das agências de veículos para haver um *recall* efetivo. Nos contratos de compra e venda de veículos não há a previsão do compartilhamento de dados pessoais dos consumidores para tal finalidade, de modo que isso consiste em um uso secundário[182].

Notório está, à vista deste cenário, o tênue equilíbrio entre vantagens e desvantagens do uso secundário de dados. Assim como ele pode acarretar graves violações de direitos aos titulares ele pode, também, salvar suas vidas – tudo a depender de como o uso destes dados é manejado.

---

https://www.inova.rs.gov.br/upload/arquivos/202010/09200211-rastreamento-digital-de-contatos-comitecientifico16maio2020-atualizado-em-09out2020.pdf> Acesso em 5 abr 2020.

[179] PORTO ALEGRE. **Painel de mobilidade e distanciamento**. Disponível em:< https://infografico-covid.procempa.com.br/distanciamento-social> Acesso em 10 set 2020.

[180] MOURA, Raíssa; FERRAZ, Laura. **Meios de controle à pandemia da COVID-19 e a inviolabilidade da privacidade**. Disponível em: <https://content.inloco.com.br/knowledge/covid/sum%C3%A1rio> Acesso em 10 jun 2020.

[181] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 241.

[182] *Ibid*., p. 245

2. As possíveis respostas legais à datificação

2.1 A crise do consentimento: do enfoque individual à proteção coletiva

É possível dizer que estamos vivenciando um esplendor no que toca às legislações de proteção de dados pessoais. Entre 1973 e 2009, a média de novas legislações a respeito do tema era de 2.7 por ano; entre 2010 e 2019, a média foi de 5.3, chegando a um total de 134 leis em abril de 2019[183].

Na América do Sul, a Argentina é o país que apresenta, no momento, a experiência mais rica em proteção de dados pessoais[184]. Além dela, o Chile já possui uma lei protetiva desde 1999[185] - com incorporação, em 2018, da proteção de dados no rol de direitos fundamentais da Constituição[186] -, o Uruguai desde 2008[187], a Colômbia desde 2012[188] e o Equador está em processo de elaboração[189] de sua primeira lei tratando do tema.

Estas leis, assim como o RGPD[190], têm em comum o consentimento como base legal autorizativa por excelência. Danilo Doneda define este instituto da seguinte maneira:

> O consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. Sua utilização como instrumento paradigmático para a tutela dos dados pessoais deve ser observada a partir de seus efeitos na sua concreta aplicação ao caso dos dados pessoais e seus efeitos[191].

---

[183] GREENLEAF, Graham. **Countries with data privacy laws – by year 1973-2019**. Disponível em: < https://ssrn.com/abstract=3386510> Acesso em 8 set 2020, p. 2. O mesmo autor possui um interessantíssimo artigo com uma tabela tratando a respeito de todas essas leis: GREENLEAF, Graham. Global tables of privacy laws and bills. **Privacy Laws & Business International Report**, fev. 2019.

[184] 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, p. 279. Para uma explicação a respeito da experiência argentina, vide RAMINELLI, Francieli Puntel; RODEGHERI, Leticia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de Decisões Proferidas pelo Supremo Tribunal Federal. **Cadernos do Programa de Pós-Graduação em Direito/UFRGS**, v. 11, n. 2, 2016, p. 142 – 151.

[185] CHILE. **Ley nº 19.628 – Sobre protección de la vida privada**. Santiago, 18 de agosto de 1999. Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599> Acesso em 9 set 2020.

[186] CHILE. **Ley nº 21.096 – Consagra el derecho a protección de los datos personales**. Santiago, 5 de junho de 2018. Disponível em: < https://www.bcn.cl/leychile/navegar?idNorma=1119730> Acesso em 9 set 2020.

[187] URUGUAY. **Ley nº 18.331 – Ley de Protección de Datos Personales**. Montevidéu, 11 de agosto de 2008. Disponível em: < https://www.impo.com.uy/bases/leyes/18331-2008> Acesso em 10 set 2020.

[188] COLOMBIA. **Ley Estatutaria 1581 de 2012**. Bogotá, 18 de outubro de 2012. Disponível em: < http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html> Acesso em 15 set 2020.

[189] ECUADOR. **Proyecto de Ley Orgânica de Protección de Datos Personales**. Quito, 19 de setembro de 2019. Disponível em: < https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf> Acesso em 15 set 2020.

[190] A evolução das legislações europeias está, de alguma maneira, englobada nas quatro gerações de leis que serão tratadas abaixo. Desta maneira, para evitar que se repetissem informações e para uma exposição mais clara, optou-se por mencionar as leis na América do Sul neste ponto e, na Europa, mais adiante.

[191] 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, p. 298.

O consentimento é, assim, o mais importante instituto jurídico para o exercício da autodeterminação informacional[192]. Isto fica claro, no Brasil, a partir de uma análise histórica da tramitação da LGPD[193]. Na primeira versão do anteprojeto, de 2010, o consentimento possuía um dispositivo próprio[194], enquanto as demais bases legais eram tratadas como exceção, em artigo específico[195].

Em 2015, quando o Ministério da Justiça apresentou nova versão do anteprojeto de lei, houve significativa alteração neste ponto, tendo as bases legais de tratamento sido unificadas em um mesmo artigo, de forma muito semelhante ao que preceitua a LGPD. Entretanto, mesmo com estas modificações o consentimento não deixou de ser o vetor principal da lei[196]. Bioni destaca três pontos neste sentido: o adjetivamento extensivo do consentimento pela lei, o fato de grande parte dos princípios terem seu centro gravitacional no indivíduo e as diversas disposições que reforçam o controle dos dados pessoais pelo consentimento[197].

É necessária a compreensão das gerações de leis de proteção de dados para um melhor entendimento a respeito do protagonismo do titular dos dados e do papel do consentimento nas legislações a respeito do tema. Esta sistematização foi realizada por Mayer-Schönberger em

---

[192] MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais**: uma análise dos seus fundamentos e elementos. Dissertação (Mestrado em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019, p. 88.

[193] Para uma análise mais detida, vide BIONI, Bruno. **De 2010 a 2018**: a discussão brasileira sobre uma lei geral de proteção de dados. Disponível em: < https://ab2l.org.br/de-2010-2018-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/> Acesso em 5 out 2020.

[194] Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11. §1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização. §2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação. §3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique. §4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais. §5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais. §6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular. §7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade. §8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

[195] Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para: I – cumprimento de uma obrigação legal pelo responsável; II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública; III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º; IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; V – exercício regular de direitos em processo judicial ou administrativo; VI – proteção da vida ou da incolumidade física do titular ou de terceiro; VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

[196] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 127.

[197] *Ibid*., p. 127 – 128.

artigo seminal[198] já amplamente citado[199]. O autor apresenta quatro gerações para estabelecer o que significa proteção de dados, visto que as conotações associadas ao termo mudaram repetidamente e substancialmente ao longo dos anos[200].

A primeira geração de leis de proteção foi promulgada em resposta à emergência de processamento eletrônico de dados dentro de governos e grandes empresas[201]. Seus grandes exemplos são a lei do *Land* alemão de Hesse, de 1970, a lei nacional Sueca, de 1973, conhecida como *Datalag*, e o *Privacy Act* estado-unidense, de 1974. Nesse contexto, as leis propunham-se a regular um cenário no qual centros de tratamentos de dados concentrariam a coleta e a gestão de informações[202], tendo em vista que alguns países começaram a cogitar a criação de *National Data Centers*.

Outra função importante foi a de balanceamento de poderes dentro do estado, tendo em vista que é primariamente o Poder Executivo que, com a utilização de dados pessoais, aumenta desproporcionalmente seu poder[203] em relação aos outros dois poderes. A geração primogênita decorre, assim, da preocupação com o processamento massivo dos dados pessoais dos cidadãos na conjuntura de formação do Estado Moderno[204], focando-se na tecnologia, a ser regulada com normas rígidas.

A segunda geração teve, como foco, os direitos de privacidade individuais do cidadão, com as questões do *right to be alone* e da delimitação da esfera íntima de cada um voltando à tona[205]. A diferença básica em relação à primeira é sua estrutura, baseada na consideração da privacidade e na proteção de dados como uma liberdade negativa, a ser exercida pelo próprio

---

[198] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 219 – 242.

[199] Ver, por exemplo, 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, p. 174 - 180; BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 109 - 113; MENDES, Laura Schertel; BIONI, Bruno. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 800.

[200] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 219.

[201] *Ibid*., p. 221.

[202] 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, p. 175.

[203] *Ibid*., p. 175, nota de rodapé nº 112.

[204] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 110.

[205] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 226.

cidadão[206]. A mudança, portanto, se deu no âmago regulatório, preocupando-se não só com as bases de dados, mas, também, com a esfera privada[207]. Exemplos foram as leis francesa, norueguesa e austríaca de proteção de dados pessoais, todas de 1978.

Houve, aqui, uma alteração essencial nas legislações, centrando o foco no cidadão e abrindo caminho para o protagonismo do consentimento. Elas transferiram para o próprio titular a responsabilidade de proteger seus dados pessoais – obrigação esta que antes cabia ao Estado[208].

A terceira geração surge a partir da percepção de que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito essencial para uma efetiva participação na vida social[209]. A questão não era *se* o titular gostaria de integrar-se socialmente, mas *como*[210], pois percebeu-se que a interrupção no fornecimento de informações pessoais pode gerar a exclusão de alguma dimensão social. Assim, as normas de proteção buscaram assegurar a participação do indivíduo sobre toda a movimentação de seus dados pessoais, da coleta ao compartilhamento[211].

O principal marco desta geração foi a decisão do censo do Tribunal Constitucional Federal alemão. Ele coroou o controle dos dados pelo titular e a possibilidade de realista participação social ao estabelecer o direito fundamental à autodeterminação informativa. Há, aqui, uma dimensão de peso: saiu-se do binômio coleta/participação social *vs* proteção/exclusão social para as diversas nuances viabilizadas pelo controle.

A quarta geração também veio à tona em função dos problemas da geração anterior. Aqui, percebeu-se que o titular normalmente está em uma péssima posição de barganha quando busca exercer os seus direitos[212]. Assim, esta fase buscou suprir as desvantagens do enfoque individual, entendendo-se a veemente necessidade de instrumentos que elevem o padrão coletivo de proteção. Esta geração se orienta ao fortalecimento da posição da pessoa em relação

---

[206] 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, p. 177.
[207] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 110
[208] *Ibid*., p. 111.
[209] 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, p. 177.
[210] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 229.
[211] *Ibid*., p. 231.
[212] *Ibid*., p. 232.

às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação[213].

Outra fundamental característica é a disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais. Estas são tanto mais importantes quanto menor o poder de barganha dos indivíduos para autorizar o tratamento de seus dados[214] - além de serem um requisito para a obtenção da adequação europeia, por exemplo[215].

Neste contexto, fica perceptível a convergência temporal entre a perda de controle pelos titulares e a ascensão dos dados como principal ativo econômico, com a rápida disseminação do uso secundário de dados. Focar na perspectiva individual de proteção é necessariamente voltar uma geração de leis de proteção de dados, sob pena de constatar os mesmos erros que motivaram o desenvolvimento da mais recente geração.

Sob esse pano de fundo, a doutrina desenvolveu o *mito*, ou a crise, do consentimento, entendendo que ele sempre se apresenta como um elemento acessório ligado a determinada situação[216]. Ocorre que, no confronto de situações reais, a alternativa à não revelação de informações é a renúncia a bens ou serviços, em razão da disparidade de meios e poder entre o controlador e o titular dos dados.

Outra questão é que o consentimento pode ser um procedimento inócuo[217], existindo diversas barreiras psicológicas para que haja um efetivo controle dos dados pelo indivíduo. Aquela que mais importa para este trabalho diz respeito à lógica do *trade-off*, tendo em vista que há gratificações imediatas – com a utilização do produto ou serviço em troca dos dados pessoais – e prejuízos mediatos ou distantes[218] – com a violação da privacidade em momento posterior, diversas vezes nem mesmo conhecido pelo titular daquelas informações. A metáfora de Solove, de que a grande maioria dos problemas quanto à *privacy* carecem de corpos mortos[219], é perfeita para explicar esta situação.

---

[213] 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, p. 179.
[214] *Ibid*., p. 180.
[215] Artigo 45.º - Transferências com base numa decisão de adequação: 2.Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos: b) **A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes** no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros. (Grifei)
[216] 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, p. 298.
[217] *Ibid*., p. 299.
[218] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 141.
[219] SOLOVE, Daniel J.. "I've got nothing to hide" and other misunderstandings of privacy. **San Diego Law Review**, n. 745, 2007, p. 768.

Sobre o tema, Bioni traz interessantes exemplos de estudos empíricos que confirmam a insuficiência da proteção pelo consentimento[220]. O primeiro[221] mostrou que os usuários não estão capacitados para tomar decisões informadas no tocante ao controle de seus dados, visto que os modelos mentais criados em nossa mente fazem com que dificilmente consigamos conhecer efetivamente o funcionamento das tecnologias de coletas de dados. O segundo[222] mostra que a corrida armamentista tecnológica faz com que a escolha dos titulares a respeito de seus dados seja dificultada, tendo em vista que o estado da arte da tecnologia é constantemente melhorado. O terceiro[223] mostrou que é errado o discurso de que as pessoas se sentem confortáveis ao trocar seus dados por produtos e serviços, quando, a partir de entrevistas, expôs que 91% dos consumidores consideraram injusta a coleta de informações sem seu conhecimento, havendo um descompasso entre o *trade-off* e a vontade dos titulares.

Solove definiu o dilema do auto-gerenciamento[224] em dois amplos tipos de problemas: cognitivos, dizendo respeito aos desafios causados pela maneira como humanos tomam decisões, e estruturais, tratando da forma pela qual as decisões a respeito da *privacy* são projetadas[225].

O primeiro tipo de problema é dividido em dois aspectos: o problema do indivíduo não-informado[226] e o problema da tomada de decisão distorcida[227]. Aquele diz respeito tanto ao componente de informar os titulares a respeito dos dados coletados e utilizados que lhe dizem respeito – um aviso prévio –, quanto permitir que eles decidam se aceitam, ou não, estes usos e coletas – a escolha. Apesar disto, que ficou conhecido nos Estados unidos como aviso e escolha[228], a maioria das pessoas não parecem se engajar no auto-gerenciamento, notando-se uma falência das políticas de privacidade[229], pelo que é, de praxe, reclamado: elas são muito longas e de difícil compreensão, com o usuário podendo tomar pouca ou nenhuma ação em

---

[220] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 141 – 153.
[221] *Ibid*., p. 141 – 144.
[222] *Ibid*., p. 145 – 147.
[223] *Ibid*., p. 148 – 152.
[224] O termo utilizado, em inglês, é *privacy self-managment*. SOLOVE, Daniel J.. Introduction: privacy self-management and the consent dilemma. **Harvard Law Review**, v. 126, n. 7, mai./2013, p. 1880 – 1903.
[225] *Ibid*., p. 1883.
[226] O termo em inglês é *uninformed*, e pode tanto significar *desinformado* como *não informado*. Pelo desenvolvimento que o autor faz a respeito do tema optou-se pelo segundo.
[227] O termo em inglês é *skewed*, que pode significar *enviesado* ou *distorcido*. Optou-se pelo segundo por se entender que, em português, *distorcido* tem conotação mais próxima da ideia do autor de decisão sobre a qual a vontade não está clara, chegando no limiar do vício.
[228] Notice and choice. *Ibid*., p. 1884.
[229] Por exemplo, um estudo mostrando que apenas 4,5% dos entrevistados disseram sempre ler a política de privacidade dos sites que utilizam e 14,1% responderam que frequentemente o fazem. MILNE, George R.; CULNAN, Mary J. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. **Journal of Interactive Marketing**, n. 15, 2004, p. 21.

relação a ela. Há aqui, também, o dilema do aviso: simplificar e facilitar uma situação que é complexa e fica mal-explicada se dita com poucos detalhes[230].

O segundo problema cognitivo, da tomada de decisão distorcida, diz respeito ao fato de os indivíduos frequentemente entregarem os dados a eles relacionados em troca de pequenos benefícios, além de faltar expertise para corretamente verificar as consequências disto[231]. Haveria, aqui, um paradoxo entre a suposta relevância da privacidade e os comportamentos tomados pelos indivíduos. O nó é desfeito pela psicologia: é falso assumir que as pessoas tomam decisões racionais em seu melhor interesse em todos os momentos, além de perceber que a percepção de privacidade é contextual, e não abstrata[232].

É exatamente neste ponto que Nissenbaum busca construir uma teoria para solucionar os problemas trazidos pelas novas tecnologias. O ponto central de sua tese é que o *right to privacy* não é nem um direito ao segredo, nem um direito ao controle, mas um direito a um adequado fluxo de informações pessoais[233]. Como explica Bioni, ela propõe que o trânsito das informações pessoais tem um valor social, guiado por considerações políticas e morais, sendo estes os critérios que determinam ser ele apropriado ou não[234]. Nesta base, haverá uma violação à *privacy* quando houver um descumprimento à *integridade contextual*[235].

A integridade contextual, assim, vincula uma adequada proteção à *privacy* a contextos específicos, exigindo que tanto a coleta, quanto a disseminação de informações, sejam apropriadas ao contexto, obedecendo as normas reguladoras de distribuição dentro de cada um destes[236]. Ela está calcada em três elementos: os atores e os atributos, ou tipos, de dado pessoal – aos quais Bioni, propondo uma leitura progressiva, incluiu no fluxo interno[237] – e a forma de disseminação – que o mesmo autor abarcou no fluxo externo[238].

---

[230] SOLOVE, Daniel J.. Introduction: privacy self-management and the consent dilemma. **Harvard Law Review**, v. 126, n. 7, mai./2013, p. 1885.
[231] *Ibid*., p. 1886.
[232] *Ibid*., p. 1887.
[233] NISSENBAUM, Helen. **Privacy in context**: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010, p. 127.
[234] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 197.
[235] *Contextual Integrity*, no termo em inglês. O conceito foi desenvolvido em artigo publicado pela autora em 2004: NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review**, v. 79, n. 1, fev. 2004, especialmente p. 136 e ss.
[236] *Ibid*., p. 119.
[237] Aqui, trata-se de identificar o vínculo entre os dois e determinar a esfera social em que estão inseridos, o que parametrizará todo o fluxo informacional. BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 199 – 200.
[238] O fluxo interno, ao final, diz respeito ao contexto e a expectativa de privacidade que ele exprime. *Ibid*., p. 200 – 201.

A autora define contexto como configurações sociais estruturadas com características que evoluem ao longo do tempo, e que estão sujeitas a uma série de fatores e contingências de propósito, lugar, cultura, acontecimentos históricos etc[239]. É um processo de decisão heurístico, cujo centro de análise não está focado em capturar o significado completo da *privacy*, mas identificar como sucedem a violação a tal direito[240]. A integridade contextual é, desta maneira, uma alternativa normativa em que a proteção de dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados[241].

Os problemas estruturais, por outro lado, são subdivididos em três: o de escala, o de agregação e o de avaliação de danos. Mesmo se desconsiderarmos os problemas cognitivos, as questões estruturais estabelecem uma grande dificuldade à proteção da privacidade, como impedir a possibilidade dos titulares de avaliar os custos e os benefícios de consentir nas mais diversas hipóteses e situações[242].

O auto-gerenciamento não funciona em grande escala, tendo em vista a enormidade de empresas que coletam e usam os dados pessoais – e o número tende a crescer, uma vez que as informações ganham cada dia mais valor. O problema se torna ainda maior porque a escala facilita a falta de transparência: muitas vezes as pessoas sabem que seus dados estão sendo tratados por determinada entidade, mas desconhecem quais ou de que maneira isto é realizado[243].

O problema da agregação está intimamente ligado à noção da inexistência de dados irrelevantes. O titular não consegue determinar, no momento da coleta dos dados a ele relativos, como aquelas informações poderão ser agregadas a outras no futuro, compondo dados inteiramente novos e, muitas vezes, mais valiosos. É o que Solove denomina efeito agregacional; pequenos *bits* de dados inócuos podem dizer muito quando combinados[244].

Por fim, a última questão estrutural, de avaliação de danos, possui íntima relação com a lógica do *trade-off*: a privacidade é uma questão de gerenciamento informacional de longo período, enquanto decisões a respeito do consentimento estão vinculadas a benefícios de curto prazo[245].

---

[239] NISSENBAUM, Helen. **Privacy in context**: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010, p. 130.
[240] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 198, nota de rodapé nº 14.
[241] *Ibid*., p. 198.
[242] SOLOVE, Daniel J.. Introduction: privacy self-management and the consent dilemma. **Harvard Law Review**, v. 126, n. 7, mai./2013, p. 1888.
[243] *Ibid*., p. 1889.
[244] *Ibid*., p. 1890.
[245] *Ibid*., p. 1891.

Em consonância com o cenário apontado por estes estudos, Floridi defende a atenção à perspectiva coletiva de proteção de dados pessoais a partir da constatação de que as novas tecnologias tratam as pessoas não como indivíduos, mas como membros de grupos específicos, onde o grupo é o foco de interesses como portadores de direitos, valores e potenciais riscos[246]. Isto tem especial relevância, como vimos na parte 1.1, em uma sociedade marcada pelo *Big Data* – e que o autor faz questão de explicitar:

> O *Big Data*, especialmente, tem maior probabilidade de tratar gêneros (de consumidores, usuários, cidadãos, demografia populacional, etc) do que espécies (você, Alice, eu), e, consequentemente, grupos em vez de indivíduos. Mesmo de um ponto de vista nominalista, nós devemos reconhecer que tanto usuários hostis quanto usuários admiradores do *Big Data* talvez não se importem especificamente sobre Alice, mas apenas se Alice, quem quer que ela seja, pertence ao grupo que regularmente vai à igreja local, ou à mesquita, ou à sinagoga, usa o *Grindr*, ou tirou uma licença médica para fazer um aborto, ou compartilha de alguma característica que você escolha. Em uma terminologia militar, Alice dificilmente será um *High Value Target*, como um prédio específico. Ela frequentemente será parte de uma *High Pay-Off Target*, como um tanque em uma coluna de tanques. É a coluna que importa[247].

Para solucionar este problema, Floridi propõe uma nova maneira de interpretação: entender a informação como parte constitutiva da identidade do grupo[248] e, por isto, merecedora de proteção[249]. Uma hermenêutica da privacidade em termos da proteção da informação que constitui um indivíduo, tanto individualmente considerado, quanto em termos de grupo, é mais adequada para dar sentido à proteção coletiva dos dados[250]. A partir disto, chega o autor a

---

[246] FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 97.

[247] *Ibid*., p. 98. Especificamente sobre o tratamento da perspectiva coletiva de proteção da privacidade na era do *Big Data*, vide KAMMOURIEH, Lanah (*et. al*). Group privacy in the age of Big Data. In: FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 37 – 66.

[248] O autor trata longamente no artigo o que seriam grupos e quais seriam eles. Menciona duas correntes: o nominalismo, entendendo que existem apenas indivíduos e que os grupos sociais seriam inventados, e o realismo, que entende existirem também os universais, ou *tipos*, defendendo que os grupos seriam descobertos. O autor argumenta por uma terceira visão: de que os grupos seriam projetados (*desgined*), sendo o resultado da conjunção entre o mundo e a mente. Para que isso seja possível, entende que os grupos são resultado das escolhas que fazemos a respeito das nossas observações – e, a partir disto, chega em um conceito fundamental da sua teoria: o nível de abstração (*Level of Abstraction,* ou *LoA*), que é o conjunto de observações. Tendo os observáveis características comuns, os indivíduos formam um grupo; tendo características diferentes, não o formam. Em resumo, Floridi entende que os grupos são projetados pelos nossos interesses epistemológicos e nossas práticas em conjunto com os nossos recursos ontologicamente restritos fornecidos pelo mundo. Também tratando da complexidade da definição de grupo, veja VITORELLI, Edilson. **O devido processo legal coletivo**: dos direitos aos litígios coletivos. 2 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 4.

[249] FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 95.

[250] *Ibid*., p. 85.

conjecturar justamente o tipo de informação como critério quando se tratar de venda de dados: prenuncia que a comercialização de algumas mais sensíveis podem ser proibidas, fazendo um paralelo com a venda de órgãos, enquanto outras, tidas como irrelevantes[251], poderiam ser alienadas, como ocorre atualmente com o cabelo ou com o sangue.

A mesma questão enfrentada pela quarta geração de leis de proteção de dados – a tutela do sujeito ao coletivo – foi encarada pelo processo civil brasileiro. Teori Zavaski inicia seu *Tutelas Coletivas* justamente tratando da evolução do sistema de tutela jurisdicional: do sujeito ao coletivo[252].

Zavaski estabeleceu sua taxonomia a partir dos mecanismos de tutela jurisdicional. A primeira possibilidade são as formas de tutela de direitos subjetivos individuais, classificados naquelas destinadas a serem tuteladas pelo próprio titular (disciplinados pelo Código de Processo Civil), e nas destinadas a tutelar coletivamente os direitos individuais, em regime de substituição processual (como a ação civil coletiva, compreendidos os mandados de segurança e o de injunção coletivos). Outra possibilidade são as ferramentas de tutela de direitos transindividuais, sendo direitos pertencentes a grupos ou a classes de pessoas indeterminadas (ações populares e ações civis públicas, por exemplo)[253]. Em razão desta divisão, ficou célebre o subtítulo de seu livro *tutela de direitos coletivos e tutela coletiva de direitos*.

Com isto, fica evidente que o Brasil possui um robusto arcabouço teórico e normativo para que a LGPD efetivamente se enquadre na mais recente geração de leis de proteção de dados, aumentando sua eficácia e gerando maior segurança jurídica. Fundamental será, neste ponto, o papel da Autoridade Nacional de Proteção de Dados, a quem cabe zelar pela proteção dos dados pessoais[254]: ela poderá elaborar diretrizes e regulamentos a respeito da melhor maneira a ser realizada a proteção coletiva. Além disso, poderá, também, atuar diretamente na tutela dos direitos transindividuais quando verificar possíveis infrações à LGPD.

---

[251] Há, neste ponto há uma divergência direta com o que decidiu o Tribunal Constitucional Federal alemão na decisão do censo e que foi posteriormente adotado pela doutrina: de que nenhuma informação é irrelevante, tendo em vista o poder de processamento computacional e a possibilidade de cruzamento de banco de dados. Além disto, também choca-se com a ideia de Danilo Doneda e Laura Schertel Mendes, já mencionada neste trabalho, a respeito da impossibilidade de considerar dados pessoais como *res in commercium*.

[252] ZAVASKI, Teori. **Processo Coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. São Paulo: Editora Revista dos Tribunais, 2016. Interessante notar que este livro tem origem em um artigo publicado pelo autor quando ainda professor da UFRGS, na revista desta faculdade de direito. A diferença fundamental entre o livro e o artigo é o termo utilizado: passou-se de *defesa* de direitos a *tutela* de direitos. O artigo é o seguinte: ZAVASKI, Teori Albino. Defesa de direitos coletivos e defesa coletiva de direitos. **Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul**, v. 11, 1996, p. 177 – 192.

[253] ZAVASKI, Teori. **Processo Coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. São Paulo: Editora Revista dos Tribunais, 2016, p. 26.

[254] Conforme o art. 2º, I, do Decreto nº 10.474/2020, que aprovou a estrutura da ANPD: Art. 2º Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação;

Outra maneira de retirar o ônus da proteção do indivíduo é utilizando outras bases legais autorizativas para tratar os dados. Pode, neste ponto, haver, *a priori*, uma contradição: poderá o titular estar mais protegido quando seus dados estiverem sendo tratados por outra base legal que não o consentimento? Como vimos até agora, sim: em função dos problemas estruturais e cognitivos, somado ao fato de as informações pessoais serem o ativo econômico mais importante da sociedade atual, a proteção atual é insuficiente para que haja um efetivo controle, pelo sujeito, de seus próprios dados, impossibilitando a concreta autodeterminação informacional. Transferir o ônus da salvaguarda aos operadores e controladores de dados, por meio de outras bases autorizativas, é uma maneira de diminuição da assimetria informacional, além de facilitar o fluxo de dados e de realizar o desenvolvimento econômico.

Talvez o grande exemplo neste sentido seja o tratamento baseado no legítimo interesse do controlador. Esta possibilidade foi positivada tanto no artigo 10º da LGPD[255], quanto no artigo 6º, f, do GDPR[256], e pormenorizado em considerandos deste último[257]. A distinção desta base legal em relação às outras positivadas é, justamente, não ter surgido sustentada no direito à autodeterminação informacional. Além disso, sua importância prática é enorme: cerca de 70% das empresas europeias utilizam esta norma como autorização para tratar dados pessoais[258].

Em razão de sua amplitude, maleabilidade e, por conseguinte, possível subjetividade, que poderiam causar a desproteção do titular, foi desenvolvido[259] o que ficou conhecido como teste do legítimo interesse[260], composto de quatro etapas.

---

[255] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

[256] Artigo 6º- Licitude do tratamento: 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

[257] O RGPD adotou uma técnica legislativa diversa da LGPD: trouxe considerandos, que não são vinculantes, antes do texto legal, explicitando algumas questões a respeito da matéria de proteção de dados e esclarecendo alguns pontos que poderiam restar duvidosos. Refere-se aqui especificamente aos considerandos 47 a 49.

[258] JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8, jul./set. 2020, p. 2.

[259] A origem é a opinião do Grupo de Trabalho do artigo 29: ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> Acesso em 6 out 2020.

[260] Ele está positivado no próprio 10º da LGPD.

A primeira etapa busca verificar a legitimidade do interesse. Para isto, são analisadas a situação concreta e a finalidade legítima do interesse do controlador. Será observado, portanto, se há algum benefício ou alguma vantagem ao controlador com o uso desses dados, perquirindo a existência de uma situação concreta que lhe dê suporte[261].

O segundo passo intenta verificar a necessidade da coleta daquelas informações para atingir a finalidade pretendida[262]. O objetivo é aferir a aplicação do princípio da minimização, diminuindo o impacto para os titulares dos dados.

A terceira fase consiste em um balanceamento entre os impactos sobre o titular dos dados pessoais e as legítimas expectativas do controlador. É a principal fase, com o sopesamento entre estes interesses aparentemente contrapostos, sendo uma tarefa árdua e complexa[263]. Neste ponto, é fundamental perquirir se o novo uso atribuído ao dado está dentro das legítimas expectativas do titular dos dados – parametrizado pela noção de compatibilidade – e de que forma os titulares serão impactados[264].

O quarto, e último, estágio, cuida das salvaguardas, reforçando o dever de transparência, e a possibilidade de o sujeito a quem as informações se refere optar por se opor ao tratamento, conhecido como *opt-out*. Somado a isto, deve o controlador adotar ações que mitiguem os riscos do titular dos dados, como a anonimização e a necessidade de elaboração de relatório de impacto à privacidade[265].

Fato é que nós nunca deixamos de nos tornarmos nós mesmos[266] e a tecnologia se aperfeiçoa cada vez mais rapidamente, alterando os instrumentos necessários para a proteção de dados pessoais. Esta é justamente a importância de fazer uma análise das ações que estamos tomando à luz das gerações de leis de proteção, tendo em vista sua evolução em razão da desproteção a partir dos avanços tecnológicos. Em um mundo onde o uso secundário de dados pessoais pode trazer terríveis implicações para os titulares dos dados pessoais, e onde o consentimento já não é mais suficiente para que se exerça um efetivo controle, apostar na proteção individual significa aumentar ainda mais a assimetria informacional, econômica e

---

[261] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 236.
[262] *Ibid*., p. 236.
[263] JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8, jul./set. 2020, p. 16.
[264] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 237.
[265] *Ibid*., p. 238.
[266] FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 97.

instrumental entre ele e o controlador destes dados – o que, ao final, gera uma desproteção ainda maior. A violação da privacidade é também prejudicial às companhias: a demanda por regras claras de proteção de dados veio, igualmente, dos setores empresariais, buscando um mercado com bases comuns mínimas de *compliance*, tornando-o mais competitivo[267] e menos selvagem.

2.2 A conciliação entre proteção e desenvolvimento

Nesta última parte, buscaremos trazer soluções – e, com elas, critérios – para a proteção do titular dos dados, tendo como farol a sociedade baseada em dados. Como vimos, não é possível onerar ainda mais o sujeito quanto à salvaguarda de sua privacidade. Assim, com as gerações de leis de proteção de dados, o equilíbrio entre privacidade e desenvolvimento econômico como pano de fundo, dividiremos a abordagem entre a proteção individual e a coletiva – aqui entendida em sentido amplo, como a retirada de encargos do indivíduo sem desprotegê-lo – pois é apenas quando pensadas em conjunto que podemos minimizar os perigos e maximizar os benefícios trazidos pelo uso secundário.

Quanto à primeira, justificaremos a partir da ideia de obrigação como processo, criadora de deveres anexos e norteada pela boa-fé. Quanto à segunda, e com o uso para finalidades distintas, dividiremos em dois cenários: i) defenderemos a possibilidade do uso de uma nova base legal autorizativa que não o consentimento do titular, com critérios a estabelecerem um efetivo resguardo dos direitos do titular; ii) levantaremos a possibilidade de acolhimento, no Direito brasileiro, da aplicação do teste de proporcionalidade trazido pelo GDPR, com as adaptações necessárias ao contexto nacional.

A extração de valor dos dados pessoais se dá por um *processo* de tratamento[268], que traz obrigações, orientadas por princípios, tanto para o controlador, quanto para o operador. Este procedimento está cada vez mais refinado, mais rápido e com menos intervenção humana. Os dados são ocorrências dinâmicas que, quanto mais lapidados, maior relevância possuem – por isto é tão importante o uso secundário de dados pessoais. O cruzamento entre bancos de dados e a coleta massiva de informações pessoais viraram uma espécie de caça ao tesouro da

---

[267] Daniela Copetti Cravo tratou com maestria a respeito da concorrência, especialmente em mercados digitais e com foco nos diversos custos que são propositalmente gerados (como custos de troca, de procura, de substituição, de comunicação) além de seus efeitos (como o *lock-in effect*). Para uma análise aprofundada, vide CRAVO, Daniela Copetti. **Direito à portabilidade de dados**: interface entre defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018, p. 64 e ss.

[268] 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, p. 178.

sociedade contemporânea: quem melhor desenvolver modelos preditivos e mais cedo conseguir prever o comportamento do usuário, melhor colocado estará no mercado.

No campo do Direito Civil brasileiro, a obrigação como processo[269], de Clóvis do Couto e Silva, se encaixa com maestria neste processo de tratamento de dados pessoais:

> Com a expressão "obrigação como processo", tenciona-se sublinhar o ser dinâmico da obrigação, as várias fases que surgem no desenvolvimento da relação obrigacional e que entre si se ligam com interdependência. (...) **Atos, evidentemente, tendem a um fim. E é precisamente a finalidade que determina a concepção da obrigação como processo[270]**. (Grifei)

A finalidade foi erguida à corolário da proteção de dados pessoais justamente por estarmos lidando com um processo de tratamento. Isto se explica pelo fato de o fim se constituir em um dos elementos mais fecundos para a sistematização jurídica, sendo a *causa finalis* um dos muitos conceitos transmitidos pela filosofia aristotélica[271].

É apenas garantindo as legítimas expectativas da outra parte que se mantém uma relação de continuidade – e o pilar de sua proteção no ordenamento jurídico é o princípio da boa-fé. Não é coincidência, também, que ele tenha sido erigido como uma das premissas norteadoras da LGPD: é o único princípio a estar no *caput*[272] do artigo 6º[273], que trata sobre eles. Assim como o respeito a estas expectativas, é comum que a ela se associem os deveres de cooperação e lealdade. Com ela são trazidas diversas novas funções, a principal sendo a eficácia criadora de deveres anexos àqueles que decorrem da lei ou do conteúdo expresso da relação jurídica[274].

Entendemos que, no campo da proteção de dados, o dever anexo mais importante na contínua relação entre o titular e o controlador, tendo sido estabelecida a finalidade, é a transparência. Isto ocorre porque nenhum controle pode ser exercido quando não se sabe o que controlar; é apenas quando o sujeito sabe quais informações a seu respeito estão sendo tratadas que ele poderá exercer os seus direitos.

Propomos a criação, para que haja esta direção pelos titulares, de uma *timeline* de dados pelas redes sociais, na mesma configuração das tradicionais *timelines* de cada um dos sites.

---

[269] O próprio Clóvis reconhece, na introdução do livro, que Larenz "chegou mesmo a definir a obrigação como um processo, embora no curso de sua exposição não se tenha utilizado, explicitamente, desse conceito". SILVA, Clóvis do Couto e. **A obrigação como processo**. Rio de Janeiro: Editora FGV, 2006, p. 20.
[270] *Ibid.,* p. 20 – 21.
[271] *Ibid*., p. 21, nota de rodapé nº 19.
[272] Neste sentido, a professora Judith Martins-Costa já alertava que a *estrutura fala*. MARTINS-COSTA, Judith. **Pessoa, personalidade, dignidade**: ensaio de uma qualificação. Tese (Livre-docência). Faculdade de Direito. Universidade de São Paulo. São Paulo, 2003, p. 233.
[273] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
[274] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019, p. 5.

Neste local, poderiam os indivíduos verificar quais informações estão sendo tratadas, para quais finalidades, com qual frequência e para quem estão sendo transferidas. Mais do que isto: poderiam exercer diretamente ali os direitos que lhe confere o artigo 9º da LGPD. Para as demais empresas que possuam endereço virtual, recomendamos a esquematização, no próprio portal do cliente, dos dados utilizados. Há empresas, como a Apple, que estão montando estas informações inspiradas na forma de uma tabela nutricional, mostrando quais dados estão sendo utilizados para quais fins. Com o objetivo de que não haja distorções que muitas vezes podem inviabilizar negócios, entendemos que pode haver procedimentos simplificados às micro e pequenas empresas, a serem estabelecidos pela ANPD[275] – visto que, ao contrário das *big techs*, aquelas dificilmente utilizarão o *Big Data* como modelo de negócio.

Ainda neste ponto, é primordial pensar em estratégias de privacidade por padrão (*privacy by default*[276]) como forma de atender ao princípio da necessidade. Como o nome mesmo diz, esta técnica busca estabelecer a proteção de dados como regra – deixando desmarcadas as caixas de preenchimento que permitem aos sites a coleta de dados para fins de *profiling* ou de marketing, por exemplo. Assim, é possível mitigar um dos problemas do consentimento: o de autorizar o processamento de dados excessivos por acreditar que, sem esta permissão, não seria possível acessar determinado produto ou serviço. O cerne, aqui, é a inversão da lógica: o "eu concordo" seria dado para a utilização mínima, e não máxima, de informações, protegendo o titular.

Outra ferramenta que deve ser levada em conta é a privacidade por desenho[277] (*privacy by design*). Ela diz respeito à criação de sistemas que facilitem o manuseio pelo usuário, construídos tendo, como pilar, a privacidade de quem utilizará a aplicação[278]. Na prática, o desenvolvimento e a manutenção, seja das redes sociais, seja de sites, deve ser pensado a partir dos princípios norteadores da disciplina protetiva dos dados, principalmente a minimização, a transparência, a confidencialidade e o controle[279].

---

[275] Conforme o artigo 2º, XVIII, do Decreto nº 10.474: Art. 2º Compete à ANPD: XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação possam adequar-se ao disposto na Lei nº 13.709, de 2018;
[276] Sobre o tema, especialmente no âmbito do GDPR, ver JASMONTAITE, Lina (*et. al*). Data protection by design and by default: framing guiding principles into legal obligations in the GDPR. **European Data Protection Law Review**, v. 4, n. 2, p. 168 – 189, 2018.
[277] O termo também é traduzido como *privacidade pelo projeto*. Optamos, aqui, por traduzir como *desenho* em razão da formação do produto levando em conta a privacidade – *desenhando-o* a partir disto.
[278] ARTICLE 29 DATA PROTECTION WORKING PARTY. **The future of privacy**: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf> Acesso em 20 out 2020, p. 14.
[279] *Ibid*, p. 15.

Com base nisto, a tutela da confiança no campo da proteção de dados pessoais

> abrange tanto a crença nas informações prestadas quando de que aquele que tenha acesso aos seus dados, por força do consentimento dado, não se comporte de modo contraditório a elas e respeite a vinculação à finalidade de utilização informada originalmente[280].

Exatamente por isto que a doutrina entende que os princípios da boa-fé e da confiança estão entrelaçados e detêm uma relação de complementaridade um para o outro[281]. A partir dos deveres decorrentes da boa-fé que se estabelecem as situações de confiança a serem tuteladas.

Fica claro, assim, que o cidadão também exerce domínio sobre seus dados quando estes são tratados de acordo com suas legítimas expectativas. A ausência de consentimento não equivale à ausência de controle: muitas vezes, *a contrario sensu*, levando em conta os problemas estruturais e cognitivos, o consentimento cria uma falsa impressão de proteção. Mais do que isso: a perspectiva subjetiva do direito fundamental à proteção de dados envolve a proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face do processo de tratamento[282], não dependendo exclusivamente de uma ação individual. A dimensão objetiva diz respeito à atribuição ao indivíduo da garantia de controlar o fluxo de seus dados[283].

É fundamental, por isto, que se vislumbre a privacidade em dois aspectos[284]: o negativo, desenvolvido desde o *right to privacy* de Brandeis e Warren, sendo uma obrigação de não-intervenção estatal, quanto pelo enfoque positivo, vista como uma função promocional, um dever de promover um estado de coisas.

A autodeterminação informacional estará, também, protegida quando o ônus não couber ao titular, visto que a chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais recai sobre os riscos atribuídos ao seu processamento por terceiros[285]. Esta proteção abrangente desloca o eixo da proteção para as possibilidades e finalidades do processamento[286]. Mais do que isso:

---

[280] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019, p. 5.
[281] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 229.
[282] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 176.
[283] *Ibid*., p. 177.
[284] Sobre isto, vide 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, p. 128 e ss..
[285] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. **Voto do Ministro Gilmar Mendes**. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020, p. 20.
[286] *Ibid*., p. 19.

> A impossibilidade de concretizar a autodeterminação informativa baseada meramente na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e uma estrutura dirigida à coleta de seus dados e preparada a excluí-lo de certas vantagens caso decida por não fornecê-los[287].

Esta é a justificativa para trazermos propostas que diminuam o ônus do titular. Buscaremos estabelecer critérios para que estas sugestões sejam efetivamente aplicáveis na prática, tendo em vista o papel da academia de formular modelos doutrinários destinados a explicitar, examinar e desenvolver os modelos jurídicos[288].

Levando em consideração que o uso secundário de dados não é permitido, em virtude de violar i) o dever de atingir o estado de coisas originariamente vinculado pela finalidade estabelecida ao tratar informações à novos fins e ii) o artigo 6º, I, *in fine*, da LGPD, não possibilita o *tratamento posterior de forma incompatível com a finalidade*[289], pode-se pensar na aplicação de bases legais distintas do consentimento para o tratamento do mesmo dado com finalidades diversas. Esta possibilidade se baseia no fato de que os dados são multi-relacionais, podendo uma mesma informação tanto se referir a mais de um titular, quanto ser polissêmica, com significados distintos a depender do contexto.

Se torna possível, desta maneira, que os direitos do titular se mantenham resguardados e que os dados sejam utilizados como fonte de inovação e tecnologia. Interessante notar que a LGPD exige apenas a notificação do titular dos dados quando seu tratamento tiver sido autorizado com base no consentimento e houver posterior mudança de finalidade, incompatível com a originalmente anuída:

> Art. 9º, § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Pela análise do dispositivo, percebe-se que não é necessário um novo consentimento; o direito que o titular dos dados possui, em caso de mudança de finalidade, é de revogar o consentimento anteriormente exercido. A nossa proposta, de possibilitar o tratamento a partir

---

[287] 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, p. 320.
[288] MARTINS-COSTA, Judith. Apresentação – Autoridade e utilidade da doutrina: a construção dos modelos doutrinários. In: MARTINS-COSTA, Judith. **Modelos de Direito Privado**. São Paulo: Marcial Pons, 2014, p. 11.
[289] 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**; (Grifei).

de uma base legal distinta, parte de três constatações pragmáticas. A primeira, de que há um maior resguardo ao controlador quando este baseia seu tratamento em uma base autorizativa, e não apenas em um comunicado ao titular apto a gerar neste um direito potestativo, de revogar seu consentimento. Este esquema, então, trará maior segurança jurídica aos agentes de tratamento, impactando, inclusive, em uma possível ação posterior de responsabilidade civil[290]. A segunda, de que se manterá o titular dos dados protegido, visto que o tratamento terá lastro em uma das hipóteses admitidas pela LGPD, ao mesmo tempo que retirará um encargo do titular dos dados. A terceira, de que não será necessária uma interpretação extensiva do termo consentimento quando o tratamento original tiver sido lastreado em outra base legal.

O dispositivo que muito provavelmente será utilizado, neste caso, é o legítimo interesse do controlador. Em isto ocorrendo, mostra-se necessária a documentação[291] das quatro etapas do teste, a fim de possibilitar um controle posterior tanto pela ANPD, tanto pelo titular dos dados.

Neste ponto, por fim, a LGPD traz um tratamento diferenciado para os dados cujo acesso é público, dispensando a exigência de consentimento nos casos em que as informações foram tornadas manifestamente públicas pelo titular. Em ocorrendo esta situação, aplicar-se-á o seguinte dispositivo:

> Art. 7º, § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

Desta maneira, entendemos que a nossa proposta não se aplica nesta circunstância, tendo em vista a vontade do titular de publicização e as salvaguardas trazidas pelo próprio artigo.

---

[290] Isto fica claro quando se analisam os dispositivos que tratam das sanções. Destaca-se o seguinte: 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: § 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: **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**; (Grifei).

[291] Bioni esclarece que há divergência, principalmente no âmbito europeu, quanto à obrigatoriedade da documentação do teste. O autor entende que no Brasil, em razão de as etapas estarem explícitas na lei e com uma leitura conjunta do princípio da *accountability*, desagua-se na necessidade de documentação. Sobre isto, vide BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 245 – 247.

O tratamento do uso secundário de dados nos contextos brasileiro e europeu possui uma pequena distinção: o GDPR trouxe uma exceção à limitação da finalidade no que ficou conhecido como teste de compatibilidade. Ele é trazido pelo artigo 6º, 4, do GDPR:

> Art. 6º - Licitude do tratamento
> 4 - Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
> a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
> b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
> c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º;
> d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
> e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

O termo compatibilidade é utilizado em razão do cerne do dispositivo: verificar se o tratamento para outros fins é compatível com a finalidade originalmente estabelecida. Sendo compatível, o tratamento é lícito: a finalidade originalmente estipulada funciona, neste arcabouço, como vetor hermenêutico a distinguir contextos próprios e impróprios para o tratamento das informações, diminuindo a possibilidade de danos. Assim, o teste proporciona proteção ao titular e destrava possíveis impedimentos ao processo.

O primeiro passo busca vislumbrar toda e qualquer relação entre a finalidade originalmente acordada e aquela a ser estabelecida. Se trata de listar as possíveis – e necessárias - correspondências entre a situação existente e aquela que se buscará realizar. Interessante notar o termo qualquer, que institui um nível mínimo ao qual possa ser realizado o teste.

A segunda parte trata do contexto original no qual os dados foram tratados, nos remetendo à ideia de integridade contextual de Nissenbaum, anteriormente tratada. É o que Miragem define como conceito contextual da privacidade:

> recorde-se que a proteção dos dados pessoais se justifica pela proteção à privacidade do titular dos dados. Privacidade é conceito objetivo, mas também contextual, uma

> vez que se vincula à expectativa legítima do titular do direito em ter preservada, sob certas condições, informações a seu respeito da exposição pública[292].

O terceiro quesito trata do que a LGPD define como dados sensíveis[293], chamados de dados especiais pelo RGPD[294]. Dado sensível é aquele tipo de informação que, caso conhecida e submetida a tratamento, pode se prestar a uma potencial utilização discriminatória ou lesiva, e que apresenta maior risco potencial de dano[295]. Seu conteúdo apresenta uma vulnerabilidade especial: a possível discriminação[296]. A LGPD traz, por isto, um rol taxativo de possibilidades de tratamento[297]. Interessante notar que o teste de Carpenter, enunciado pela Suprema Corte dos Estados Unidos, também leva em conta a sensibilidade e a intimidade das informações coletadas, tendo em vista que ela pode conter as privacidades da vida.

Tendo em vista o risco ainda mais elevado do tratamento para outros fins, além de que a circulação de determinadas espécies de informações apresentaria um elevado potencial lesivo aos seus titulares[298], especialmente com avançadas tecnologias preditivas, faz-se mister levar em consideração, em uma das etapas de um teste que busca diminuir a possibilidade de dano, os dados mais propensos a esta situação.

O quarto ponto a ser considerado são as consequências do tratamento destes dados. Aqui, seriam necessários dois documentos, a serem elaborados pelo controlador, para que a operação não seja considerada irregular[299]: um relatório de risco, para controle *a priori*, e um relatório de impacto à proteção de dados, para controle *a posteriori*.

O relatório de risco seria elaborado antes de iniciado um novo tratamento e em conjunto com a base legal que irá justificar o processo. Propomos três parâmetros fundamentar o parecer:

---

[292] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019, p. 5.

[293] Art. 5º, 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;

[294] Há apenas uma referência a *dados sensíveis* no RGPD: entre aspas e dentro de parêntesis, no considerando 10: "(...) O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»)". Os consierandos 51 a 54, 71, 80, 91 e 97 também tratam do tema.

[295] 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, p. 143.

[296] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 83.

[297] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...)

[298] 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, p. 143.

[299] Seguindo o que determina o artigo 44, II, da LGPD: 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: II - o resultado e os riscos que razoavelmente dele se esperam.

a precisão da informação de que está se tratando, a frequência que será utilizada e por quanto tempo, além do número de pessoas constantes naquela base de dados.

O relatório de impacto é definido pelo artigo 5º, XVII[300], da LGPD, e, de regra, não é obrigatório: segundo o artigo 38[301], ele poder vir a ser solicitado pela ANPD. Entendemos que, neste caso, ele deve ser indispensável, em função do perigo que este tipo de utilização representa aos titulares. Isto deverá ocorrer a partir de um mapeamento, pelo controlador, dos procedimentos que utilizam dados, determinando as pessoas que a eles têm acesso, as salvaguardas existentes no próprio sistema – controle de acesso, por exemplo -, além das transferências que são realizadas.

O quinto passo menciona as garantias de criptografia e pseudonomização. Curioso notar que não se fala em *anonimização*. Isto se dá por uma razão simples: tanto o GDPR[302], quanto a LGPD[303], não consideram pessoais os dados anônimos e, por consequência, os posicionam fora do âmbito de aplicação da legislação.

Fica evidente, assim, a existência de uma substancial diferença[304] entre pseudonimização e anonimização. Naquela, as informações adicionais que permitiriam a identificação do titular são mantidas em separado pelos agentes de tratamento que podem, assim, reidentificar os dados se fizerem o uso desta informação[305]. Há uma sistematização maior

---

[300] Art. 5º, XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

[301] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

[302] Considerando 26: (...) Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

[303] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Sobre a questão da reversibilidade e da razoabilidade, ver BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 61 – 75.

[304] Sobre isto, vide DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 99 – 125.

[305] BIONI, Bruno. **Proteção de dados pessoais**: a função e os limites do consentimento. 2 ed. Rio de Janeiro: Forense, 2020, p. 69, nota de rodapé nº 118.

no GDPR se comparado à LGPD, com previsões, inclusive, de relaxamento de obrigações legais quando utilizada esta técnica protetiva[306].

A criptografia se dedica ao estudo, projeto e implementação de técnicas para comunicação segura entre múltiplas partes na presença de atacantes ou adversários – tendo estes, como objetivo, impedir a comunicação livre de perigos[307]. Como se verifica pela definição com amplo espectro de possibilidades, há uma diversidade de modelos regulatórios ao redor do mundo[308], além de diferentes maneiras de aplicação técnica – como a Infraestrutura de Chaves Públicas[309], por exemplo.

Na prática, este teste foi aplicado pelo Tribunal Europeu dos Direitos do Homem com base em interesses legítimos[310], direitos do titular[311], postulado da proporcionalidade[312] e informações a serem fornecidas ao titular dos dados[313]. As Autoridades holandesa e espanhola também o utilizaram para impor multas administrativas.

A Autoridade Nacional de Proteção de Dados Holandesa multou[314], em quinhentos e vinte e cinco mil euros, a Associação Real Holandesa de Tênis pela venda ilegal de dados de 350 mil membros a dois patrocinadores distintos, que utilizaram estas informações para marketing direcionado. A Autoridade justificou sua decisão em razão de a finalidade originalmente consentida para o tratamento dos dados não ser compatível com a venda subsequentemente ocorrida. Houve, assim, incompatibilidade com o princípio da finalidade, principalmente em razão de o procedimento ter ocorrido em um contexto diverso daquele que as expectativas legítimas confiavam. O fundamento jurídico, à vista disto, foi a falta de uma base legal que justificasse o tratamento, infringindo os artigos 5º e 6º do GDPR.

---

[306] *Ibid*., p. 69 – 70.
[307] ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito?. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 27.
[308] Para uma análise aprofundada do tema, ver LIGUORI FILHO, Carlos Augusto. Criptografia em debate: modelos regulatórios ao redor do mundo. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 61 – 76.
[309] Tratando detidamente do tema, MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 83 – 98.
[310] UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-13/16**. Disponível em: < http://curia.europa.eu/juris/liste.jsf?language=en&num=C-13/16> Acesso em 12 set 2020.
[311] UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-131/12**. Disponível em: < http://curia.europa.eu/juris/liste.jsf?num=c-131/12> Acesso em 12 set 2020.
[312] UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-293/12**. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-293/12> Acesso em 12 set 2020.
[313] UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-201/14**. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-201/14> Acesso em 12 set 2020.
[314] O caso é de março de 2020. AUTORITEIT PERSOONSGEGEVENS. **Boete voor tennisbon vanwege verkoop van persoonsgegevens**. Disponível em: < https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens> Acesso em 6 out 2020.

Por outro lado, a Agência Espanhola de Proteção de Dados aplicou[315] uma multa de cinco mil euros ao Partido Socialista da Catalunha (PSCPSOE). No caso, foram transferidos dados de uma relação médico-paciente ao partido político, sendo isto constatado em razão de constar, no cabeçalho da correspondência enviada pelo PSCPSOE, o nome do médico do destinatário da mensagem. A autoridade entendeu que houve descumprimento ao princípio de limitação da finalidade em razão de ter havido incompatibilidade no uso dos dados, violando as legítimas expectativas do paciente (que recebeu a carta) de suas informações permanecerem no âmbito médico.

É essencial que tenhamos uma Autoridade Nacional independente para que tudo isto funcione. Segundo Doneda, a independência é atributo intrínseco à própria razão de ser dessas autoridades, sendo efetivamente aplicada por meio de mecanismos que busquem isolar sua atuação da influência dos poderes estatais[316]. Nós corremos o risco de que isto não ocorra em razão do atual desenho institucional adotado pela LGPD[317]-[318]: a vinculação da Autoridade à Presidência da República, ao invés de estabelecê-la como entidade da administração indireta. O temor se justifica à vista da experiência tanto da primeira autoridade argentina, quanto da autoridade uruguaia – esta última também vinculada à Presidência[319]. Deveríamos, neste ponto, nos inspirar no artigo 8º da Carta de Direitos Fundamentais da União Europeia:

> Artigo 8º Protecção de dados pessoais 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm

---

[315] O caso é de agosto de 2020. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). Procedimiento Nº: PS/00449/2019. Reclamante: A.A.A. Reclamado: Partir dels Socialistes de Catalunya (PSCPSOE). Directora de la Agencia Española de Protección de Datos: Mar España Martí. Agosto de 2020. Disponível em: <https://www.dataguidance.com/sites/default/files/ps-00449-2019.pdf> Acesso em 2 out 2020.

[316] 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, p. 314.

[317] Cabe, aqui, uma explicação: originalmente a ANPD seria integrante da administração pública indireta e vinculada ao Ministério da Justiça. O artigo 55 do texto original, que determinava isto, foi vetado pelo então presidente Michel Temer, sob argumento de inconstitucionalidade do processo legislativo (especificamente sobre este ponto, vide VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 727 – 731). Após conversão da MP nº 869 na Lei nº 13.853/2019, criou-se o agora vigente artigo 55-A, que retirou o termo indireta além de vinculá-la à Presidência da República, e não mais ao Ministério da Justiça: Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. O Decreto que aprovou a estrutura regimental da Autoridade brasileira foi publicado apenas em 27 de agosto de 2020 (Decreto nº 10.474.20), entrando em vigor apenas com a nomeação do diretor-presidente.

[318] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. **IDEC – Instituto Brasileiro de Defesa do Consumidor**. São Paulo. 2019. Disponível em <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina> Acesso em 21 out 2020, p. 36.

[319] *Ibid*., p. 36.

> o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. **O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.** (Grifei).

O cumprimento eficaz dos limites e finalidades específicas do tratamento de dados invariavelmente perpassa a atribuição dessa função a uma autoridade independente[320]. Esta autonomia é atributo fundamental para que a missão da ANPD seja exitosa, tanto para a tutela do cidadão, quanto para a estruturação do sistema normativo de proteção de dados[321], além de essencial para exercer as competências que lhe cabem[322].

É somente com um robusto arcabouço teórico-pragmático que será possível usufruir das importantes benesses que a reutilização dos dados pessoais pode trazer sem descuidar da salvaguarda à privacidade dos titulares. Havendo coexistência de mecanismos de proteção coletiva e individual associada a uma ANPD independente é possível conciliar a tutela dos dados pessoais e o desenvolvimento econômico.

---

[320] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. **Voto do Ministro Gilmar Mendes**. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020, p. 26.

[321] 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, p. 315.

[322] As competências da ANPD estão no artigo 2º do Anexo I do Decreto nº 10.474 de 26 de agosto de 2020.

Conclusão

A proteção irrestrita dos dados pessoais impossibilita o desenvolvimento, e a proteção irrestrita do desenvolvimento gera uma sociedade imóvel e não-democrática, incapaz de qualquer atitude em razão da exposição absoluta. Possibilitar que as empresas obedeçam à LGPD e, ao mesmo tempo, que possam utilizar de dados para o desenvolvimento de soluções inovadoras, que melhorem a vida de todos, foi a ideia por trás deste trabalho. A partir desta concepção, buscou-se em doutrina, jurisprudência e demais fontes informativas, soluções para estabelecer este complicado equilíbrio.

O uso secundário de dados pessoais não é permitido no atual ordenamento brasileiro, seja por disposição expressa da LGPD, que proíbe usos que não observem o princípio da finalidade, seja pela estruturação teórica que Humberto Ávila construiu a respeito desta espécie normativa. Apesar disto, é possível compatibilizar a proteção de dados pessoais e o uso de dados para uma finalidade distinta da originalmente autorizada, desde que amparada em critérios que, primordialmente, retirem do titular o peso de proteger suas informações; é esta a hipótese que melhor responde a pergunta a que esse trabalho se propôs a abordar.

Como vimos, esta *reutilização* dos dados, a partir dos critérios propostos, acarreta uma nova finalidade – e, justamente por isto, está de acordo com o ordenamento jurídico brasileiro. A grande questão que ficou demonstrada é a possibilidade de utilização de bases autorizativas distintas do consentimento para permitir esta reutilização. Apenas neste contexto, permitindo a reutilização desde que observados tanto os princípios estruturantes do tema, quanto parâmetros controláveis, se torna possível conciliar a proteção da privacidade, a autodeterminação informativa e o desenvolvimento econômico, tendo em vista que o uso secundário de dados pessoais é aquele que mais valor traz às companhias –se tornando um ilícito lucrativo.

Confiar ao titular o controle de suas informações em uma sociedade inundada por dados é proteger a privacidade apenas em sentido formal, e não material, resultando em uma enorme falta de proteção. O senso comum vem ao encontro disto: marcar que se leu e se acordou com os termos de uso e a política de privacidade sem nem mesmo ter lido uma palavra ali escrita é um claro sintoma da falência em resguardar a privacidade. Não se pode forçar o titular a simplesmente concordar com o fornecimento de seus dados sob pena de restar socialmente excluído; deve-se protegê-lo sem que isto lhe seja extremamente oneroso.

A metáfora da mercadoria, claro, é uma hipérbole. Os dados a nós relacionados, mesmo que constitutivos de nossa personalidade, podem ser usados para desenvolver soluções que tornem nossos dias mais confortáveis. O problema, em verdade, não é a utilização em si, mas

justamente para qual finalidade ela se dará; a questão não é *o que*, mas *como* – e este é essencialmente um dilema de controle. Exatamente em vista disto que foi dedicada uma parte da presente monografia à teoria de Ávila: a Teoria do Direito tem, há muito, lidado com o problema do controle, seja das espécies normativas, seja da prestação jurisdicional. Necessitamos de uma sociedade transparente o suficiente para que seja possível a gerência sobre estes dados, mas que não se furte de utilizá-los com fins legítimos.

É exatamente este o ponto enfrentado pelas fundamentais obras que tratam da discriminação gerada a partir do processo de tratamento de dados – como o *Weapons of Math Destruction*, essencial à esta monografia -, tema no qual se inserem os pontos negativos trazidos pelo uso secundário de dados pessoais. Foi somente a partir da contraposição entre estes e os aspectos positivos que foi possível vislumbrar a miríade de situações benignas que este tipo de uso pode, também, proporcionar.

Decorrência disto é a constatação de que o tratamento de dados pessoais não pode ser demonizado apenas em função de seus riscos. Eles existem, e devem ser tratados – mais do que isto: evitados e demonstradas as providências tomadas para mitiga-los – a partir, principalmente, do postulado da proporcionalidade. As legislações protetivas de dados vieram para regular e trazer segurança jurídica no uso destas informações, não para proibi-las. Os operadores e controladores necessitam saber quais as obrigações lhe dizem respeito e quais cuidados precisam tomar em relação aos diferentes dados, nas diversas possíveis situações de utilização. Os titulares, por sua vez, precisam ter certeza de que seus direitos estão resguardados e, preferencialmente, devem conseguir verificar o esforço dos agentes de tratamento neste sentido.

Entendemos que a doutrina desta área em crescente expansão no Brasil deve evitar exageros protetivos que, por fim, acabam deixando de resguardar os titulares – esta situação ocorreu, no ordenamento brasileiro, logo após o advento do Código de Defesa do Consumidor, quando, a partir das diversas teorias que buscavam definir o que fosse este novo sujeito, passou a ser possível enquadrar relações clássicas de Direito Civil, gerando enormes distorções. É, sim, possível proteger os dados enquanto eles são tratados – e é exatamente este o espírito da LGPD.

Este trabalho, todavia, gerou mais questionamentos que soluções; ao fim, quanto mais aprendemos melhores perguntas fazemos, e não obrigatoriamente melhores respostas temos. Como conciliar o *Big Data* e o princípio da necessidade? Pode haver um mercado de dados, com valores maiores de acordo com a sensibilidade do dado? O capítulo dos direitos da personalidade do Código Civil se aplica à proteção de dados pessoais? Se sim, como fica a questão da proibição da limitação voluntária, tendo em vista que a proteção de dados é direito

da personalidade? Se aplicam estas regras às pessoas jurídicas? Estas são perguntas a serem respondidas por trabalhos que virão.

Bibliografia

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD). Procedimiento Nº: PS/00449/2019. Reclamante: A.A.A. Reclamado: Partir dels Socialistes de Catalunya (PSCPSOE). Directora de la Agencia Española de Protección de Datos: Mar España Martí. Agosto de 2020. Disponível em: <https://www.dataguidance.com/sites/default/files/ps-00449-2019.pdf> Acesso em 2 out 2020.

AGUIAR JÚNIOR, Ruy Rosado de. Interpretação. **Revista da Ajuris**, ano XVI, n. 45, mar. 1989.

ALDRICH, Rick. Privacy's Third-Party Doctrine: Initial Developments in the Wake of Carpenter. **SciTech Lawyer**, v. 15, n. 3, 2019.

ARAL, Sinan; ROY, Deb; VOSOUGHI, Soroush. The spread of true and false news online. **Science**, v. 359, n. 6380, mar. 2018, p. 1146 – 1151.

ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito?. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 27 – 40.

ARGENTINA. **Constituición de la Nación Argentina**. Buenos Aires, 3 de janeiro de 1995. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm> Acesso em 8 out 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2013 on Purpose Limitation**. Bruxelas, 2013. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> Acesso em 12 jul 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> Acesso em 6 out 2020.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **The future of privacy**: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf> Acesso em 20 out 2020.

ARTYUSHINA, Anna. **The EU is launching a market for personal data. Here's what that means for privacy**. Disponível em: <www.technologyreview.com/2020/08/11/1006555/eu-data-trust-trusts-project-privacy-policy-opinion> Acesso em 21 ago. 2020.

AUTORITEIT PERSOONSGEGEVENS. **Boete voor tennisbon vanwege verkoop van persoonsgegevens**. Disponível em: < https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens> Acesso em 6 out 2020.

ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 18 ed., rev. e atual. São Paulo: Malheiros, 2018.

BAKER JR., John S; PRYOR JR., William H. Justice Scalia on federalism and separation of powers. **Regent University Law Review**, v. 30, n. 57, p. 57 – 103, 2017.

BARTLETT, Jamie. **The people vs. tech**: how the internet is killing democracy. Londres: Ebury, 2018.

BERNSTEIN, Peter L. **Against the Gods**: the remarkable story of risk. Hoboken: Wiley, 1998.

BIONI, Bruno. **De 2010 a 2018**: a discussão brasileira sobre uma lei geral de proteção de dados. Disponível em: < https://ab2l.org.br/de-2010-2018-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/> Acesso em 5 out 2020.

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

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, dez./ 1890, p. 193 – 220.

BRASIL. **Decreto nº 10.474, de 26 de Agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226> Acesso em 20 out 2020.

BRASIL. **Lei nº 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9504.htm> Acesso em 3 out 2020.

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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.>. Acesso em 19 jun. 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm.>. Acesso em 19 jun. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em 19 jun. 2020.

BRASIL. Ministério da Justiça. **Anteprojeto de Lei para a proteção de Dados Pessoais**. Disponível em: < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/> Acesso em 20 set. 2020.

BRASIL. Ministério da Justiça. **Anteprojeto de Lei para a proteção de Dados Pessoais – nova versão**. Disponível em: < https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf> Acesso em 20 set 2020.

BRASIL. **Proposta de Emenda à Constituição nº 17 de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594> Acesso em 10 set. 2020.

BRASIL. Secretaria Nacional do Consumidor. **Ministério da Justiça notifica telefônica-vivo por serviço Smart Steps**. Disponível em: < https://www.justica.gov.br/news/ministerio-da-justica-notifica-telefonica-vivo-por-servico-smart-steps> Acesso em 3 out 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 22.337-8/RS. Relator: Ministro Ruy Rosado de Aguiar Júnior. 20 de março de 1995. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-eletronica-1996_77_capQuartaTurma.pdf> Acesso em 15 jun. 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.419.697/RS. Relator: Ministro Paulo de Tarso Sanseverino. 12 de novembro de 2014. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201303862850&dt_publicacao=17/11/2014> Acesso em 25 ago. 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.457.199/RS. Relator: Ministro Paulo de Tarso Sanseverino. 12 de novembro de 2014. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1364998&num_registro=201401261302&data=20141217&formato=PDF> Acesso em 25 ago. 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.758.799/MG. Relatora: Ministra Nancy Andrighi. 12 de novembro de 2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019> Acesso em 25 ago. 2020.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. **Voto do Ministro Gilmar Mendes**. Relatora: Ministra Rosa Weber. 7 de maio de 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em 13 jul. 2020.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Disponível em: < https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019> Acesso em 3 out 2020.

BROOKE, Sian. **Preserving privacy in the age of Big Data**. Disponível em: < https://www.oii.ox.ac.uk/blog/preserving-privacy-in-the-age-of-big-data/> Acesso em 15 mai. 2020.

CABRAL, Ernesto. **Telefónica del Perú vende ubicación de clientes y pone en riesgo su privacidad.** Disponível em: < https://ojo-publico.com/1393/telefonica-vende-ubicacion-de-clientes-y-amenaza-seguridad> Acesso em 3 out 2020.

CACHAPUZ, Maria Cláudia; PEREIRA, Mariana Viale. Big Data e o conflito entre a utilização dos dados e a proteção à intimidade e a vida privada. **Revista Jurídica Luso-Brasileira,** n. 1, ano 4, 2018, p. 1067 – 1085.

CACHAPUZ, Maria Cláudia. Informação e transparência: o acesso e a proteção de dados nominativos. **Revista Jurídica Luso-Brasileira**, n. 1, ano 5, 2019, p. 1557 – 1580.

CASTELLS, Manuel. **A Sociedade em Rede**. 8 ed, rev. e ampl. São Paulo: Paz e Terra, 2005.

CASTELLS, Manuel. **Ruptura**: a crise da democracia liberal. Rio de Janeiro: Zahar, 2018.

CHAO, Bernard (et. al). Why Courts Fail to Protect Privacy: Race, Age, Bias, and **Technology. California Law Review**, v. 106, n. 2, 2018.

CHILE. **Ley nº 19.628 – Sobre protección de la vida privada**. Santiago, 18 de agosto de 1999. Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599> Acesso em 9 set 2020.

CHILE. **Ley nº 21.096 – Consagra el derecho a protección de los datos personales**. Santiago, 5 de junho de 2018. Disponível em: < https://www.bcn.cl/leychile/navegar?idNorma=1119730> Acesso em 9 set 2020.

CLARKE, Roger A. Information technology and dataveillance. **Communications of the ACM**, v. 31, n. 5, mai./1988, p. 498 – 512.

COHEN, Julie E. What is privacy for. **Harvard Law Review**, v. 126, 2013.

COLOMBIA. **Ley Estatutaria 1581 de 2012**. Bogotá, 18 de outubro de 2012. Disponível em: < http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html> Acesso em 15 set 2020.

CONSELHO DA EUROPA. **Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (ETS nº 108)**. Disponível em: < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Acesso em 22 jun 2020.

CONSELHO DA EUROPA. **Protocolo de Emenda à Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (CETS nº 223)**. Disponível em: < https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> Acesso em 22 jun 2020.

CONVERGÊNCIA DIGITAL. **MP de Brasília abre inquérito para apurar venda de dados pessoais**. Disponível em: < https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=53773&sid=4> Acesso em 3 out 2020.

COVER, Robert M. **The Supreme Court, 1982 Term – Foreword: Nomos and Narrative**. Harvard Law Review, v. 97, n. 4, 1983 – 1984.

CRAVO, Daniela Copetti. **Direito à portabilidade de dados**: interface entre defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018.

CRAVO, Daniela Copetti. **Direito à portabilidade de dados**: necessidade de regulação ex ante e ex post. Tese (Doutorado em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2018.

CRAVO, Daniela Copetti. Direitos do titular dos dados no poder público: análise da portabilidade de dados. **Revista da ESDM**, v. 6, n. 11, 2020.

CRAVO, Daniela Copetti. O direito à portabilidade na Lei de Proteção de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 347 – 366.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 85 – 99.

CUSTERS, Bart; VRABEC, Helena U. Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. **International Data Privacy Law**, 2016.

DATA COUP. **The Personal Data Revolution**. Disponível em: < https://datacoup.com/#> Acesso em 3 out 2020

DECLARAÇÃO de Santa Cruz de la Sierra. In: CUMBRE IBEROAMERICANA DE JEFES DE ESTADO Y DE GOBIERNO, 13., Santa Cruz de la Sierra, 2003. **Anais**. Disponível em: <https://www.segib.org/wp- content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf.> Acesso em: 5 ago 2020.

DEUTSCHLAND. **BVerfGE 65, 1**. Bundesverfassungsgericht, Karlsruhe, 1983. Disponível em: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html.> Acesso em 10 mai 2020.

DEUTSCHLAND. **Grundgesetz**. Bonn, 1948. Disponível em: < https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz> Acesso em 5 abr 2020.

DIAS, Tatiana. **Vigiar e lucrar**: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. Disponível em: < https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/> Acesso em 3 out 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91 – 108, jul./dez. 2011.

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.

DONEDA, Danilo; MACHADO, Diego. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 99 – 125.

DONEDA, Danilo; MENDES, Laura Schertel. Reflexões iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, p. 469 - 483, nov./dez. 2018.

DOSTOIÉVSKI, Fiódor. **Memórias do Subsolo**. 6 ed.. São Paulo: Editora 34, 2009.

DUHIGG, Charles. **Is Amazon Unstoppable?**. Disponível em: < https://www.newyorker.com/magazine/2019/10/21/is-amazon-unstoppable> Acesso em 23 abr. 2020.

DUQUE, Marcelo Schenk. Fundamentação em torno da chamada Drittwirkung dos direitos fundamentais. In: GRUNDMANN, Stefan; MENDES, Gilmar Ferreira; MARQUES, Claudia Lima (orgs.). **Direito Privado, Constituição e Fronteiras**: encontros da associação luso-alemã de juristas no Brasil. 2 ed. rev., atual. e ampl.. São Paulo: Editora Revista dos Tribunais, 2014, p. 57 – 90.

ECO, Umberto. **Obra Aberta**. São Paulo: Perspectiva, 1969

ECUADOR. **Proyecto de Ley Orgânica de Protección de Datos Personales**. Quito, 19 de setembro de 2019. Disponível em: < https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf> Acesso em 15 set 2020.

EMPOLI, Giuliano da. **Os engenheiros do caos**. São Paulo: Vestígio, 2019.

ESPÍRITO SANTO. **Pesquisa de demanda e fluxo turístico por meio de sinal de telefonia móvel no estado do Espírito Santo**. Vila Velha, 2017. Disponível em: < https://observatoriodoturismo.es.gov.br/Media/observatorio/Pesquisas/Telefonia%20M%C3%B3vel/Descritivo%20Metodol%C3%B3gico.pdf> Acesso em 3 out. 2020.

ESPÓSITO, Filipe. **Facebook exec says ad-based businesses are 'under assault' by Apple's privacy changes**. Disponível em: < https://9to5mac.com/2020/10/06/facebook-exec-

says-ad-based-businesses-are-under-assault-by-apples-privacy-changes/> Acesso em 10 out 2020.

EUBANKS, Virginia. **Automating Inequality**: how high-tech tools profile, police, and punish the poor. Nova Iorque: St. Martin's Press, 2018.

FEDERAL TRADE COMMISSION. **Data Brokers**: A call for Transparency and Accountability. 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may- 2014/140527databrokerreport.pdf.> Acesso em: 10 jul. 2020.

FEIJÓ, Laura Schroder. **A titularidade de dados pessoais**: uma análise da aplicabilidade do regime jurídico da propriedade. Trabalho de Conclusão (Graduação em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019.

FERNANDES, Elora Raad; OLIVEIRA, Jordan Vinícius de. **Quanto valem seus dados**? O caso google opinion rewards. Revista de Direito e as Novas Tecnologias, v. 7, abr./jun. 2020.

FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 83 – 100.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 23 -52.

GEDIEL, José Antonio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito – UFPR**, Curitiba, n. 7, p. 141 – 153, 2008.

GLEICK, James. **The Information**: a history, a theory, a flood. Nova Iorque: Pantheon Books, 2011.

GOULART, Guilherme; SERAFIAN, Vinicius. **Proteção de Dados Pessoais e o Coronavírus**. Disponível em: <https://www.segurancalegal.com/2020/04/episodio-234-protecao-de-dados-pessoais-e-o-coronavirus/> Acesso em 10 ago. 2020.

GOULART, Guilherme; SERAFIAN, Vinicius. **Data brokers, privacidade e discriminação**. Disponível em: <https://www.segurancalegal.com/2014/06/episodio-52-databrokers-privacidade-e-discriminacao/> Acesso em 20 set. 2020.

GREENLEAF, Graham. **Countries with data privacy laws – by year 1973-2019**. Disponível em: < https://ssrn.com/abstract=3386510> Acesso em 8 set 2020.

GREENLEAF, Graham. Global tables of privacy laws and bills. **Privacy Laws & Business International Report**, fev. 2019.

GPT-3. **A robot wrote this entire article**: are you scared yet, human?. Disponível em: <https://www.theguardian.com/commentisfree/2020/sep/08/robot-wrote-this-article-gpt-3> Acesso em 9 set. 2020.

HAN, Byung-Chul. **No enxame: perspectivas do digital**. 2 reimp. Petrópolis: Vozes, 2019.

HAN, Byung-Chul. **Sociedade da transparência**. 4 reimp. Petrópolis: Vozes, 2019.

HARARI, Yuval Noah. **21 lições para o Século 21**. São Paulo: Companhia das Letras, 2018.

HENDERSON, Stephen E. After United States v. Jones, after the Fourth Amendment Third Party Doctrine. **North Carolina Journal of Law & Technology**, v. 14, n. 2, 2013.

HENDERSON, Stephen E. Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too. **Pepperdine Law Review**, v. 34, n. 4, 2007.

HILL, Kashmir. **Wrongfully Accused by an Algorithm**. Disponível em: <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> Acesso em 4 ago. 2020.

IGNACIO, Laura. **Comissão de juristas elabora proposta para a LGPD penal**. Disponível em: <https://valor.globo.com/legislacao/noticia/2020/09/15/comissao-de-juristas-elabora-proposta-para-a-lgpd-penal.ghtml> Acesso em 10 out. 2020.

ILLINOIS. **Dwyer v. American Express Co. (1995)**. 273 Ill. App. 3d 742 (1995). Disponível em: <https://www.quimbee.com/cases/dwyer-v-american-express-co> Acesso em 20 ago 2020.

JASMONTAITE, Lina (*et. al*). Data protection by design and by default: framing guiding principles into legal obligations in the GDPR. **European Data Protection Law Review**, v. 4, n. 2, p. 168 – 189, 2018.

JOELSONS, Marcela. Autodeterminação informativa em direito comparado: análise dos contextos históricos e decisões paradigmas das Cortes Constitucionais alemã e brasileira. **Revista de Direito Constitucional e Internacional**, v. 119, p. 233 – 272, mai./jun. 2020.

JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, v. 8, jul./set. 2020.

JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros**. São Paulo: Thomson Reuters, 2020.

KAFKA, Franz. **O processo**. São Paulo: Companhia das Letras, 2005.

KAMARA, Irene; DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **Brussels Privacy Hub**, v. 4, n. 12, ago. 2018.

KAMMOURIEH, Lanah (*et. al*). Group privacy in the age of Big Data. In: FLORIDI, Luciano. Group Privacy: a defence and an interpretation. In: FLORIDI, Luciano; SLOOT, Bart van der; TAYLOR, Linnet (eds.). **Group Privacy**: new challenges of data technologies. Springer: Cham, 2017, p. 37 – 66.

KEMENY, Richard. **Brazil is sliding into techno-authoritarism**. Disponível em: <www.technologyreview.com/2020/08/19/1007094/brazil-data-privacy-cadastro-base/amp/> Acesso em 20 ago. 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 445 – 464.

KOSTADINOVA, Zhasmina Radkova. **Purpose limitation under the GDPR: can Article 6 (4) be automated?** Dissertação (Mestrado em Direito). Universidade de Tilburg, 2018.

LANIER, Jaron. **Dawn of the new everything**: encounters with reality and virtual reality. Nova Iorque: Henry Holt & Co., 2017.

LIBERATORE, Stacy. **More than 500,000 zoom user credentials have been stolen and sold on the dark web for less than a penny each**. Disponível em: < https://www.dailymail.co.uk/sciencetech/article-8218723/More-500-000-Zoom-user-credentials-sold-dark-web-PENNY-each.html> Acesso em 10 ago. 2020.

LIGUORI FILHO, Carlos Augusto. Criptografia em debate: modelos regulatórios ao redor do mundo. In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 61 – 76.

LIMA, Clarissa Fernandes de. **O profiling e a proteção de dados pessoais**. Trabalho de Conclusão (Graduação em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019.

LORENZETTI, Ricardo L. **Comércio Eletrônico**. Trad. Fabiano Menke. São Paulo: Editora Revista dos Tribunais, 2004.

MALADY, Matthew J. X. **The ghosts in our machines**. Disponível em: < https://www.newyorker.com/culture/culture-desk/the-ghosts-in-our-machines> Acesso em 11 ago. 2020.

MALGIERI, Gianclaudio. **The concept of Fairness in the GDPR**: a linguistic and contextual interpretation. Proceedings of FAT, jan. 2020.

MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais**: uma análise dos seus fundamentos e elementos. Dissertação (Mestrado em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019.

MARANTZ, Andrew. **Silicon Valley's Crisis of Conscience**: where Big Tech goes to ask deep questions. Disponível em: < https://www.newyorker.com/magazine/2019/08/26/silicon-valleys-crisis-of-conscience> Acesso em 22 jun. 2020.

MARR, Bernard. **How much data do we create every day**? The mind-blowing stats everyone should read. Disponível em: < https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#25545f6460ba> Acesso em 8 ago. 2020.

MARTINS, Leonardo. (org.) **Cinqüenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2 ed. São Paulo: Saraiva, 2018.

MARTINS-COSTA, Judith. Apresentação – Autoridade e utilidade da doutrina: a construção dos modelos doutrinários. In: MARTINS-COSTA, Judith. **Modelos de Direito Privado**. São Paulo: Marcial Pons, 2014, p. 9 – 40.

MARTINS-COSTA, Judith. **Pessoa, personalidade, dignidade**: ensaio de uma qualificação. Tese (Livre-docência). Faculdade de Direito. Universidade de São Paulo. São Paulo, 2003.

MASSARO, Heloisa; SANTOS, Bruna; BIONI, Bruno; BRITO CRUZ, Francisco; RIELLI, Mariana; VIEIRA, Rafael. **Proteção de Dados nas Eleições:** democracia e privacidade. Grupo de Estudos em Proteção de Dados e Eleições, 2020.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. Nova Iorque: First Mariner Books, 2014.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (orgs.). **Technology and Privacy**: The new landscape. Cambridge: The MIT Press, 1997, p. 219 – 242.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. Londres: John Murray, 2019.

MELLO, Patrícia Campos. **A máquina do ódio**. São Paulo: Companhia das Letras, 2020.

MENAND, Louis. **Why do we care so much about privacy**?. Disponível em: < https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy> Acesso em 28 jul. 2020.

MENDES, Gilmar Ferreira. Direitos fundamentais: eficácia das garantias constitucionais nas relações privadas. In: GRUNDMANN, Stefan; MENDES, Gilmar Ferreira; MARQUES, Claudia Lima (orgs.). **Direito Privado, Constituição e Fronteiras**: encontros da associação luso-alemã de juristas no Brasil. 2 ed. rev., atual. e ampl.. São Paulo: Editora Revista dos Tribunais, 2014, p. 31 – 56.

MENDES, Laura Schertel. **A encruzilhada da proteção de dados no Brasil e o caso do IBGE**. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020> Acesso em 15 ago. 2020.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-81, jul./set. 2011.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; BIONI, Bruno. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 797 – 820.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança: uma perspectiva comparada. In: GRUNDMANN, Stefan; MENDES, Gilmar Ferreira; MARQUES, Claudia Lima (orgs.). **Direito Privado, Constituição e Fronteiras**: encontros da associação luso-alemã de juristas no Brasil. 2 ed. rev., atual. e ampl.. São Paulo: Editora Revista dos Tribunais, 2014, p. 271 – 286.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Faculdade de Direito. Universidade de Brasília. Brasília, 2008.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). In: DONEDA, Danilo (org.). **Caderno Especial**: a regulação da criptografia no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2018, p. 83 – 98.

MENKE, Fabiano. A interpretação das cláusulas gerais: a subsunção e a concreção de conceitos. **Doutrinas Essenciais de Direito do Consumidor**, v. 4, p. 107 – 136, abr. 2011.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Disponível em: <https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa> Acesso em 31 out 2020.

MENKE, Fabiano; FALEIROS JÚNIOR, José Luiz de Moura. **"Teilrechtsfähigkeit": uma proposta para a responsabilização civil na IA**. Disponível em: < https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/331652/teilrechtsfahigkeit-uma-proposta-alema-para-a-responsabilizacao-civil-na-ia> Acesso em 8 ago. 2020.

MILNE, George R.; CULNAN, Mary J. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. **Journal of Interactive Marketing**, n. 15, 2004.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, v. 1009, nov. 2019.

MIRAGEM, Bruno. **Direito administrativo aplicado**. 3 ed., rev., atual. e ampl.. São Paulo: Editora Revista dos Tribunais, 2017.

MOHRI, Mehryar; ROSTAMIZADEH, Afshin; TALWALKAR, Ameet. **The Foundations of machine learning**. 2 ed. Cambridge: The MIT Press, 2018.

MOORE, Martin. **Democracy hacked**: political turmoil and information warfare in the digital age. Londres: Oneworld, 2018.

MOUNK, Yasha. **O Povo contra a Democracia**: por que nossa liberdade corre perigo e como salvá-la. São Paulo: Companhia das Letras, 2019.

MOURA, Raíssa; FERRAZ, Laura. **Meios de controle à pandemia da COVID-19 e a inviolabilidade da privacidade**. Disponível em: <https://content.inloco.com.br/knowledge/covid/sum%C3%A1rio> Acesso em 10 jun 2020.

MUCELIN, Guilherme; ROSA, Dezyree Rodrigues da. Comercialização de big data e direitos fundamentais: um novo desafio para a temática de empresas e direitos humanos dos consumidores. In: SARLET, Ingo Wolfgang (coord.). **Os Direitos Fundamentais num Mundo em Transformação: tópicos atuais aos 30 anos da CF e 70 anos da DUDH**. Porto Alegre: Editora Fi, 2019.

NIPPERDEY, Hans Carl. Livre Desenvolvimento da Personalidade. In: HECK, Luís Afonso (org.). **Direitos Fundamentais e Direito Privado**: textos clássicos. Porto Alegre: Sergio Antonio Fabris, 2011, p. 71 – 90.

NISSENBAUM, Helen. A contextual approach to pricacy online. **Daedalus**, v. 140, n. 4, p. 32 – 48, 2011.

NISSENBAUM, Helen. Privacy as contextual integrity. **Washington Law Review**, v. 79, n. 1, fev. 2004, p. 119 – 158.

NISSENBAUM, Helen. **Privacy in context**: technology, policy and the integrity of social life. Stanford: Stanford University Press, 2010.

OECD. **Guidelines on the protection of privacy and transborder flows of personal data**. Disponível em: < https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em 10 ago 2020.

OHM, Paul. Sensitive Information. **Southern California Law Review**, v. 88, n. 5, 2015.

OHM, Paul. The many revolutions of Carpenter. **Harvard Journal of Law & Technology**, v. 32, n. 2, 2019.

O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. Londres: Penguin Books, 2017.

PARAGUAY. **Constituición de la República del Paraguay**. Asunción, 20 de junio de 1992. Disponível em: < http://digesto.senado.gov.py/archivos/file/Constituci%C3%B3n%20de%20la%20Rep%C3%BAblica%20del%20Paraguay%20y%20Reglamento%20Interno%20HCS.pdf> Acesso em 10 out 2020.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PORTO ALEGRE. **Painel de mobilidade e distanciamento**. Disponível em:< https://infografico-covid.procempa.com.br/distanciamento-social> Acesso em 10 set 2020.

POSNER, Richard A. **Our Domestic Intelligence Crisis**. Disponível em: <https://www.washingtonpost.com/archive/opinions/2005/12/21/our-domestic-intelligence-crisis/a2b4234d-ba78-4ba1-a350-90e7fbb4e5bb/> Acesso em 1 set. 2020.

RAMINELLI, Francieli Puntel; RODEGHERI, Leticia Bodanese. A Proteção de Dados Pessoais na Internet no Brasil: Análise de Decisões Proferidas pelo Supremo Tribunal Federal. **Cadernos do Programa de Pós-Graduação em Direito/UFRGS**, v. 11, n. 2, 2016.

RIO GRANDE DO SUL. Comitê Científico de apoio ao enfrentamento à pandemia COVID-19. **Nota técnica sobre o rastreamento digital de contatos com smartphones, de 16 de maio de 2020**. Disponível em: < https://www.inova.rs.gov.br/upload/arquivos/202010/09200211-rastreamento-digital-de-contatos-comitecientifico16maio2020-atualizado-em-09out2020.pdf> Acesso em 5 abr 2020.

ROBERTSON, Viktoria. Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data. **Common Market Law Review**, 2020.

RODRIGUES, Artur. **Agência vendia em site cadastro para envio ilegal de Whatsapp na eleição de 2018**. Disponível em: <https://www1.folha.uol.com.br/poder/2020/03/agencia-vendia-em-site-cadastro-para-envio-ilegal-de-whatsapp-na-eleicao-de-2018.shtml> Acesso em 10 set. 2020.

RODRIGUES JR., Otavio Luiz. **Direito Civil Contemporâneo**: estatuto epistemológico, constituição e direitos fundamentais. Rio de Janeiro: Forense Universitária, 2019.

ROESSLER, Beate. Should personal data be a tradable good? On the moral limits of the markets in privacy. In: ROSSLER, Beate; MOKROSINSKA, Dorota (orgs.). **Social Dimensions of privacy**. Cambridge: Cambridge University Press, 2015, p. 141 – 161.

ROMEO, Nick. **What can America learn from Europe about regulating big tech**?. Disponível em: <https://www.newyorker.com/tech/annals-of-technology/what-can-america-learn-from-europe-about-regulating-big-tech?> Acesso em 19 ago. 2020.

ROMM, Tony. **Arizona sues Google over allegations it illegally tracked Andoid smartphone users' locations**. Disponível em: <https://www.washingtonpost.com/technology/2020/05/27/google-android-privacy-lawsuit/> Acesso em 3 out 2020.

ROOSE, Kevin. **Rabbit Hole**: what is the internet doing to us?. Disponível em: <https://www.nytimes.com/column/rabbit-hole> Acesso em 10 ago. 2020.

ROSENVALD, Nelson. **Do risco da atividade ao "alto" risco da atividade algorítmica**. Disponível em: < https://www.nelsonrosenvald.info/single-post/2019/09/18/DO-RISCO-DA-ATIVIDADE-AO-%E2%80%9CALTO%E2%80%9D-RISCO-DA-ATIVIDADE-ALGOR%C3%8DTMICA> Acesso em 19 set. 2020.

SANDEL, Michael J. **What Money Can't Buy**: the moral limits of markets. Nova Iorque: Farrar, Straus and Giroux, 2013.

SÃO PAULO. Sentença nº 1080233-94.2019.8.26.0100. 13ª Vara Cível do Foro Central de São Paulo. Juíza de Direito: Tonia Yuka Koroku. 29 de setembro de 2020. Disponível em: < https://migalhas.uol.com.br/arquivos/2020/9/B05F37C296A643_decisaoLGPD.pdf> Acesso em 01 out 2020.

SARLET, Ingo Wolfgang. **Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF?**. Disponível em: < https://www.conjur.com.br/2020-set-04/direitos-fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf> Acesso em 21 out 2020.

SAVIGNY, Friedrich Karl von. **Metodologia Jurídica**. Campinas: Edicamp, 2001.

SCHREMS, Max. ***Ad hoc* Paper (v 0.3) SARS-CoV-2 tracking under GDPR**. Disponível em: < https://noyb.eu/sites/default/files/2020-04/ad_hoc_paper_corona_tracking_v0.3.pdf> Acesso em 5 mai 2020.

SEABROOK, John. **Dressing for the Surveillance Age**. Disponível em: < https://www.newyorker.com/magazine/2020/03/16/dressing-for-the-surveillance-age> Acesso em 18 mar. 2020.

SEABROOK, John. **Can a Machine learn to write for the New Yorker?**. Disponível em: < https://www.newyorker.com/magazine/2019/10/14/can-a-machine-learn-to-write-for-the-new-yorker> Acesso em 14 abr. 2020.

SILVA, Clóvis do Couto e. **A obrigação como processo**. Rio de Janeiro: Editora FGV, 2006.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. Autoridades de proteção de dados na América Latina: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. **IDEC – Instituto Brasileiro de Defesa do Consumidor**. São Paulo. 2019. Disponível em <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina> Acesso em 21 out 2020.

SIMITIS, Spiros. Reviewing privacy in an information society. **University of Pennsylvania Law Review**, v. 135, n. 3, mar./1987, p. 707 – 746.

SMILEY, Lauren. **A Brutal Murder, a Wearable Witness, and an Unlikely Suspect**. Disponível em: < https://www.wired.com/story/telltale-heart-fitbit-murder/> Acesso em 20 jun. 2020.

SOLOVE, Daniel J.. A taxonomy of privacy. **University of Pennsylvania Law Review**, v. 154, jan./ 2006, p. 477 – 560.

SOLOVE, Daniel J.. Conceptualizing privacy. **California Law Review**, v. 90, 2002, p. 1087 – 1156.

SOLOVE, Daniel J.. Introduction: privacy self-management and the consent dilemma. **Harvard Law Review**, v. 126, n. 7, mai./2013, p. 1880 – 1903.

SOLOVE, Daniel J.. "I've got nothing to hide" and other misunderstandings of privacy. **San Diego Law Review**, n. 745, 2007.

STATISA. **Volume of data/information created worldwide from 2010 to 2024**. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/> Acesso em 15 set. 2020.

STRANDBURG, Katherine J.. **Free Fall: The Online Market's Consumer Preference Disconnect**. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2323961> Acesso em 5 jul. 2020.

STEPHENS-DAVIDOWITZ, Seth. **Everybody lies**: Big Data, New Data, and what the internet can tell us about who we really are. Nova Iorque: Harper Collins, 2017.

TSAI, Chun-Wei; LAI, Chin-Feng; CHAO, Han-Chieh; VASILAKOS, Athanasios. Big data analytics: a survey. **Journal of Big data**, n. 2, 2015.

TUFEKCI, Zeynep. Engineering the public: Big Data, surveillance and computational politics. **First Monday**, v. 19, n 7, jul./2014.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. **Jornal Oficial das Comunidades Europeias**, n. C364/1, 18 dez. 2000. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf.> Acesso em: 10 jun 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, n. L119/1, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT> Acesso em: 5 jun 2020.

UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-13/16**. Disponível em: < http://curia.europa.eu/juris/liste.jsf?language=en&num=C-13/16> Acesso em 12 set 2020.

UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-131/12**. Disponível em: < http://curia.europa.eu/juris/liste.jsf?num=c-131/12> Acesso em 12 set 2020.

UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-201/14**. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-201/14> Acesso em 12 set 2020.

UNIÃO EUROPEIA. Tribunal Europeu dos Direitos do Homem. **C-293/12**. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-293/12> Acesso em 12 set 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States. **389 U.S. 347 (1967)**. Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States. **425 U.S. 435 (1976)**. Disponível em: <https://supreme.justia.com/cases/federal/us/425/435/> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States**. 442 U.S. 735 (1979)**. Disponível em: <https://supreme.justia.com/cases/federal/us/442/735/> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States**. 533 U.S. 27 (2001)**. Disponível em: <https://supreme.justia.com/cases/federal/us/533/27/> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States**. 573 U.S. 13-132 (2014)**. Disponível em: <https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. Supreme Court of the United States. **585 U.S. 16-402 (2018**). Disponível em: <https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf> Acesso em 3 ago 2020.

UNITED STATES OF AMERICA. **Computer Matching and Privacy Protection Act (1988)**. Disponível em: < https://www.congress.gov/bill/100th-congress/senate-bill/496> Acesso em 13 ago 2020.

UNITED STATES OF AMERICA. **Gramm-Leach-Billey Act (1999)**. Disponível em: < https://www.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf> Acesso em 13 ago 2020.

UNITED STATES OF AMERICA. **Health Insurance Portability and Accountability Act (1996)**. Disponível em: < https://www.cdc.gov/phlp/publications/topic/hipaa.html> Acesso em 13 ago 2020.

UNITED STATES OF AMERICA. **Records, computers, and the rights of citizens**: report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm/> Acesso em 16 jun 2020.

URUGUAY. **Ley nº 18.331 – Ley de Protección de Datos Personales**. Montevidéu, 11 de agosto de 2008. Disponível em: < https://www.impo.com.uy/bases/leyes/18331-2008> Acesso em 10 set 2020.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 717 – 740.

VITORELLI, Edilson. **O devido processo legal coletivo**: dos direitos aos litígios coletivos. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

WESTIN, Alan. **Privacy and freedom**. Nova Iorque: Atheneum, 1967.

WINN, Peter. Katz and the Origins of the Reasonable Expectation of Privacy Test. **McGeorge Law Review**, v. 40, n. 1, 2009.

WORLD ECONOMIC FORUM. **How Much Data is Generated Each Day?**. Disponível em: <https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/> Acesso em 23 fev. 2020.

ZAVASKI, Teori Albino. Defesa de direitos coletivos e defesa coletiva de direitos. **Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul**, v. 11, 1996, p. 177 – 192.

ZAVASKI, Teori. **Processo Coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. São Paulo: Editora Revista dos Tribunais, 2016.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019.