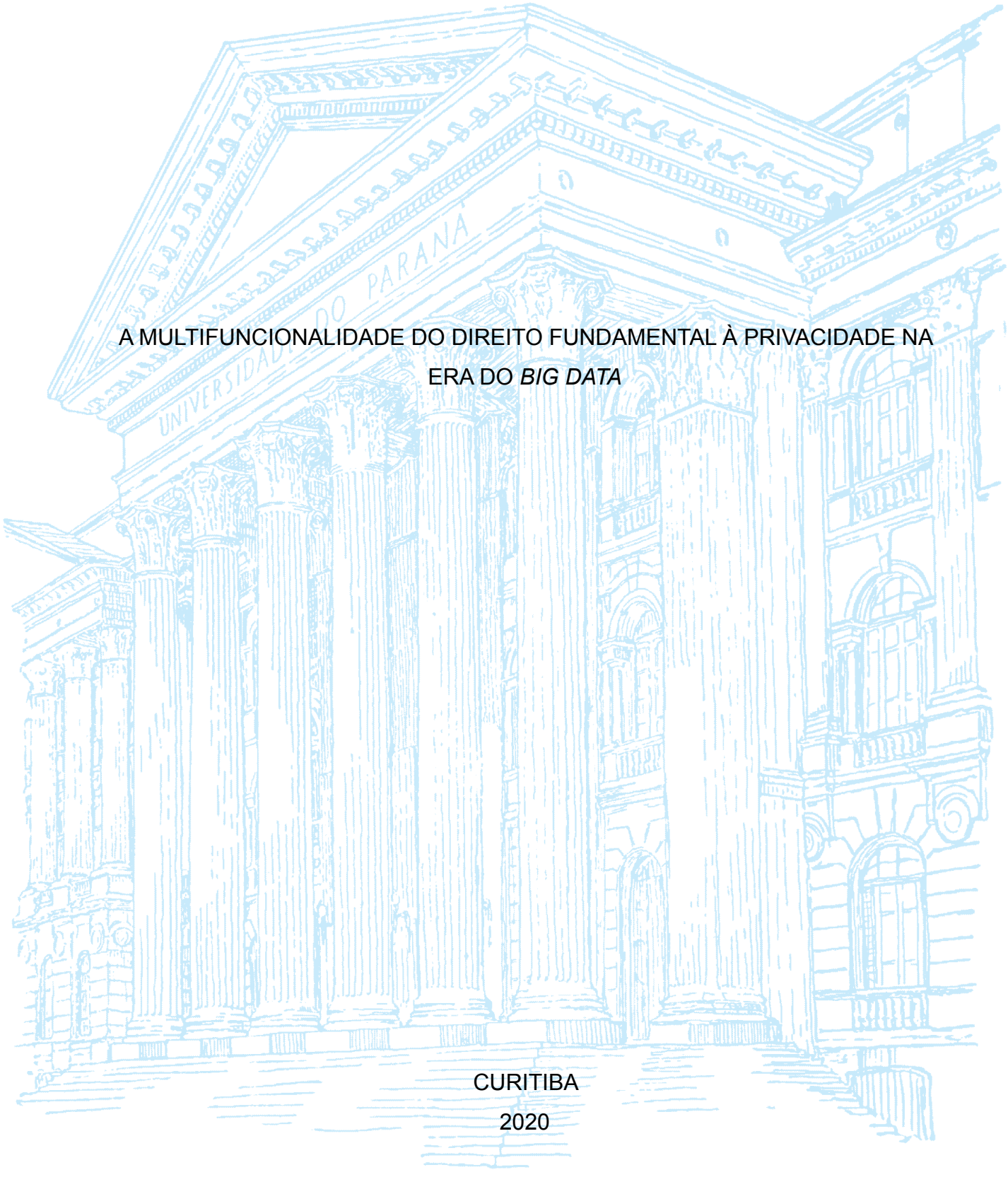
UNIVERSIDADE FEDERAL DO PARANÁ

VITORIA HIROMI SAITO



A MULTIFUNCIONALIDADE DO DIREITO FUNDAMENTAL À PRIVACIDADE NA ERA DO *BIG DATA*

CURITIBA

2020

VITORIA HIROMI SAITO

A MULTIFUNCIONALIDADE DO DIREITO FUNDAMENTAL À PRIVACIDADE NA ERA DO *BIG DATA*

Trabalho de Conclusão de Curso apresentado ao Curso de Direito, Setor de Ciências Jurídicas, Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Prof. Dra. Eneida Desiree Salgado

CURITIBA

2020

TERMO

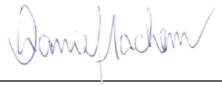
A MULTIFUNCIONALIDADE DO DIREITO FUNDAMENTAL À PRIVACIDADE NA ERA DO BIG DATA

VITORIA HIROMI SAITO

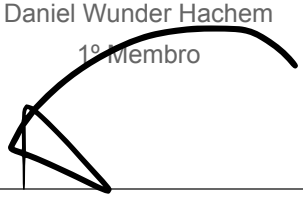
Monografia aprovada como requisito parcial para obtenção de Graduação no Curso de Direito, da Faculdade de Direito, Setor de Ciências jurídicas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Eneida Desiree Salgado
Orientador

Coorientador



Daniel Wunder Hachem
1º Membro



Ana Cristina Aguilar Viana
2º Membro

AGRADECIMENTOS

À minha orientadora, Professora Eneida Desiree Salgado, por proporcionar a melhor orientação acadêmica e intelectual que eu poderia ter pedido, sem a qual certamente esta monografia não teria sido possível.

À minha família, por toda a compreensão, e por ser a base que sei que sempre posso encontrar suporte.

Aos amigos, de dentro e de fora da faculdade, pelos momentos de leveza e pelo apoio incondicionado.

RESUMO

Nesta monografia, o objetivo foi de analisar o direito à privacidade em relação às novas tecnologias de informação do século XXI. Para tanto, traça-se um panorama histórico do direito à privacidade, desde a concepção clássica do direito de ser deixado a sós até sua definição mais recente, a qual tem profundas ligações com a proteção dos dados pessoais. Analisam-se os obstáculos proporcionados pelo Big Data quanto à proteção da privacidade na era da vigilância, bem como as diferentes formas que a coleta de dados pessoais pode incorrer na violação desse direito e os limites do consentimento dos usuários. Sustenta-se que muitos indivíduos não têm real conhecimento da quantidade de informações relativas à sua pessoa que são coletadas por entes públicos e privados, tampouco sabem para quais finalidades seus dados são utilizados. Portanto, o usuário se encontra em posição de considerável vulnerabilidade dentro da relação informacional, algo ilustrado com clareza pelo escândalo Cambridge Analytica. Aponta-se a insuficiência da visão clássica do direito à privacidade frente aos desafios trazidos pela inovação tecnológica, de modo que uma adequada tutela da privacidade requer observar esse direito sob uma ótica contemporânea, que reconheça a complexidade inerente à estrutura da privacidade. Com base na teoria da multifuncionalidade dos direitos fundamentais, sustenta-se que a tutela da privacidade ainda impõe deveres negativos de abstenção ao Estado e a terceiros, mas simultaneamente se desdobra em deveres positivos de prestações fáticas e normativas, o que pode ser visto, no Brasil, com a edição da Lei Geral de Proteção de Dados. Conclui-se que proteger o direito à privacidade na era digital não significa pleitear o fim da coleta de dados pessoais, mas defender que tais práticas sejam realizadas em prol da transparência e da *accountability*, a fim de diminuir a assimetria entre os polos da relação informacional.

Palavras-Chave: Privacidade. Dados Pessoais. Big Data. Direitos Fundamentais. Direito Constitucional. Lei Geral de Proteção de Dados.

ABSTRACT

In this monograph, the aim was to analyze the right to privacy in relation to the new information technologies developed in the 21st century. For this purpose, the work traces the historical background of privacy, from its classical concept of the right to be let alone to its most recent definition, which has deep links to data protection. The work analyzes the obstacles brought by Big Data regarding privacy protection in the age of surveillance, as well as the different forms in which data collection might violate privacy and the limits of users' consent. It argues that many individuals have no knowledge of the amount of personal information that is collected by governments and private companies, neither they know to which purposes their data are being utilized. As such, one finds oneself in a position of considerable vulnerability in the informational relation, which is clearly exemplified by the Cambridge Analytica data scandal. The work points to the insufficiency of the classical notion of privacy in relation to the challenges brought by technological innovation, therefore an adequate idea of privacy protection requires it to be observed under a contemporary light, one that recognizes the inherent complexity of the structure of the right to privacy. Based on the theory of the multifunctionality of fundamental rights, the monograph argues that privacy protection still requires governments and third parties to comply with negative obligations, but simultaneously translates itself in positive obligations, materially and normatively, which can be seen in Brazil by its most recent Data Protection Law. The work concludes that protecting the right to privacy in the digital age does not mean supporting the end of data collection practices, but defending these practices to be guided by the notions of transparency and accountability, in order to diminish the assymetry between the subjects of the informational relationship.

Keywords: Privacy. Data Protection. Big Data. Fundamental Rights. Constitutional Law. Brazilian Data Protection Law.

SUMÁRIO

INTRODUÇÃO

No início de 2015, o Colégio Bandeirantes – um dos colégios particulares mais tradicionais da cidade de São Paulo – passou por uma situação que o transportou para as notícias de todo o país. Ao final do mês de março daquele ano, a instituição sofreu um vazamento de dados pessoais de seus estudantes, por meio da divulgação em massa nas redes sociais de fichas estudantis anotadas entre 2007 a 2012, as quais continham informações de alunos escritas em reuniões sigilosas realizadas entre professores e orientadores[1]. O vazamento teria sido causado por um aluno do último ano do ensino médio, que teria feito um vídeo e divulgado para os colegas em grupos do aplicativo de mensagens WhatsApp como ter o acesso às informações encontradas.

O caso chamou a atenção, em especial, pelo conteúdo das anotações realizadas pelos professores e pedagogos nas fichas individuais de cada aluno, que envolviam dados familiares, diagnósticos médicos e comentários dos professores sobre a postura e a aparência dos discentes. Conforme reportagem da Folha de S. Paulo, um dos comentários incluía que um aluno “tem olheiras, boca de ódio, tem cara de criança de filme de suspense”, enquanto outro sugeria que uma garota possivelmente não teria conhecimento sobre ser filha adotiva. A ficha de uma adolescente apontava preocupações de professores com o seu peso, ao passo em que um jovem teve seu diagnóstico de Transtorno Obsessivo-Compulsivo vazado[2]. Uma das anotações noticiadas pelo G1 chama uma aluna da 5ª série de “inadequada e infantil”; outra foi descrita como “falsa”, enquanto um garoto “joga um professor contra o outro”. Um rapaz foi criticado por usar uma “calça muito feminina”, um segundo foi comparado ao personagem Forrest Gump, e uma terceira “parece apresentar traços de depressão e rebeldia”[3], dentre muitos outros relatórios.

---

[1] GUIMARÃES, Saulo Pereira. Vazamento de dados do Colégio Bandeirantes causa polêmica. **Exame,** São Paulo, 19 mar. 2015. Disponível em: <https://exame.abril.com.br/tecnologia/vazamento-de-dados-do-colegio-bandeirantes-causa-polemica/> Acesso em: 13 abr. 2020.

[2] BOLDRINI, Angela; PORTINARI, Natália; BILENKY, Thais. Fichas sobre estudantes de colégio tradicional de SP vazam na internet. **Folha de S. Paulo**, São Paulo, 19 mar. 2015. Disponível em: <https://www1.folha.uol.com.br/educacao/2015/03/1604926-fichas-sobre-estudantes-de-colegio-tradicional-de-sp-vazam-na-internet.shtml> Acesso em: 13 abr. 2020.

[3] MACEDO, Letícia. Vazamento de fichas de alunos gera protesto e punição no Bandeirantes. **G1,** São Paulo, 19 mar. 2015. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2015/03/vazamento-de-fichas-de-alunos-gera-protesto-e-punicao-no-bandeirantes.html> Acesso em: 13 abr. 2020.

Em nota oficial, o Colégio Bandeirantes afirmou que os dados foram acessados de forma irregular pelo adolescente que os vazou, configurando violação de dados sigilosos. A nota anunciou que o aluno supostamente responsável fora suspenso das aulas por oito dias e que o colégio adotaria as providências judiciais cabíveis contra a sua família. Muitos alunos disputaram a visão institucional, alegando que o conteúdo estava disponível na internet por meio de fácil acesso, bastando digitar os nomes dos discentes no mecanismo de busca do site do colégio ou se utilizando de *login* e senha[4]. Independentemente de as informações terem sido violadas ou não, o mal-estar entre pais e alunos já estava instaurado. Na opinião de vários estudantes, o erro do rapaz de ter compartilhado as fichas não isentava a responsabilidade da instituição de se atentar aos riscos de uma possível brecha no sistema, e principalmente, por ter permitido aos docentes expressarem comentários pejorativos acerca dos jovens, ultrapassando os limites da atuação profissional[5], ao incorrer em pré-julgamentos acerca da vida privada de crianças e de adolescentes que não lhes competiam analisar.

Esse caso é apenas um dentre vários que exemplificam algumas das preocupações mais recentes suscitadas pelos indivíduos quanto à proteção do direito à privacidade, frente ao surgimento constante de novas formas de tecnologias de comunicação digitais. O século XXI se caracteriza por ser um momento no qual a humanidade passa por um acentuado desenvolvimento tecnológico, o que leva a uma crescente digitalização da vida cotidiana. A ampla utilização das mídias sociais e dos sistemas de novas tecnologias de informação – tais como a coleta de dados pessoais mediante a utilização de sistemas de inteligência artificial e o *Big Data* – tornou-se prática corrente no meio público e no privado, o que repercute de maneira significativa nas esferas pessoais daqueles envolvidos, em especial quanto à proteção do direito à privacidade.

O caráter relativamente recente das tecnologias atreladas à chamada Internet 4.0 traz uma série de obstáculos ao Direito, uma vez que ele nem sempre é capaz de trazer uma tutela jurídica suficientemente apta a acompanhar a rapidez dos avanços tecnológicos contemporâneos. Torna-se necessário, portanto, promover

---

[4] BOLDRINI, Angela; PORTINARI, Natália; BILENKY, Thais. Fichas sobre estudantes de colégio tradicional de SP vazam na internet.

[5] RODRIGUES, Cinthia. A rede de intrigas do Colégio Bandeirantes. **CartaCapital**, São Paulo, 11 maio 2015. Disponível em: <https://www.cartacapital.com.br/educacao/a-rede-de-intrigas-do-colegio-bandeirantes/> Acesso em: 13 abr. 2020.

a proteção do direito à privacidade conforme as necessidades inerentes a cada época, o que requer compreender como a concepção deste direito se transmutou ao longo do tempo, até chegar ao complexo leque de fenômenos que abrange atualmente.

Desta maneira, este trabalho se volta inicialmente a realizar um panorama histórico do direito à privacidade, desde o estabelecimento do *right to privacy* estadunidense, fundamentado por Warren e Brandeis como o direito de ser deixado a sós (*the right to be let alone*). Já no século XX, a privacidade deixa de ser integralmente associada à concepção clássica do direito de ser deixado a sós, passando a se identificar com a necessidade de tutela dos dados pessoais dos cidadãos: em um primeiro momento, frente à coleta de dados realizada pelo Estado, e, posteriormente, por entes privados, o que é potencializado com o avanço da informática e com o surgimento da internet. Na virada para o século XXI, a relação entre a privacidade e os dados pessoais se aprofunda e se complexifica de forma inédita perante as mais recentes inovações tecnológicas, desde a proliferação das mídias sociais até o aperfeiçoamento de algoritmos que levaram ao surgimento do *Big Data* – os grandes bancos de dados, por meio do qual todo o processamento de dados se intensifica, de maneira nunca antes vista. Conclui-se no primeiro capítulo, portanto, que se a proteção da privacidade e dos dados pessoais já era vista com preocupação por parte da doutrina e da jurisprudência nos primórdios da era digital – anteriormente ao *Big Data* e à Internet 4.0 –, o surgimento e a proliferação destas tecnologias mais recentes tornam imperativo analisar quais são os efeitos que elas criam e até que ponto eles ferem o direito à privacidade.

Na segunda parte, será estudado o fenômeno do *Big Data* de maneira mais pormenorizada, de modo a observar sua lógica de funcionamento. Defende-se que, apesar das inúmeras utilidades promovidas pelo processamento ampliado de dados, a sua má utilização apresenta potenciais lesivos para a autonomia privada do indivíduo, ao aperfeiçoar um sistema de vigilância difuso, líquido e constante. Os dados são coletados, processados e comercializados em enormes quantidades a todo momento, permitindo que os algoritmos montem extensos perfis de potenciais consumidores e promovam bens e serviços sob medida ao usuário individualizado, com base nos seus hábitos, gostos, preferências e sentimentos, o que o coloca em uma considerável posição de vulnerabilidade na relação informacional. Ademais,

analisar-se-á o papel do consentimento como autorização individual para o tratamento de dados, bem como os seus limites, de modo a verificar até que ponto o ato de consentir efetivamente significa uma manifestação de vontade livre do indivíduo. Também serão observados os riscos advindos da má utilização dos sistemas de *Big Data* de maneira concreta, especificamente a partir do caso paradigmático envolvendo a rede social Facebook e a empresa de mineração de dados Cambridge Analytica.

Finalmente, o terceiro capítulo buscará defender que a proteção do direito à privacidade na sociedade da informação implica a necessidade de enxergá-lo em todas as suas dimensões, conforme a perspectiva da multifuncionalidade dos direitos fundamentais. Assim, a leitura clássica do direito à privacidade já o defendia como um direito de abstenção estatal, do titular não ter sua esfera jurídica invadida pelo Estado; no entanto, esta não é a única faceta que o direito assume. Proteger a privacidade também requer ações estatais positivas, tanto no nível de prestações fáticas como também por prestações normativas – o que pode ser visto no contexto de ascensão das legislações voltadas à proteção de dados pessoais, como a *General Data Protection Regulation* na União Europeia e a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018) –, sendo que estas últimas abarcam igualmente a proteção do direito em relação a interferências de terceiros e a instalação de órgãos especificamente voltados ao controle da qualidade do tratamento de dados, como formas de garantia de que as disposições legais relativas à proteção de dados sejam respeitadas na prática.

Conclui-se, assim, que a necessidade de proteção da privacidade em âmbito prestacional não pode levar ao cerceamento de liberdades ou a alguma forma de paternalismo estatal, pois isso traz o risco de acentuar ainda mais a sociedade de vigilância. A proteção desse direito deve se dar em prol da transparência e da *accountability* dos entes que promovem o processamento ampliado de dados. Desta maneira, proteger a privacidade não significa que a coleta e a comercialização de dados devam ser completamente impedidas, uma vez que tal medida se demonstra impossível. O desenvolvimento das tecnologias de informação se acelerou ao ponto de basear todo um modelo econômico contemporâneo – a denominada *data driven economy*, ou economia movida a dados –, de modo que acreditar que a tutela da privacidade requer o fim de todas essas práticas é uma posição, no mínimo,

ingênua. É possível defender a inovação tecnológica de maneira complementar à proteção da privacidade, haja vista que elas não necessariamente são posições antinômicas. É preciso, no entanto, reconhecer que os indivíduos que têm seus dados coletados se encontram automaticamente em uma posição de vulnerabilidade em relação às entidades que promovem o tratamento destes dados, o que torna imperativo estabelecer medidas voltadas a diminuir a assimetria informacional. Ao mesmo tempo, não se deve esquecer que o direito à privacidade é um direito fundamental garantido constitucionalmente, o que torna imprescindível refletir sobre como conciliar o crescimento e a difusão dos novos aparatos tecnológicos com a proteção da dignidade humana, dentro de uma sociedade que tem o controle da informação como um de seus principais pressupostos.

1 O DIREITO À PRIVACIDADE NA TEORIA DOS DIREITOS FUNDAMENTAIS

1.1 DESENVOLVIMENTO HISTÓRICO DO DIREITO À PRIVACIDADE

A concepção moderna da privacidade como um direito propriamente dito surgiu em contexto relativamente recente nos Estados Unidos, ao final do século XIX[6]. O seu advento se deu em um momento histórico específico, de transição de um perfil de caráter rural para um perfil eminentemente urbano da sociedade estadunidense[7], em que a disseminação da imprensa escrita passou a gerar preocupações quanto a eventuais ingerências da mídia sobre as vidas pessoais das figuras que se tornavam objetos de reportagens jornalísticas.

Nesse sentido, a ideia de privacidade relacionada ao surgimento dos meios de comunicação em massa possui profundas relações com a necessidade de proteção da vida íntima dos sujeitos afetados. Apesar de ser possível encontrar na *common law* casos relativos à proteção da intimidade desde o século anterior[8], o moderno debate sobre a privacidade apenas assumiu feições específicas com a publicação do artigo *The Right to Privacy*, de autoria de Samuel Warren e Louis Brandeis, em 1890[9]. Para estes autores, a privacidade é estabelecida como manifestação de uma *"inviolate personality"* inerente a cada indivíduo. Ou seja, cada indivíduo possui uma esfera pessoal inviolável, na medida em que ele tem o direito de escolher compartilhar com terceiros informações relativas a aspectos de sua personalidade e de sua vida íntima.

Portanto, o *right to privacy* de Warren e Brandeis é essencialmente o direito de cada um de exercer controle sobre as informações relativas a si mesmo, evitando ingerências externas, com a finalidade de proteger sua integridade psicológica, uma vez que a violação deste direito poderia incorrer na distorção da própria

---

[6] GLANCY, Dorothy J. The Invention of the Right to Privacy. **Arizona Law Review**, Tucson, v. 21, n. 1, p. 1-39, jan. 1979, p. 1. Disponível em: <https://digitalcommons.law.scu.edu/facpubs/317/> Acesso em: 18 fev. 2020.

[7] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 218.

[8] Por exemplo, já em 1741 houve o caso *Pope v. Curl*, "referido pela literatura da *common law* como o caso mais antigo no qual se discute o tema da *privacy*". Ibid., p. 125.

[9] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, Cambridge, v. IV, n. 5, p. 193-220, 15 dez. 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> Acesso em: 18 fev. 2020.

personalidade do indivíduo, em especial quanto à sua auto-imagem[10]. É o direito de não ser incomodado, de ser deixado em paz, de tal maneira que o direito à privacidade é comumente explanado, nesse sentido, como o direito de ser deixado a sós *(the right to be let alone*).

No entanto, Warren e Brandeis não inventaram o conceito de privacidade, haja vista que este pode ser traçado desde o surgimento da dualidade moderna entre público e privado, que coincide com o fortalecimento da burguesia e a valorização do individualismo a partir do século XVI. Tal transição está atrelada ao surgimento da concepção moderna de ente público enquanto um Estado-nação dotado de soberania e, como consequência, ao "estabelecimento de uma esfera privada livre das ingerências desse ente público"[11]. Contudo, a privacidade sob a ótica do individualismo burguês dos séculos XVII e XVIII se baseia no ideal iluminista que estabelece a propriedade privada como fundamento da liberdade, de modo que a proteção da privacidade é igualmente vista como proteção da propriedade individual[12].

Como apontado por Danilo Doneda, o que Warren e Brandeis propuseram de novo foi retirar a tutela da privacidade do âmbito da propriedade privada, observando-a como um direito de natureza pessoal, ao perceber a necessidade de proteção da *inviolate personality* de cada indivíduo[13]. Outrossim, o fato de os autores terem passado a analisar a privacidade como resposta a um novo fato social – a disseminação de jornais e fotografias – fez com que os seus estudos ganhassem uma relevância até antes não vista, na medida em que estabeleceram uma intrínseca relação entre o direito à privacidade e o desenvolvimento das novas tecnologias de informação, relação esta que perdura até os dias atuais.

Todavia, o artigo *The Right to Privacy* foi publicado em um período específico, voltado a tutelar um direito que emergia conforme as necessidades específicas de uma parcela da população estadunidense da época, tradicionalmente burguesa e com elevada projeção social, uma vez que muitos dos casos envolviam a insatisfação de figuras públicas com a forma em que eram retratadas pela imprensa[14]. Se naquele período o reconhecimento da privacidade como um direito

---

[10] GLANCY, Dorothy J. The Invention of the Right to Privacy, p. 2.
[11] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 118.
[12] Ibid., p. 119.
[13] Ibid., p. 126.
[14] Ibid., p. 33.

de ser deixado a sós era suficiente para garantir a sua tutela, o rápido desenvolvimento dos meios de comunicação em massa e das tecnologias de informação ao longo do século XX – em especial ao ganhar contornos exponenciais a partir da década de 1970 – torna imperioso que o conceito de privacidade seja revisto e reavaliado conforme as necessidades históricas inerentes a cada período.

Assim, a partir da segunda metade do século XX, o desenvolvimento tecnológico tornou corrente a utilização de informações pessoais dos indivíduos[15], em especial pelas mãos do Estado, com as mais diversas finalidades possíveis, mas principalmente para otimizar os graus de controle e de eficiência na organização da Administração Pública[16]. Portanto, com a expansão do uso de informações relativas à personalidade dos cidadãos pelo ente estatal, o conceito de privacidade não mais se limitou à proteção da vida íntima, mas passou a ter profundas relações com o direito ao controle dos dados pessoais[17].

Uma vez ultrapassada a associação inicial traçada entre progresso tecnológico e bem-estar social, surgiu a insegurança quanto ao número de situações não previstas nas quais o Estado poderia utilizar a tecnologia em ameaça ao direito à privacidade, o que possibilitou o surgimento de teorias fatalistas que previam o fim da privacidade como o primeiro passo para o estabelecimento de governos totalitários que se utilizassem dos meios tecnológicos como forma de controle social e de repressão[18]. De fato, a concentração do controle da informação é um elemento característico de regimes totalitários; no entanto, tais visões fatalistas se atrelaram em demasiado ao papel do Estado na coleta de dados pessoais, tendendo a ignorar a tendência mais importante que começou a se sedimentar com o avanço da informática: a coleta de dados pessoais realizada por entes privados, o que propiciou a formação de uma nova arquitetura informacional, com uma nova

---

[15] Cabe ressaltar que, em termos técnicos, “dados” e “informações” não são equivalentes. Dados são os fatos brutos coletados que, ao serem processados, tornam-se informações, possibilitando o acréscimo do conhecimento. Assim, os dados são a forma primitiva da informação. No entanto, não é raro que os vocábulos sejam utilizados como sinônimos pela doutrina e pela legislação (como a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação), dada a sua profunda relação, de modo que esta monografia também se refere aos termos de maneira intercambiável. Nesse sentido: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 136.

[16] Ibid., p. 34.

[17] MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 323-345.

[18] DONEDA, Danilo. op. cit., p. 37.

estrutura de poder também vinculada a ela[19]. Esta arquitetura se consolidou conforme os dados pessoais se tornaram um dos recursos mais valiosos do mercado contemporâneo, na medida em que eles são passíveis de serem transformados em informações necessárias ou úteis para a geração de valor dentro de uma determinada atividade, fundando, assim, toda uma economia movida a dados *(data driven economy)*[20].

Nesse diapasão, conforme Stefano Rodotà, enquanto a noção clássica de privacidade se apoiava na relação "pessoa-informação-sigilo", o advento da sociedade de informação fez com que a relação mais relevante se tornasse "pessoa-informação-circulação-controle"[21]. Aponta o jurista italiano, pois, que a redefinição do conceito de privacidade faz com que ela, simultaneamente, se estabeleça como um direito fundamental, se especifique como um direito à autodeterminação informativa – o poder do sujeito de ter o controle sobre suas próprias informações – e se torne precondição da própria ideia de cidadania na era digital.

No Brasil, o direito à privacidade se encontra consolidado no rol de direitos fundamentais previsto na Constituição de 1988, uma vez que o art. 5º, incisos X e XII, se voltam à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, bem como estabelecem o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ao passo em que os incisos LXIX, LXXII e LXXVII preveem a concessão do *habeas data* para o conhecimento e a ratificação de dados relativos ao impetrante. A legislação infraconstitucional também tutela a privacidade e os dados pessoais em campos específicos do Direito, podendo ser encontradas legislações esparsas que tangenciam o tema. Quanto à legislação ordinária, Marco Aurélio Bellizze Oliveira e Isabela Maria Pereira Lopes pontuam que a Lei de Arquivos Públicos (Lei nº 8.159/1991) e a Lei do *Habeas Data* (Lei nº 9.507/1997) foram as primeiras leis de caráter público voltadas à tutela desses direitos[22], o que reflete a supramencionada preocupação histórica com a

---

[19] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 35.
[20] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 23-52.
[21] RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.
[22] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 53-83.

coleta e o tratamento de dados realizado pelo ente público. Por outro lado, a prática igualmente já se disseminava entre entidades privadas, tornando necessária a regulação do tema no âmbito do Direito Privado. Assim, já na mesma época, o Código de Defesa do Consumidor (Lei 8.078/1990) estabeleceu em seu art. 43 que o consumidor tem direito de acesso às informações arquivadas sobre ele em bancos de dados e cadastros, ao passo em que o art. 21 do Código Civil de 2002 situou a inviolabilidade da vida privada no rol de direitos de personalidade, o que, mediante analogia, também abarca a proteção da intimidade e do direito ao segredo[23].

Apesar de mais recente, a Lei de Acesso à Informação (Lei nº 12.527/2011) também assume grande importância ao regulamentar o direito do cidadão de obter informações constantes em documentos públicos, na medida em que que o acesso à informação é imprescindível para assegurar a transparência da Administração Pública e, por conseguinte, garantir que a sua atuação esteja conforme os princípios constitucionais da moralidade, da legalidade, da impessoalidade e da publicidade[24].

Outra legislação é a Lei do Cadastro Positivo (Lei nº 12.414/2011), que trata de informações de adimplemento constantes em bancos de dados de consumidores, tendo sido inovadora ao prever uma proteção mais significativa dos dados sensíveis dos consumidores[25], ou seja, das informações relativas a questões como religião, orientação sexual, origem racial e étnica, dados genéticos e de saúde do indivíduo, entre outros. Poucos anos depois foi promulgado o Marco Civil da Internet (Lei nº 12.965/2014), que prevê em seu art. 3º, incisos II e III, a proteção da privacidade e dos dados pessoais como princípios da disciplina do uso da internet no Brasil.

Este panorama geral demonstra que, apesar da formalização do direito à privacidade como direito fundamental constitucionalmente protegido e como direito de personalidade, a tutela da privacidade em nível infraconstitucional se encontrava esparsa, fragmentada e inapta a promover uma proteção integral do indivíduo, uma

---

[23] SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. 2. ed. São Paulo: Revista dos Tribunais, 2005, p. 192.

[24] Na prática, no entanto, a garantia dos princípios que regem a Administração Pública é relativizada, uma vez que nem todos os entes federativos possuem uma cultura de transparência estabelecida, o que pode ser observado, por exemplo, no difícil acesso a determinadas informações relativas a servidores estaduais e municipais. SALGADO, Eneida Desirée; VIOLIN, Tarso Cabral. Transparência e acesso à informação: o caminho para a garantia da ética na Administração Pública. In: BLANCHET, Luiz Alberto; HACHEM, Daniel Wunder; SANTANO, Ana Cláudia (Coord.). **Eficiência e ética na Administração Pública.** Curitiba: Íthala, 2015, p. 271-294.

[25] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018, p. 70.

vez que acabava restrita às hipóteses setoriais de aplicação de cada dispositivo. O desenvolvimento de tais normas específicas permitiu a gradual formação de um sistema brasileiro de proteção de dados e da privacidade, que, contudo, ainda necessitava de uma lei que se debruçasse específica e integralmente sobre o tema, para poder se consolidar[26] – o que eventualmente seria traduzido na forma da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Desta forma, o advento da Lei Geral de Proteção de Dados não foi propriamente um ineditismo, tampouco algo completamente inesperado, uma vez que o art. 3º, inciso III, do Marco Civil da Internet já havia previsto o princípio da proteção dos dados pessoais, "na forma da lei". O que a LGPD inova é ter uma pretensão de unificação e de organização formal daquele sistema em formação[27], ao pretender conferir ampla proteção a *todas* as formas de tratamento de dados pessoais dos indivíduos[28]. Contudo, o caráter recente da lei faz com que, neste momento, seja difícil prever com precisão até que ponto a LGPD será capaz de consolidar um sistema de proteção de dados efetivo, que não apenas esteja a par dos impactos trazidos pelas atuais – e futuras – inovações tecnológicas às esferas pública e privada, mas que também seja apto a garantir uma confiável tutela à privacidade dos cidadãos, enquanto manifestação de sua personalidade, autonomia, autodeterminação e dignidade humana.

1.2 A INSUFICIÊNCIA DA LEITURA CLÁSSICA DO DIREITO À PRIVACIDADE NA ERA DIGITAL PRÉ-*BIG DATA*

Como mencionado anteriormente, a concepção clássica do direito à privacidade é aquela formalizada ao final do século XIX, que se consubstancia como o *the right to be let alone.* É, pois, o direito a poder estar só, de não ter violada sua esfera pessoal, direito este que é inerente ao direito à própria vida, uma vez que a garantia de poder ser deixado em paz se encontra inserida na prerrogativa de gozar da própria vida[29].

---

[26] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018, p. 71.
[27] Ibid., p. 72.
[28] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 99-129.
[29] GLANCY, Dorothy J. The Invention of the Right to Privacy, p. 4.

O conteúdo individualista da privacidade como o direito de ser deixado a sós demonstra que a leitura clássica a inseriu dentro do denominado paradigma da *zero-relationship*[30], ou seja, no qual a privacidade é uma "relação zero" entre dois sujeitos ou grupos, ao pressupor a ausência de comunicação entre eles. Portanto, o respeito a esse direito necessariamente incorre em um dever de abstenção por parte do outro, seja pelo ente estatal ou por particulares – como por exemplo, por agentes da mídia, que eram as figuras contra as quais Warren e Brandeis originalmente sustentaram o *right to privacy*.

Nesse sentido, leciona Dorothy J. Glancy que o indivíduo que tem sua privacidade tutelada dentro do conceito clássico de Warren e Brandeis exerce simultaneamente duas formas de liberdade[31]: por um lado, uma liberdade positiva *(positive freedom-to)*[32] de ter controle sobre a própria vida, com a capacidade de estabelecer os limites das informações divulgadas sobre sua esfera privada e, consequentemente, controlar a possibilidade de ficar a sós; por outro lado, uma liberdade negativa *(negative freedom-from)* de ser protegido em relação a potenciais interferências externas que pudessem vir a gerar danos à personalidade do indivíduo. Tal concepção se assemelha à teoria das esferas da liberdade de Isaiah Berlin, para quem a liberdade positiva é definida por uma pretensão do indivíduo de ser dono de si mesmo, ao passo em que a liberdade negativa se encontra na área em que o indivíduo pode atuar sem que haja a interferência do outro[33].

Com efeito, apesar de Warren e Brandeis terem publicado seu artigo como resposta imediata à proliferação da imprensa escrita, regida por entes privados, o âmbito de proteção do *right to privacy* clássico igualmente pode ser estendido em

---

[30] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 30.
[31] GLANCY, Dorothy J. The Invention of the Right to Privacy, p. 24.
[32] Necessário observar que Glancy utiliza o vocábulo *"freedom"*, que não pode ser confundido com o direito à liberdade *(right to liberty)* consagrado no constitucionalismo estadunidense, uma vez que, para Warren e Brandeis, sendo a *privacy* inerente ao direito à vida (*right to life),* ela está desassociada das esferas do direito individual à liberdade (*liberty)* e à propriedade *(property).* Por outro lado, tal visão é oposta muitas vezes pela própria Suprema Corte dos Estados Unidos, que frequentemente traça uma correlação direta entre a *privacy* e a *liberty*. Ibid., p. 4.
[33] Apesar de Berlin afirmar a existência destas duas esferas de liberdade, o autor é crítico da concepção de liberdade positiva, afirmando que a "liberdade autêntica" é, essencialmente, aquela de caráter negativo, pois a pretensão de ser dono de si relativa à esfera positiva "coloca em questão a possibilidade de que alguém que seja escravo da natureza ou de suas próprias paixões não possa ser reputado livre". RUZYK, Carlos Eduardo Pianovski. **Liberdade(s) e Função:** Contribuição crítica para uma nova fundamentação da dimensão funcional do Direito Civil brasileiro. 2009. 402 f. Tese (Doutorado em Direito das Relações Sociais) - Setor de Ciências Jurídicas, Universidade Federal do Paraná, Curitiba (PR), 2009, p. 26. Disponível em: <http://hdl.handle.net/1884/19174> Acesso em: 24 mar. 2020.

relação ao governo. Isto porque não importava propriamente quem era o sujeito que agia para interferir na vida privada do particular, mas o próprio ato de interferência nas decisões do indivíduo sobre quais aspectos de sua vida ele desejava compartilhar[34]. Desta maneira, a visão oitocentista sobre a privacidade se coaduna com a perspectiva liberal europeia dos direitos fundamentais enquanto direitos de defesa do cidadão contra o Estado, uma vez que voltados à proteção do indivíduo contra as ingerências do Poder Público[35].

Em sentido amplo, os direitos de defesa se consubstanciam em uma ação negativa por parte do Estado, vez que implicam um dever negativo de abstenção. Para Robert Alexy, os direitos a ações negativas se subdividem em três grupos: a) direitos ao não-embaraço de ações, ou seja, que o Estado não impeça ou não dificulte a realização de determinadas ações às quais o indivíduo tem um direito (exemplos incluem os direitos de locomoção, manifestação de crença e a expressão de opiniões, entre outros); b) direitos à não-afetação de características e situações, nos quais não é permitido ao Estado que afete determinadas características e situações do titular de um direito; e c) direitos à não-eliminação de posições jurídicas do titular do direito[36]. Nessa leitura, é possível situar o conceito clássico do direito à privacidade mais especificamente no segundo grupo de direitos a ações negativas, ou seja, enquanto um direito à não-afetação de características e situações, uma vez que o Estado e terceiros têm o dever de respeitar a situação de inviolabilidade da vida privada do particular.

Todavia, como mencionado no panorama histórico do direito à privacidade, o rápido desenvolvimento tecnológico culminado com a crescente associação entre privacidade e proteção de dados fez com que, nas décadas seguintes, a mera classificação do direito à privacidade como um direito de defesa se tornasse obsoleta. Frente aos novos cenários trazidos pela realidade histórica do século XX, limitar o estudo da privacidade ao dever negativo de abstenção é uma perspectiva reducionista, pois cinge-se a enxergá-la como um simples direito de primeira geração, ou seja, enquanto parte de um rol de direitos individuais surgidos a partir do século XVIII, cujo conteúdo se resume à restrição da interferência do ente público na esfera jurídica do particular. Em contraposição, os direitos de segunda geração

---

[34] GLANCY, Dorothy J., The Invention of the Right to Privacy,, p. 28.
[35] ALEXY, Robert. **Teoria dos Direitos Fundamentais**. 2. ed. São Paulo: Malheiros, 2017, p. 433.
[36] Ibid., p. 196 e ss.

seriam os direitos sociais advindos do Estado de bem-estar social, que requerem uma prestação positiva do Estado, enquanto os de terceira geração seriam aqueles direitos de titularidade coletiva e difusa, tais como a proteção do meio ambiente[37].

No entanto, a própria classificação dos direitos fundamentais em gerações distintas é simplista, ao pressupor que os direitos de primeira geração apenas possuem função de defesa, que os direitos sociais estão circunscritos a prestações fáticas e que os direitos coletivos devem ser observados apenas no aspecto de sua titularidade[38]. Tal perspectiva ignora a estrutura básica de um direito fundamental[39], qual seja, a que um direito a algo abarca de modo concomitante tanto deveres negativos estatais como deveres positivos de proteção, além de também ostentarem "a titularidade transindividual alegadamente exclusiva dos 'direitos de terceira geração', bem como, simultaneamente, a titularidade individual pretensamente típica dos 'direitos de primeira e segunda geração'"[40].

Portanto, não se quer dizer que o dever de abstenção não seja mais relevante para a proteção da privacidade. O que se pretende dizer é que o aumento da complexidade nas relações que envolvem o direito à privacidade – a já mencionada transição do trinômio "pessoa-informação-sigilo" para a relação "pessoa-informação-circulação-controle" descrita por Rodotà – tornou necessário que a tutela da privacidade não mais se restringisse à sua esfera negativa, passando a requerer igualmente uma posição prestacional positiva por parte do Estado.

Esta necessidade de uma proteção positiva da privacidade e dos dados pessoais se reflete, por exemplo, a partir da década de 1970, quando adveio a preocupação em garantir uma tutela normativa dos dados pessoais, o que culminou nas primeiras leis de proteção de dados, em países como Alemanha e Suécia, além dos Estados Unidos, com o *Privacy Act* de 1974[41]. Estes textos legais se voltavam principalmente à proteção dos dados no contexto de surgimento de bancos de dados controlados por órgãos públicos, de modo que o Estado era o principal destinatário

---

[37] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais. **Revista de Direitos Fundamentais e Democracia**, Curitiba, v. 14, n. 14, p. 618-688, jul./dez. 2013.
[38] Ibid., p. 621.
[39] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 195.
[40] HACHEM, Daniel Wunder. op. cit., p. 621-622.
[41] CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 85-98.

das normas. Entretanto, a multiplicação dos centros de processamento de dados – e, portanto, a descentralização do controle das mãos do Estado – dificultou em grande forma um devido controle do tratamento de dados, de modo que não tardou para que as referidas leis logo se tornassem obsoletas[42]. Tudo isso demonstra a mutabilidade inerente à proteção da privacidade, pois a efetiva proteção desse direito necessariamente requer que os dispositivos legais estejam atentos aos avanços tecnológicos e às mudanças operadas na maneira em que as informações são distribuídas e disseminadas.

Percebe-se, novamente, que a leitura clássica da privacidade é insuficiente para tutelá-la desde o início da era digital. Nas décadas seguintes, o abismo entre a proteção da privacidade e a exponencial informatização da realidade apenas aumentaria, muito antes de ser concebível a ideia de uma internet fundamentada em sistemas de inteligência artificial e de *Big Data*. O avanço da informática começara a complexificar a relação entre privacidade, dados pessoais e informação mesmo anteriormente à virada do segundo milênio, o que pode ser observado em algumas questões práticas surgidas já nas últimas décadas, como por exemplo, a problemática do *habeas data* e do direito ao esquecimento.

O *habeas data* é um instituto originariamente brasileiro, tendo sido introduzido com a Constituição de 1988, cujo art. 5º, incisos LXIX, LXXII e LXXVII, o preveem como instrumento jurisdicional para assegurar o direito do impetrante de conhecer e retificar dados relativos à sua pessoa constantes em bancos de dados públicos, além de ser também regulamentado por lei própria (Lei nº 9.507/1997). Há uma razão de ser para o surgimento do instituto em solo brasileiro e a sua disseminação para outros ordenamentos da América Latina entre as décadas de 1980 e 1990, uma vez que em muitos destes países "persistia o trauma pelo uso autoritário da informação"[43] promovido durante os regimes militares.

Em tese, o *habeas data* não se limita à proteção dos dados pessoais, pois igualmente seria reflexo do direito de acesso à informação pública, direito este que por sua vez é basilar ao exercício de direitos políticos, de participação na comunidade e, consequentemente, na promoção do próprio direito de igualdade[44].

---

[42] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 175 e ss.
[43] Ibid., p. 267.
[44] DURÁN MARTÍNEZ, Augusto. **Derecho a la protección de datos personales y al acceso a la información pública:** hábeas data. 2. ed. Montevideo: Amalio M. Fernandez, 2012, p. 9.

Ainda que a lei não seja explícita, a doutrina acolhe a perspectiva de existirem diversas modalidades de *habeas data*[45], quais sejam: a) *informativo*, quando se busca o próprio acesso aos dados, subdividindo-se em *exibitório* (quais dados estão registrados), *finalista* (qual a finalidade do registro) e *autoral* (quem obteve os dados registrados); b) *aditivo*, para a inserção de dados, subdividindo-se em *atualizador* e *inclusivo*; c) *retificador*, para a correção de informações falsas ou imprecisas; d) de *reserva*, para assegurar que o acesso aos dados seja proporcionado somente a pessoas autorizadas; e) *cancelatório* ou *exclusivo*, a fim de excluir o registro; f) *impugnativo*, para impugnar o tratamento de dados em decisões automáticas; g) *bloqueador*, a fim de evitar o uso dos dados; h) *dissociativo*, para eliminar a associação entre o dado e o seu titular, ainda que ele continue registrado; i) *assecuratório*, para evitar uma fuga de dados não autorizada; e j) *reparador*, voltado à reparação de danos em decorrência da violação da proteção de dados. Contudo, a exploração das diversas modalidades do *habeas data* decorre muito mais da experiência de outros países da América Latina do que propriamente a experiência brasileira[46].

O *nomen juris* do instituto apresenta claros paralelos com o *habeas corpus*: enquanto a expressão *"habeas corpus"* pode ser traduzida para algo no sentido de "tenha seu corpo" – quando o indivíduo tenha restringida sua liberdade de ir e vir mediante violência, coação ilegal ou abuso de poder (art. 5º, inciso LXVIII, da Constituição de 1988) –, o vocábulo *"habeas data"* pode ser traduzido como "tenha seus dados", reconhecendo ao indivíduo o direito de dispor de seus dados pessoais, da mesma forma que ele tem o direito de dispor do próprio corpo[47].

Entretanto, esta vinculação semântica com o *habeas corpus* chega por demonstrar uma das próprias limitações do *habeas data* quanto à proteção da privacidade, haja vista que este instrumento acaba tendo uma vinculação muito maior com a proteção da liberdade pessoal – ainda que informática, não propriamente física – do que efetivamente com o direito à privacidade[48]. Ademais, não são poucas as críticas ao instituto[49], em especial as que apontam que a redação

---

[45] DURÁN MARTÍNEZ, Augusto. **Derecho a la protección de datos personales y al acceso a la información pública**, p. 152-156.
[46] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais,** p. 284.
[47] Ibid., p. 270-271.
[48] Ibid., p. 270.
[49] Ibid., p. 286.

genérica da lei brasileira tornou as hipóteses de aplicabilidade demasiado restritas, limitando-as ao acesso e à retificação de informações, o que esvazia o instrumento e o torna inócuo. Assim, apesar de o Brasil ser o local de origem do instituto, a legislação brasileira é vista como uma das mais fracas quanto ao tema, por não ter fixado parâmetros específicos de atuação e de proteção, preferindo restringir-se ao acesso e à retificação, além de ser aplicável apenas às informações contidas em bancos de dados e registros de caráter público.

A mencionada inocuidade do *habeas data* pode ser observada, por exemplo, no baixo interesse dos juristas brasileiros de se debruçarem sobre o tema e na sua pouca utilização na prática jurídica[50]. Como os objetivos de utilização do instrumento estão intimamente associados a um período histórico específico, o *habeas data* acaba por se revelar como uma simples "garantia para o passado"[51], incapaz de trazer as respostas adequadas às necessidades inerentes à problemática do acesso à informação. Na prática, portanto, tornou-se instrumento meramente simbólico, ao oferecer um remédio que "parece mais condizente com as concepções liberais que consideram a proteção de dados pessoais e a própria privacidade como liberdades negativas"[52]. Nesse sentido, é necessário observar o *habeas data* como "um produto de seu tempo"[53], criado para lidar com um problema específico – o direito de acesso e de retificação dos dados constantes em arquivos e registros governamentais, no momento pós-regime militar[54] –, e que, portanto, encontra dificuldades de aplicação em situações diversas, principalmente frente ao tratamento de dados realizado exclusivamente por entes de caráter privado e à própria mutabilidade do fenômeno tecnológico como um todo.

Outra problemática surgida ainda no século XX quanto à relação entre o direito à privacidade e o controle da informação é a questão do direito ao esquecimento. Trata-se do "direito de não ser lembrado eternamente por equívocos

---

[50] DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 97, p. 239-253, 2002. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67544>. Acesso em: 24 mar. 2020.
[51] Ibid., p. 243.
[52] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 289.
[53] Ibid., p. 272.
[54] Contudo, Dallari afirma que mesmo no período militar o *habeas data* seria esvaziado, em que pese ter sido criado como resposta ao uso autoritário da informação. É o que o autor denomina de "paradoxo do habeas data", pois o instrumento teria grande utilidade caso já fosse previsto nos anos da ditadura militar, mas, ao mesmo tempo, igualmente "teria sido suspenso pelos militares, (…) o que o torna inútil nos momentos em que prevalece a arbitrariedade e a utilização de dados falsos se torna prática rotineira." Em: DALLARI, Dalmo de Abreu, op. cit., p. 244.

pretéritos ou situações constrangedoras que digam respeito à vida privada do indivíduo”[55], quando a publicização do fato pretérito se demonstra prejudicial ao pleno desenvolvimento da personalidade do indivíduo. Percebe-se, pois, uma relação clara entre o conceito do direito ao esquecimento e a proteção da vida privada, na vertente clássica da privacidade enquanto um direito a ser deixado em paz, além de ser intimamente vinculado à dignidade da pessoa humana.

Ressalte-se que, no ordenamento brasileiro, não há nenhum dispositivo legal que expressamente preveja a figura do direito ao esquecimento, de modo que a sua construção foi realizada pela doutrina e pela jurisprudência. Alguns dos casos mais pertinentes que permitiram erigir o instituto se referem à recordação midiática de crimes passados de grande repercussão, como foi o caso do precedente fixado pelo Superior Tribunal de Justiça no julgamento do Recurso Especial 1.334.097/RJ[56], que reconheceu o direito ao esquecimento de um indivíduo que havia sido absolvido pelo Tribunal do Júri quanto ao seu envolvimento na denominada “Chacina da Candelária”, frente a reportagens jornalísticas que ainda o associavam ao fato, sem o devido consentimento quanto a divulgação de seu nome e de sua imagem.

Este julgado tratou do tema apenas em relação à liberdade de imprensa, mas o leque de proteção do direito ao esquecimento não se limita à divulgação midiática do fato pretérito, como também abarca uma série de outras situações. O que importa não é a forma como os dados do passado são rememorados, mas que o ato de rememoração em si implique uma “recordação opressiva de fatos pretéritos”[57] perante a esfera pública, o suficiente para influir na formação de uma opinião social e se opor ao pleno desenvolvimento e construção da identidade pessoal do afetado, ao fornecer ao público uma falsa projeção acerca da atual realidade do indivíduo. Assim, o cidadão pode opor o direito ao esquecimento tanto em relação ao Poder Público como à atuação de agentes privados.

Contudo, novamente, a situação se complica ao adicionar o elemento do avanço tecnológico e informático, na medida em que o direito ao esquecimento é

---

[55] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 219-241.
[56] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.334.097/RJ. Quarta Turma. Relator: Min. Luis Felipe Salomão. J. 28.05.2013, DJe 10.09.2013.
[57] SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 367-383.

frequentemente suscitado em pedidos de desindexação de páginas e de buscadores de pesquisa da *web*[58]*.* Em regra, a internet permite a eterna recordação e o arquivamento dos conteúdos existentes na rede, tanto que o Marco Civil da Internet contém disposição expressa no art. 19, caput e §1º, que a remoção de informações da internet apenas pode ser determinada por decisão judicial, sendo que a ordem deve especificamente indicar qual o conteúdo infringente a ser retirado, sob pena de nulidade[59]. Contudo, para Ricardo Villas Bôas Cueva, tal dispositivo é genérico e abrangente, tendo em vista que não define especificamente o que é considerado conteúdo infringente e não estipula prazos para a sua remoção, o que abre espaço para uma discricionariedade judicial demasiado ampla e insuficiente para garantir a plena proteção dos princípios e garantias do indivíduo associadas à internet[60].

Com o surgimento da Lei Geral de Proteção de Dados, a doutrina se debruçou quanto à possibilidade de o texto fundamentar de maneira expressa a existência de um direito ao esquecimento, eis que o art. 15 estipula que, em regra, o término do tratamento de dados pessoais ensejará a sua automática eliminação, não sendo necessário que o titular dos dados realize requerimento expresso para tanto[61], sob pena de responsabilidade civil do controlador de dados. Compreende-se a confusão entre os dois institutos, uma vez que o *General Data Protection Regulation* da União Europeia – o texto de proteção de dados pessoais de maior inspiração para a redação da LGPD – previu a eliminação dos dados ao término do tratamento a partir da denominação “direito ao apagamento dos dados” *(right to erasure)*, ou o “direito a ser esquecido” *(right to be forgotten)*.

No entanto, a similitude no vocábulo não implica a existência de identidade com o direito ao esquecimento erigido pela doutrina e pela jurisprudência brasileira, pois o *right to erasure* constante na GDPR – e, consequentemente, na LGPD – simplesmente se refere ao direito do indivíduo de requerer o apagamento de seus dados pessoais assim que a finalidade do tratamento se exaurir, na medida em que a coleta e o tratamento de dados pessoais estão estritamente limitados à finalidade

---

[58] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados, p. 226-227.
[59] CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça, p. 93.
[60] Ibid., p. 96.
[61] LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 211.

informada ao titular[62]. Tanto não há uma identidade entre o direito ao apagamento de dados e o direito ao esquecimento que, ao transportar o dispositivo da GDPR para o texto da LGPD, o legislador brasileiro não faz nenhuma menção ao vocábulo “direito a ser esquecido”, preferindo denominá-lo como “término de tratamento de dados”. Portanto, o instrumento previsto pela lei brasileira se trata de “simples remédio associado à dinâmica específica da proteção de dados pessoais”[63], não tendo qualquer relação com a proteção do indivíduo perante a memória pública de fatos pretéritos que seja prejudicial ao desenvolvimento da personalidade.

Desta maneira, até o presente momento, não há regulação legislativa acerca do direito ao esquecimento no Brasil, portanto cabendo ao julgador, nos ditames do caso concreto, verificar se a publicização de determinados fatos pretéritos está obstando o pleno desenvolvimento da identidade pessoal do indivíduo atrelado a esses acontecimentos, ou se está dentro do âmbito da liberdade de expressão, da liberdade de imprensa e do acesso à informação, sem esquecer que “o verdadeiro fundamento do direito ao esquecimento está na Constituição”[64].

1.3 A ASCENSÃO DO CAPITALISMO DE VIGILÂNCIA

Finalmente, cabe pontuar que as questões suscitadas acerca do *habeas data* e do direito ao esquecimento não são os únicos problemas práticos advindos da proteção da privacidade na era digital. Elas são apenas parcela de uma variedade de situações advindas da relação cada vez mais complexa entre privacidade, controle de dados e disseminação da informação, haja vista que, a partir do momento em que se tornou claro que as tecnologias informáticas tinham grande utilidade para correlacionar dados constantes nas redes, a utilização destas informações se tornou basilar para o desenvolvimento de estratégias de vigilância por parte do Estado – sendo que o significado de vigilância, aqui, engloba todo um “mundo de monitoramento, controle, observação, classificação, checagem e atenção

---

[62] 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.

[63] SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018, p. 377-378.

[64] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados, p. 228.

sistemática"[65] dos indivíduos a partir do processamento de dados. Isso permitiu a ascensão de toda uma sociedade de vigilância, cujos aparatos criam uma constante tensão entre as noções de privacidade, informação e segurança[66]. Nesse cenário, a coleta e o tratamento de informações pessoais em prol da segurança formam um espelho de única face ("*one-way mirror*"[67]), de tal forma que os controladores têm amplo conhecimento dos indivíduos, ao passo em que estes nada sabem sobre aqueles agentes.

Outrora, a preocupação com a vigilância se dava em relação à possibilidade de concentração do poder estatal mediante o uso indiscriminado de dados constantes em bancos de dados centralizados[68], que poderia levar à concretização do *Big Brother* de Orwell[69] ou de um modelo de controle social conforme a arquitetura do panóptico de Bentham[70] – baseado em uma vigilância constante do indivíduo sob o olhar inafastável do controlador. No entanto, esta não é mais a realidade. A descentralização das estruturas de poder e a dispersão dos sistemas de informação faz com que, atualmente, não seja mais possível rastrear um centro específico de controle social, visto que ele se encontra pulverizado em bases de dados descentralizadas e dispersas, mas ainda assim ligadas entre si.

Assim, a preocupação não é tanta com a formação de um "Grande Irmão" orwelliano, mas com o processamento de dados realizado pelos "pequenos irmãos" do setor privado[71]. Vive-se na era do *pós-panóptico*, pois, enquanto no panóptico clássico se presumia que o controlador estava presente, de alguma forma, na torre de controle, as atuais relações de poder permitem que o controlador simplesmente

---

[65] BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.
[66] MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 157-197.
[67] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais, p. 27.
[68] STEFIK, Mark. **The Internet Edge:** Social, technical and legal challenges for a networked world. Cambridge: The MIT Press, 2000, p. 201-202.
[69] Líder governamental do Estado distópico constante na obra literária *1984*, de George Orwell. O governo do Grande Irmão é totalitário e caracterizado, dentre vários aspectos, pela vigilância constante, sob a qual não há qualquer espaço para a liberdade de pensamento ou de expressão.
[70] Modelo arquitetônico prisional proposto pelo filósofo utilitarista Jeremy Bentham. A prisão é projetada em formato circular, estando as celas dispostas no perímetro exterior, completa e constantemente visíveis ao vigia localizado na torre central, que, em contrapartida, não consegue ser visto pelos prisioneiros. A figura do panóptico se popularizou com Michel Foucault, que a utilizou como ilustração em seus estudos sobre vigilância, disciplina e domesticação dos corpos, na medida em que o panóptico tem o efeito de "induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder". Em: FOUCAULT, Michel. **Vigiar e punir:** o nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014, p. 195.
[71] WHITAKER, Reg. **The End of Privacy:** how total surveillance is becoming a reality. New York: The New Press, 1999, p. 133.

vá ao plano do inacessível[72]. Nesse mesmo sentido, Reg Whitaker aponta que o panóptico contemporâneo tem como diferencial o fato de ser descentralizado, por não ter mais como referência um sistema arquitetônico físico de poder, e predominantemente consensual, eis que as pessoas tendem a consentir ceder sua privacidade por acreditarem receber benefícios em troca, por exemplo, acreditando que isso irá incorrer no aumento do grau de sua segurança pessoal[73].

Na era do capitalismo de vigilância, portanto, o controle sobre as tecnologias de informação permite a gradual consolidação de um modelo de negócio em que os dados pessoais assumem papel central, fomentando toda uma "economia de vigilância e de varejo dos dados pessoais"[74]. Os dados se tornam os principais ativos dessa nova organização econômica (*"data as the new oil"*[75]), estruturada no monitoramento constante dos "cidadãos-potenciais consumidores"[76] pelos grandes agentes econômicos.

Nos termos elencados por Zygmunt Bauman e David Lyon, a vigilância contemporânea é caracterizada por ser líquida, fluida, esparramada ao longo de todos os estratos sociais[77], não sendo possível traçar suas origens com facilidade. Trata-se de uma sociedade de controle cujo sistema de dominação é instalado de forma progressiva e dispersa, em oposição ao poder centralizado do sistema panóptico característico das sociedades disciplinares[78]. Nesse contexto de liquidez e de difusão dos aparatos de segurança, o desenvolvimento desenfreado de novas formas de tecnologia corre o risco de promover uma "cegueira moral" nos indivíduos, tendo em vista que a aplicação de algoritmos sem a regulação adequada "promove decisões que prejudicam pessoas mais pobres, reforça estereótipos e intensifica desigualdades sociais"[79], ao delinear perfis de potenciais consumidores e classificá-

---

[72] BAUMAN, Zygmunt. **Vigilância líquida,** p. 19.
[73] WHITAKER, Reg. **The End of Privacy**, p. 140.
[74] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. E-book. Disponível em: <https://www.amazon.com.br/Prote%C3%A7%C3%A3o-Dados-Pessoais-Limites-Consentimento-ebook/dp/B08287RSNK/> Acesso em: 6 abr. 2020.
[75] TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 601-619.
[76] BIONI, Bruno Ricardo, op. cit., p. 134.
[77] BAUMAN, Zygmunt. op. cit., p. 10.
[78] DELEUZE, Gilles. Postscript on the Societies of Control. **October,** v. 59, Winter 1992, p. 3-7, 1992. Disponível em: <https://www.jstor.org/stable/778828> Acesso em: 6 abr. 2020.
[79] BACHMANN, Philipp. Public relations in liquid modernity: how big data and automation cause moral blindness. **Public Relations Inquiry**, v. 8., n. 3, p. 319-331, set. 2019. Disponível em: <https://dx.doi.org/10.1177/2046147X19863833> Acesso em: 6 abr. 2020.

los conforme a avaliação de seus riscos. Isso pode ser utilizado de maneira discriminatória, pois a categorização de um indivíduo como um consumidor de alto risco – taxando-o como alguém com menores capacidades econômicas ou mais propenso ao inadimplemento, por exemplo – pode levar à exclusão deste do acesso a determinados bens e serviços[80].

Bauman e Lyon afirmam que o adjetivo líquido não é inerente à definição propriamente dita de vigilância, mas um elemento decorrente do atual estado da própria modernidade, que é, por si, líquida, "fluida e perturbadora"[81], na medida em que "todas as formas sociais se desmancham mais depressa que a velocidade com que se criam novas formas"[82]. Não é apenas a vigilância que se demonstra muito mais flexível e móvel que outrora; tal característica perpassa todos os campos afetados pela sociedade da informação.

Nesse cenário também se insere a economia. Conforme Laura Schertel Mendes, foi a crise da economia de produção em massa operada a partir da década de 1970 que permitiu o surgimento e a consolidação de um novo modelo econômico, a denominada "economia com especialização flexível"[83]. Aponta a autora que essa transição ocorreu em decorrência da saturação dos mercados industriais de massa, o que levou à necessidade de as empresas começarem a oferecer produtos diferenciados para chamarem a atenção dos consumidores, iniciando assim uma tendência de diferenciação e de individualização do produto, a fim de atender necessidades e anseios mais específicos e singularizados de cada consumidor. A produção passou a ser customizada, e, consequentemente, também o marketing. A publicidade não se volta mais a uma massa indistinta de pessoas, mas a uma segmentação específica de consumidores com interesses próprios e muito mais individualizados do que anteriormente.

Com a popularização da internet, o movimento no sentido da diferenciação dos produtos comercializados e das estratégias de marketing se intensifica. Para que a flexibilização direcionada seja eficaz, é necessário que as empresas saibam

---

[80] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. E-book. Disponível em: <https://www.amazon.com.br/Privacidade-prote%C3%A7%C3%A3o-dados-defesa-consumidor-ebook/dp/B076CL4XXW> Acesso em: 6 abr. 2020.
[81] BAUMAN, Zygmunt. **Vigilância líquida**, p. 10.
[82] Ibid., p. 11.
[83] MENDES, Laura Schertel. op. cit., posição 1687.

qual é o perfil de seus clientes, conhecimento este que apenas consegue ser adquirido pela coleta de informações dos consumidores, em especial acerca de seus hábitos, preferências e comportamentos. Desta maneira, a coleta de dados pessoais é instrumento central para a economia com especialização flexível, ao tornar factível a efetivação da publicidade comportamental e do marketing individualizado, além de facilitar o próprio processo de desenvolvimento dos produtos e serviços fornecidos pelas empresas[84], conforme as informações são correlacionadas com a finalidade de prever padrões de comportamento e, por conseguinte, padrões de consumo.

Uma das técnicas mais difundidas para a coleta e o processamento de dados de possíveis clientes é a utilização de *cookies*, voltados ao desenvolvimento e aprimoramento de perfis de consumidores na internet[85]. Os *cookies* são pequenos arquivos compostos por cadeias de números, que, ao serem instalados em um computador, permitem a sua identificação, de tal forma que, toda vez que o indivíduo regressa ao site onde inicialmente se registrou, o *cookie* automaticamente o reconhece, sem que seja preciso que o usuário reinsira as informações[86]. São eles, por exemplo, que permitem que um site lembre a senha da conta de um usuário.

Mais do que isso, a atuação dos *cookies* não se limita ao site em que houve o registro inicial. Além de gravar essas informações iniciais, eles também podem expandir a coleta para outros sites que o indivíduo visite, a fim de que o servidor reconheça o usuário por várias páginas em que navega da internet, o que possibilita, por exemplo, a veiculação de anúncios personalizados com base no rastreamento do conteúdo navegado pela pessoa na *web.* Assim, fortalece-se o *profiling*, ou seja, a técnica de formação de perfis dos usuários a partir de seus dados de navegação, gostos, hábitos e preferências pessoais[87].

Apesar da grande utilidade dos *cookies* para o próprio funcionamento da internet, a sua onipresença causa certa preocupação no âmbito de proteção da privacidade, especialmente ao se tratar de *third-party cookies* – *cookies* inseridos por terceiros, que não o site visitado pelo indivíduo – e *cookies* adaptados, como os *Flash cookies*, que são mais eficazes no rastreamento dos usuários e muito mais

---

[84] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**, posição 1763.
[85] TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais, p. 610.
[86] WHITAKER, Reg. **The End of Privacy**, p. 103.
[87] TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. op. cit., p. 611-612.

difíceis de serem removidos que os *cookies* tradicionais[88]. O rastreamento se torna ininterrupto, colocando o usuário em considerável posição de vulnerabilidade, uma vez que o *profiling* permite a identificação de dados sensíveis. Ademais, a comercialização dos perfis de usuários implica a transformação do indivíduo em simples mercadoria, reduzindo sua autonomia. Nesse sentido, não há apenas invasão da privacidade, mas também redução da esfera da liberdade individual, visto que o rastreamento e a vigilância são aprimorados de acordo com o comportamento online do indivíduo, mas conforme "uma lógica que está fundamentalmente fora de seu controle"[89].

Importante ressaltar, novamente, que todas estas preocupações com a privacidade e o surgimento da sociedade de vigilância já surgem na transição para o século XXI, tendo em vista que a crescente descentralização dos centros de processamento e tratamento de dados promoveu uma transição de uma anterior era de "vigilância" *(surveillance),* para um momento mais recente de "vigilância de dados" *("dataveillance")*[90]. Assim, se ao final do século XX já conseguiram ser demonstradas as limitações da leitura clássica do direito à privacidade frente ao desenvolvimento da informática, as novas tendências das tecnologias de informação a partir da década de 2010 – que envolvem *Big Data, analytics*, *machine learning*, sistemas de inteligência artificial, entre outros – demonstram que a esfera da privacidade nunca estará isenta de ameaças, motivo pelo qual se mostra constante "a necessidade do fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade"[91], o que será analisado nos próximos capítulos.

---

[88] TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais, p. 612.
[89] COHEN, Julie E. What Privacy is For. **Harvard Law Review,** Cambridge, v. 126, n. 7, p. 1904-1933, maio 2013. Disponível em: <https://ssrn.com/abstract=2175406> Acesso em: 7 abr. 2020.
[90] WHITAKER, Reg. **The End of Privacy**, p. 125.
[91] RODOTÀ, Stefano. **A vida na sociedade de vigilância**, p. 95.

2 A PRIVACIDADE NA ERA DOS GRANDES DADOS

2.1 *BIG DATA,* AS NOVAS TECNOLOGIAS DE INFORMAÇÃO E AS RESTRIÇÕES AO DIREITO À PRIVACIDADE

Se as preocupações com a proteção do direito à privacidade já eram patentes com a popularização da internet na transição para os anos 2000, elas se intensificam de maneira substantiva nos anos seguintes, em especial com o surgimento do denominado *Big Data*, os grandes bancos de dados. Outrora, como mencionado, a coleta e o tratamento de dados pessoais já se demonstravam indispensáveis para o devido desenvolvimento dos perfis de usuários e o consequente aprimoramento dos produtos e serviços fornecidos na *web*, no contexto do advento da economia de especialização flexível. Esta técnica de processamento de dados é denominada mineração de dados *(data mining)*, por meio da qual uma grande quantidade de dados em estado bruto pode ser transformada em informações de potencial utilidade para as empresas, a partir da "busca de correlações, recorrências, formas, tendências e padrões significativos […], com o auxílio de instrumentos estatísticos e matemáticos"[92].

Com o advento do *Big Data*, a mineração de dados atinge o seu pico. Julie Cohen descreve que o *Big Data* é tanto uma tecnologia como um processo: enquanto tecnologia, estabelece a configuração de sistemas de processamento computacional que permitem a coleta e o tratamento de uma quantidade massiva de dados em um curto período de tempo; enquanto processo, utiliza-se da mineração de dados para inferir padrões e traduzi-los em análises preditivas de potencial interesse[93]. O diferencial do *Big Data* está naquilo que se denomina os 3 V's: volume, velocidade e variedade[94]. Volume, na medida em que a coleta de dados se dá em quantidades muito maiores se comparada às formas tradicionais de *data mining;* velocidade, pois tais quantias de dados são processadas de forma quase instantânea; e variedade dos dados a serem coletados, desde arquivos de texto, áudios, vídeos, dados extraídos de aplicativos móveis, de redes sociais, entre

---

[92] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 154.
[93] COHEN, Julie E. What Privacy is For, p. 14.
[94] BIONI, Bruno Ricardo. **Proteção de dados pessoais**, p. 34.

outros. Há autores que ainda apontam mais dois elementos: a veracidade dos dados, e o valor obtido deles, em termos de utilidade[95].

Para Alexandre Veronese, *Big Data* significa a transição do processamento regular para o processamento ampliado de dados. A ampliação se opera nos campos: a) do próprio objeto do tratamento, que são os dados, com o aumento considerável na capacidade de coleta e de estocagem; b) dos meios tecnológicos utilizados, a partir do aprimoramento de equipamentos de alto desempenho e de novos programas de computadores; c) do meio intelectual pelo qual os dados são processados, conforme surgem tecnologias de ponta para inovação das práticas de análise e de correlação dos dados[96]. Viktor Mayer-Schönberger e Kenneth Cukier afirmam que, na sua essência, *Big Data* se trata de previsões, "aplicando-se a matemática em enormes quantidades de dados com a finalidade de extrair probabilidades"[97], o que é aplicado nas mais diversas áreas do cotidiano, desde o reconhecimento de e-mails como *spam*, até o aprendizado do sistema de autocorreção embutido nos teclados dos *smartphones,* a possibilidade de determinar quais perfis são mais compatíveis em serviços de relacionamento, entre outros.

Todas as empresas gigantes da Internet – como Google, Amazon, Facebook, Microsoft – já se utilizam do *Big Data* de alguma forma ou outra, tendo dados e informações como alguns de seus principais insumos[98]. Assim, a tendência de difusão do *Big Data* em todas as esferas da realidade é crescente, pois ele tem a potencialidade de "modificar aspectos fundamentais da vida, ao dá-la uma dimensão quantitativa que antes nunca teve"[99], bem como a capacidade de impulsionar a economia, transformando modelos de negócio a partir do uso de inteligência e *analytics*[100].

---

[95] BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento:** desafios para a regulação da propaganda eleitoral. 2019, 171 f. Dissertação (Mestrado em Direito Político) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte (MG), 2019. Disponível em: <http://hdl.handle.net/1843/DIRS-BELHWW> Acesso em: 7 abr. 2020.

[96] VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 385-415.

[97] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data:** a revolution that will transform how we live, work and think. New York: Houghton Mifflin Harcourt, 2013, p. 11-12.

[98] RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? **International Data Privacy Law,** Oxford, v. 3, n. 2, p. 74-87, maio 2013. Disponível em: <https://doi.org/10.1093/idpl/ips036> Acesso em: 8 abr. 2020.

[99] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. op. cit., p. 12.

[100] TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and user control in the age of analytics. **Northwestern Journal of Technology and Intellectual Property,** Chicago, v. 11, n. 5, p. 1-36, 1 nov. 2013. Disponível em: <https://ssrn.com/abstract=2149364>. Acesso em: 7 abr. 2020.

Não se pode negar que a disseminação do *Big Data* em conjunto com inovações tecnológicas associadas – tais como a computação em *cloud* e o desenvolvimento de sistemas de *machine learning* – tem suas vantagens. Omer Tene e Jules Polonetsky pontuam que não apenas há um aumento de produtividade para as empresas que o utilizam, com a diminuição de custos e de tempo em comparação ao processamento regular de dados, mas também apresenta benefícios à própria sociedade. Por exemplo, na medicina, sendo possível extrair padrões de grandes bancos de dados com o fim de identificar quais são os efeitos colaterais que surgem de determinadas interações medicamentosas; ou para o planejamento urbano, em que dados de localização geográfica são úteis para identificar os pontos mais movimentados das cidades, o que pode contribuir para políticas públicas de construção e reformas de rodovias, mitigação de congestionamento de trânsito, planejamento habitacional, entre outras medidas[101].

Não se pretende assumir uma postura negacionista em relação ao *Big Data*, pois é preciso reconhecer a posição de destaque que as novas formas de tecnologia têm assumido no cotidiano e que, no futuro, a tendência é apenas de intensificação da utilização dessas técnicas. Por outro lado, também não é possível defender o outro extremo, de que não há qualquer falha nos novos modelos de processamento ampliado de dados, sustentando a inovação tecnológica como um valor absoluto em detrimento dos direitos fundamentais de cada indivíduo. É necessário reconhecer os amplos benefícios proporcionados pelo *Big Data*, ponderando-os com os riscos que ele proporciona à privacidade dos usuários das redes. Nesse sentido, a proteção da privacidade não está em direta oposição ao ideal de progresso tecnológico: ambas as ideias podem ser desenvolvidas de maneira complementar, e, ao contrário do que os entusiastas mais extremistas do *Big Data* poderiam afirmar, a percepção de que a inovação tecnológica só é possível com a ausência de regulação é uma falácia[102].

No entanto, na prática, observa-se que as novas tecnologias de informação não têm sido desenvolvidas de forma complementar à proteção da privacidade, mas sim proporcionando riscos desnecessários aos usuários, que têm seus dados coletados, processados e comercializados sem o seu devido conhecimento ou

---

[101] TENE, Omer; POLONETSKY, Jules. Big Data for All, p. 8-11.
[102] Para Julie Cohen, trata-se de uma visão simplista da relação entre privacidade e inovação, pois ignora tanto a complexidade das práticas inovadoras como a dinamicidade que caracteriza a privacidade. COHEN, Julie E. What Privacy is For, p. 13.

consentimento. Não são poucos os casos relevantes de violação da privacidade de dados que vieram à tona na mídia nos últimos anos, desde o escândalo entre o Facebook e a empresa especializada em *data mining* Cambridge Analytica (objeto de análise do ponto 2.3), o vazamento de dados da rede social Ashley Madison[103], até, no Brasil, uma brecha no aplicativo "E-saúde", do Ministério da Saúde, que causou o vazamento de dados sensíveis sobre a saúde de milhões de usuários do SUS em 2018[104] .

Dentro de todo esse contexto, proteger a privacidade se torna mais difícil com o aumento exponencial de informações coletadas e o compartilhamento crescente delas com múltiplas entidades ao redor do mundo[105]. Para Ira Rubinstein, um dos maiores perigos associados ao *Big Data* é a possibilidade de identificação dos indivíduos mesmo quando os dados inicialmente coletados sejam anonimizados, o que faz com que a agregação de dados, junto com o monitoramento contínuo dos usuários, se torne "mais granular, mais revelador e mais invasivo"[106]. Isso demonstra que, no fim das contas, técnicas como a anonimização de dados – que justamente tem a finalidade de não identificar quem seja o titular – acabam proporcionando ao indivíduo mais uma ilusão de proteção de sua esfera de privacidade, do que uma proteção propriamente dita.

Perante o *Big Data*, mesmo alguns princípios clássicos da proteção da privacidade e dos dados pessoais encontram dificuldades de serem devidamente aplicados. É o caso, por exemplo, do princípio da especificação dos propósitos, por meio do qual o tratamento de dados pessoais deve ser limitado a uma finalidade específica, que tenha sido autorizada pelo titular; surgindo uma nova finalidade para a coleta de dados, é preciso haver uma nova manifestação de consentimento pelo indivíduo[107]. Este princípio é basilar para garantir a autodeterminação informativa do

---

[103] Rede social de relacionamentos com o objetivo de promover relacionamentos extraconjugais. Em 2015, um grupo de *hackers* vazou os dados do serviço, incluindo dados sensíveis de seus usuários, tais como nomes verdadeiros, endereços de e-mail, números de telefone e de cartões de crédito, preferências sexuais e senhas encriptadas. Em: GIBBS, Samuel. Ashley Madison condemns attacks as experts say hacked database is real. **The Guardian**, London, 19 ago. 2015. Disponível em: <https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports> Acesso em: 8 abr. 2020.

[104] FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. **Folha de S. Paulo,** São Paulo, 26 jan. 2018. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml> Acesso em: 8 abr. 2020.

[105] TENE, Omer; POLONETSKY, Jules. Big Data for All, p. 13.

[106] RUBINSTEIN, Ira S. Big Data, p. 77.

[107] BIONI, Bruno Ricardo. **Proteção de dados pessoais**, p. 221.

cidadão, mas cuja aplicação encontra empecilhos quando se trata de *Big Data*. Mayer-Schönberger e Cukier descrevem a problemática sucintamente, na forma de questionamentos: como é possível especificar de maneira predeterminada quais são os propósitos e a finalidade da coleta de dados, se a própria lógica do *Big Data* é integralmente voltada a descobrir novos padrões e novas formas de utilização dos dados apenas *após* o tratamento? E como pode o usuário consentir com a finalidade da coleta de dados se esta ainda é desconhecida?[108]

Dificuldade similar encontra o princípio da minimização de dados, que sustenta que a coleta de dados deve se limitar ao mínimo estritamente necessário para que seja viável alcançar a finalidade pretendida. Tal como o princípio da especificação dos propósitos, a minimização de dados se opõe à própria natureza do *Big Data*, pois este se baseia na maximização de dados, buscando agregar a maior quantidade de dados possíveis para extrair correlações de informações, sem que haja restrições prévias que visem a reduzir sua capacidade de coleta[109].

Até o presente momento, não há uma solução clara para este problema. Bruno Bioni sustenta que, no contexto do *Big Data*, a proteção da privacidade requer uma abordagem normativa mais flexível que não foque tanto na necessidade do consentimento do indivíduo, reduzindo, nesses casos, a posição de protagonismo do titular de dados, uma vez que "o conteúdo da autodeterminação informacional é circular ao consentimento, mas a ele não se resume"[110]. Para Tene e Polonetsky, torna-se necessário relaxar, até certo ponto, a minimização de dados e a exigência de especificação dos propósitos, para, no seu lugar, dar mais ênfase às ideias de transparência, acesso à informação e veracidade no tratamento de dados[111]. Afinal, é permitindo às pessoas o devido acesso a seus dados – de maneira transparente, compreensível e que permita o seu engajamento com as formas em que os dados são tratados[112] – que surge a possibilidade de empoderamento dos indivíduos dentro da relação com as entidades que se utilizam do *Big Data*, e, por conseguinte, a mitigação da sua situação de hipervulnerabilidade.

---

[108] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**, p. 153.
[109] RUBINSTEIN, Ira S., Big Data, p. 78.
[110] BIONI, Bruno Ricardo. op. cit., p. 223.
[111] TENE, Omer; POLONETSKY, Jules. Big Data for All, p. 5.
[112] Ibid., p. 33.

2.2 O PARADOXO DA PRIVACIDADE E OS LIMITES DO CONSENTIMENTO

Outro ponto que merece uma análise destacada no âmbito da proteção da privacidade de dados é referente à ideia de consentimento*,* pois é um dos elementos centrais a permitirem a coleta e o processamento de dados pessoais. Observa-se no texto da Lei Geral de Proteção de Dados: "Art. 7º: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular". Nesse sentido, apesar de o texto legal trazer hipóteses em que o consentimento não é exigido, ele ainda é considerado como principal base legal a permitir o tratamento dos dados pessoais[113].

Define-se o consentimento como o "poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade"[114], por meio do qual o indivíduo exerce a liberdade de escolha para a construção e delimitação de sua esfera privada[115], enquanto expressão da autonomia privada do cidadão[116]. Quando transportada para o campo da proteção da privacidade na sociedade da informação, o consentimento é forma de manifestação da autodeterminação informativa do titular dos dados, ao proporcionar ao particular a possibilidade de ter controle sobre a obtenção, a titularidade, o tratamento e a transmissão dos dados coletados[117].

Laura Schertel Mendes aponta que a doutrina alemã apresenta três correntes quanto à discussão sobre qual é a natureza jurídica do consentimento. A primeira o define enquanto declaração de vontade negocial, estabelecendo um negócio jurídico entre o titular dos dados e o sujeito que irá tratá-los. A corrente oposta sustenta que se trata de um ato jurídico unilateral, sem qualquer natureza negocial. Já a terceira corrente – defendida pela autora – apresenta um meio-termo, afirmando que o consentimento é um ato que se assemelha ao negócio jurídico sem o ser: ele apresenta características negociais, pois, tal como a declaração de vontade em um negócio jurídico, o consentimento se volta à autodeterminação da

---

[113] LIMA, Caio César Carvalho. Do tratamento de dados pessoais, p. 179.
[114] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 298.
[115] TEPEDINO, Gustavo; TEFFÉ; Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 287-322.
[116] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**, posição 1000.
[117] TEPEDINO, Gustavo; TEFFÉ; Chiara Spadaccini de. op. cit., p. 291.

pessoa; no entanto, ele também tem um caráter personalíssimo que não pode ser ignorado[118]. Danilo Doneda assume uma posição similar, mas tendendo a afastar de forma mais contundente o caráter negocial do consentimento, porquanto fixá-lo dentro dos limites de um negócio jurídico legitima "a inserção desse consentimento em estruturas contratuais, dificultando a sua valoração em função dos atributos da personalidade que estão em jogo"[119]. Para este autor, portanto, é preciso valorizar o consentimento mais como exercício do direito à autodeterminação informativa, que tem caráter pessoal, e não patrimonial.

Para que o consentimento seja considerado válido, nos termos elencados pelo art. 5º, inciso XII da Lei Geral de Proteção de Dados, ele deve ser manifestado de forma: a) livre; b) informada; c) inequívoca; devendo o titular d) concordar com o uso de seus dados voltado a uma finalidade específica. Primeiramente, o consentimento deve ser *livre*, tendo sido proporcionado ao titular o poder de escolher se quer dispor ou não de suas informações pessoais, não se admitindo o tratamento de dados mediante vício de consentimento (erro, dolo ou coação)[120].

Em segundo lugar, deve ser *informado*, ou seja, o cidadão tem o direito de ser informado sobre como seus dados estão sendo colhidos e a maneira como se dá o tratamento, bem como as suas reais consequências e como isso pode afetá-lo em sua esfera privada. O direito de informação, assim, tem profundas relações com o princípio da transparência, devendo a informação ser proporcionada ao indivíduo de maneira clara e de fácil compreensão – por exemplo, caso se dê por escrito, deve haver uma cláusula contratual destacada em relação ao consentimento[121]. Em terceiro lugar, o consentimento deve ser *inequívoco*, restando claro que o titular efetivamente concorda com os termos pelos quais o tratamento de dados será realizado. Por fim, mas não menos importante, a validade do consentimento nos termos legais também exige sua vinculação com o *princípio da finalidade*, por meio do qual a coleta e o processamento de dados devem ser voltados a objetivos legítimos, específicos, explícitos e informados ao particular (art. 6º, inciso I, LGPD),

---

[118] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**, posição 1039.
[119] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 302.
[120] TEPEDINO, Gustavo; TEFFÉ; Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD, p. 299.
[121] VAINZOF, Rony. Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.)., op. cit., p. 19-177.

“sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, mesmo nos casos em que a base legal não for o consentimento do titular”[122]. Cabe observar que, por se tratar de manifestação da vontade do indivíduo, também é permitido a ele a revogação do consentimento a qualquer momento, mediante manifestação expressa, por meio de procedimento gratuito e facilitado (art. 8º, §5º).

Esses são os elementos essenciais ao consentimento válido, que devem estar presentes em todas as situações em que ele é exigido para o devido tratamento de dados, nos termos da legislação. Em alguns casos determinados e taxativamente previstos na lei, exige-se ainda que o consentimento ocorra de maneira específica (ou expressa). Trata-se da carga de proteção máxima, ao exigir que ele seja ainda mais especificado e pontual do que o mero consentimento livre, informado e inequívoco. São hipóteses em que o titular precisa saber quais as consequências do tratamento de seus dados de maneira mais clara e precisamente detalhada, permitindo que ele acompanhe o tratamento de dados em todos os seus movimentos[123], por se encontrar em uma posição de maior vulnerabilidade na relação de tratamento de suas informações. São os casos de quando há o compartilhamento dos dados com terceiros com os quais o titular não tem relação direta (art. 7º, §5º), no tratamento de dados sensíveis (art. 11, inciso I), de dados relativos a crianças, mediante consentimento fornecido por pelo menos um dos pais ou responsáveis legais (art. 14, §1º), e para a transferência internacional de dados (art. 33, inciso VIII).

Na prática, no entanto, a ideia de consentimento válido encontra algumas limitações para efetivamente ser aplicada. Já se mencionou a incompatibilidade entre o princípio da finalidade e a lógica de funcionamento dos sistemas de *Big Data*, uma vez que não há como pré-estabelecer uma finalidade específica a uma modalidade de processamento de dados cujo principal objetivo é justamente descobrir novas formas de utilização das informações apenas após o tratamento delas. Nesse ponto, a necessidade de obter consentimento expresso para o tratamento de dados sensíveis pode se tornar uma medida inócua, pois as

---

[122] TEPEDINO, Gustavo; TEFFÉ; Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD, p. 302.
[123] BIONI, Bruno Ricardo. **Xeque-Mate:** o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: USP-GPoPAI, 2015. Relatório técnico.

tecnologias de processamento ampliado têm a capacidade de extrair informações sensíveis a partir de dados que inicialmente não o sejam, ou mesmo de dados anonimizados[124].

No contexto de *Big Data,* a dificuldade de encontrar um ponto de equilíbrio entre a inovação tecnológica e a proteção da privacidade está no fato de que o consentimento ou se apresenta de forma demasiado restritiva ao modelo de funcionamento das novas tecnologias, ou de maneira insuficiente para garantir uma efetiva tutela da privacidade[125]. Soma-se a isso o fenômeno que Danilo Doneda denomina de "paradoxo da privacidade": o fato de que o titular dos dados só conseguirá obter a tutela de sua privacidade em um momento posterior ao consentimento. Ou seja, para a pessoa conseguir obter a proteção de sua esfera privada, primeiramente ela teria que concordar com a sua violação, na medida em que a tutela se efetivaria apenas após a constatação do dano[126], o que é particularmente perigoso nas situações relativas a dados de pessoas mais vulneráveis, por exemplo, de crianças e adolescentes.

Outro obstáculo no qual o consentimento esbarra está na dificuldade de constatar, na prática, o que efetivamente configura uma manifestação de vontade livre, informada e inequívoca por parte do titular dos dados. Na concepção de Bruno Bioni, tal dificuldade reside no fato de que o próprio ser humano apresenta limitações cognitivas que o impedem de exercer um genuíno processo de tomada de decisões, tendo em vista que a capacidade cognitiva dos indivíduos não é ampla o suficiente para absorver todas as informações com que eles têm contato. O autor sustenta, ainda, a teoria da decisão da utilidade subjetiva, por meio da qual o ser humano tem a tendência de preferenciar decisões que gerem benefícios imediatos, protelando aquelas que estejam mais distantes temporariamente[127]. Nesse contexto, o acesso a determinados bens e serviços fornecidos pela internet proporciona um benefício imediato ao consumidor, que tende a ignorar os riscos promovidos contra a sua privacidade, pois as chances de sofrerem danos se encontram muito mais distantes em um nível temporal.

---

[124] TENE, Omer; POLONETSKY, Jules. Big Data for All, p. 14.
[125] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data**, p. 154.
[126] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 299.
[127] BIONI, Bruno Ricardo. **Proteção de dados pessoais**, p. 139-140.

Essa teoria pode explicar uma segunda modalidade de “paradoxo da privacidade”, desta vez descrita por Patricia Norberg, Daniel Horne e David Horne, como o paradoxo comportamental entre a maneira como os indivíduos desejam proteger a privacidade e como efetivamente eles agem na prática[128]. Ou seja, existe uma dissonância entre as intenções manifestadas pelos consumidores e as ações praticadas por eles: se, por um lado, eles demonstram ter preocupação com a proteção da privacidade de forma abstrata, por outro, esta preocupação não é suficiente para impedi-los de divulgar seus dados quando há a possibilidade concreta de receber benefícios diretos – por exemplo, divulgando informações pessoais em troca de descontos em supermercados.

Fatores externos como a mídia tendem a influenciar as pessoas a se preocuparem com a privacidade, ao ressaltarem os aspectos negativos associados à sua violação, em especial ao abordar casos de grande repercussão relativos à ascensão da sociedade de vigilância, tal como o caso Edward Snowden[129]. Todavia, em âmbitos como o comércio, observa-se igualmente uma trivialização do requerimento de dados pessoais, que se tornou atualmente uma prática rotineira. Isso, somado com a baixa percepção dos consumidores quanto a potenciais danos causados por essas práticas cotidianas, proporciona a impressão de não haver uma correlação direta entre o fornecimento de dados e a violação da privacidade[130], de modo que o particular nunca imaginaria que a situação pela qual ele passa rotineiramente ao fazer compras seja de alguma maneira comparável com a gravidade dos casos de violação de privacidade veiculados na mídia.

Desta forma, a valoração da importância da privacidade também depende do contexto direto em que ela se insere, uma vez que, dependendo da situação, o indivíduo pode exibir desde a preocupação mais extrema até um grau de apatia em

---

[128] NORBERG, Patricia A.; HORNE, Daniel R.; HORNE, David A. The Privacy Paradox: Personal information disclosure intentions versus behaviors. **Journal of Consumer Affairs,** New Jersey, v. 41, n. 1, p. 100-126, mar. 2007. Disponível em: <https://doi.org/10.1111/j.1745-6606.2006.00070.x> Acesso em: 10 abr. 2020.

[129] *Whistleblower* estadunidense que, em 2013, vazou documentos confidenciais da Agência de Segurança Nacional dos Estados Unidos (NSA), revelando inúmeros programas de vigilância global coordenados pelos EUA. O impacto causado pelo vazamento foi tanto que Snowden é considerado atualmente “o *whistleblower* mais importante dos tempos modernos”. Em: BURROUGH, Bryan; ELLISON, Sarah; ANDREWS, Suzanna. The Snowden Saga: A shadowland of secrets and light. **Vanity Fair**, New York, 23 abr. 2014. Disponível em: <https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview> Acesso em: 10 abr. 2020.

[130] NORBERG, Patricia A.; HORNE, Daniel R.; HORNE, David A. op. cit., p. 106-109.

relação à proteção de sua esfera privada[131], o que pode justificar a dissonância constatada entre a intenção abstrata e a práxis concreta.

Tudo isso demonstra o quão vulnerável o particular se encontra dentro da complexa relação entre a proteção da privacidade e a sociedade da informação, pois, mesmo sendo o consentimento elemento central para a garantia da proteção individual, constata-se que em muitos casos as pessoas simplesmente não sabem o que é com o que eles estão consentindo ou quais as consequências de sua concordância. Portanto, não há como considerar como consentimento apto a autorizar o tratamento de dados aquele em que a parte se limita a selecionar opções pré-validadas, o que é o problema observado nos termos de serviço e políticas de privacidade de grande parte dos *websites*.

Uma característica desses termos de serviço é que eles tendem a funcionar sob a lógica do "tudo ou nada" *(take it or leave it)*, na qual resta ao usuário apenas duas opções: ou aceitar todos os termos e condições pré-definidas pelo serviço, ou ser impedido de utilizá-lo. Assim, a opção por não divulgar os dados pessoais implica uma renúncia ao acesso a determinados bens e serviços[132]. Portanto, há quem afirme que as políticas de privacidade e os termos de uso possuem natureza de contrato de adesão[133], visto que não é proporcionado ao consumidor a possibilidade de negociar os termos contratuais com os quais ele está aderindo.

Resta claro que há uma manifesta assimetria na relação entre o coletor dos dados e o indivíduo que renuncia o seu controle para ter acesso ao produto desejado. Considerando-se a posição de vulnerabilidade da pessoa, não há como pressupor que o consentimento exprimido por ele seja válido – livre, informado e inequívoco – apenas por ter apertado um botão com os dizeres "leio e concordo com os termos de serviço", sabendo-se que a vasta maioria dos usuários não tem o costume de ler as políticas de privacidade das páginas em que navegam, e que, mesmo se o tivessem, não haveria muitos benefícios práticos, porquanto grande parte desses instrumentos são redigidos em linguajar técnico que não permite a devida compreensão por parte do indivíduo médio[134].

---

[131] ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science,** Washington D.C., v. 347, n. 6221, p. 509-514, 30 jan. 2015. Disponível em: <https://dx.doi.org/10.1126/science.aaa1465>. Acesso em: 10 abr. 2020.
[132] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 298-299.
[133] BIONI, Bruno Ricardo. **Proteção de dados pessoais**, p. 162.
[134] ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. op. cit., p. 513.

Como resposta a esses problemas, surge a proposta de implementação do consentimento granular, com a finalidade de inverter a lógica binária da escolha do "tudo ou nada" e priorizar a transparência da informação. Ao invés de estabelecer o consentimento como um único ato de condição de acesso ao produto ou serviço, ele passa a ser espalhado ao longo da navegação do usuário, resguardando "a opção do titular em emitir autorizações fragmentadas no tocante ao fluxo de seus dados pessoais"[135].

A princípio, a ideia de consentimento granular se apresenta como boa alternativa para garantir maior proteção do consumidor em *websites* estruturados em termos e condições de uso. No entanto, ela também pode ter sua aplicação dificultada em serviços fundamentados em *Big Data*, pois, como explorado, o processamento ampliado de dados ocorre em quantidades tão maiores e em tempo tão mais reduzido que se torna faticamente impossível exigir o consentimento do usuário para cada fluxo de informações analisado ou de dados correlacionados.

Até o presente momento, não há simples solução para este problema. É possível sugerir medidas para mitigá-lo, por exemplo, a partir do conceito de *privacy by design*, que estabelece que as medidas de segurança devem estar presentes desde a concepção do produto ou do serviço, "trazendo a preocupação com o tratamento de dados e com a proteção da privacidade para a prancheta"[136], de modo que a privacidade venha a ser protegida sob uma racionalidade *ex ante*[137], e não apenas após a constatação do dano, o que foi recepcionado pelo art. 46, §2º da Lei Geral de Proteção de Dados[138]. Contudo, apenas estas medidas não serão suficientes perante a crescente complexidade dos sistemas de *Big Data* e das novas tecnologias associadas a ele.

É necessário, portanto, garantir que os padrões de segurança sejam constantes, mas também flexíveis, uma vez que precisam se adaptar à evolução

---

[135] BIONI, Bruno Ricardo. **Xeque-Mate**, p. 55.
[136] SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 418-440.
[137] BIONI, Bruno Ricardo. **Proteção de dados pessoais**, p. 165.
[138] Art. 46: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

permanente dos desafios postos à privacidade[139]. Trata-se de estabelecer medidas minimamente capazes de garantir ao cidadão a oportunidade de tomar decisões de maneira racional e informada[140], com o intuito de reduzir a assimetria informacional. Com isso, espera-se que o consentimento não seja mera ilusão de tutela, mas que possa efetivamente ser uma garantia da autonomia privada e atuar como verdadeiro instrumento de proteção do indivíduo.

2.3 O CASO FACEBOOK-CAMBRIDGE ANALYTICA

Tendo sido observados alguns dos desafios proporcionados pelas novas tecnologias de informação para a proteção da privacidade e dos dados pessoais, oportuno analisar situações mais concretas, em especial a partir de um dos casos mais relevantes sobre violação da privacidade dos últimos anos.

A rede social Facebook foi criada no ano de 2004 por Mark Zuckerberg e colegas da Universidade de Harvard. Inicialmente restrito ao campus universitário, o site foi aberto para o público em geral a partir de 2006. Nos anos seguintes, a popularidade da plataforma aumentou vertiginosamente, tornando-se a rede social mais utilizada do mundo, tendo atingido a marca dos 2 bilhões de usuários mensais ativos em 2017[141]. Desde então, o crescimento de usuários parece ter se estabilizado, havendo indicativos de que uma porção significativa de pessoas estariam abandonando o site, ao menos dentre os usuários estadunidenses[142]. No entanto, tal estabilização não necessariamente implica uma redução do poderio da empresa, uma vez que ela também é dona de uma série de outros serviços, incluindo outros três dos aplicativos móveis mais baixados da década[143] – Facebook Messenger, WhatsApp e Instagram.

---

[139] CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. **International Data Privacy Law,** Oxford, v. 3., n. 2, p. 67-73, 1 maio 2013. Disponível em: <https://doi.org/10.1093/idpl/ipt005>. Acesso em: 11 abr. 2020.

[140] ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information, p. 514.

[141] CONSTINE, Josh. Facebook now has 2 billion monthly users… and responsibility. **TechCrunch**, San Francisco, 27 jun. 2017. Disponível em: <https://techcrunch.com/2017/06/27/facebook-2-billion-users/> Acesso em: 12 abr. 2020.

[142] STATT, Nick. Facebook's US user base declined by 15 million since 2017, according to survey. **The Verge**, New York, 6 mar. 2019. Disponível em: <https://www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-million-people-united-states-privacy-scandals> Acesso em: 12 abr. 2020.

[143] PERRY, Alex. Facebook owns the 4 most downloaded apps of the decade. **Mashable**, New York, 16 dez. 2019. Disponível em: <https://mashable.com/article/facebook-most-downloaded-apps-2010s/> Acesso em: 12 abr. 2020.

O tamanho da base de usuários do Facebook significa que a coleta e o tratamento de dados realizados diariamente são consideráveis, sendo a empresa uma das protagonistas no mundo do *Big Data*, juntamente com outras plataformas como Google, Microsoft e Amazon. A amplitude de dados minerados permite a construção de "arquiteturas de persuasão para capturar a atenção de seus bilhões de usuários em nível individualizado, utilizando-se para isso de algoritmos de personalização"[144]. Com isso, há uma crescente sofisticação das técnicas de *profiling* utilizadas pelo Facebook, capturando a maior e mais variada quantidade de dados possíveis – por exemplo, desde fotos postadas a páginas curtidas, comentários escritos e amigos colecionados –, a fim de personalizar a experiência de cada usuário na rede e, por conseguinte, retroalimentar o "ciclo sem fim entre captura de dados e melhoria do algoritmo"[145].

Já a Cambridge Analytica surgiu no ano de 2013, tendo se consolidado como uma firma especializada em mineração de dados para comunicações estratégicas e análises comportamentais, principalmente para o âmbito eleitoral[146]. Boa parte dos dados minerados por ela eram coletados sem a devida permissão do particular para esta finalidade específica, uma vez que provinham de perfis de usuários do Facebook.

A partir de 2014, a empresa passou a receber uma grande quantidade de dados de usuários da rede social que haviam utilizado um aplicativo chamado "thisisyourdigitallife", que coletava dados pessoais de participantes que acreditavam estar preenchendo um teste de personalidade[147]. Cabe ressaltar que o aplicativo não havia sido criado pela firma, mas por um grupo denominado Global Science Research, para usos alegadamente acadêmicos. Contudo, conforme Christopher Wylie, o *whistleblower* que trouxe o escândalo à tona, a Cambridge Analytica pagou para obter os dados coletados pelo grupo de pesquisa para fins políticos, ainda que

---

[144] BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento**, p. 94.
[145] Ibid., p. 94.
[146] INGRAM, David. Factbox: Who is Cambridge Analytica and what did it do? **Reuters**, San Francisco, 19 mar. 2018. Disponível em: <https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F> Acesso em: 12 abr. 2020.
[147] BERGHEL, Hal. Malice Domestic: The Cambridge Analytica Dystopia. **Computer,** Washington D.C., v. 51, n. 5, p. 84-89, maio 2018. Disponível em: <https://dx.doi.org/10.1109/MC.2018.2381135> Acesso em: 12 abr. 2020.

o Facebook afirme que a comercialização dos dados de seus usuários para terceiros seja contrária às regras da plataforma[148].

Uma vez na posse dos dados, a Cambridge Analytica era capaz de manipulá-los a partir de uma técnica denominada “microdirecionamento psicográfico” (*psychographic targeting)*[149], por meio da qual se construíam perfis de personalidade de cada indivíduo. Com base nos cliques, nos *likes*, nas postagens realizadas e em outros padrões de comportamento observados pela navegação no Facebook, tornou-se possível inferir os hábitos, gostos, preferências e estados emocionais dos usuários, podendo situá-los dentro do “modelo OCEAN”, que é uma sigla para cinco tipos de personalidade distintos (*openness, conscientiousness, extraversion, agreeableness* e *neuroticism*)[150].

Acrescem-se a isso, ainda, a coleta de dados demográficos e geográficos, de modo que a Cambridge Analytica tinha a capacidade de traçar perfis extremamente detalhados acerca da vida não apenas dos usuários do Facebook que haviam preenchido o teste de personalidade, mas também de toda a lista dos seus amigos. Com isso, a empresa poderia se utilizar de tais informações para influenciar o comportamento desses indivíduos, a partir da divulgação de conteúdo moldado especificamente conforme seus traços de personalidade e de seus interesses pessoais.

O que há de especialmente perigoso nesse caso não é apenas o alto grau de sofisticação que as técnicas de *profiling* e de marketing direcionados alcançaram, mas principalmente o poder de influência que elas assumiram na racionalidade decisória de cada indivíduo, haja vista que uma das principais finalidades da Cambridge Analytica era se utilizar da segmentação psicográfica para favorecer campanhas políticas, por exemplo, a campanha presidencial de Ted Cruz[151], bem

---

[148] ROSENBERG, Matthew; CONFESSORE, Nicholas; CADWALLADR, Carole. How Trump consultants exploited the Facebook data of millions. **The New York Times,** New York, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> Acesso em: 12 abr. 2020.

[149] GIBNEY, Elizabeth. The scant science behind Cambridge Analytica’s controversial marketing techniques. **Nature**, London, 29 mar. 2018. Disponível em: <https://www.nature.com/articles/d41586-018-03880-4> Acesso em: 12 abr. 2020.

[150] Também conhecidos como os cinco grandes fatores da personalidade na psicologia (*Big Five*), são a abertura para a experiência, a conscienciosidade, extroversão, amabilidade e neuroticismo. BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento**, p. 117.

[151] DAVIES, Harry. Ted Cruz using firm that harvested data on millions of unwitting Facebook users. **The Guardian**, London, 11 dez. 2015. Disponível em: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> Acesso em: 12 abr. 2020.

como possivelmente a campanha de Donald Trump[152] e a votação do Brexit[153]. O próprio CEO da empresa, Alexander Nix, abertamente defendeu a utilização do microdirecionamento psicográfico para a propaganda de Ted Cruz, mediante o cruzamento entre a ciência comportamental, a análise de dados e tecnologias de marketing individualizado; nas suas palavras, “é a personalidade que dirige o comportamento, e é o comportamento que influencia como você vota”[154].

Hal Berghel afirma que a adoção de métodos moralmente questionáveis para influenciar o processo eleitoral não é nenhuma novidade; no entanto, o caso Cambridge Analytica representa um marco, por apresentar a diferença significativa de ter a tecnologia digital como elemento essencial para as campanhas políticas[155]. Conforme o autor, o microdirecionamento psicográfico para fins eleitorais permite que candidatos se aproveitem de todas as nossas emoções e fraquezas, sendo sua eficácia tão maior quanto for mais capaz de influenciar o comportamento, da maneira menos perceptível possível[156]. Daniel Susser, Beate Roessler e Helen Nissenbaum possuem posicionamento similar, sustentando que as técnicas empregadas pela Cambridge Analytica são uma forma de manipulação, pois são intencionalmente voltadas a influenciar a tomada de decisões dos indivíduos, a partir da exploração de medos e de vulnerabilidades, reduzindo a esfera de autonomia individual[157].

Ainda, essas táticas apenas intensificam a criação de bolhas virtuais, dentro das quais os usuários são cercados apenas por anúncios, notícias e outros usuários que tenham a mesma visão de mundo que a sua. Como elencado por Julia Rocha de Barcelos, se por um lado o algoritmo é segregador, ao apresentar apenas aquilo que filtrou como ser de interesse do usuário, por outro lado o fenômeno também é alimentado pelas próprias pessoas, que “por vezes bloqueiam, desfazem a amizade

---

[152] LAPOWSKY, Issie. What did Cambridge Analytica really do for Trump’s campaign? **Wired,** San Francisco, 26 out. 2017. Disponível em: <https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/> Acesso em: 12 abr. 2020.
[153] CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. **The Guardian**, London, 7 maio 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> Acesso em: 12 abr. 2020.
[154] NIX, Alexander. **Cambridge Analytica:** The Power of Big Data and Psychographics. Disponível em: <https://www.youtube.com/watch?v=n8Dd5aVXLCc> Acesso em: 12 abr. 2020.
[155] BERGHEL, Hal. Malice Domestic, p. 85.
[156] Ibid., p. 85-86.
[157] SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy and manipulation. **Internet Policy Review**, Berlin, v. 8, n. 2, p. 1-22, 30 jun. 2019. Disponível em: <https://dx.doi.org/10.14763/2019.2.1410> Acesso em: 12 abr. 2020.

ou ocultam a visualização de conteúdos aos quais são contrários”[158], alimentando um ciclo vicioso. Por exemplo, com o *profiling* psicográfico, a Cambridge Analytica era capaz de verificar que, se um cidadão estadunidense apresentasse um perfil com tendências republicano-conservadoras e uma personalidade de caráter neurótico, nos termos do modelo OCEAN, um anúncio político capaz de afetar seu comportamento de maneira eficiente seria um que defendesse o porte de armas a partir de uma mensagem fundamentada no medo da insegurança[159]. Dado o seu viés ideológico, não haveria eficiência para o algoritmo mostrar a esse indivíduo anúncios que promovessem, por exemplo, a descriminalização de drogas.

Desta forma, os algoritmos que fomentam as redes sociais e a mineração de dados para fins de marketing individualizado tendem a perpetuar crenças pré-definidas e impedir que as pessoas tenham contato com o outro que pense de maneira distinta, uma vez que o pensamento que esteja fora da bolha de interesse do usuário é filtrado como algo irrelevante, e, portanto, inexistente – o que acentua a polarização política entre grupos com visões de mundo distintas. No campo eleitoral, o *psychographic targeting* propositalmente se aproveita de preconceitos, vieses e agendas políticas para fins de controle comportamental e de manipulação[160].

Os grandes atores econômicos, tais como o Facebook, podem querer vender a imagem de neutralidade e imparcialidade, no entanto, o próprio ato de negar uma ideologia é, por si, uma posição ideológica[161]. Os algoritmos não são imparciais, são “opiniões incorporadas em código matemático que refletem objetivos, ideologias, e refletem as falhas de seus criadores”[162], que, se utilizados para fins de manipulação – tal como feito pela Cambridge Analytica –, têm o poder de perpetuar desigualdades e fomentar polarizações. Apesar de suas inúmeras qualidades, quando os sistemas de *Big Data* são utilizados em desprezo da ética, eles apresentam um potencial destrutivo considerável[163], ao ponto de Cathy O’Neil denominá-los de “armas de destruição matemática”[164].

---

158 BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento**, p. 99.
159 Ibid., p. 117.
160 BERGHEL, Hal. Malice Domestic, p. 86.
161 COHEN, Julie E. What Privacy Is For, p. 17.
162 BARCELOS, Julia Rocha de. op. cit., p. 80.
163 BACHMANN, Philipp. Public relations in liquid modernity: how big data and automation cause moral blindness, p. 8.
164 O’NEIL, Cathy. **Weapons of math destruction:** how big data increases inequality and threatens democracy. New York: Crown, 2016.

Ressalte-se, no entanto, que no que tange ao caso Cambridge Analytica, restam dúvidas quanto ao verdadeiro envolvimento do Facebook e até que ponto a empresa tinha real ciência de os dados de seus usuários estarem sendo utilizados para fins de propaganda política, ou se a coleta de dados praticada pela Cambridge Analytica estava realmente em desacordo com as políticas de privacidade do Facebook naquela época[165]. Contudo, tais incertezas não eximem a rede social de qualquer responsabilidade, pois ainda é dever dela manter o controle sobre como as informações de seus usuários estão sendo tratadas e estabelecer parâmetros e limitações à sua comercialização para terceiros.

Quanto a esse ponto, é inegável que a atuação do Facebook foi insuficiente para a proteção da privacidade, em especial ao se considerar que não eram apenas os usuários que participaram do teste de personalidade do aplicativo associado "thisisyourdigitallife" que tinham seus dados coletados, mas também todos os seus amigos, que em nenhum momento consentiram especificamente com a cessão de suas informações pessoais para aquela finalidade – o que resultou na transmissão indevida de dados de mais de 87 milhões de pessoas, cifra divulgada pela própria companhia[166]. Mesmo que o Facebook tenha se comprometido a melhorar suas políticas de privacidade após o escândalo, ainda há legítimas preocupações sobre se essas promessas serão cumpridas; nas palavras de Zeynep Tufekci, Mark Zuckerberg não aparenta ter problemas em estabelecer medidas de privacidade quando estas são aptas a reduzir a responsabilidade da empresa, mas se apresenta resistente quando tais medidas tenham o potencial de reduzir os lucros advindos das propagandas de terceiros[167].

Toda essa exposição se voltou a demonstrar algumas das maneiras como a má utilização dos sistemas de *Big Data* pode ser pervasiva e causar danos aos direitos fundamentais de cada cidadão. Como analisado, o crescimento vertiginoso e a sofisticação das técnicas de mineração de dados promovem a violação da privacidade, na medida em que os dados pessoais são coletados, tratados e

---

165 BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento**, p. 115-116.
166 FACEBOOK. **An update on our plans to restrict data access on Facebook.** 4 abr. 2018. Disponível em: <https://about.fb.com/news/2018/04/restricting-data-access/> Acesso em: 12 abr. 2020.
167 TUFEKCI, Zeynep. Zuckerberg's so-called shift towards privacy. **The New York Times**, New York, 7 mar. 2019. Disponível em: <https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html> Acesso em: 12 abr. 2020.

comercializados indiscriminadamente, promovendo uma vigilância difusa e constante no cotidiano. Para além da privacidade, todavia, há igualmente uma violação da liberdade individual, pois a mineração de dados em patamares tão extensos torna as empresas capazes de inferir dos particulares o seu estado emocional, suas fraquezas, vulnerabilidades e desejos, e explorá-los conforme lhes forem mais convenientes para promover produtos e serviços[168].

Para Julie Cohen, a diminuição da liberdade não ocorre apesar da diminuição da privacidade, mas em decorrência dela. A pervasividade dos sistemas de vigilância promove a redução da privacidade, a partir da mitigação da capacidade de autodeterminação do indivíduo[169]; com isso, ele deixa de ser sujeito e se torna simples objeto da relação informacional[170], pois sua liberdade de escolha é comprometida por fatores externos que muitas vezes passam despercebidos. Assim, sua autonomia individual é minada, eis que esses elementos externos podem levá-lo a atuar em prol de fins que não necessariamente escolheu, por razões que não são autenticamente suas próprias[171]. Com o escândalo Cambridge Analytica, torna-se claro que a discussão sobre a utilização das tecnologias como forma de manipulação não se restringe mais apenas à proteção da esfera individual – mas também pode assumir aspectos políticos que coloquem em risco o próprio conceito de democracia.

---

[168] SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy and manipulation, p. 2.
[169] COHEN, Julie E. What Privacy is For, p. 7.
[170] COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review,** Stanford, v. 52, n. 5, p. 1373-1438, maio 2000. Disponível em: <http://www.jstor.org/stable/1229517> Acesso em: 13 abr. 2020.
[171] SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. op. cit., p. 9.

3 A MULTIFUNCIONALIDADE DO DIREITO À PRIVACIDADE

3.1 ASPECTOS GERAIS DA TEORIA DA MULTIFUNCIONALIDADE DOS DIREITOS FUNDAMENTAIS

Tendo sido observados o desenvolvimento histórico do direito à privacidade – desde a concepção clássica do *right to privacy* até a intrínseca relação atual dentre a privacidade e a proteção da dignidade da pessoa humana no meio digital – e os novos desafios proporcionados pelos sistemas de *Big Data* para a proteção dos dados pessoais, verifica-se que o direito à privacidade possui um caráter complexo, cuja proteção não consegue ser efetivada somente pela imposição de um dever geral de abstenção ao Estado e aos particulares.

O reconhecimento de tal complexidade é imprescindível para a devida tutela do direito, pois ela somente é possível com a proteção de todas as posições jurídicas pelas quais a privacidade se espraia. Contudo, antes de se adentrar na análise específica das diferentes dimensões que compõem o direito à privacidade, necessário compreender que esta pluralidade de dimensões é característica comum de todos os direitos fundamentais, em decorrência de sua multifuncionalidade.

Tradicionalmente, contudo, os direitos fundamentais não eram explorados conforme a sua multifuncionalidade, preferindo a doutrina constitucionalista separá-los em três gerações distintas, o que foi brevemente mencionado no primeiro capítulo deste trabalho (ponto 1.2). De maneira a facilitar a análise histórica dos direitos fundamentais, eles são classificados, portanto, em três grupos estanques[172]: a) a *primeira geração* abrange os direitos decorrentes do liberalismo iluminista a partir do século XVIII, ou seja, as liberdades individuais, que estabelecem ao Poder Público o dever de não interferir na esfera jurídica dos cidadãos; b) a *segunda geração*, referente aos direitos sociais surgidos com o Estado Social de Direito a partir do século XX, que obrigam o Estado a realizar ações positivas de intervenção (em prol, por exemplo, do direito à saúde, à assistência social, à educação, entre outros); e c) a *terceira geração*, relativa aos direitos de titularidade difusa e coletiva a partir do último quarto do século XX, que tutelam bens jurídicos indivisíveis, tais

[172] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 619-620.

como a proteção do meio ambiente ecologicamente equilibrado e a conservação do patrimônio histórico e cultural.

Apesar da qualidade didática desta classificação, ela acaba por ser reducionista e prejudicial à devida compreensão dos direitos fundamentais em toda sua complexidade, uma vez que induz à conclusão – errônea – de que a tutela dos direitos de liberdade se limita à simples abstenção do ente estatal e que a titularidade transindividual é inerente apenas aos ditos direitos de terceira geração, quando na realidade *todos* os direitos fundamentais apresentam características de todas as três gerações[173]. Ademais, o reducionismo das gerações de direitos também leva a uma "sobrevalorização da força jurídico-imperativa dos direitos integrantes da assim chamada 'primeira geração'"[174], pois apenas esses poderiam ser verdadeiramente considerados como direitos subjetivos. Ou seja, apenas os direitos de liberdade teriam aplicabilidade imediata, pois a sua efetivação poderia ser integralmente realizada mediante uma simples determinação judicial de não fazer ao ente público, sem necessitar de regulamentação infraconstitucional ou infralegal ou mesmo qualquer atuação positiva estatal. Por sua vez, os direitos sociais e os direitos de titularidade transindividuais careceriam de aplicabilidade imediata, pois a sua satisfação demandaria tanto regulamentação específica como disponibilidade orçamentária[175].

A análise realizada nos prévios capítulos demonstra que tal argumento não se sustenta, uma vez que a integral proteção do direito à privacidade – classicamente inserida dentro do rol de direitos de primeira geração, surgida num contexto liberal-burguês oitocentista – não pode se resumir à simples determinação de um dever negativo de abstenção, pois a concepção da privacidade como o direito de ser deixado a sós há muito se encontra superada. A profunda relação existente entre privacidade, proteção de dados e as novas tecnologias de informação demonstram a imprescindibilidade de determinação conjunta de deveres negativos e de deveres de prestação. Note-se que isso não é uma peculiaridade do direito à

---

[173] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 621.
[174] HACHEM, Daniel Wunder. São os direitos sociais "direitos públicos subjetivos"? **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito**, São Leopoldo, v. 11, n. 3, p. 404-436, dez. 2019. Disponível em: <https://dx.doi.org/10.4013/rechtd.2019.113.08>. Acesso em: 27 maio 2020.
[175] Ibid., p. 409.

privacidade, mas elemento característico de todos os direitos fundamentais. É preciso, portanto, observar aquilo que Robert Alexy denomina como direitos fundamentais “completos”, reconhecendo que um único direito fundamental abrange um feixe de posições jurídicas distintas, abarcando simultaneamente direitos de defesa e direitos a prestações, que vão desde prestações normativas até prestações no mundo fático[176].

Assim, sustentar a multifuncionalidade dos direitos fundamentais significa reconhecer que esses direitos se revelam em diversas pretensões jurídicas jusfundamentais, e, consequentemente, apresentam múltiplas funções. A doutrina varia em relação à definição e à quantidade específica das funções exercidas pelos direitos fundamentais[177], de modo que, para os fins deste trabalho, adotar-se-á a classificação empregada por Daniel Wunder Hachem, que sustenta que as posições jurídicas jusfundamentais se revelam nas seguintes dimensões: a) de *defesa*, ou seja, impondo um dever de abstenção ao Poder Público; e b) de *prestação*, que determina uma atuação estatal positiva em prol do direito fundamental. Este dever de prestação ainda se subdivide em: i) *prestação fática* (ou *material*), por meio da qual a atuação estatal se dá no plano concreto, e ii) *prestação normativa*, mediante a criação de normas de *proteção* do bem jurídico para protegê-lo de investidas de outros particulares, bem como pela criação de estruturas de *organização e procedimentos* que auxiliem na promoção do direito fundamental[178].

Nesse contexto, o direito fundamental em um sentido amplo abrange um conjunto de pretensões jurídicas diversas, tanto de defesa como de prestações positivas, sendo que cada uma dessas posições jusfundamentais também pode ser isoladamente chamada de direito fundamental, em acepção estrita[179]. A pluralidade de posições jurídicas inerentes a cada direito fundamental *lato sensu* faz com que não seja possível afirmar se esse direito se trata de um direito subjetivo ou se a sua aplicabilidade é imediata, sendo necessário analisar de qual direito fundamental *strictu sensu* está se falando. Enquanto determinadas pretensões jusfundamentais

---

[176] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 443.
[177] Ingo Sarlet aponta, por exemplo, que Albert Bleckmann sustentou a multifuncionalidade dos direitos fundamentais em uma classificação que abrange doze diferentes funções. SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2009, p. 156.
[178] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 628.
[179] Ibid., p. 629.

podem ser postuladas individualmente em juízo, outras podem requerer a utilização de mecanismos de tutela coletiva[180]; enquanto algumas posições possuem uma aplicabilidade imediata facilmente evidenciada, outras requerem instrumentos infraconstitucionais para serem instituídas.

Para além disso, essa pluralidade de posições jurídicas faz com que os direitos fundamentais apresentem uma dupla dimensão: a) *subjetiva*, pois investe o titular do direito na prerrogativa de exigir sua proteção, bem como autoriza sua exigibilidade judicial na hipótese de descumprimento; e b) *objetiva*, na medida em que estabelece ao Estado deveres objetivos gerais de tutela desses direitos, independentes de prévia postulação judicial e voltados a favor de todos os cidadãos, por todo o ordenamento jurídico. Desta maneira, a eficácia dos direitos fundamentais não pode ser valorada exclusivamente a partir de uma perspectiva individualista, "mas também sob o ponto de vista da sociedade, da comunidade na sua totalidade, já que se cuida de valores e fins que esta deve respeitar e concretizar"[181]. Portanto, a tentativa de definir os direitos fundamentais apenas enquanto direitos subjetivos é uma visão reducionista fadada ao fracasso, que ignora que os direitos fundamentais se tratam de uma "categoria jurídica própria"[182] apta a agregar distintas dimensões de proteção, sem que haja contradição lógica entre elas.

Estabelecidas as bases teóricas que fundamentam a multifuncionalidade dos direitos fundamentais, cabe analisar, agora, como o direito à privacidade se manifesta dentro de tal arquitetura, e como a sua efetiva proteção requer que a tutela ocorra em todas as suas posições jusfundamentais – tanto na esfera de defesa como nas esferas prestacionais normativa e fática.

3.2 AS LEGISLAÇÕES DE PROTEÇÃO DE DADOS ENQUANTO PRESTAÇÃO NORMATIVA ESTATAL

Dentro da teoria da multifuncionalidade dos direitos fundamentais, uma das pretensões que compõem o feixe de posições jurídicas jusfundamentais se refere à dimensão prestacional do Estado, ou seja, que demanda uma atuação estatal

---

[180] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 629.
[181] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**, p. 145.
[182] HACHEM, Daniel Wunder, op. cit., p. 632.

positiva em prol do bem jurídico. Como observado anteriormente, a dimensão prestacional comporta tanto deveres de prestação no mundo *fático* como em âmbito *normativo*, sendo que este ainda se subdivide nos direitos de *proteção* e de *organização e de procedimento*. Este item buscará, portanto, realizar uma análise da tutela do direito à privacidade a partir da dimensão da prestação normativa.

Afirmar que o Estado tem um dever de prestação normativa significa, nesse sentido, que cumpre ao Poder Público o papel de tutelar os direitos fundamentais mediante a criação de normas[183], que podem ser voltadas especificamente à proteção do direito contra a interferência de particulares (função de proteção) ou para a "criação de órgãos, instituições e procedimentos que viabilizem de forma universalizada o desempenho das demais funções"[184] (função de organização e de procedimento).

No que tange ao direito à privacidade, a importância da dimensão de prestação normativa foi reconhecida em outros ordenamentos jurídicos logo na segunda metade do século XX, conforme a relação entre a privacidade e a proteção de dados pessoais começava a se aprofundar. Esse reconhecimento incorreu no surgimento das primeiras leis de proteção de dados pessoais, que eventualmente seriam conhecidas como a "primeira geração" de legislações, a qual inclui a lei do *Land* alemão de Hesse (1970), a lei de proteção de dados sueca (1973) e o *Privacy Act* estadunidense (1974), cujo enfoque era a regulamentação dos bancos de dados estatais. Nos anos seguintes, com a descentralização e a proliferação dos centros de processamento de dados, não tardou a chegada da segunda geração de leis, que teve como modelo a lei francesa de 1978, mas ainda baseada numa concepção da privacidade enquanto liberdade negativa[185].

A evolução das tecnologias de informação no decorrer das décadas demonstrou a necessidade de evolução também dos dispositivos normativos sobre proteção de dados, de tal forma que Danilo Doneda aponta que atualmente é possível constatar, ainda, a existência de uma terceira e de uma quarta gerações legislativas[186], tendo ambas reconhecido novas camadas de complexidade inerentes à proteção da privacidade, além de associá-la à ideia de autodeterminação

---

[183] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 202.
[184] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 628.
[185] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 177.
[186] Ibid., p. 178-179.

informativa e reconhecer a posição de vulnerabilidade do usuário dentro da relação informacional.

Portanto, em comparação com outros países, que possuem dispositivos legais sobre a proteção de dados desde as décadas de 1970 e 1980, observa-se que a discussão normativa brasileira acerca do tema ainda está em seus estágios iniciais, tendo em vista que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) foi promulgada apenas em 2018, na esteira da consolidação do *General Data Protection Regulation* da União Europeia em 2016. Mencionou-se no primeiro capítulo (ponto 1.1) que, antes da nova lei, havia disposições infraconstitucionais esparsas sobre a privacidade e a proteção de dados, que, contudo, eram insuficientes para regular o tratamento de dados e a privacidade sob um sistema uniformizado. Isso significa que o debate sobre a proteção de dados no Brasil ainda tem um longo caminho a percorrer, em especial ao se considerar o grau de insegurança jurídica que assola a própria data de entrada em vigor da lei[187]. No final das contas, quem se beneficia de tal insegurança jurídica são os próprios agentes que vêm protelando a adoção de políticas de *compliance,* prejudicando aqueles que buscaram providenciar medidas de adequação à lei desde o início.

No entanto, as críticas às formas como os entes políticos têm obstaculizado a implementação da Lei Geral de Proteção de Dados não exclui a sua importância para o ordenamento jurídico brasileiro, que há décadas necessitava de regulação específica sobre o tema, uma vez que é ela que tem o condão de cumprir a pretensão jusfundamental de uma prestação estatal normativa, tanto na dimensão do direito à proteção como na de organização e procedimento.

O texto legal explicitamente adota normas voltadas ao cumprimento da posição jurídica jusfundamental prestacional de *proteção* da privacidade e dos dados pessoais, destinadas a proteger o titular dos direitos contra intervenções de terceiros

---

[187] A redação original da Lei Geral de Proteção de Dados previa sua entrada em vigor no mês de janeiro de 2020, o que foi adiado para agosto de 2020 pela Lei nº 13.853/2019, decorrente da Medida Provisória nº 869/18. Em outubro de 2019, o deputado federal Carlos Bezerra (MDB-MT) apresentou o Projeto de Lei nº 5.762/2019, que prorroga a *vacatio legis* da LGPD até agosto de 2022, projeto este que até o presente momento ainda está em tramitação na Câmara dos Deputados. Em abril de 2020, por força da crise provocada pela pandemia do coronavírus (Covid-19), foi editada a Medida Provisória nº 959/20, estendendo a *vacatio legis* até maio de 2021. Contudo, no mês seguinte, também em decorrência da pandemia, o Senado aprovou o Projeto de Lei nº 1.179/2020, retornando a data de vigência para agosto de 2020, ao passo em que os dispositivos relativos às sanções dos agentes de tratamentos de dados só entrarão em vigor em agosto de 2021. Caso a MP 959/20 venha a ser convertida em lei, prevalecerá a data de maio de 2021; contudo, caso caduque, prevalecerá a data de agosto de 2020.

e de outros particulares. Isso ocorre na medida em que a Lei nº 13.709/2018 não estabelece apenas uma base principiológica e axiológica para a proteção de dados, como também institui deveres tanto ao Estado como a entes privados, quando realizem operações de tratamento de dados pessoais em território brasileiro ou relativos a titulares localizados em território nacional[188]. Ainda, o descumprimento dos preceitos legais pode incorrer na aplicação de sanções administrativas aos agentes de tratamento, nos termos do art. 52 ao art. 54, sem prejuízo da aplicação do instituto da responsabilidade civil quando constatado o dano em relação ao titular dos dados, conforme disposto pelo art. 42 ao art. 45.

Desta maneira, a proteção normativa do direito à privacidade e à proteção de dados não se limita à relação entre indivíduo e Estado, mas igualmente busca proteger as situações entre particulares, demarcando "as esferas dos sujeitos de direito de mesma hierarquia, bem como a exigibilidade e a realização dessa demarcação"[189]. Torna-se possível observar, nesse caso, a denominada eficácia horizontal dos direitos fundamentais, ou seja, o fato de que as normas de direitos fundamentais incidem sobre as relações privadas, mesmo quando *a priori* se tratem de um direito dirigido de maneira imediata ao Estado[190]. Isso ocorre por força do efeito de irradiação dessas normas sobre todo o ordenamento jurídico[191], uma vez que, como explorado pela teoria da multifuncionalidade, os direitos fundamentais se desdobram tanto em posições subjetivas que permitem a sua exigibilidade judicial, como em valores objetivos de proteção que devem ser respeitados pelo ente estatal e por todos os cidadãos.

Para além do dever de proteção contra ingerências de terceiros, a dimensão da prestação normativa também impõe ao Estado o dever de estabelecer *organizações e procedimentos* voltados justamente a facilitar a concretização do direito fundamental. É incumbência do Poder Público, portanto, fornecer as condições jurídicas e materiais necessárias para a efetivação dos direitos

---

[188] Art. 3º: Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
[189] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 451.
[190] HACHEM, Daniel Wunder. São os direitos sociais "direitos públicos subjetivos"?, p. 419.
[191] ALEXY, Robert, op. cit., p. 524-525.

fundamentais, a partir da formatação de “estruturas organizativas e mecanismos procedimentais que possibilitem o seu adequado exercício para todos os seus titulares, independentemente de provocação”[192]. A relação existente entre direitos fundamentais e o dever de organizações e procedimentos é mútua, uma vez que, ao mesmo tempo em que os direitos fundamentais dependem da organização e do procedimento para que sejam devidamente exercidos, esses próprios mecanismos devem ser estabelecidos de acordo com as normas de direitos fundamentais, utilizando-as como parâmetro para a construção das estruturas organizacionais e como diretrizes para a aplicação das normas procedimentais[193].

Danilo Doneda pontua que o instrumento mais adotado pelas legislações de proteção de dados no que tange às estruturas de organização e de procedimento é a previsão normativa de uma autoridade administrativa independente (a *Data Protection Authority*, ou DPA), que atue em prol da proteção dos usuários, uma vez que a rápida evolução das tecnologias de informação – como a proliferação do *Big Data* e a sofisticação das técnicas de mineração de dados – dificulta a possibilidade de o cidadão, sozinho, conseguir acompanhar de forma eficaz como seus dados estão sendo coletados e tratados por pessoas jurídicas de direito público e de direito privado[194].

Além disso, o estabelecimento de uma autoridade reguladora é apto a promover “a busca de eficiência, a redução de custos para o Estado, a estabilização dos mercados e a especialização dos órgãos decisionais do Estado”[195], bem como garante maior segurança jurídica e uniformidade na aplicação da legislação, eis que a centralização ao redor de uma autoridade “evita o risco da fragmentação da interpretação da lei entre tribunais e mesmo outros órgãos administrativos com competências eventualmente concorrentes”[196], o que permite que a tutela da privacidade e da proteção de dados ocorra de maneira mais eficiente.

Na Lei Geral de Proteção de Dados, a preocupação com a previsão de uma autoridade administrativa específica levou à criação da Autoridade Nacional de Proteção de Dados (ANPD), prevista pelo art. 55-A como órgão da administração pública federal integrante da Presidência da República, depois do veto da redação

---

[192] HACHEM, Daniel Wunder. São os direitos sociais “direitos públicos subjetivos”?, p. 420.
[193] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**, p. 194.
[194] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 308.
[195] Ibid., p. 312.
[196] Ibid., p. 315.

original, a qual inicialmente previa a Autoridade enquanto autarquia especial vinculada ao Ministério da Justiça. Enquanto manifestação da posição fundamental prestacional normativa de organização e procedimento, a ANPD se volta à regulamentação específica de determinados dispositivos gerais estabelecidos pela Lei nº 13.709/2018 – tais como, por exemplo, os acordos contratuais para transferência internacional de dados pessoais e o dever dos agentes de tratamento de notificar eventuais vazamentos de dados[197].

Cabe ainda à Autoridade a publicação de orientações técnicas para que os agentes públicos e privados se adequem à LGPD, a fiscalização e a aplicação de sanções administrativas nas situações de descumprimento do texto legal, dentre outras atribuições[198]. Para tanto, torna-se imprescindível que a atuação da Autoridade se dê a partir de um diálogo constante com os setores sociais diretamente afetados, bem como que a composição do Conselho Diretor seja multidisciplinar[199], ante a complexidade e a especificidade dos temas relacionados ao desenvolvimento tecnológico, cuja rápida mutação "exige tecnicidade, atualização constante, conhecimento de ponta e garantia de atuação independente"[200].

Para que a implementação de uma autoridade reguladora efetivamente sirva ao fortalecimento e à consolidação de uma cultura de proteção da privacidade e dos dados pessoais, imperioso que ela seja dotada de independência e autonomia funcional, financeira e administrativa, de modo a "isolar sua atuação da influência dos poderes estatais constituídos na administração pública direta"[201].

É apenas com a autonomia que é possível garantir que as atividades da autoridade sejam conduzidas em prol dos direitos fundamentais, impedindo que ela se sujeite a eventuais interferências políticas que venham a ser contrárias à fiscalização dos agentes de tratamento de dados. Considerando que há diversas situações concretas em que o Poder Público pode ter interesse em coletar os dados pessoais dos cidadãos como forma de tornar a atuação estatal mais eficiente, a

---

197 GUTIERREZ, Andriei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.). op. cit., p. 387-402.
198 Ibid., p. 398.
199 Ibid., p. 396.
200 VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). op. cit., p. 717-739.
201 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, p. 314.

ausência de um grau substantivo de independência pode levar o Estado a se aproveitar de sua influência sobre a autoridade reguladora "para beneficiar a implementação ou execução de serviços públicos e políticas públicas do Poder Executivo"[202] em detrimento da privacidade e da proteção de dados.

Contudo, ao se analisar a Autoridade Nacional de Proteção de Dados da forma como foi instituída pela Lei nº 13.709/2018, percebe-se que não foi conferida a ela o grau de independência e de autonomia necessária para a devida proteção dos direitos fundamentais dos usuários que têm seus dados coletados, uma vez que ela foi criada enquanto órgão da administração direta integrante da Presidência da República, sendo que os membros do Conselho Diretor e do Conselho Nacional de Proteção dos Dados Pessoais e da Privacidade deverão ser nomeados por ato do Presidente da República[203].

Cabe observar que a redação original da Lei Geral de Proteção de Dados previa a Autoridade enquanto integrante da administração pública indireta, tratando-se de autarquia especial vinculada ao Ministério da Justiça, a qual foi vetada pelo então Presidente Michel Temer por inconstitucionalidade formal por vício de iniciativa[204]. A ANPD veio a ser criada posteriormente por meio da Medida Provisória nº 869/2018, com a atual redação, convertida em lei pela Lei nº 13.853/2019. Como forma de dirimir o problema, inseriu-se também o art. 55-B, que prevê "autonomia técnica e decisória à ANPD", o qual, contudo, não é capaz de assegurar de maneira isolada o grau de independência necessário para uma atuação efetivamente voltada à proteção de dados e da privacidade, na medida em que "mero enunciado normativo de autonomia técnica não afasta as exigências fáticas que caracterizam uma entidade de fato autônoma"[205].

---

[202] GUTIERREZ, Andriei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, p. 399.

[203] Art. 55-D: O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente.

§1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5.

Art. 58-A: O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (…)

§1º Os representantes serão designados por ato do Presidente da República, permitida a delegação.

[204] VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados, p. 728.

[205] Ibid., p. 731.

Enquanto persistir a possibilidade de o Poder Público se utilizar de influência política sobre a Autoridade Nacional de Proteção de Dados para afrouxar seus deveres legais e reduzir seu grau de *accountability*, estabelecendo tratamentos distintos entre a coleta de dados realizada por pessoas jurídicas de direito público e a realizada pelas pessoas de direito privado[206], a devida tutela dos direitos fundamentais dos cidadãos necessariamente se encontrará em posição de vulnerabilidade.

3.3 O DIREITO À PRIVACIDADE NAS DIMENSÕES DE PRESTAÇÃO FÁTICA E DE DEFESA

Retornando à teoria da multifuncionalidade dos direitos fundamentais, observou-se que a pretensão jusfundamental de prestação se trata de uma obrigação positiva imposta ao Estado, que pode se desdobrar tanto no dever de prestação normativa – que se subdivide nas esferas de proteção e de organização e de procedimento –, como no dever de prestação fática, também conhecido como deveres a prestação em sentido estrito (em oposição às prestações em sentido amplo, que são as prestações normativas).

Afirmar que o Poder Público tem o dever de realizar prestações fáticas significa que a ele incumbe o dever de garantir *materialmente* as condições necessárias para que o direito fundamental possa ser fruído por seus titulares, sendo que, a princípio, essas prestações também poderiam ser realizadas por particulares, caso o indivíduo "dispusesse de meios financeiros suficientes e se houvesse uma oferta suficiente no mercado"[207]. Além disso, a dupla dimensão relativa à estrutura dos direitos fundamentais – em suas perspectivas subjetiva e objetiva – faz com que o eventual descumprimento do dever *objetivo* por parte do Estado possibilite ao cidadão pleitear individualmente a tutela de seu direito, em sua posição *subjetiva*; afinal, "o titular do direito fundamental tem um direito a uma ação estatal, que é imprescindível para a proteção de sua esfera de liberdade constitucionalmente protegida"[208].

---

[206] VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados, p. 733.
[207] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 499.
[208] Ibid., p. 250.

Na medida em que tais prestações são concretas e voltadas à realidade fática, há uma pluralidade de instrumentos que podem ser utilizados para garanti-las, o que, portanto, torna irrelevante a forma jurídica a ser adotada para a satisfação do direito (elemento este que é justamente o critério de distinção entre os direitos a ações positivas fáticas e as ações positivas normativas, conforme Robert Alexy[209]). Não havendo previsão legal expressa acerca de procedimentos e mecanismos específicos que devem ser utilizados pelo Estado, as diferentes maneiras como podem ser cumpridos os deveres de prestação material recaem dentro da esfera de discricionariedade da Administração Pública[210]. De tal maneira, seria impossível tentar estabelecer um rol exaustivo de prestações fáticas no âmbito da proteção do direito à privacidade e da proteção de dados, portanto, cabendo ao escopo deste trabalho apenas citar alguns exemplos.

Observando-se o texto da Lei Geral de Proteção de Dados, é possível verificar deveres gerais estabelecidos pelo legislador em relação aos controladores de dados que podem se traduzir no âmbito das prestações fáticas. O art. 18, por exemplo, elenca o direito dos titulares dos dados de obter dos agentes de tratamento uma variedade de práticas, como o acesso aos dados pessoais, a sua correção, anonimização, bloqueio, eliminação, o fornecimento de informações e até mesmo a revogação do consentimento – que impede a continuidade da coleta e do tratamento dos dados do usuário –, entre outras medidas. Nas situações em que seja o Poder Público a realizar a coleta dos dados pessoais, atender aos pedidos dos usuários nos termos do art. 18 se trata de uma prestação material, cujo eventual descumprimento pode levar à aplicação do instituto da responsabilidade civil, nos termos do art. 42[211].

Outrossim, todo o capítulo IV da legislação é destinado à regulação do tratamento de dados pessoais realizado pelas pessoas jurídicas de direito público, sem prejuízo da aplicação de outros textos legais que tratem de direitos dos

---

[209] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 202.

[210] Importante observar que a discricionariedade não se refere à proteção ou à ausência de proteção do direito fundamental, mas às maneiras concretas relacionadas a como ele será protegido. Não pode o ente estatal arguir a cláusula da reserva do possível, por exemplo, para se escusar de tutelar o direito fundamental, mas apenas em relação a como pode instituir diferentes políticas públicas voltadas à sua proteção. Nesse sentido: HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 653.

[211] Art. 42: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

cidadãos concernentes à relação informacional entre o indivíduo e o Estado, tais como a Lei de Acesso à Informação, a Lei do *Habeas Data* e o Marco Civil da Internet – leis que, por si só, também estabelecem deveres de prestação normativa e fática ao Poder Público. Da leitura da Lei Geral de Proteção de Dados extrai-se que diversos dispositivos efetivamente requerem a instalação da Autoridade Nacional para tornar factível a proteção material do direito à privacidade e dos dados pessoais, o que demonstra haver uma profunda interdependência entre as posições jusfundamentais de prestações normativas e fáticas para garantir a tutela dos direitos fundamentais em sua integralidade. Isso porque não há como viabilizar a realização de prestações positivas fáticas sem que haja uma estrutura normativa organizacional e procedimental apta a sustentá-las, ao mesmo tempo em que não há sentido em estabelecer mecanismos de organização e de procedimento se estes não venham a ser utilizados como sustentáculos para a tutela do direito em plano material.

Tal interdependência[212] não se limita às categorias de prestação positiva estatais, mas abarca todo o feixe de pretensões jurídicas jusfundamentais que compõem o direito fundamental como um todo, desde os direitos a ações prestacionais normativas e fáticas até os direitos de defesa. Desta maneira, ao mesmo tempo em que há situações em que o Estado deve efetivar ações positivas em prol da concretização dos direitos fundamentais, há outras hipóteses em que a tutela se dá justamente a partir de sua abstenção, impondo-lhe o dever negativo de não interferir no âmbito de autonomia pessoal dos indivíduos. Aponta Ingo Sarlet que a existência de uma dimensão de defesa não significa a completa exclusão da atuação estatal de qualquer ingerência realizada sobre a esfera privada dos cidadãos, mas apenas a proibição de intromissões do Poder Público que estejam em desconformidade com a Constituição. Reconhecer o direito à ação negativa estatal implica, portanto, “a formalização e limitação de sua intervenção, no sentido de uma vinculação da ingerência por parte dos poderes públicos a determinadas condições e pressupostos de natureza material e procedimental”[213].

Em relação ao direito à privacidade, não há nenhuma novidade no reconhecimento de um dever de abstenção por parte do Estado e de outros

---

[212] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**, p. 203.
[213] Ibid., p. 168.

particulares, pois esta é justamente a base sobre a qual o *right to privacy* clássico se estruturou. Ele é tradicionalmente inserido dentro do rol de direitos de liberdade típicos da primeira geração de direitos fundamentais, na medida em que o indivíduo tem a liberdade de ficar a sós quando bem entender, bem como a prerrogativa de não ser incomodado por terceiros e não ter revelados publicamente os elementos de sua vida privada que deseja manter em segredo. Veja-se, por exemplo, a concepção de Tércio Sampaio Ferraz Júnior, que definiu como conteúdo da privacidade a possibilidade de "constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, as situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão"[214].

Como analisado (ponto 1.1), a visão tradicional do direito à privacidade como o *right to be let alone* foi superada ainda na segunda metade do século XX, com a sua crescente associação com as práticas de coleta de dados pessoais e as tecnologias informáticas. Contudo, o fato de o conceito de Warren e Brandeis não ser mais capaz de tutelar o direito à privacidade em sua integralidade não significa que ele deve ser completamente abandonado em prol de defendê-lo apenas em uma vertente que exige uma ação estatal positiva. Repete-se: reconhecer a multifuncionalidade do direito à privacidade implica reconhecer a multiplicidade de pretensões jurídicas que um direito fundamental completo abarca, é observar que a sua proteção efetiva requer tanto prestações positivas normativas e fáticas como a abstenção estatal, a depender da situação sendo analisada.

Imperioso reiterar que todos os direitos fundamentais em geral apresentam uma "dupla dimensão negativa (defensiva) e positiva (prestacional)"[215], pois o atual debate acerca da intrincada relação entre privacidade, proteção de dados, autodeterminação informativa e novas tecnologias de informação pode levar leitores mais desatentos a uma sobrevalorização da esfera prestacional em detrimento da dimensão de defesa, quando na realidade se tratam de posições jurídicas que são distintas, mas nunca auto-excludentes, cujas diferenças se complementam para

---

[214] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1 jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231> Acesso em: 30 maio 2020.
[215] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**, p. 207.

demonstrar a complexidade estrutural dos direitos fundamentais, tornando-os uma categoria jurídica autônoma merecedora de um tratamento especial[216].

Necessário reafirmar a existência de uma dimensão de defesa inerente ao direito à privacidade mesmo no contexto de proteção dos dados pessoais, pois os sucessivos casos de violação à privacidade de dados veiculados na mídia na última década demonstram que sequer a privacidade em seu sentido tradicional tem sido respeitada, com a ascensão da sociedade de vigilância. De fato, o desenvolvimento tecnológico recente promoveu a transição de um monitoramento panóptico – centralizado pelo Estado – para um modelo pós-panóptico que dissolveu a vigilância e espalhou-a para os entes privados, mas esse movimento de descentralização não pode nos fazer ignorar que o Estado continua sendo um poderoso agente de tratamento de dados e, portanto, passível de promover diversas violações.

Casos como o Facebook-Cambridge Analytica demonstram o protagonismo que as grandes empresas privadas assumiram na relação informacional, mas em nenhum momento afastam a responsabilidade do Poder Público de continuar respeitando a esfera de liberdade dos cidadãos ao coletar e processar dados em prol de maior eficiência na Administração Pública. A proliferação de escândalos envolvendo o setor privado não implica a diminuição da vigilância estatal, mas demonstra apenas a sofisticação dos aparatos com potencial de violação do direito à privacidade e da proteção de dados.

As denúncias de Edward Snowden quanto aos diversos programas de espionagem e de vigilância global coordenados pelo governo estadunidense em parceria com companhias de telecomunicação demonstram que a extensão do poderio governamental sobre a sociedade da informação não pode ser ignorada, especialmente quando a vigilância é fundamentada no argumento de proteção da segurança pública. Não se pretende dizer que a segurança pública seja um valor inferior que a todo custo deve ser ignorado em prol da privacidade; pelo contrário, o próprio art. 4º, inciso III da Lei Geral de Proteção de Dados aponta que a lei não se aplica ao tratamento de dados pessoais realizado para fins de segurança pública, defesa nacional e segurança do Estado. Contudo, esse dispositivo não pode ser aplicado de maneira indiscriminada com a finalidade de legitimar qualquer

---

[216] HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 624.

tratamento de dados realizado pelo ente público; há de se reconhecer que tanto o direito à privacidade quanto a segurança pública têm caráter de normas-princípios passíveis de colisão que, portanto, devem ser adequadamente sopesados nos ditames do caso concreto e aplicados na maior medida possível, por se tratarem de mandados de otimização[217].

O discurso estatal de sobrevalorização da segurança pública em detrimento dos direitos fundamentais pode se tornar mais incisivo em momentos de crise. Veja-se, por exemplo, que no mês de abril de 2020, em meio à crise de saúde pública promovida pelo coronavírus Sars-CoV-2, causador da pandemia de Covid-19, foi editada a Medida Provisória nº 954/2020, que permitiu que empresas de telecomunicação compartilhassem dados pessoais de usuários para o Instituto Brasileiro de Geografia e Estatística (IBGE) em favor da produção estatística relacionada ao controle da doença.

A eficácia do ato veio a ser suspensa por decisão liminar da Ministra Relatora Rosa Weber na ADI 6.387, uma vez que a Medida Provisória "não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude"[218], além de não esclarecer como os dados coletados serão efetivamente utilizados. Desta maneira, a problemática da MP nº 954/2020 não é o fato de o Poder Público eventualmente necessitar coletar dados pessoais de usuários de serviços de telefonia para viabilizar políticas públicas de contenção do vírus e o desestímulo de aglomerações, mas, sim, a ausência de transparência sobre como a coleta será efetivada e para quais finalidades, o que torna a previsão normativa carente de proporcionalidade e em desrespeito aos princípios norteadores da proteção de dados pessoais.

Em uma sociedade de vigilância na qual a coleta e o processamento de dados pessoais se tornam imprescindíveis para viabilizar mesmo transações comerciais básicas, as técnicas de monitoramento utilizadas pelo Poder Público e por entes privados não devem ser entendidas como fenômenos distintos, mas como duas faces da mesma moeda[219]. Nesse contexto, tentativas de estabelecer

---

[217] ALEXY, Robert. **Teoria dos Direitos Fundamentais**, p. 94-95.
[218] BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF. Decisão monocrática. Relator: Min. Rosa Weber. J. 24.04.2020, DJe 28.04.2020.
[219] RICHARDS, Neil M. The Dangers of Surveillance. **Harvard Law Review**, Cambridge, v. 126, n. 7, p. 1934-1965, maio 2013. Disponível em: <http://ssrn.com/abstract=2239412> Acesso em: 31 maio 2020.

tratamentos distintos entre eles, como se houvesse a possibilidade de afrouxar as amarras da proteção da privacidade e dos dados pessoais em favor do Estado e em prejuízo das empresas privadas, ou vice-versa, devem ser consideradas como inadmissíveis[220].

Defender uma adequada tutela do direito à privacidade na economia movida a dados não significa defender o fim da coleta de dados pessoais, pois não há nenhum grau de factibilidade em defender uma medida como essa, além de ser um posicionamento que ignora todas as vantagens que as novas tecnologias de informação proporcionam à realidade contemporânea. Significa exigir maiores níveis de *accountability* dos agentes de tratamentos de dados[221], sejam eles pessoas jurídicas de direito público ou de direito privado; é possibilitar ao usuário ter o conhecimento real das diferentes maneiras como seus dados serão utilizados e para quais finalidades eles estão sendo coletados e, nas hipóteses em que a especificação prévia das finalidades seja dificultada pelo próprio arranjo técnico do sistema (tais como no *Big Data*), que seja fortalecido ao indivíduo o acesso à informação e, acima de tudo, a transparência por parte do controlador dos dados. É reconhecer que a fundamentalidade do direito à privacidade lhe proporciona uma estrutura complexa e multifacetada, que abarca uma pluralidade de pretensões jurídicas igualmente complexas e multifacetadas, desde direitos de defesa até direitos a ações estatais positivas normativas e fáticas.

---

[220] VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados, p. 733.
[221] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais, p. 42.

CONSIDERAÇÕES FINAIS

O crescimento tecnológico exponencial que tem sido observado desde meados do século XX torna a discussão sobre a proteção do direito à privacidade mais relevante do que nunca. Se outrora a classificação do direito à privacidade como direito fundamental de primeira geração pode ter sido suficiente para garantir a sua tutela, atualmente não o é mais. Os novos desafios proporcionados pela sociedade de informação tornam necessário analisar a privacidade em todas as suas dimensões, bem como compreender a complexidade inerente à estrutura dos direitos fundamentais, demarcados por sua multifuncionalidade.

Nesse sentido, realizou-se um panorama histórico do direito à privacidade, a fim de analisar como se deu o desenvolvimento do instituto ao longo dos anos e compreender como a delimitação do seu conteúdo de proteção variou conforme o contexto histórico-social de cada época. Desta maneira, em que pese a definição da vida privada já ter surgido a partir do século XVI – com a ideia de “privado” em oposição à esfera do “público” –, a privacidade enquanto um direito propriamente dito, em sua acepção moderna, é estabelecida ao final do século XIX, por Samuel Warren e Louis Brandeis. O *right to privacy* é preceituado enquanto o direito de ser deixado a sós, de poder usufruir a vida sem ser incomodado por ingerências externas, conforme uma mentalidade tradicionalmente liberal-burguesa de proteção das elites que eram importunadas pela imprensa recém surgida.

A esfera de proteção da privacidade se transmutou logo na primeira metade do século XX, passando a se associar com a pretensão do indivíduo de ter um efetivo controle sobre as informações relativas à sua pessoa, uma vez que se intensificou a coleta de dados por entes públicos para fins de aperfeiçoamento da atividade estatal. Com o aprimoramento tecnológico nas décadas seguintes – marcado, principalmente, pelo surgimento dos computadores e da internet –, a coleta de dados pessoais se torna prática corrente também entre as entidades privadas, o que potencializa os aparatos de vigilância característicos da sociedade da informação. Nesse período, a discussão de temas como o *habeas data* e o direito ao esquecimento ganha espaço na doutrina e na jurisprudência, demonstrando que a concepção clássica da *privacy* já não é mais suficiente para garantir sua efetiva proteção.

Com o surgimento dos *smartphones*, das mídias sociais e da denominada Internet 4.0 – marcada por tecnologias disruptivas como computação em nuvem, sistemas de inteligência artificial, *machine learning* e Internet das Coisas, entre outros –, a reflexão sobre a privacidade e a proteção de dados pessoais se torna imperativa, em especial com o advento do *Big Data*, por meio do qual a coleta e o processamento de dados assumem proporções outrora inimagináveis. Movidos pelos três V's – volume, velocidade e variedade –, os sistemas de *Big Data* sofisticam a mineração de dados pessoais, inferindo padrões e extraindo deles análises preditivas que podem ser utilizadas, por exemplo, para o aperfeiçoamento de técnicas de *profiling*, por meio dos quais são traçados perfis de potenciais consumidores com base nos hábitos, gostos e preferências de cada indivíduo, sendo possível direcionar de maneira individualizada anúncios e produtos personalizados.

Vive-se, portanto, dentro de uma economia movida a dados, na qual os sistemas de vigilância são descentralizados e difusos, espalhando-se ao longo das camadas sociais sem haver um ponto de origem, motivo pelo qual se afirma que a sociedade da informação é caracterizada por ser uma vigilância líquida. Apesar dos benefícios, o processamento ampliado de dados deve ser lidado com cautela, pois, dentro de um contexto de vigilância pós-panóptica, a utilização do *Big Data* em desrespeito à ética pode perpetuar preconceitos, vieses e discriminações, bem como obliterar os direitos à privacidade e à proteção de dados pessoais. Ademais, essa nova arquitetura informativa dificulta a aplicação mesmo de princípios clássicos da proteção de dados, como os princípios da finalidade e da minimização de dados, por serem opostos à própria natureza operacional do *Big Data*, o qual se baseia na maximização de dados e na descoberta de novos padrões de utilização desses dados apenas após o seu processamento.

Mesmo a ideia de consentimento livre, informado e inequívoco encontra empecilhos para ser efetivamente caracterizado, eis que análises comportamentais demonstram que o indivíduo tende a ignorar riscos à privacidade nas situações em que o fornecimento de dados pessoais lhe proporciona um benefício imediato. É o denominado paradoxo da privacidade: se por um lado o indivíduo apresenta preocupações abstratas com a proteção do direito, tal preocupação muitas vezes não é traduzida na prática concreta. Com isso, não é possível considerar como manifestação válida de consentimento aquela em que o usuário é levado a clicar em

opções pré-validadas (“li e aceito os termos de serviço”) como condição de acesso ao produto ou serviço desejado.

Analisou-se, ainda, uma manifestação concreta das ameaças atuais à proteção da privacidade e dos dados pessoais, traduzida no emblemático caso envolvendo a empresa de *data mining* Cambridge Analytica, que culminou no compartilhamento indevido de dados de mais de 87 milhões de usuários da rede social Facebook. Este caso chama particular atenção não apenas pelo tamanho da brecha, mas principalmente pela sofisticação das técnicas de *profiling* empregadas, as quais se traduziam no microdirecionamento de propagandas políticas para usuários com o intuito de favorecer campanhas políticas, desde a votação do Brexit até campanhas presidenciais nos Estados Unidos. Trata-se de um caso exemplar na demonstração do poderio dos algoritmos, que afeta não apenas o direito à privacidade, mas também a liberdade, a autodeterminação individual e o próprio conceito de democracia.

A complexidade de todas essas novas situações demonstra que uma tutela efetiva da privacidade é igualmente complexa. Sendo reconhecida a insuficiência da concepção oitocentista do *right to privacy*, há de se reconhecer também a insuficiência da classificação do direito à privacidade como direito fundamental de primeira geração, que determina ao Poder Público somente um dever negativo de abstenção. Nesse contexto, adotou-se a teoria da multifuncionalidade dos direitos fundamentais para evidenciar que a privacidade possui múltiplas facetas e, portanto, requer múltiplos instrumentos de tutela. A fundamentalidade do direito à privacidade o desdobra em diversas posições jurídicas jusfundamentais, abarcando tanto um direito de defesa como deveres de prestações normativas (de proteção e de organização e procedimento) e fáticas.

A esfera de prestação normativa é evidenciada pelas leis de proteção de dados, o que se verifica no Brasil com a Lei Geral de Proteção de Dados (Lei 13.709/2018). Há, no texto legal, mecanismos de proteção, voltados à proteção do titular de dados contra intervenções de outros particulares, bem como mecanismos de organização e procedimento, em especial pela previsão da Autoridade Nacional de Proteção de Dados. No entanto, o nível de autonomia técnica e funcional da Autoridade prevista na legislação é insuficiente para garantir uma devida proteção dos dados pessoais, haja vista estar prevista enquanto órgão integrante da

Presidência da República e, portanto, se encontrar mais vulnerável a eventuais pressões políticas que visem eximir a responsabilidade do Poder Público quanto à coleta de dados.

Profundamente relacionada com as prestações normativas está a esfera de prestações fáticas. Nesse sentido, cabe ao Estado garantir materialmente a possibilidade de fruição do direito à privacidade pelos cidadãos, sendo que o descumprimento de deveres objetivos pela Administração Pública pode gerar ao indivíduo a posição subjetiva de pleitear individualmente a tutela do direito. Por fim, igualmente importante reconhecer que a superação histórica do conceito oitocentista do direito à privacidade não significa que a esfera negativa de abstenção não mais exista. Pelo contrário, ela ainda assume posição de extrema relevância na tutela contemporânea da privacidade, o que parece ser esquecido pelos entes públicos e privados, haja vista os diversos casos de violação de dados e de vigilância abusiva reportados continuamente. Ou seja, sequer a concepção clássica do direito à privacidade tem sido respeitada na prática.

Reitera-se: reconhecer os desafios proporcionados pelas novas tecnologias de informação não significa, necessariamente, uma rejeição de tais tecnologias ou uma tentativa de impedir a sua difusão. Tampouco significa defender a adoção de uma posição estatal paternalista, haja vista o risco de acentuar de maneira ainda mais contundente uma sociedade de vigilância pautada em ideais antidemocráticos. O intuito do trabalho não é condenar o desenvolvimento tecnológico contemporâneo, mas apontar que este não pode ser promovido de forma irrestrita em detrimento de direitos fundamentais garantidos pela Constituição. A proteção do direito à privacidade deve ocorrer no sentido de empoderar o sujeito – parte vulnerável na relação informacional –, mediante a promoção de mecanismos de *accountability* e de transparência, a fim de que o desenvolvimento tecnológico não ocorra em detrimento do indivíduo, mas em conformidade com a dignidade humana.

REFERÊNCIAS BIBLIOGRÁFICAS

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science,** Washington D.C., v. 347, n. 6221, p. 509-514, 30 jan. 2015. Disponível em: <https://dx.doi.org/10.1126/science.aaa1465>. Acesso em: 10 abr. 2020.

ALEXY, Robert. **Teoria dos Direitos Fundamentais.** 2. ed. São Paulo: Malheiros, 2017.

BACHMANN, Philipp. Public relations in liquid modernity: how big data and automation cause moral blindness. **Public Relations Inquiry**, v. 8., n. 3, p. 319-331, set. 2019. Disponível em: <https://dx.doi.org/10.1177/2046147X19863833> Acesso em: 6 abr. 2020.

BARCELOS, Julia Rocha de. **Big data, algoritmos e microdirecionamento:** desafios para a regulação da propaganda eleitoral. 2019, 171 f. Dissertação (Mestrado em Direito Político) – Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte (MG), 2019. Disponível em: <http://hdl.handle.net/1843/DIRS-BELHWW> Acesso em: 7 abr. 2020.

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

BERGHEL, Hal. Malice Domestic: The Cambridge Analytica Dystopia. **Computer,** Washington D.C., v. 51, n. 5, p. 84-89, maio 2018. Disponível em: <https://dx.doi.org/10.1109/MC.2018.2381135> Acesso em: 12 abr. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. E-book. Disponível em: <https://www.amazon.com.br/Prote%C3%A7%C3%A3o-Dados-Pessoais-Limites-Consentimento-ebook/dp/B08287RSNK/> Acesso em: 6 abr. 2020.

BIONI, Bruno Ricardo. **Xeque-Mate:** o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: USP-GPoPAI, 2015. Relatório técnico.

BOLDRINI, Angela; PORTINARI, Natália; BILENKY, Thais. Fichas sobre estudantes de colégio tradicional de SP vazam na internet. **Folha de S. Paulo**, São Paulo, 19 mar. 2015. Disponível em: <https://www1.folha.uol.com.br/educacao/2015/03/1604926-fichas-sobre-estudantes-de-colegio-tradicional-de-sp-vazam-na-internet.shtml> Acesso em: 13 abr. 2020.

BURROUGH, Bryan; ELLISON, Sarah; ANDREWS, Suzanna. The Snowden Saga: A shadowland of secrets and light. **Vanity Fair**, New York, 23 abr. 2014. Disponível em: <https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview> Acesso em: 10 abr. 2020.

CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. **The Guardian**, London, 7 maio 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> Acesso em: 12 abr. 2020.

CATE, Fred H.; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. **International Data Privacy Law,** Oxford, v. 3., n. 2, p. 67-73, 1 maio 2013. Disponível em: <https://doi.org/10.1093/idpl/ipt005>. Acesso em: 11 abr. 2020.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review,** Stanford, v. 52, n. 5, p. 1373-1438, maio 2000. Disponível em: <http://www.jstor.org/stable/1229517> Acesso em: 13 abr. 2020.

COHEN, Julie E. What Privacy is For. **Harvard Law Review,** Cambridge, v. 126, n. 7, p. 1904-1933, maio 2013. Disponível em: <https://ssrn.com/abstract=2175406> Acesso em: 7 abr. 2020.

CONSTINE, Josh. Facebook now has 2 billion monthly users… and responsibility. **TechCrunch**, San Francisco, 27 jun. 2017. Disponível em: <https://techcrunch.com/2017/06/27/facebook-2-billion-users/> Acesso em: 12 abr. 2020.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 85-98.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 97, p. 239-253, 2002. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67544>. Acesso em: 24 mar. 2020.

DAVIES, Harry. Ted Cruz using firm that harvested data on millions of unwitting Facebook users. **The Guardian**, London, 11 dez. 2015. Disponível em: <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> Acesso em: 12 abr. 2020.

DELEUZE, Gilles. Postscript on the Societies of Control. **October,** New York, v. 59, Winter 1992, p. 3-7, 1992. Disponível em: <https://www.jstor.org/stable/778828> Acesso em: 6 abr. 2020.

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

DURÁN MARTÍNEZ, Augusto. **Derecho a la protección de datos personales y al acceso a la información pública:** hábeas data. 2. ed. Montevideo: Amalio M. Fernandez, 2012.

FACEBOOK. **An update on our plans to restrict data access on Facebook.** 4 abr. 2018. Disponível em: <https://about.fb.com/news/2018/04/restricting-data-access/> Acesso em: 12 abr. 2020.

FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. **Folha de S. Paulo,** São Paulo, 26 jan. 2018. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml> Acesso em: 8 abr. 2020.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1 jan. 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231> Acesso em: 30 maio 2020.

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

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

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 99-129.

GIBBS, Samuel. Ashley Madison condemns attacks as experts say hacked database is real. **The Guardian**, London, 19 ago. 2015. Disponível em: <https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports> Acesso em: 8 abr. 2020.

GIBNEY, Elizabeth. The scant science behind Cambridge Analytica's controversial marketing techniques. **Nature**, London, 29 mar. 2018. Disponível em: <https://www.nature.com/articles/d41586-018-03880-4> Acesso em: 12 abr. 2020.

GLANCY, Dorothy J. The Invention of the Right to Privacy. **Arizona Law Review**, Tucson, v. 21, n. 1, p. 1-39, jan. 1979. Disponível em: <https://digitalcommons.law.scu.edu/facpubs/317/> Acesso em: 18 fev. 2020.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 219-241.

GUIMARÃES, Saulo Pereira. Vazamento de dados do Colégio Bandeirantes causa polêmica. **Exame,** São Paulo, 19 mar. 2015. Disponível em: <https://

exame.abril.com.br/tecnologia/vazamento-de-dados-do-colegio-bandeirantes-causa-polemica/> Acesso em: 13 abr. 2020.

GUTIERREZ, Andriei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 387-402.

HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais. **Revista de Direitos Fundamentais e Democracia**, Curitiba, v. 14, n. 14, p. 618-688, jul./dez. 2013.

HACHEM, Daniel Wunder. São os direitos sociais “direitos públicos subjetivos”? **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito**, São Leopoldo, v. 11, n. 3, p. 404-436, set./dez. 2019. Disponível em: <https://dx.doi.org/10.4013/rechtd.2019.113.08>. Acesso em: 27 maio 2020.

INGRAM, David. Factbox: Who is Cambridge Analytica and what did it do? **Reuters**, San Francisco, 19 mar. 2018. Disponível em: <https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F> Acesso em: 12 abr. 2020.

LAPOWSKY, Issie. What did Cambridge Analytica really do for Trump’s campaign? **Wired,** San Francisco, 26 out. 2017. Disponível em: <https://www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/> Acesso em: 12 abr. 2020.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 179-213.

MACEDO, Letícia. Vazamento de fichas de alunos gera protesto e punição no Bandeirantes. **G1,** São Paulo, 19 mar. 2015. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2015/03/vazamento-de-fichas-de-alunos-gera-protesto-e-punicao-no-bandeirantes.html> Acesso em: 13 abr. 2020.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data:** a revolution that will transform how we live, work and think. New York: Houghton Mifflin Harcourt, 2013.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. E-book. Disponível em: <https://www.amazon.com.br/Privacidade-prote%C3%A7%C3%A3o-dados-defesa-consumidor-ebook/dp/B076CL4XXW> Acesso em: 6 abr. 2020.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA,

Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 157-197.

MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709/2018). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 323-345.

NIX, Alexander. **Cambridge Analytica:** The Power of Big Data and Psychographics. Disponível em: <https://www.youtube.com/watch?v=n8Dd5aVXLCc> Acesso em: 12 abr. 2020.

NORBERG, Patricia A.; HORNE, Daniel R.; HORNE, David A. The Privacy Paradox: Personal information disclosure intentions versus behaviors. **Journal of Consumer Affairs,** New Jersey, v. 41, n. 1, p. 100-126, mar. 2007. Disponível em: <https://doi.org/10.1111/j.1745-6606.2006.00070.x> Acesso em: 10 abr. 2020.

O'NEIL, Cathy. **Weapons of math destruction:** how big data increases inequality and threatens democracy. New York: Crown, 2016.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 53-83.

PERRY, Alex. Facebook owns the 4 most downloaded apps of the decade. **Mashable**, New York, 16 dez. 2019. Disponível em: <https://mashable.com/article/facebook-most-downloaded-apps-2010s/> Acesso em: 12 abr. 2020.

RICHARDS, Neil M. The Dangers of Surveillance. **Harvard Law Review**, Cambridge, v. 126, n. 7, p. 1934-1965, maio 2013. Disponível em: <http://ssrn.com/abstract=2239412> Acesso em: 31 maio 2020.

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

RODRIGUES, Cinthia. A rede de intrigas do Colégio Bandeirantes. **CartaCapital**, São Paulo, 11 maio 2015. Disponível em: <https://www.cartacapital.com.br/educacao/a-rede-de-intrigas-do-colegio-bandeirantes/> Acesso em: 13 abr. 2020.

ROSENBERG, Matthew; CONFESSORE, Nicholas; CADWALLADR, Carole. How Trump consultants exploited the Facebook data of millions. **The New York Times,** New York, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> Acesso em: 12 abr. 2020.

RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? **International Data Privacy Law,** Oxford, v. 3, n. 2, p. 74-87, maio 2013. Disponível em: <https://doi.org/10.1093/idpl/ips036> Acesso em: 8 abr. 2020.

RUZYK, Carlos Eduardo Pianovski. **Liberdade(s) e Função:** Contribuição crítica para uma nova fundamentação da dimensão funcional do Direito Civil brasileiro. 2009. 402 f. Tese (Doutorado em Direito das Relações Sociais) - Setor de Ciências Jurídicas, Universidade Federal do Paraná, Curitiba (PR), 2009. Disponível em: <http://hdl.handle.net/1884/19174> Acesso em: 24 mar. 2020.

SALGADO, Eneida Desirée; VIOLIN, Tarso Cabral. Transparência e acesso à informação: o caminho para a garantia da ética na Administração Pública. In: BLANCHET, Luiz Alberto; HACHEM, Daniel Wunder; SANTANO, Ana Cláudia (Coord.). **Eficiência e ética na Administração Pública.** Curitiba: Íthala, 2015, p. 271-294.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 367-383.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 418-440.

STATT, Nick. Facebook's US user base declined by 15 million since 2017, according to survey. **The Verge**, New York, 6 mar. 2019. Disponível em: <https://www.theverge.com/2019/3/6/18253274/facebook-users-decline-15-million-people-united-states-privacy-scandals> Acesso em: 12 abr. 2020.

STEFIK, Mark. **The Internet Edge:** Social, technical and legal challenges for a networked world. Cambridge: The MIT Press, 2000.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy and manipulation. **Internet Policy Review**, Berlin, v. 8, n. 2, p. 1-22, 30 jun. 2019. Disponível em: <https://dx.doi.org/10.14763/2019.2.1410> Acesso em: 12 abr. 2020.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. 2. ed. São Paulo: Revista dos Tribunais, 2005.

TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and user control in the age of analytics. **Northwestern Journal of Technology and Intellectual Property,**

Chicago, v. 11, n. 5, p. 1-36, 1 nov. 2013. Disponível em: <https://ssrn.com/abstract=2149364>. Acesso em: 7 abr. 2020.

TEPEDINO, Gustavo; TEFFÉ; Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 287-322.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 601-619.

TUFEKCI, Zeynep. Zuckerberg's so-called shift towards privacy. **The New York Times**, New York, 7 mar. 2019. Disponível em: <https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html> Acesso em: 12 abr. 2020.

VAINZOF, Rony. Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 19-177.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 717-739.

VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais:** e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 385-415.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. **Harvard Law Review**, Cambridge, v. IV, n. 5, p. 193-220. 15 dez. 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> Acesso em: 18 fev. 2020.

WHITAKER, Reg. **The End of Privacy:** how total surveillance is becoming a reality. New York: The New Press, 1999.

DECISÕES E DIPLOMAS NORMATIVOS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, 12 jan. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991.** Dispõe sobre a política nacional de arquivos públicos e dá outras providências. Brasília, DF, 8 jan. 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF, 10 jun. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm> Acesso em: 21 fev. 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. Brasília, DF, 18 nov. 2011. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 21 fev. 2020.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.334.097 (2012/0144910-7)**. Recorrente: Globo Comunicações e Participações S/A. Recorrido: Jurandir Gomes de França. Relator: Min. Luis Felipe Salomão. Brasília, DF, 28 maio 2013. Diário de Justiça Eletrônico, 10 set. 2013. Disponível em: <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 21 fev. 2020.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF, 9 jul. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm> Acesso em: 31 maio 2020.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF, 17 abril 2020. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm> Acesso em: 31 maio 2020.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Interessado: Presidente da República. Relator: Min. Rosa Weber. Brasília, DF, 24 abr. 2020. Diário de Justiça Eletrônico, 28 abr. 2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> Acesso em: 31 maio 2020.