

DESAFIOS CONTEMPORÂNEOS PARA A TUTELA DOS DIREITOS À PRIVACIDADE E AOS DADOS PESSOAIS

CONTEMPORARY CHALLENGES FOR THE PROTECTION OF THE RIGHT TO PRIVACY AND PERSONAL DATA

Vitoria Hiromi Saito*

RESUMO

Inicialmente concebido como o direito de ser deixado a sós, o direito à privacidade teve seu âmbito de proteção consideravelmente expandido ao longo das últimas décadas, na medida em que passou a ter profundas relações com o desenvolvimento tecnológico e, por conseguinte, com a proteção de dados pessoais. No contexto de crescente digitalização da vida cotidiana, os dados pessoais se tornaram um dos insumos de maior importância econômica do século XXI, o que faz com que o cidadão esteja em posição de vulnerabilidade dentro da relação informacional. Desta maneira, a devida tutela da privacidade e dos dados pessoais não mais se limita ao reconhecimento de um dever de abstenção por parte de terceiros, mas requer igualmente prestações positivas por parte do Estado. Isso pode ser observado mesmo anteriormente à promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), com a discussão sobre temas como o habeas data e o direito ao esquecimento. A proliferação da internet, dos smartphones e das novas tecnologias disruptivas apenas exacerbou os desafios para a proteção dos dados pessoais, com a aceleração das técnicas de vigilância e de monitoramento dos indivíduos. Portanto, uma adequada reflexão sobre como diminuir a assimetria entre os polos da relação informacional necessariamente requer compreender que os direitos à privacidade e à proteção de dados não se encontram em um vácuo, mas possuem profundas ligações com outros direitos fundamentais, tais como a liberdade e a dignidade humana.

PALAVRAS-CHAVE

Privacidade. Proteção de dados. Lei Geral de Proteção de Dados. Direito Digital.

SUMÁRIO

Introdução. 1. Desenvolvimento histórico dos direitos à privacidade e à proteção de dados. 2. A insuficiência da concepção clássica da privacidade na era digital: habeas data e direito ao esquecimento. 3. A tutela dos dados pessoais frente à economia movida a dados. Considerações finais. Referências bibliográficas.

ABSTRACT

Originally conceived as the right to be let alone, the right to privacy has had its scope of protection considerably expanded in the last few decades, as it became increasingly related to both technological development and data protection. In the wake of the digitalization of everyday life, personal data have become one of the most important economic products of the 21st century, which puts citizens in a position of vulnerability in the informational relationship. Therefore, an adequate protection of the right to privacy and the right to personal data cannot be reduced to simply recognizing negative obligations, but equally requires the State to comply with positive obligations. This can be seen even before the emergence of Brazil's most recent data protection law (Lei nº 13.709/2018), with the discussion of themes such as habeas data and the right to be forgotten. The proliferation of the internet, smartphones and new technologies have only exacerbated the challenges of data protection, as well as the acceleration of surveillance techniques. Thus, an adequate reflection on how to diminish the asymmetry in the informational relationship makes it necessary to understand that the right to privacy and data protection are not isolated, but are instead deeply linked to other fundamental rights, such as liberty and human dignity.

KEYWORDS

Privacy. Data protection. Brazilian Data Protection Law. Digital Law.

* Graduanda em Direito pela Universidade Federal do Paraná. Pesquisadora do Núcleo de Investigações Constitucionais (NINC-UFPR). Pesquisadora voluntária do programa de Iniciação Científica 2018/2019.

REFERÊNCIA: SAITO, Vitoria Hiromi. Desafios contemporâneos para a tutela dos direitos à privacidade e aos dados pessoais. *Res Severa Verum Gaudium*, v. 5, n. 2, Porto Alegre, p. 52-79, dez. 2020.

INTRODUÇÃO

No dia 18 de setembro de 2020, entrou parcialmente em vigor no ordenamento jurídico brasileiro a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais. O período de aproximados dois anos de *vacatio legis* foi marcado por turbulências e por insegurança jurídica: inicialmente prevista para entrar em vigor em janeiro de 2020, a lei teve a data adiada para agosto de 2020 pela Lei nº 13.853/2019, decorrente da Medida Provisória nº 869/18. Em abril de 2020, em consequência da crise provocada pela pandemia do coronavírus (Covid-19), foi editada a Medida Provisória nº 959/20, a qual estendeu o período de vacância até maio de 2021. Durante o trâmite de conversão da MP nº 959/20 em lei ordinária, a Câmara dos Deputados optou por adiantar a data para 31 de dezembro de 2020; contudo, o referido dispositivo veio a ser declarado prejudicado pelo Senado – de tal maneira que a maior parte da LGPD entrou em vigor no dia de publicação da nova lei (Lei nº 14.058/2020). Por outro lado, em decorrência da Lei nº 14.010/2020, a qual também foi editada no contexto da pandemia, os dispositivos relativos às sanções previstas na LGPD (arts. 52 a 54) estão previstos para entrar em vigor apenas em agosto de 2021.

O caráter recente da lei indica que o debate sobre a proteção de dados no Brasil ainda está em fase gestacional; o processo de adequação dos agentes de tratamento de dados à legislação é complexo e requer uma abordagem multissetorial, ao passo em que uma verdadeira efetivação dos dispositivos legais será possibilitada apenas com o devido funcionamento da Autoridade Nacional de Proteção de Dados, a qual, neste momento, também está em seus estágios iniciais de formação.¹ Em menos de uma semana da entrada em vigor da LGPD, já foram ajuizadas as primeiras ações nela fundamentadas; para o futuro imediato, a tendência é apenas de aumento do número de demandas judiciais.

Por um lado, a crescente conscientização dos operadores do direito em relação aos impactos trazidos pela LGPD é positiva, visto que impulsiona o fortalecimento da adoção de políticas de *compliance* em favor da proteção dos dados dos titulares. Por outro lado, a precipitação no ajuizamento imediato de ações baseadas na LGPD pode ter um impacto negativo, uma vez que, dado o caráter recente da lei, ainda não há uma cultura de privacidade

¹ A estrutura regimental da ANPD foi definida com o Decreto nº 10.474, de 26 de agosto de 2020, o qual, no entanto, entrou em vigor apenas em 6 de novembro de 2020, com a publicação da nomeação de Waldemar Gonçalves Ortunho Junior para o cargo de Diretor-Presidente do Conselho Diretor da ANPD.

propriamente consolidada no Brasil, tampouco uma regulamentação adequada para preencher as lacunas contidas na lei, de modo que “a existência de múltiplas decisões ao redor do país, potencialmente conflitantes, ampliará a insegurança jurídica.”²

O caminho a se percorrer é longo e tortuoso, o qual demonstra a grande relevância que o tema da proteção da privacidade e dos dados pessoais assumiu nos dias atuais – momento em que as fronteiras da realidade digital e da realidade física se encontram cada vez mais indistinguíveis. Na era da internet e das redes sociais, do *e-commerce* e dos *smartphones*, os rastros digitais de cada indivíduo são praticamente impossíveis de serem apagados. O usuário que navega pelas redes pode ter a impressão de estar em uma posição de controle, afinal, centenas de milhares de páginas estão na ponta de seus dedos, a poucos cliques de distância. Contudo, esse controle não passa de uma ilusão: para os grandes atores econômicos, o verdadeiro produto não é a mercadoria física ofertada nos *websites*, mas o próprio usuário que a busca, cuja identidade pode ser facilmente rastreada e reconstruída pelas pegadas digitais e por seus dados pessoais.³ A relação entre o titular dos dados e os agentes de tratamento é, portanto, manifestamente assimétrica, encontrando-se o indivíduo em posição de considerável vulnerabilidade, com o constante risco de ter seus direitos fundamentais violados.⁴ Para que o empoderamento do indivíduo e o consequente reequilíbrio na relação informacional se tornem possíveis, é imprescindível compreender, em primeiro lugar, quais são esses direitos que estão sendo violados.

Nesse sentido, o presente artigo busca analisar esses direitos em jogo, com especial enfoque na ideia de privacidade e proteção de dados pessoais. Realiza-se, primeiramente, um panorama histórico do desenvolvimento do direito à privacidade, desde a definição estadunidense do *right to privacy* até a crescente associação deste direito com a autodeterminação informativa e a proteção de dados pessoais, a qual, por sua vez, vem a se tornar um direito autônomo. Por conseguinte, explica-se a insuficiência da concepção clássica da *privacy* para regulamentar os novos desafios promovidos pela sociedade da informação à luz

² PALHARES, Felipe. O que a aplicação da LGPD já revela. *O Globo*, 2020. Disponível em: <<https://oglobo.globo.com/opiniao/o-que-aplicacao-da-lgpd-ja-revela-24719053>> Acesso em: 29 dez. 2020.

³ SNOWDEN, Edward. *Permanent Record*. London: Macmillan, 2019, p. 11. Livro eletrônico.

⁴ Um dos exemplos que demonstram a vulnerabilidade do indivíduo está nas políticas de privacidade dos *websites*, que comumente apresentam duas opções: ou o usuário aceita todos os termos e condições pré-definidos, ou ele é impedido de utilizar o serviço como um todo, de modo que ele deve renunciar o seu controle para ter acesso ao produto desejado. Ainda que formalmente o usuário pressione um botão com os dizeres “leio e concordo com os termos de serviço”, não há como pressupor que o consentimento exprimido por ele seja livre, informado e inequívoco, porquanto grande parte das políticas de privacidade são redigidas em linguajar técnico que não permite a devida compreensão por parte do indivíduo médio. BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 162. Livro eletrônico.

de temas como o *habeas data*⁵ e o direito ao esquecimento,⁶ que mesmo antes do segundo milênio já demonstravam que a privacidade e os dados pessoais não conseguem ser adequadamente tutelados por um simples não-fazer por parte de terceiros, requerendo prestações positivas por parte do Estado.⁷

A partir disso, observa-se a complexidade inerente aos direitos à privacidade e à proteção de dados, cujos conteúdos se aprofundam a depender do contexto histórico e tecnológico em que se encontram inseridos.⁸ Assim, a crescente virtualização da vida cotidiana, o surgimento de uma economia movida a dados e a sofisticação exponencial de mecanismos de vigilância, somados ao desenvolvimento das novas tecnologias disruptivas, fazem com que a privacidade e a proteção de dados assumam contornos mais importantes do que nunca, uma vez que estão diretamente associados com a proteção da liberdade, da autonomia e da dignidade humana.

1 DESENVOLVIMENTO HISTÓRICO DOS DIREITOS À PRIVACIDADE E À PROTEÇÃO DE DADOS

A concepção moderna da privacidade como um direito propriamente dito surgiu em contexto relativamente recente nos Estados Unidos, ao final do século XIX.⁹ O seu advento se deu em um momento histórico específico, 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.¹⁰ 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,¹¹ o moderno debate sobre a privacidade apenas assumiu feições

⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 267-289.

⁶ 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.

⁷ SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. *International Journal of Digital Law*, ano 1, n. 3, p. 117-137, 2020. Disponível em: <<https://doi.org/10.47975/IJDL/3hiromi>> Acesso em: 25 mar. 2021.

⁸ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 69.

⁹ GLANCY, Dorothy J. The Invention of the Right to Privacy. *Arizona Law Review*, v. 21, n. 1, p. 1-39, 1979, p. 1. Disponível em: <<https://digitalcommons.law.scu.edu/facpubs/317/>> Acesso em: 12 dez. 2020.

¹⁰ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 32-33.

¹¹ 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*”. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 125.

específicas com a publicação do artigo *The Right to Privacy*, de autoria de Samuel Warren e Louis Brandeis, em 1890.¹² 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 personalidade do indivíduo, em especial quanto à sua auto-imagem.¹³ Trata-se do 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*).

Não obstante, 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.¹⁴ O que os juristas 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.¹⁵ 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, ao estabelecerem uma intrínseca relação entre o direito à privacidade e o desenvolvimento das novas tecnologias de informação, relação esta que perdura até os dias atuais.

Insta ressaltar, contudo, que o artigo *The Right to Privacy* foi publicado em resposta aos anseios de uma parcela específica da população estadunidense ao final do século XIX, com elevados poder de influência e prestígio social, de modo que grande parte dos casos envolviam a insatisfação das elites burguesas em relação às intromissões da imprensa em suas vidas

¹² WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*. *Harvard Law Review*, v. IV, n. 5, p. 193-220, 1890. Disponível em: <<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>> Acesso em: 12 dez. 2020.

¹³ GLANCY, Dorothy J. *The Invention of the Right to Privacy*, p. 2.

¹⁴ Tal transição está atrelada ao surgimento da concepção moderna de ente público enquanto Estado-nação dotado de soberania e, como consequência, ao “estabelecimento de uma esfera privada livre das ingerências desse ente público”. 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, nesse contexto, como proteção da propriedade individual. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 117-119.

¹⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 126.

privadas.¹⁶ Se naquele momento o reconhecimento da privacidade como um direito de ser deixado a sós era suficiente para garantir a sua tutela, o exponencial desenvolvimento dos meios de comunicação em massa e das tecnologias de informação ao longo do século XX tornou imperioso que o conceito de privacidade fosse revisto e reavaliado conforme as necessidades históricas inerentes a cada época.¹⁷

Assim, a partir da segunda metade do século XX, o desenvolvimento tecnológico tornou corrente a utilização de informações pessoais dos indivíduos,¹⁸ 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.¹⁹ 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 a ideia de autodeterminação informativa,²⁰ ou seja, com a possibilidade de o indivíduo exercer o controle sobre seus dados pessoais e definir dentro de quais limites eles podem ser utilizados.²¹

Uma vez ultrapassada a associação inicial entre progresso tecnológico e bem-estar social, surgiu a insegurança quanto ao número de possíveis situações nas quais o Estado poderia se utilizar de tecnologias em ameaça ao direito à privacidade – o que possibilitou o surgimento de teorias fatalistas que previam que a utilização desenfreada dos meios tecnológicos levaria ao fim da privacidade e ao estabelecimento de governos totalitários, nos quais as informações dos cidadãos seriam coletadas para fins de controle social e de repressão, colocando fim a regimes democráticos.²² 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

¹⁶ Um desses casos envolvia o próprio autor Samuel Warren, membro da elite social da cidade de Boston, por força de seu casamento com Mabel Bayard, filha do então senador Thomas F. Bayard. Alega-se que uma das supostas inspirações para a redação do artigo *The Right to Privacy* teria sido a publicação de detalhes da vida privada de Warren pelo periódico *The Saturday Evening Gazette*. GLANCY, Dorothy J. *The Invention of the Right to Privacy*, p. 6.

¹⁷ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 35.

¹⁸ 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 este artigo também se refere aos termos de maneira intercambiável. Nesse sentido: DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 136.

¹⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 34.

²⁰ 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*, p. 323-345.

²¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 168-169.

²² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 37.

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*, a qual propiciou a formação de uma nova arquitetura informacional, com uma nova estrutura de poder também vinculada a ela.²³ 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*)²⁴ e tornando necessária, conseqüentemente, a implementação de mecanismos de proteção nos ordenamentos jurídicos para tutelar esta nova realidade.

Observa-se, portanto, que o direito à privacidade se desenvolveu historicamente no sentido de se estruturar em torno da proteção dos dados pessoais, mas com ela não se confunde. Esta decorre daquela ao mesmo tempo em que se estabelece como um *novo* direito da personalidade, com dinâmica e características próprias.²⁵ Nas palavras de Danilo Doneda, a proteção de dados “propõe o tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão”,²⁶ visto que “garantias a princípio relacionadas com a privacidade passam a ser vistas em uma ótica mais abrangente.”²⁷ Bruno Bioni elucida que, diferentemente da privacidade, o direito à proteção de dados extrapola a dicotomia público x privado, pois a sua incidência independe que o dado pessoal esteja vinculado a um aspecto da vida íntima do titular, “bastando que a informação esteja atrelada a uma pessoa – conceito de dado pessoal – para deflagrá-lo.”²⁸

No Brasil, o direito à privacidade se encontra consolidado no rol de direitos fundamentais previsto na Constituição Federal de 1988, uma vez que o art. 5º, 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. Até o presente momento não há previsão constitucional expressa acerca do direito à proteção de

²³ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 35.

²⁴ 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*, p. 23-52.

²⁵ BIONI, Bruno Ricardo. *Proteção de dados pessoais*, p. 89.

²⁶ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 173.

²⁷ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 173.

²⁸ BIONI, Bruno Ricardo. *Proteção de dados pessoais*, p. 95.

dados,²⁹ o que, contudo, não é empecilho ao reconhecimento da importância do tema pelo Supremo Tribunal Federal.³⁰

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,³¹ o que reflete a supramencionada preocupação histórica com a coleta e o tratamento de dados realizado pelo Estado. 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.³²

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 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.³³

Outro diploma normativo 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

²⁹ Em 03 de julho de 2019, foi apresentada perante o Senado a PEC 17/2019, que visa incluir no texto constitucional a proteção de dados pessoais no rol do art. 5º e fixar a competência privativa da União para legislar sobre o tema. A proposta atualmente aguarda votação no Plenário da Câmara dos Deputados.

³⁰ STF. Medida Cautelar na ADI 6.387/DF. Decisão monocrática. Rel. Min. Rosa Weber. J. 24/04/2020.

³¹ 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*, p. 53-83.

³² SZANIAWSKI, Elimar. *Direitos de personalidade e sua tutela*. 2. ed. São Paulo: Revista dos Tribunais, 2005, p. 192.

³³ 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 Desiree; 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.

inovadora ao prever uma proteção mais significativa dos dados sensíveis dos consumidores,³⁴ ou seja, das informações relativas a questões como religião, orientação sexual, origem racial e étnica, dados genéticos e de saúde do indivíduo. Poucos anos depois foi promulgado o Marco Civil da Internet (Lei nº 12.965/2014), que prevê em seu art. 3º, 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 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 consolidar³⁵ – 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, 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,³⁶ ao pretender conferir ampla proteção a *todas* as formas de tratamento de dados pessoais dos indivíduos.³⁷ 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 e aos dados pessoais dos cidadãos, em todas as suas esferas de manifestação.

2 A INSUFICIÊNCIA DA CONCEPÇÃO CLÁSSICA DA PRIVACIDADE NA ERA DIGITAL: HABEAS DATA E O DIREITO AO ESQUECIMENTO

³⁴ 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.

³⁵ 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.

³⁶ 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. 72.

³⁷ 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*, p. 99-129.

Como mencionado, 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.³⁸

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*,³⁹ 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 incorreria em um dever de abstenção por parte do outro.

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* do século XIX pode ser igualmente estendido em relação aos entes públicos. 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 manter em segredo.⁴⁰ Desta maneira, a visão oitocentista estadunidense 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.⁴¹ Mais especificamente, conforme classificação de Robert Alexy, é possível situar a *privacy* 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.⁴²

Todavia, 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 a um dever negativo de abstenção é uma perspectiva reducionista, pois se limita a enxergá-la como

³⁸ GLANCY, Dorothy J. *The Invention of the Right to Privacy*, p. 4.

³⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 30.

⁴⁰ GLANCY, Dorothy J., *The Invention of the Right to Privacy*, p. 28.

⁴¹ ALEXY, Robert. *Teoria dos Direitos Fundamentais*. 2. ed. São Paulo: Malheiros, 2017, p. 433.

⁴² Além dos direitos à não-afetação de características e situações, Alexy elenca outras duas categorias de direitos a ação negativa, quais sejam, os direitos ao não-embaraço de ações e os direitos à não-eliminação de posições jurídicas do titular do direito. ALEXY, Robert. *Teoria dos Direitos Fundamentais*, p. 196 e ss.

um simples direito de primeira geração, cujo conteúdo se resume à proteção da liberdade em relação a possíveis interferências do ente público na esfera jurídica do particular.⁴³

Insta ressaltar que a classificação do direito à privacidade como direito fundamental de primeira geração é simplista, pois pressupõe que este apenas possui função de defesa. Tal perspectiva ignora a estrutura básica de um direito fundamental, qual seja, a que um direito a algo abarca de modo concomitante deveres negativos estatais e deveres positivos de proteção,⁴⁴ além de também ostentarem simultaneamente titularidade individual e transindividual, a depender de qual dimensão do direito fundamental que está sendo analisada no caso concreto⁴⁵ – motivo pelo qual se afirma que os direitos fundamentais devem ser analisados conforme a sua multifuncionalidade.⁴⁶

Portanto, não se quer dizer que o dever de abstenção não seja mais relevante para a proteção da privacidade e dos dados pessoais. O que se pretende dizer é que o aumento da complexidade nas relações que envolvem tais direitos tornou necessário que a tutela não mais se restrinja à esfera negativa, sendo imprescindível igualmente uma posição prestacional positiva por parte do Estado. Isto se reflete, por exemplo, a partir da década de 1970, momento em que adveio a preocupação em garantir uma tutela normativa dos dados pessoais, culminando nas primeiras leis de proteção de dados – em países como Alemanha e Suécia, além dos Estados Unidos, com o *Privacy Act* de 1974⁴⁷ –, as quais 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 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.⁴⁸ Tudo isso demonstra a mutabilidade inerente à proteção da privacidade e dos dados pessoais, pois a efetiva proteção desses direitos necessariamente requer que os

⁴³ Em contraposição, os direitos de segunda geração 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. HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais. *Revista de Direitos Fundamentais e Democracia*, v. 14, n. 14, p. 618-688, 2013.

⁴⁴ ALEXY, Robert. *Teoria dos Direitos Fundamentais*, p. 195.

⁴⁵ HACHEM, Daniel Wunder. A dupla titularidade (individual e transindividual) dos direitos fundamentais econômicos, sociais, culturais e ambientais, p. 621-622.

⁴⁶ SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade, p. 120 e ss.

⁴⁷ 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*, p. 85-98.

⁴⁸ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 175 e ss.

dispositivos legais estejam atentos aos avanços tecnológicos e às mudanças operadas na maneira em que as informações são distribuídas e disseminadas.⁴⁹ Nas décadas seguintes, o abismo entre a proteção de dados e a exponencial informatização da realidade apenas aumentaria. O avanço da informática começara a complexificar a relação entre privacidade, dados pessoais e informação mesmo anteriormente à virada do segundo milênio,⁵⁰ o que pode ser observado em determinadas questões práticas surgidas 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 pelo art. 5º, LXIX, LXXII e LXXVII da Constituição Federal, que o preveem como instrumento jurisdicional apto a 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”⁵¹ 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, conseqüentemente, na promoção do próprio direito de igualdade.⁵² Ainda que a lei não seja explícita, a doutrina acolhe a perspectiva de existirem diversas modalidades de *habeas data*,⁵³ 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)

⁴⁹ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, posição 597. Livro eletrônico.

⁵⁰ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*, posição 565-576.

⁵¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 267.

⁵² 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.

⁵³ DURÁN MARTÍNEZ, Augusto. *Derecho a la protección de datos personales y al acceso a la información pública*, p. 152-156.

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.⁵⁴

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, LXVIII, da Constituição Federal) –, 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.⁵⁵

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.⁵⁶ Ademais, não são poucas as críticas ao instituto, em especial as que apontam que, diferentemente dos outros países da América Latina, a redação 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.⁵⁷ 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.⁵⁸

A mencionada inocuidade do *habeas data* pode ser observada, por exemplo, no baixo interesse dos juristas brasileiros em se debruçar sobre o tema e na sua pouca utilização na prática jurídica.⁵⁹ 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”,⁶⁰ incapaz de trazer as respostas adequadas às necessidades inerentes à problemática do acesso à informação. Na prática, portanto, tornou-se instrumento meramente

⁵⁴ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 284.

⁵⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 270-271.

⁵⁶ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 270.

⁵⁷ DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 97, p. 239-253, 2002. Disponível em: <<http://www.revistas.usp.br/rfdusp/article/view/67544>>. Acesso em: 12 dez. 2020.

⁵⁸ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 286.

⁵⁹ DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro, p. 243.

⁶⁰ DALLARI, Dalmo de Abreu. O *habeas data* no sistema jurídico brasileiro, p. 243.

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.”⁶¹ Nesse sentido, é necessário observar o *habeas data* como “um produto de seu tempo”,⁶² 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 militar⁶³ –, 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 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 pretéritos ou situações constrangedoras que digam respeito à vida privada do indivíduo”,⁶⁴ 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.⁶⁵ Neste caso, reconheceu-se 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 à divulgação de seu nome e de sua imagem.

⁶¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 289.

⁶² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 272.

⁶³ 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.” DALLARI, Dalmo de Abreu. *O habeas data no sistema jurídico brasileiro*, p. 244.

⁶⁴ 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*, p. 219-241.

⁶⁵ STJ. REsp 1.334.097/RJ. Quarta Turma. Rel. Min. Luis Felipe Salomão. J. 28/05/2013.

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”⁶⁶ 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 poderia 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 frequentemente suscitado em pedidos de desindexação de páginas e de buscadores de pesquisa da *web*.⁶⁷ 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.⁶⁸ Entretanto, 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.⁶⁹

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,⁷⁰ sob pena de responsabilidade civil do controlador de dados. Compreende-se a confusão entre os dois institutos, uma vez que o *General Data*

⁶⁶ SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências, p. 374.

⁶⁷ GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados, p. 226-227.

⁶⁸ CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça, p. 93.

⁶⁹ CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça, p. 96.

⁷⁰ 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.

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 leva a uma relação de identidade com o direito ao esquecimento erigido pela doutrina e pela jurisprudência brasileiras, pois o *right to erasure* constante na GDPR – e, conseqüentemente, 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 informada ao titular.⁷¹ 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”,⁷² não tendo qualquer relação com a proteção do indivíduo perante a memória pública de fatos pretéritos que seja prejudicial ao desenvolvimento da personalidade.

De qualquer modo, é possível afirmar que os debates acerca do tema não serão esgotados no futuro imediato – especialmente à luz do posicionamento firmado pelo Supremo Tribunal Federal em fevereiro de 2021, que, por maioria de votos, estabeleceu tese de repercussão geral afirmando a incompatibilidade do direito ao esquecimento com a ordem jurídico-constitucional brasileira, de modo que “eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso.”⁷³ Ao negar a sua existência enquanto direito genérico e pleno, o STF vem aparentemente em sentido contrário à expressiva parcela doutrinária e à construção jurisprudencial erigida pelo STJ ao longo dos anos, que vinha se

⁷¹ 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.

⁷² SCHREIBER, Anderson. Direito ao Esquecimento e Proteção de Dados Pessoais na Lei 13.709/2018: distinções e potenciais convergências, p. 377-378.

⁷³ Tema 786: “É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível”. *Leading case*: STF. RE 1.010.606. Plenário. Rel. Min. Dias Toffoli. J. 11/02/2021.

posicionando, no geral, de modo favorável à condição do direito ao esquecimento enquanto direito fundamental.⁷⁴

Não obstante, Ingo Wolfgang Sarlet afirma que o entendimento do STF não incorre em um afastamento completo do tema, pois a tese de repercussão geral “rechaçou muito mais o rótulo do que a existência e o conteúdo propriamente dito”⁷⁵ do direito ao esquecimento, o qual é voltado à responsabilização de agentes pela disseminação de certos tipos de informações sobre a vida passada de outrem em determinados contextos, a depender do caso concreto – sendo que tal responsabilização não é realizada apenas com a interdição de divulgação de informações, podendo ser feita mediante outros remédios que não necessariamente impliquem uma limitação à liberdade de expressão, como a complementação do conteúdo divulgado ou a reparação pecuniária pelo dano moral sofrido.⁷⁶ Para Rafael Mansur, a maioria formada pelos Ministros compreendeu erroneamente que o instituto estaria voltado a “fazer com que a sociedade esqueça fatos do passado, impedindo a formação de uma memória coletiva que se afigura essencial a qualquer democracia”⁷⁷, quando, ao contrário, ele apenas busca proteger a pessoa humana cuja dignidade tenha sido violada pela recordação opressiva de fatos pretéritos que não mais refletem sua identidade atual. Na concepção do autor, o próprio fato de o STF ter afirmado a necessidade de ponderação de direitos em colisão no caso concreto demonstra que a Corte verdadeiramente acolheu o núcleo material do direito ao esquecimento, uma vez que os seus defensores jamais defenderam “uma exclusão automática de notícias ou um direito absoluto ao apagamento de informações a partir de meros caprichos individuais.”⁷⁸

Desta maneira, dentro de uma realidade digital em que o armazenamento de informações torna a memória um fato onipresente, “igualmente importante se torna nossa habilidade de esquecer, de nos libertar das correntes do nosso passado e de viver no presente”,⁷⁹ de modo que impedir o esquecimento nos momentos em que a lembrança viola o pleno desenvolvimento do indivíduo implica obstar a concretização da própria dignidade humana. Portanto, o que era sustentado pelos defensores do direito ao esquecimento anteriormente à decisão do STF ainda

⁷⁴ SARLET, Ingo Wolfgang. STF e direito ao esquecimento: julgamento a ser esquecido ou comemorado? *ConJur*, 2021. Disponível em: <<https://www.conjur.com.br/2021-mar-05/direitos-fundamentais-stf-direito-esquecimento-julgamento-esquecido-ou-comemorado>> Acesso em: 26 mar. 2021.

⁷⁵ SARLET, Ingo Wolfgang. STF e direito ao esquecimento: julgamento a ser esquecido ou comemorado?

⁷⁶ MANSUR, Rafael. Decisão do STF não é “pá de cal” no direito ao esquecimento. *ConJur*, 2021. Disponível em: <<https://www.conjur.com.br/2021-fev-24/mansur-stf-nao-jogou-pa-cal-direito-esquecimento>> Acesso em: 26 mar. 2021.

⁷⁷ MANSUR, Rafael. Decisão do STF não é “pá de cal” no direito ao esquecimento.

⁷⁸ MANSUR, Rafael. Decisão do STF não é “pá de cal” no direito ao esquecimento.

⁷⁹ MAYER-SCHÖNBERGER, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. New Jersey: Princeton, 2009, p. 115. Livro eletrônico.

se aplica,⁸⁰ uma vez que caberá ao julgador, nos ditames do caso concreto, verificar se a publicização de determinados fatos pretéritos está obstando os direitos fundamentais 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.

3 A TUTELA DOS DADOS PESSOAIS FRENTE À ECONOMIA MOVIDA A DADOS

Finalmente, cabe pontuar que as questões suscitadas acerca do *habeas data* e do direito ao esquecimento não são os únicos problemas práticos decorrentes da proteção da privacidade e dos dados pessoais 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. Isto porque, 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 e de entes privados – sendo que o significado de vigilância, aqui, engloba todo um “mundo de monitoramento, controle, observação, classificação, checagem e atenção sistemática”⁸¹ 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.⁸² Nesse cenário, a coleta e o tratamento de informações pessoais em prol da segurança formam um espelho de única face (“*one-way mirror*”),⁸³ tendo em vista 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,⁸⁴ que poderia levar à concretização do *Big Brother* de Orwell⁸⁵ ou de

⁸⁰ MANSUR, Rafael. Decisão do STF não é “pá de cal” no direito ao esquecimento.

⁸¹ BAUMAN, Zygmunt. *Vigilância líquida: diálogos com David Lyon*. Rio de Janeiro: Zahar, 2013, p. 7.

⁸² 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*, p. 157-197.

⁸³ FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados, p. 27.

⁸⁴ STEFIK, Mark. *The Internet Edge: Social, technical and legal challenges for a networked world*. Cambridge: The MIT Press, 2000, p. 201-202.

⁸⁵ 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.

um modelo de controle social conforme a arquitetura do panóptico de Bentham⁸⁶ – 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.

Por conseguinte, 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.⁸⁷ 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 vá ao plano do inacessível.⁸⁸ 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.⁸⁹

Nesse sentido, não se fala somente em uma sociedade de vigilância, mas também no surgimento de um *capitalismo de vigilância*, o qual estabelece uma nova ordem econômica em que “a produção de bens e serviços está subordinada a uma nova arquitetura global de modificação comportamental”,⁹⁰ tendo como matéria prima a própria experiência humana, extraída a partir dos aparatos tecnológicos. Dentro desse cenário, 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.”⁹¹ Os dados se tornam os principais ativos dessa nova organização econômica

⁸⁶ Modelo arquitetônico prisional proposto pelo filósofo utilitarista Jeremy Bentham. A prisão é projetada em formato circular, de modo que as celas sejam constantemente visíveis ao vigia localizado na torre central, que, em contrapartida, não consegue ser visto pelos prisioneiros. Michel Foucault utilizou o panóptico como ilustração em seus estudos sobre vigilância, disciplina e domesticação dos corpos, pois ele tem o efeito de “induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder”. FOUCAULT, Michel. *Vigiar e punir: o nascimento da prisão*. 42. ed. Petrópolis: Vozes, 2014, p. 195.

⁸⁷ WHITAKER, Reg. *The End of Privacy: how total surveillance is becoming a reality*. New York: The New Press, 1999, p. 133.

⁸⁸ BAUMAN, Zygmunt. *Vigilância líquida*, p. 19.

⁸⁹ WHITAKER, Reg. *The End of Privacy*, p. 140.

⁹⁰ ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs, 2019, p. 8.

⁹¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais*, p. 41.

(“*data as the new oil*”),⁹² estruturada no monitoramento constante dos “cidadãos-potenciais consumidores”⁹³ pelos grandes agentes econômicos.

Em uma perspectiva baumaniana, a vigilância contemporânea é caracterizada por ser líquida, fluida, esparramada ao longo de todos os estratos sociais,⁹⁴ não sendo possível traçar suas origens com facilidade, em que o sistema de dominação é instalado de forma progressiva e dispersa, em oposição ao poder centralizado do sistema panóptico característico das sociedades disciplinares. Para Bauman, o adjetivo líquido não é inerente à definição propriamente dita de vigilância, mas é um elemento decorrente do atual estado da própria modernidade, que é, por si, líquida, “fluida e perturbadora”,⁹⁵ na medida em que “todas as formas sociais se desmancham mais depressa que a velocidade com que se criam novas formas.”⁹⁶ 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, desde em nível individual até em nível econômico.

Em nível individual, o desenvolvimento desenfreado de novas formas de tecnologia corre o risco de promover uma *cegueira moral*⁹⁷ nas pessoas, porquanto a aplicação de algoritmos sem a regulação adequada “promove decisões que prejudicam pessoas mais pobres, reforça estereótipos e intensifica desigualdades sociais”,⁹⁸ ao delinear perfis de potenciais consumidores e classificá-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.⁹⁹

Nesse contexto, em um segundo momento, 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

⁹² 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*, p. 601-619.

⁹³ BIONI, Bruno Ricardo. *Proteção de dados pessoais*, p. 134.

⁹⁴ BAUMAN, Zygmunt. *Vigilância líquida*, p. 10.

⁹⁵ BAUMAN, Zygmunt. *Vigilância líquida*, p. 10.

⁹⁶ BAUMAN, Zygmunt. *Vigilância líquida*, p. 11.

⁹⁷ BAUMAN, Zygmunt; DONSKIS, Leonidas. *Cegueira Moral: A perda da sensibilidade na modernidade líquida*. Rio de Janeiro: Zahar, 2014. Livro eletrônico.

⁹⁸ 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, 2019. Disponível em: <<https://dx.doi.org/10.1177/2046147X19863833>> Acesso em: 12 dez. 2020.

⁹⁹ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*, posição 1009.

denominada “economia com especialização flexível.”¹⁰⁰ 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, por conseguinte, 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 qual é o perfil de seus clientes, conhecimento este que 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,¹⁰¹ conforme as informações são correlacionadas com a finalidade de prever padrões de comportamento e, conseqüentemente, 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.¹⁰² 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.¹⁰³ 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

¹⁰⁰ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*, posição 1687.

¹⁰¹ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*, posição 1763.

¹⁰² TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais, p. 610.

¹⁰³ WHITAKER, Reg. *The End of Privacy*, p. 103.

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.¹⁰⁴

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 difíceis de serem removidos que os *cookies* tradicionais.¹⁰⁵ 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.”¹⁰⁶

Importante ressaltar, novamente, que todas estas preocupações com privacidade, proteção de dados e a sociedade de vigilância já surgem na transição para o segundo milênio, 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*”).¹⁰⁷ Se ao final do século XX já conseguiu ser demonstrada a insuficiência da concepção do *right to privacy* enquanto mera liberdade negativa, o desenvolvimento mais recente de tecnologias disruptivas – que envolvem *Big Data*, sistemas de inteligência artificial e de aprendizado de máquinas, computação em nuvem, entre outros – demonstra que os direitos à privacidade e à proteção de dados dificilmente estarão isentos 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.”¹⁰⁸

A rapidez do avanço tecnológico indica que tentativas de estabelecer uma acurada

¹⁰⁴ TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais, p. 611-612.

¹⁰⁵ TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais, p. 612.

¹⁰⁶ COHEN, Julie E. What Privacy is For. *Harvard Law Review*, v. 126, n. 7, p. 1904-1933, 2013. Disponível em: <<https://ssrn.com/abstract=2175406>> Acesso em: 12 dez. 2020.

¹⁰⁷ WHITAKER, Reg. *The End of Privacy*, p. 125.

¹⁰⁸ RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 95.

regulação normativa estarão corriqueiramente atrasadas em relação às novas tendências; o elemento da imprevisibilidade intrínseco à tecnologia faz com que seja possível alcançar, no máximo, aproximações às novas realidades digitais.¹⁰⁹ No entanto, frente à violação da privacidade no contexto do capitalismo de vigilância,¹¹⁰ mesmo as aproximações são necessárias, quando os elementos em jogo se referem a direitos fundamentais de cada cidadão, enquanto manifestação de sua personalidade, autonomia, autodeterminação e dignidade humana.

CONSIDERAÇÕES FINAIS

O crescimento tecnológico exponencial que tem sido observado desde meados do século XX torna a discussão sobre a proteção dos direitos à privacidade e aos dados pessoais mais relevante do que nunca. Se outrora a classificação da privacidade como simples direito de defesa pode ter sido suficiente para garantir a sua tutela, atualmente não o é mais. Os novos desafios proporcionados pela sociedade de informação tornam imprescindível analisar estes direitos fundamentais em toda sua complexidade, demarcados por sua multifuncionalidade.

Conforme foi visto, a delimitação do conteúdo de proteção da privacidade varia conforme o contexto histórico-social de cada época. Conquanto a ideia do “privado” surgiu em oposição à esfera do “público” ainda no século XVI, é apenas ao final do século XIX que a privacidade é consolidada como um direito em sua acepção moderna, enquanto o direito de ser deixado a sós, consoante uma mentalidade tradicionalmente liberal-burguesa de proteção de elites da época.

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

¹⁰⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, p. 51.

¹¹⁰ FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados, p. 26.

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.

A coleta de dados se sofisticou ao ponto de possibilitar a formulação de uma nova arquitetura de poder, consubstanciada em 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. Dentro desse contexto, as práticas de mineração de dados praticadas pelo Estado e pelos grandes atores econômicos devem ser vistas com cautela, pois, dentro de um contexto de vigilância pós-panóptica, a manipulação desses dados em desrespeito à ética pode perpetuar preconceitos, vieses e discriminações, bem como obliterar direitos fundamentais dos cidadãos. A indústria de comercialização de dados pessoais faz com que o titular dos dados deixe de ser o destinatário final da mercadoria e se transforme na própria mercadoria.

A proteção da privacidade e dos dados pessoais, portanto, não é algo isolado; ao contrário, ela possui profundas relações com a proteção da liberdade, da autonomia e da autodeterminação de cada cidadão. Com efeito, imperioso promover mecanismos voltados ao empoderamento do sujeito, parte vulnerável na relação informacional, de modo que o desenvolvimento tecnológico não ocorra de forma irrestrita em detrimento do indivíduo, mas em conformidade com os direitos fundamentais garantidos pela Constituição.

REFERÊNCIAS

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, 2019. Disponível em: <<https://dx.doi.org/10.1177/2046147X19863833>> Acesso em: 12 dez. 2020.

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

BAUMAN, Zygmunt; DONSKIS, Leonidas. *Cegueira Moral: A perda da sensibilidade na modernidade líquida*. Rio de Janeiro: Zahar, 2014. Livro eletrônico.

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

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.334.097/RJ*. Quarta Turma. Rel. Min. Luis Felipe Salomão. J. 28/05/2013, DJe 10/09/2013.

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: 12 dez. 2020.

BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF*. Decisão monocrática. Rel. Min. Rosa Weber. J. 24/04/2020. DJe, 28/04/2020.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 1.010.606*. Plenário. Rel. Min. Dias Toffoli. J. 11/02/2021. DJe 18/02/2021.

COHEN, Julie E. What Privacy is For. *Harvard Law Review*, v. 126, n. 7, p. 1904-1933, 2013. Disponível em: <<https://ssrn.com/abstract=2175406>> Acesso em: 12 dez. 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*, v. 97, p. 239-253, 2002. Disponível em: <<http://www.revistas.usp.br/rfdusp/article/view/67544>>. Acesso em: 12 dez. 2020.

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

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.

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.

GLANCY, Dorothy J. The Invention of the Right to Privacy. *Arizona Law Review*, v. 21, n. 1, p. 1-39, 1979. Disponível em: <<https://digitalcommons.law.scu.edu/facpubs/317/>> Acesso em: 12 dez. 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.

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

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, 179-213.

MANSUR, Rafael. Decisão do STF não é “pá de cal” no direito ao esquecimento. *ConJur*, 2021. Disponível em: <<https://www.conjur.com.br/2021-fev-24/mansur-stf-nao-jogou-pa-cal-direito-esquecimento>> Acesso em: 26 mar. 2021.

MAYER-SCHÖNBERGER, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. New Jersey: Princeton, 2009. Livro eletrônico.

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

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.

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.

PALHARES, Felipe. O que a aplicação da LGPD já revela. *O Globo*, 2020. Disponível em: <<https://oglobo.globo.com/opiniao/o-que-aplicacao-da-lgpd-ja-revela-24719053>> Acesso em: 29 dez. 2020.

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

SALGADO, Eneida Desiree; 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.

SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. *International Journal of Digital Law*, ano 1, n. 3, p. 117-137, 2020. Disponível em: <<https://doi.org/10.47975/IJDL/3hiromi>> Acesso em: 29 dez. 2020.

SARLET, Ingo Wolfgang. STF e direito ao esquecimento: julgamento a ser esquecido ou comemorado? *ConJur*, 2021. Disponível em: <<https://www.conjur.com.br/2021-mar->

05/direitos-fundamentais-stf-direito-esquecimento-julgamento-esquecido-ou-comemorado>

Acesso em: 26 mar. 2021.

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.

SNOWDEN, Edward. *Permanent Record*. London: Macmillan, 2019. Livro eletrônico.

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

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

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.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, v. IV, n. 5, p. 193-220, 1890. Disponível em: <<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>> Acesso em: 12 dez. 2020.

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

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs, 2019.

Recebido em: 31/12/2020

Aceito em: 29/04/2021

