UNIVERSIDADE FEDERAL DE JUIZ DE FORA - *CAMPUS* AVANÇADO GOVERNADOR VALADARES
CURSO DE DIREITO

Júlia Bueno Dias

As implicações da constitucionalização da proteção de dados pessoais como direito fundamental no Brasil: um estudo comparado com o regime de proteção de dados adotado pela União Europeia

Governador Valadares – MG
2021

Júlia Bueno Dias

As implicações da constitucionalização da proteção de dados pessoais como direito fundamental no Brasil: um estudo comparado com o regime de proteção de dados adotado pela União Europeia

Trabalho de conclusão de curso apresentado ao curso de Direito da Universidade Federal de Juiz de Fora - *campus* avançado Governador Valadares como requisito parcial à obtenção do título de bacharel em Direito.

Orientador: Prof. Lucas Costas dos Anjos

Governador Valadares – MG

2021

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Dias, Júlia Bueno.
As implicações da constitucionalização da proteção de dados pessoais como direito fundamental no Brasil : um estudo comparado com o regime de proteção de dados adotado pela União Europeia / Júlia Bueno Dias. -- 2021.
45 p.

Orientador: Lucas Costas dos Anjos
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Juiz de Fora, Campus Avançado de Governador Valadares, Instituto de Ciências Sociais Aplicadas - ICSA, 2021.

1. Proteção de dados. 2. Direitos Fundamentais. 3. União Europeia. 4. Brasil. I. Anjos, Lucas Costas dos, orient. II. Título.

Júlia Bueno Dias

As implicações da constitucionalização da proteção de dados pessoais como direito fundamental no Brasil: um estudo comparado com o regime de proteção de dados adotado pela União Europeia

Trabalho de conclusão de curso apresentado ao curso de Direito da Universidade Federal de Juiz de Fora - *campus* avançado Governador Valadares como requisito parcial à obtenção do título de bacharel em Direito.

Aprovada em 19 de março de 2021.

BANCA EXAMINADORA

_____

Prof. Lucas Costa dos Anjos
Universidade Federal de Juiz de Fora

_____

Prof. Pablo Georges Cicero Fraga Leurquin
Universidade Federal de Juiz de Fora

_____

Prof. Fabio Pereira Queiroz
Universidade Federal de Minas Gerais

_____

Prof. Branco di Fátima
Instituto Universitário de Lisboa

AGRADECIMENTOS

Agradeço ao meu pai, Júlio, meu alicerce e fonte de inspiração.

Agradeço também, a minha mãe Andressa, por vibrar pelas minhas vitórias como se dela fossem, por me apoiar nos momentos bons e me acolher nos momentos desafiadores.

Agradeço a toda minha família, assim como aos meus amigos, pela paciência nas horas de ausência, pelo apoio e companheirismo.

Dedico um agradecimento especial ao meu orientador, Lucas Anjos, que foi peça chave nesse trabalho. Obrigada por ter aceitado me acompanhar nessa caminhada, pelos ensinamentos, pelo incentivo, pela sensibilidade. Sinto que tive um verdadeiro mentor.

Enfim, um grande obrigada a todos que estiveram comigo e contribuíram de alguma forma para a minha graduação.

O capitalismo industrial recrutou a natureza apenas para sobrecarregar as gerações seguintes com o fardo de um planeta em chamas. Será que nós vamos aumentar ainda mais esse fardo com a invasão do capitalismo de vigilância e a conquista da natureza humana? Ficaremos inertes assistindo a como ele se impõe sutilmente na vida da colmeia ao mesmo tempo que exige que abandonemos o santuário e o direito ao tempo futuro em prol de sua riqueza e poder? (ZUBOFF, 2020, p. 553)

RESUMO

A nova era da informação traz a necessidade de criar meios de proteção nesse contexto de uso e processamento de dados pessoais. Em busca de efetivar a garantia desta proteção, a União Europeia, além de colocar em vigor o Regulamento Geral de Proteção de Dados Pessoais (GDPR), também a reconhece como um direito fundamental do cidadão. Esse foi um avanço que está agindo como efeito dominó em grande parte do mundo. No Brasil, A Lei Geral de Proteção de Dados (LGPD) já é uma realidade. Com isso é notável dizer que, o país está caminhando para ter uma política de segurança da informação cada vez mais forte e efetiva. O próximo passo seria, então, o reconhecimento da proteção de dados como um direito fundamental constitucional. Este trabalho visa analisar essa prerrogativa por meio de um estudo de direito comparado com a União Europeia.

Palavras-chave: Proteção de Dados. Direitos Fundamentais. União Europeia. Brasil.

ABSTRACT

The new information era we live in brings the necessity to craft ways to protect the citizen, in this context of use and processing of personal data. In the intent of making this protection effective, the European Union not only sanctioned the General Data Protection Regulation (GDPR) but also recognized it as a fundamental right of its citizens. In Brazil, the General Law of Data Protection (LGPD) is already a reality. Therefore, it is clear that the country is moving towards establishing a culture of data protection ever stronger and effective. The next step would be recognizing data protection as a constitutional fundamental right. This paper seeks to analyze this prerogative through a comparison of European Union`s laws and Brazil`s.

Keywords: Data protection. Fundamental Rights. European Union. Brazil.

LISTA DE ABREVIATURAS E SIGLAS

ABES	Associação Brasileira de Engenharia Sanitária e Ambiental
ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CN	Congresso Nacional
EUA	Estados Unidos da América
GDPR	Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*)
IRIS	Instituto de Referência em Internet e Sociedade
ITS	Instituto de Tecnologia e Sociedade
LAI	Lei de Acesso a Informação
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MP	Medida Provisória
PEC	Projeto de Emenda Constitucional
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A chamada era da sociedade da informação é caracterizada pelo espaço que as tecnologias tomaram nos contextos sociais e econômicos. As ferramentas de comunicação, fruto do avanço dessas tecnologias, estão cada vez mais acessíveis e essenciais nas relações entre indivíduo, mercado e Estado. Advindo da coleta, tratamento e sistematização dos dados pessoais, a informação se tornou o novo suprassumo das relações de poder. Daí emerge a sociedade da informação.

O processo de globalização hoje está intimamente vinculado ao desenvolvimento da tecnologia, dos meios de comunicação e do conhecimento. Isso possibilita o diálogo entre diversos países do mundo, no que diz respeito até mesmo de suas conjunturas jurídicas. Há garantias fundamentais que se convergem em variados ordenamentos jurídicos internacionais, como o direito à privacidade, liberdade e igualdade. A globalização, sem dúvidas, oferece meios para que esse processo ocorra.

O surgimento de novos direitos emerge da necessidade de lidar com novas demandas e complexidades das relações em sociedade, que estão sempre em transformação. A era da sociedade da informação, portanto, trouxe a urgência de se instituir proteções estatais aos tratamentos de dados pessoais. Com relevante atuação nesse sentido, a União Europeia, começa a regulamentar o direito a proteção de dados pessoais, com a Diretiva 05/46/CE, ainda em 1995, que posteriormente foi substituída pelo Regulamento Geral de Proteção e Dados, em 2016. Outro marco regulatório da UE, foi constar este direito em sua Carta de Direitos Fundamentais, em 2000.

Assim, com essa movimentação da UE, em regulamentar os tratamentos de dados pessoais, outros países também fizeram constar essa matéria em seus diplomas jurídicos. Nota-se uma crescente preocupação em proteger os direitos dos titulares dos dados e a criar mecanismos para o enfretamento de eventuais indiscricionariedades e violações. O que por sua vez, vem ocorrendo em proporções cada vez mais assustadoras.

Nos últimos anos são constantes as notícias que publicizam violações de dados, por meio de fraudes ou vazamentos, global e nacionalmente, expondo a fragilidade desse sistema. Em 2014, mais de 500 milhões de dados foram vazados dos bancos de dados do Yahoo (ROHR,

2016); Em 2016, 360 milhões de contas do MySpace foram vazadas (ROHR, 2016); Em 2018, o Banco Inter pagou R$1,5 milhão em danos morais, destinados a órgãos públicos que combatem crimes cibernéticos e a instituições de caridade, pelo vazamento de dados de seus correntistas (VENTURA, 2018); Em 2019, um único vazamento expôs dados de mais de 1,2 bilhão de pessoas (LOUBAK, 2019); Em janeiro de 2021, foi noticiado que o Brasil teve o maior vazamento de dados da sua história, expondo informações de mais de 220 milhões de brasileiros (RODRIGUES, 2021).

Com o advento da pandemia do COVID-19, esse cenário se fortificou. A CNN Brasil relata um aumento de 80% nas tentativas de fraudes digitais em bancos, sendo que 70% está vinculada a manipulação do usuário, para que forneça suas informações confidenciais. (CNN Brasil Business, 2020)

No entanto, o abuso quanto aos dados pessoais não para por ai. O capitalismo de vigilância[1], como é caracterizado por Zuboff (2020), se pauta na angariação indiscriminada e a sistematização dos dados pessoais em bancos de dados, criando um superávit informacional. Isso permite que a indústria digital utilize suas plataformas/aplicativos como ferramentas de controle e manipulação. O caso da Cambridge Analytica evidência como a manipulação dos dados está atrelada a viralização de fake news e a à vitória de Donald Trump, nas eleições americanas de 2016. (ANJOS, 2018).

Em que se pese o construção jurídica brasileira estar caminhando em prol de garantir mecanismos para a proteção desta matéria, por meio da promulgação da Lei nº 13.709/19, a Lei Geral de Proteção de Dados Pessoais (LGPD), assim como com a emblemática decisão monocrática da ADI 6387/DF, que reconhece a proteção de dados como um direito constitucional. Ainda há um caminho a percorrer para que este direito seja efetivamente expresso da Constituição Federal.

---

[1] Termo conceituado por Shoshana Zuboff como: “Uma nova ordem econômica que pauta na experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas; 2. Uma lógica econômica parasita, na qual a produção de bens e serviços está subordinada a uma nova arquitetura global de modificação comportamental; 3. Uma mutação desonesta do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade” (ZUBOFF, 2020, p. 03)

Diante do avançado progresso da União Europeia, em garantir a proteção dos dados pessoais, é que se justifica sua utilização como parâmetro neste trabalho. Por ter estabelecido um importante precedente nessa matéria através dos marcos normativos anteriormente mencionados, que tem influenciado diversos países construírem e fortificarem um rede de proteção ao titular de dados.

A justificativa deste trabalho se pauta na emergente necessidade de se garantir a proteção de dados pessoais, como um direito constitucionalmente expresso na Constituição Federal, como direito fundamental do cidadão brasileiro. Este estudo, divido em dois capítulos visará abordar, no capítulo um, a proteção de dados na era da sociedade da informação, fazendo um breve histórico deste direito e suas implicações no contexto da União Europeia e do Brasil. E no Capítulo dois, dialoga mais sobre o precedente criado pela UE, o caminho da reconhecimento de um direito fundamental a proteção de dados no Brasil, e os seus possíveis efeitos.

2 METODOLOGIA

Esta pesquisa visa a analisar a elevação da proteção de dados pessoais a um patamar constitucional, ou seja, busca-se explorar os possíveis impactos sociais e jurídicos de uma situação legislativa que ainda é hipotética. Para que seja possível realizar a discussão acerca do problema proposto, será feita uma pesquisa exploratória, a partir de levantamento bibliográfico, em que serão utilizados livros e artigos publicados por profissionais da área do direito e tecnologia que contribuíram para o tema. Além disso, uma análise de direito comparado é necessária, e aqui será realizada entre a legislação da União Europeia e do Brasil. Isso ocorre porque a cultura da proteção de dados é um assunto que tem ganhado destaque a somente após a criação da LGPD, porém, na UE tem-se já uma cultura da proteção da informação muito mais desenvolvida, vez que possui dispositivos legais a esse respeito desde 1995, ponto que será abordado adiante.

Será realizada uma abordagem qualitativa, que contará com análise de uma extensa bibliografia, composta de teses de mestrado e doutorado de profissionais relevantes na área, livros, artigos, matérias de jornais e revistas, sendo que todas essas fontes podem ser encontradas na internet. Cabe ressaltar, que este trabalho foi desenvolvido durante a pandemia do COVID-19, situação extraordinária, que levou a população a se manter em isolamento social, fato que ensejou a busca, exclusivamente, de referências bibliográficas disponíveis online.

3 CAPÍTULO I: A PROTEÇÃO DE DADOS PESSOAIS NA ERA DA SOCIEDADE DA INFORMAÇÃO

3.1 Privacidade x Proteção de Dados

Pioneiramente concebido por Samuel Warren e Louis Brandeis, em 1890, nos Estados Unidos, o direito à privacidade, continha a ideia do direito de "ser deixado só" (*right to be let alone*), pois as novas tecnologias da época já começavam a dar indícios de ameaças à personalidade (CUEVA, 2019, p. 08). Este é um direito que, embora tenha tido sua origem nos EUA, foi reconhecido pelos mais diversos ordenamentos jurídicos ao longo dos anos (CONSTITUTE PROJECT). Em 1948, este direito foi consagrado pela Declaração Universal de Direitos Humanos, e representa o poder do cidadão de não ter interferências em sua vida privada, familiar, no seu lar ou na sua correspondência, além de também proteger o direito à honra e à reputação.

É essencial destacar que isso demonstra a grande influência que existe entre jurisdições, mesmo que adotem diferentes tipos de escolas e sistemas jurídicos, principalmente, quando se trata de direitos fundamentais de seus cidadãos. Essa premissa é analisada por Paulo Ferreira da Cunha, que afirma: "evidentemente, há e haverá ainda certamente durante muito tempo constituições nacionais. Mas elas acabam já em grande medida por ser (ainda que os constituintes não se deem conta disso) como que « concretizações », para cada país, de uma constituição global" (CUNHA, 2010, p. 246).

Essa é uma alegação que ganha respaldo com o avanço da globalização, que está intimamente atrelada ao grande alcance que têm a comunicação e as mídias sociais. É inegável o impacto que esse alcance tem para a sociedade global. Direitos constitucionais nacionais apresentam cada vez mais, convergência e reconhecimento internacional, pois, certos direitos acabam sendo intrínsecos a todos os diferentes membros da sociedade.

> A globalização é também uma questão de comunicação. Os tempos actuais encontram-se dominados pela omnipresença dos media, e esta omnipresença – ubi commoda, ibi incommoda – torna, por um lado mais direitos mais conhecidos e mais re-conhecidos, e, por outro lado, contribui para a percepção do não-direito e mesmo anti-direito muito difundido também pelo Mundo. O audiovisual, aliás, em todas as suas fórmulas cada dia mais interactivas, poderá, no limite, mudar a percepção e mesmo a concepção do direito, que se quedou por muito tempo uma questão de escrita e de escuta (audição), por ausência do uso de outros sentidos, ou das suas metáforas (CUNHA, 2010, p. 250).

A internet e outras inteligências digitais fizeram emergir um novo paradigma social chamado de “a sociedade da informação”. Entre as suas características, destaca-se a informação como nova matéria prima, e consequentemente, como moeda de troca (CASTELLS, 1999, p. 108). O desenvolvimento das tecnologias da informação acarretou inúmeras mudanças na vida privada no contexto da coleta, uso e processamento de dados e informações pessoais, fazendo com que o direito à privacidade se abra para novos aspectos. Assim como a privacidade é um elemento fundamental para o desenvolvimento da livre personalidade do indivíduo (DONEDA, 2006, p. 6), a proteção de dados pessoais também vem a ser, pois está diretamente vinculada com alguns aspectos íntimos dos cidadãos. Contudo, mesmo que ambos os conceitos possam ter o mesmo viés de fundamentação, eles não se confundem: a proteção dos dados pessoais ultrapassa o âmbito do mero direito à privacidade (MENDES, 2008, p. 27).

> Nesse contexto de desenvolvimento da tecnologia de informação, o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos desafios impostos pelo avanço da técnica. Naturalmente, tanto o direito à privacidade, como a proteção de dados pessoais, fundamentam-se, em última medida, na proteção da personalidade e da dignidade do indivíduo. Pode-se dizer, no entanto, que a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito (MENDES, 2008, p. 26-27).

Assim, apesar de conterem valores similares, esses dois direitos se fazem divergentes em forma e conteúdo. O direito à privacidade compreende uma ideia de solitude, tendo um viés de interpretação mais individualista. Este olhar não se recai exclusivamente sob o direito a proteção de dados, muito porque ela deve ser compreendida como um fenômeno coletivo (MENDES, 2008, p. 27). Além disso, é um direito novo e ativo, que vem trazer uma imposição de um sistema de conformidades que objetiva a proteção da sociedade no âmbito da coleta e processamento de seus dados pessoais, sejam eles físicos ou digitais.

3.2 A Proteção De Dados Na União Europeia

3.2.1 Breve descrição evolutiva da proteção de dados na UE (direitos fundamentais, Diretiva 95/46/CE, GDPR)

A rápida evolução tecnológica e a globalização trouxeram novos desafios para a proteção de dados pessoais. A tecnologia permite fazer uso desses dados pessoais em escala sem precedentes. Cada vez mais, as pessoas disponibilizam suas informações pública e

globalmente. Essa transformação digital é vista com mais veemência a partir da década de 1990, e trouxe a crescente adoção de ferramentas digitais e tecnológicas que alteram os processos mais fundamentais de relações empresariais, sociais, bem como dos mais diversos segmentos de indústrias, que foram, irão ou estão sendo afetados por essa nova realidade digital (CÉSAR; ASPIS.; CHAVES, 2019).

Em decorrência desse cenário, a União Europeia estabeleceu a Diretiva 95/46/CE, a 'Diretiva de Proteção de Dados', que foi o primeiro ato legislativo adotado na UE sobre a proteção de dados pessoais (TZANOU, 2007, p. 16), que estabelece diretrizes para todos os países membros, de modo que cada um possa decidir como melhor adaptar e aplicar suas próprias leis por meio de um padrão mínimo de condutas de proteção. Este quadro acabou gerando diferentes níveis de proteção de dados em cada país europeu (IRIS, 2018, p. 07).

Posteriormente, a União Europeia passou a prever nos anos 2000, o direito à proteção de dados pessoais em sua Carta dos Direitos Fundamentais, explicitando os valores, que considera basilares à união. Nela, determina-se que o processamento de dados deve ser justo, com propósito específico, baseado no consentimento dos titulares ou em outra base legítima expressada por lei, garantindo aos titulares o direito de acesso e retificação, bem como a fiscalização por autoridade independente (ARANHA; FERREIRA, 2020).

Isto requereu um quadro de proteção de dados eficaz e mais coerente, apoiado por regulamento próprio. Seguindo esta lógica, em 2016 foi aprovado o Regulamento Geral de Proteção de Dados Pessoais (GDPR). Este, por sua vez, é um ato legislativo vinculado, que entrou em vigor em todos os países pertencentes simultaneamente, devendo ser aplicado em sua totalidade em toda União Europeia, imediatamente após sua entrada em vigor, não sendo seus termos negociáveis dentre os Estados Membros.

Em que se pese a Diretiva ter sido um marco introdutório importante, a GDPR veio a fim de ser mais eficaz e atualizada. Enquanto a Diretiva não permitia uma uniformidade dos direitos de seus titulares em toda a UE, e não fornecia proteção jurídica contra o tratamento inadequado de dados pessoais fora de sua dimensão territorial. O referido marco regulatório europeu tem um maior abrangência normativa, que intensifica as premissas já existentes e introduz novos requisitos de aplicação. Ela aborda o que antes era deficiente na Diretiva 95, como o critério de extraterritorialidade: pode-se aplicá-la independente de nacionalidade, ou local de residência do titular de dados. Ou seja, qualquer organização no mundo (pública ou

privada) que processe dados pessoais de pessoas naturais que se encontram na UE (ou que oferte seus serviços a clientes da UE), torna-se passível de ser afetada pelos dispositivos da GDPR. Logo, ela busca trazer um maior grau de especificidade e detalhamento, e busca a efetivação da proteção desse direito fundamental, frente a essa nova realidade de comércio de dados pessoais.

3.3 A proteção de dados no Brasil

3.3.1 Influência da UE no BR quanto à proteção de dados pessoais

Os dados pessoais de um indivíduo podem estar registrados tanto em meios físicos (como em papéis de contrato, fichas de consultório, e outros), quanto em meios digitais (informações em redes sociais, de compras online, cookies de navegação, etc). Todas essas informações pessoais têm grande valor de mercado, principalmente as virtuais. Estão se sobressaindo cada vez mais serviços que são sem custo, mas que utilizam de dados de usuários como produtos. Em sua obra, Shoshana Zuboff, ilustra esse sistema mercadológico com maestria, no qual demonstra que empresas como Google e Facebook produzem valor por meio da extração de dados pessoais de seus usuários, o que ela denomina de captura de superávit comportamental (ZUBOFF, 2020, p. 154-155). Esse cenário de angariação em massa de dados pessoais, pode acarretar uma situação maior de risco aos usuários, pois, quando na nuvem, a utilização indiscriminada desses dados, para fins econômicos, não se limita mais apenas ao espaço territorial.

Considerando essa realidade, da globalização da oferta de serviços digitais, emerge cada vez mais um mercado internacional interligado por empresas e usuários de diferentes jurisdições (IRIS, 2018, p. 22). Nesse contexto, a GDPR se destaca, pois, define um padrão, que deve ser interpretado como uma declaração do mercado internacional, que se faz presente em diversos países do globo (ALBRECHT, 2016, p. 288).

A GDPR pode ser aplicada também em organizações ou empresas de países externos à União Europeia, que coletem ou processem dados pessoais de cidadãos da Europa. Fica claro

em seu artigo 45, 1[2], que essa transferência de dados internacionais deve ser realizada com outros países que assegurem um nível de adequação de proteção de dados que a UE considera adequada. Assim, empresas, controladores de dados e os mais diversos governos do mundo estarão sob a influência para elevar seus padrões de proteção de dados a fim de que suas economias continuem tendo acesso ao mercado da União Europa. (ALBRECHT, 2016, p. 287). Essa situação acaba causando um efeito dominó, em que as empresas fora da UE se veem obrigadas a estar de acordo com a legislação europeia, para que sejam classificadas como adequadas aos padrões de segurança da informação e proteção de dados pessoais (regimes de adequação). Assim como o mercado privado também é afetado por essa obrigação, o que transpassa para os países que detém uma troca informacional de qualquer nível com a UE.

Sobre esse nível adequado de seguridade a respeito da proteção de dados, o Regulamento Europeu, ainda no art. 45, 1, indica critérios claros que devem ser observados. Além disso, há diretrizes que estipulam princípios e mecanismos de verificação dessa adequação, que foram elaboradas pelo Grupo de Trabalho do Artigo 29º, grupo que contém representantes de autoridades de proteção de dados pessoais de todos os estados membros da UE. (VIOLA, 2019 p. 10). Fica claro que a UE, através da GDPR, age como uma referência para outros países queiram emular, a fim de que possam estar presentes e relevantes na economia digital internacional.

O Brasil, por sua vez, até poucos anos atrás, possuía apenas dispositivos fragmentados sobre a proteção de dados pessoais, que não se faziam suficientes para atender as necessidades de uma crescente economia mundial. Em linhas mais basilares, a CF/88, em seu artigo 5º, incisos X e XII, visa proteger a privacidade, mas somente em seu inciso LXXII, que é diretamente abordado a proteção de informações pessoais, por meio da ação constitucional do *habeas data*. Este, por sua vez, visa assegurar, aos cidadãos, o conhecimento e retificação de

[2] O art. 45º da GDPR (Regulamento Geral sobre a Proteção de Dados 2016/679) disciplina in verbis "Transferências com base numa decisão de adequação. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica" (UNIÃO EUROPEIA, 2016).

informações pessoais, em registros e bancos de dados de entidades governamentais, ou de caráter público. Sobre este remédio constitucional, o POLIDO, F.B. e col. (2019), ressalta:

> Da mesma forma, a natureza das informações acessadas é muito específica: como instrumento de proteção de direitos da personalidade via remédio constitucional, o habeas data alcança apenas dados a serem conhecidos ou retificados, que se refiram à pessoa do impetrante, e destituídos de caráter genérico. Nesse sentido de análise, ele pressupõe uma espécie de autodeterminacão 'contida' de dados. (POLIDO, F.B. e col, 2019, p. 26).

Ainda, o Código de Defesa do Consumidor (CDC), em seus artigos 43[3] e 44[4], dispõe sobre banco de dados e cadastro dos consumidores. Esses dispositivos visam a proteger o consumidor em relação aos bancos de dados criados, em particular com escopo e proteção ao crédito. Por fim, a Lei nº 12.527/11, a Lei de Acesso à Informação (LAI) e o Marco Civil da Internet, Lei nº 12.965/14, são os aparatos legais que desempenhavam um papel mais importante em relação à proteção de dados. Todavia, essas proteções ainda não tratavam da matéria com a devida complexidade e importância (IRIS, 2019, p. 25-27).

Neste sentido, também a fim de estar em consonância com os novos padrões de segurança de proteção de dados impostos pela União Europeia, foi elaborada a Lei Geral de Proteção de Dados, Lei nº 13.709/19, em muitos pontos inspirada na Diretiva 95 e no Regulamento Geral sobre a Proteção de Dados da União Europeia (GUERRA, RIBAS, 2020, p. 78).

3.3.2 Relevância da proteção de dados no Brasil: LGPD e PEC 17/19.

O conceito de proteção de dados pessoais tem ganhado cada vez mais espaço de discussão no Brasil. Essa temática recebeu especial destaque nos últimos tempos, principalmente, com a aprovação da Lei Federal nº 13.709/18. A lei regula as atividades de

---

[3] O art. 43 do CDC brasileiro (Lei n.8.078, de 11 de setembro de 1990) disciplina in verbis "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes" (BRASIL, 1990).

[4] O art. 44 do CDC brasileiro (Lei n.8.078, de 11 de setembro de 1990) disciplina in verbis "Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor (BRASIL, 1990).

tratamento de dados pessoais, sejam físicos ou digitais, que até então não tinham tutela jurídica específica definida por legislação. Nota-se nesse sentido, uma ascensão a respeito da proteção jurídica de seus titulares, um avanço importante, visto que a internet está revolucionando os processos de captação e comercialização de dados pessoais (MATOS, 2004, p. 02) e faz-se necessário regulamentar o uso de dados especialmente no âmbito virtual.

Após dois anos de sua aprovação, a referida Lei entrou em vigor no mês de agosto de 2020. A Autoridade Nacional Proteção de Dados (ANPD) teve sua estrutura organizacional criada somente recentemente pelo Decreto nº 10.474, de 26 de agosto de 2020. Nota-se um avanço em termos normativos, porém, ainda há um grande caminho a ser percorrido na prática. Esse ainda é um campo de grande inconsistência, sem precedentes.

Em carta aberta ao Congresso Nacional enviada em agosto de 2020, a "Frente Empresarial em Defesa da LGPD e da Segurança Jurídica" - que reúne 70 associações e entidades, frisa que a criação da ANPD é essencial para que a LGPD funcione. Assim, como ressalta Rodolfo Fücher, presidente da ABES, em entrevista ao CanalTech (MACIEL, 2020), são dois anos desde que a Lei foi aprovada e há certa instabilidade em termos de adequação da administração pública e falta de aderência do setor privado. Essa insuficiência de direcionamento único pode trazer um caos no mercado, e por derradeiro, ocasionar grande insegurança jurídica.

Nota-se uma movimentação do mercado frente a esse cenário de instabilidade. Vez que essa é uma lei que exige uma mudança cultural, momento que exigiria conscientização dos mais diversos segmentos (institucional, comercial, até mesmo jurídico), e que para ser alcançada é necessária a ANPD. É nesse sentido, então, a intenção da carta aberta feita ao Congresso Nacional, realizada pelas associações.

Outro fator com extrema relevância nesse âmbito de discussão é a Proposta de Emenda Constitucional (PEC) 17/2019, que “altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais”. Essa emenda teve origem no Senado Federal e, como motivação, o autor Deputado João Roma argumenta que a proteção de dados pessoais é originária da evolução histórica da própria sociedade internacional, e também aponta sobre os diversos países que já adotam normas sobre o tema. Além disso, destaca as consequências da má utilização da tecnologia, e afirma que “se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria

sociedade, dando margem, inclusive, à concentração de mercados" (RELATÓRIO PEC n. 17/2019). Contudo, embora no Brasil este ainda seja um assunto que tem ganhado destaque somente recentemente, no âmbito da União Europeia, a proteção de dados já é reconhecida como um direito fundamental.

3.3.3 Das violações dos dados pessoais no âmbito privado e público

Nas últimas décadas, as tecnologias digitais tem progressivamente abraçado as empresas e organizações, trazendo uma mudança no comportamento do consumidor. Essa onda digital alimentou uma série de mudanças fundamentais na forma como as organizações produzem, vendem e atendem. (CAPGEMINI, 2011). Os mais variados segmentos de mercado necessitam do uso de dados atualmente, mas principalmente para o mercado publicitário essa é uma poderosa ferramenta, uma "mina de ouro" (BIONI, 2019, p. 59). Nessa relação de consumo, entre publicidade e consumidor, o titular carece de proteção, estando exposto a uma (hiper)vulnerabilidade (BIONI, 2019, p. 254).

Importante ressaltar, que não é a potencialidade do fluxo de informações que se faz perigosa no mundo digital, mas a forma como o mercado e as empresas se aproveitam desse grande fluxo de dados. Mendes (2008) destaca bem esse cenário:

> o cerne do problema não está situado na tecnologia. Afinal, a tecnologia não se encontra em um vácuo, devendo ser compreendida a partir do meio social, econômico e político em que está inserida. Isso porque a própria tecnologia é criada pela sociedade para atingir determinados fins e o grau de sua regulação é estabelecido pela sociedade que a criou (MENDES, 2008, p. 26).

A prova disso é a grande recorrência de ataques cibernéticos e a crescente violação de dados pessoais. O Big Data - é conceituado por Gartner - como um grande volume, variedade e velocidade de dados que demandam formas inovadoras e rentáveis de processamento da informação, para melhor percepção e tomada de decisão, que podem ser compostos desde dados irrelevantes à informações sigilosas ou sensíveis (GARTNER, s/d). Isso faz com que os dados tenham grande valor econômico, tanto para o setor público quanto para o privado. Nesse sentido, importante destacar que no ano de 2020, com o advento da pandemia mundial do vírus COVID-19, em que grande parte da sociedade se viu obrigada a migrar suas relações físicas para as digitais, houve crescente aumento de ataques cibernéticos. Fontes como o EU Observer

(NICOLÁS, 2020) e The Boston Globe (MCCLUSKEY, 2020) reportaram sobre em seus veículos, esse fenômeno.

Além disso, não é só no âmbito privado que esse assunto se faz relevante, já que a violabilidade dos direitos do usuário pela esfera pública também deve ser observada. O Estado é um grande coletor de dados pessoais, dos mais diversos segmentos. Existe hoje uma gama de aplicativos oficiais da administração pública federal, como o CNH Digital, Bolsa Família, FGTS, Meu INSS e Meu Imposto de Renda. Além desses, ainda existem aplicativos regionais, referentes às administrações estadual e municipal. Como exemplos, temos em São Paulo o aplicativo Nota Fiscal Paulista e o Metro SP; e em diversos municípios, inclusive em Governador Valadares/MG, tem-se o de Zona Azul, criado para substituir o cartão azul de estacionamento rotativo. Assim, a LGPD visa a proteger cidadãos também contra possíveis abusos nessa relação. Um bom exemplo disso é levantado por Oliveira:

> Pensemos na relação Fisco x contribuinte: anualmente, o Poder Público obtém dados relativos aos negócios e à vida privada do contribuinte, quando são entregues as declarações de renda à Receita Federal. Por exemplo, uma doação de dinheiro a determinada instituição religiosa pode demonstrar a convicção religiosa de um contribuinte pessoa física, sendo um dado sensível nos termos da lei (OLIVEIRA, 2020).

É inegável a expansão do uso de tecnologias da informação no Brasil e também dos seus riscos. Outro exemplo contundente desse fenômeno foi o uso do aplicativo da instituição financeira Caixa Econômica Federal, o Caixa Tem. Através dele, o Governo Federal realizou pagamentos de auxílio emergencial, conforme Lei nº 13.982/2020, e saque emergencial do FGTS, vide Medida Provisória nº 946/2020, para aqueles que cumpriam os respectivos requisitos, a fim de dar suporte financeiro à população para enfrentar os impactos decorrentes da pandemia do COVID-19.

Não obstante, essa modernização acarreta também riscos alarmantes. Os veículos de notícias Extra (CARDOSO, 2020), Estado de Minas (PEIXOTO; ADLER, 2020) e R7 (SARINGER, 2020) publicaram relatos de cidadãos que foram vítimas de fraudes digitais que tem ocorrido com o Caixa Tem: ao tentar acesso no aplicativo, se deparam com a informação de que o benefício emergencial já foi sacado por terceiros sem o seu consentimento. O Estado de Minas (PEIXOTO; ADLER, 2020) reportou ainda que o Ministério Público Federal está investigando as denúncias.

Esse é um sintoma da escassa cultura da segurança da informação tanto dos cidadãos brasileiros, quanto das instituições. Por parte da população, pois os fraudatários muitas vezes obtêm pistas e informações necessárias para realizar o golpe, por meio das redes sociais das próprias vítimas; e até mesmo por meio de ligações e emails falsos, em que são conduzidos a disponibilizar suas informações. Quanto à Caixa Econômica Federal, falta fortalecer a validação dos dados exigidos para acesso ao aplicativo, vez que somente são solicitados email, CPF, CEP, data de nascimento, número de telefone e nome completo. Esses são pontos relevantes levantados por Gabriel Ferreira da Conceição, o especialista em segurança e privacidade da Federação das Indústrias de Santa Catarina (Fiesc), em entrevista para o Estado de Minas (PEIXOTO; ADLER, 2020).

Outro aspecto importante dessa realidade digital diz respeito à angariação sistemática e em massa de dados pessoais em bancos de dados, ou Big Data, como já mencionado anteriormente. Para ilustrar esse cenário, a pesquisa realizada pela FGV/EAESP, que reuniu dados até junho de 2020, constata que a soma dos dispositivos digitais ativos no Brasil (computadores, notebooks, tablets e smartphones), chega aos 424 milhões, satisfazendo a média de 2 aparelhos por habitante (MEIRELLES, 2020). Embora seja cediço que não são todos os campos sociais e econômicos da população que tenham contato com essas tecnologias, também entende-se que o valor de mercado desses aparelhos digitais estão progressivamente se tornando mais acessíveis, em comparação com os anos antepassados.

Essa disseminação de aparelhos digitais tem como consequência uma onda crescente de usuários conectados à internet, fomentando o mercado do capitalismo de vigilância, como bem caracterizado por Zuboff (2020). Aqui, a diferença ocorre no caráter de utilização dos dados, vez que, isolados, não possuem tanto valor. No entanto, quando reunidos e organizados, traduzem uma série de comportamentos e sentimentos humanos que detêm um crescente valor comercial.

Essa é uma realidade em que a dinâmica competitiva de mercado leva a termos nossas vozes, personalidades e emoções, como fontes de matéria prima humana do excedente comportamental (ZUBOFF, 2020, p. 19), tem-se aí uma prática que põe em perigo diversos campos humanos e sociais. Há uma assimetria de informações, na qual os titulares dos dados são a parte vulnerável. Portanto, mediante esse cenário que surge, é imperativa a necessidade de haver regulações que objetivem mitigar os danos do uso indiscriminado dos dados pessoais.

Nesse sentido, diante dessa expansão tecnológica e digital, carece de atenção a proteção e disseminação da cultura da segurança da informação. Dessa forma, a fim de que a população esteja preparada para enfrentar as repercussões dessa nova demanda digital, e que também as instituições públicas e privadas estejam trabalhando para que possam fornecer um alto nível de eficácia na proteção da segurança digital de seus usuários, a conscientização é um dos passos importante para que ocorra a efetivação do direito a proteção de dados pessoais. Isso fortalece ainda mais a urgência de que esse direito deva ser garantido constitucionalmente pelo nosso ordenamento jurídico.

4 CAPÍTULO II: A PROTEÇÃO DE DADOS COMO UM DIREITO CONSTITUCIONAL NO BRASIL

4.1 O precedente mundial fomentado pela União Europeia: o reconhecimento da proteção de dados como direito fundamental

A União Europeia, por meio da GDPR – que embora tenha entrado em vigor somente em 2018, foi promulgada em 2016 –, permitiu a criação de um paradigma a respeito do direito à proteção de dados em diversos países. Ela motivou a já existente necessidade de concepção ou atualização das normas e leis de privacidade de dados ao redor do mundo. Como exemplos, tem-se na Islândia, a Lei de Proteção de Dados e Processamento de Dados Pessoais, de 2018; no Japão, a Lei de Proteção a Informação Pessoal, de 2017; e na Argentina, a Provisão 60 E/2016, que atualiza a Lei de Proteção de Dados Pessoais 25.326, de 2000. Nesse sentido, esses países tiveram como precedente as normas já estabelecidas pela UE. A GDPR vem servindo de orientadora para os demais países emergirem com sua própria cultura de proteção de dados, seja implementando leis similares à europeia em muitos aspectos, como no Brasil, seja apenas estabelecendo a proteção de dados normativamente em seus sistemas jurídicos.

Nota-se, portanto, um crescimento na preocupação em regulamentar o tratamento de dados pessoais, e consequente efetivação desses direitos. Essa conjuntura fomenta o debate acerca da imprescindibilidade de resguardo desses dados, seja contra o Estado, ou outros particulares. Assim como a GDPR tem representado um papel de precedente para a privacidade e proteção de dados ao redor do mundo, também pode-se considerar que o reconhecimento da proteção de dados como um direito fundamental, pela UE, age com um viés preambular de referência constitucional. Tal assunto se revela com tamanha intensidade, que a convergência das regras internacionais sobre proteção de dados é uma matéria já apontada por alguns estudiosos há mais de uma década. (DONEDA, 2019, p. 250)

Não obstante esse direito ter entrado para a Carta de Direitos Fundamentais somente em 2000, as discussões acerca da adoção de uma lista de direitos fundamentais da UE começaram na década de 1980 (TZANOU, 2007, p. 19).

> Parece, portanto, que a Carta fez muito mais do que simplesmente "reafirmar" a proteção de dados como um direito encontrado em outras fontes; a Carta introduziu um novo direito fundamental, embora com um conteúdo já familiar. O reconhecimento da proteção de dados como um direito fundamental na UE parece satisfazer amplamente os critérios empregados por estudiosos internacionais dos direitos humanos para a introdução de novos direitos

> humanos: a proteção de dados reflete valores sociais fundamentais na era do rápido avanço das novas tecnologias; é relevante há algum tempo nos sistemas nacionais, internacionais e transnacionais; é consistente com o corpo de leis existente no campo; alcançou um alto grau de consenso, pelo menos na UE; e dá origem a "direitos e obrigações identificáveis"(TZANOU, 2007, p. 20).

Mesmo diante do cenário social da era da informação, e do alcance do reconhecimento mundial da relevância da proteção de dados, a constitucionalização desse direito é ainda muito recente, e não consolidada no mundo contemporâneo, pelo menos, como um direito expressamente positivado. Perceptível, portanto, a relevância do ato da UE, em consagrar este direito de forma independente, intentando como precursora dos direitos e valores dos usuários, frente às novas demandas sociais.

Muito além de uma mera positivação de um direito, o direito à proteção de dados tem sido um preceito levantado mundialmente, decorrente de uma era em que a sociedade gera rastros digitais o tempo todo, voluntariamente. Dessa forma, se faz cada vez mais necessário controlar esse fluxo de informações, regrando o poder que ele proporciona sobre titulares de dados (em forma de marketing digital, controle comportamental, e demais influências que a internet tem sobre seus usuários). Sobretudo com a agilidade que os meios tecnológicos têm em relação à integralização e transformação dos dados pessoais em informação, paulatinamente a efetivação do direito à proteção de dados está à mercê da sua uniformização normativa internacional.

> Portanto, devido à facilidade de circulação da informação, não tardou para que se percebesse que uma efetiva proteção de dados pessoais dependeria de uma situação internacional favorável a uma coesão da matéria (DONEDA, 2019, p. 250).

4.2 A constitucionalização da proteção de dados no Brasil

4.2.1 Por que os atuais dispositivos constitucionais não são suficientes?

Como já levantado, a utilização de dados pessoais pelos mais diversos segmentos de empresas, de todos os portes, é inevitável hoje em dia, e muitas vezes crucial para seus modelos de negócio. O desenvolvimento da economia, da tecnologia e da inovação, exemplifica alguns dos setores que dependem do tratamento dos dados pessoais (FIESP, s/d, p. 7). Isso demanda do Estado o acompanhamento da crescente globalização e informatização das relações sociais, regulando o processamento desses dados contra práticas abusivas.

Atualmente, os titulares de dados pessoais têm seus direitos previstos pela Lei Federal nº 13.709/19 (LGPD), o que assegura que esse sistema seja resguardado com mecanismos de proteção e burocratização que tenham em vista a proteção dos seus usuários. Embora a promulgação desta lei infraconstitucional tenha sido um avanço significativo para nosso sistema jurídico, ainda assim é imprescindível discutir também a elevação desse direito a um patamar constitucional.

Para tanto, destaca-se que a matéria da proteção de dados pessoais aborda o tratamento das informações de seus titulares. Essa aparente tautologia, faz com que os dados sejam representações do próprio indivíduo, como por exemplo o número de inscrição no CPF, email, senha, dados bancários, cookies de navegação, entre muitos outros. Dados são, portanto, intrínsecos a qualquer indivíduo que esteja conectado à internet ou mesmo fora dela. Esse cenário exige, cada vez mais, uma proteção contundente aos usuários/indivíduos, que o garantam suas liberdades fundamentais. É em vista disso que este trabalho vem defender esse direito como autônomo e expressamente disposto na CF.

A fim de delimitar a pesquisa, será utilizado o conceito de Constituição por Inocêncio Mártires Coelho (2008, p. 202):

> Destarte, partimos da idéia de que a Constituição, embora sendo a chave de abóbada de todo o sistema jurídico - a lei suprema do país -, não é aquilo que o seu autor, o constituinte histórico, imaginou ou pretendeu que se fizesse com ela, mas o que, afinal, resultar da experiência da sua aplicação. Entregue aos seus destinatários - tanto os intérpretes/aplicadores oficiais quanto os cidadãos, que orientam a vida conforme os seus ditames -, **a Carta Política, mais do que uma obra feita, é um projeto em constante reformulação, um experimento em marcha ou, se preferirmos, um conjunto de materiais de construção, com que se poderão erguer monumentos diversos,** a depender da política constitucional que, a cada época, vier a presidir a sua utilização (MENDES, COLHO E BRANCO, 2008, p. 202). (grifou-se)

Embora a Constituição Federal tenha disposto entre seus direitos fundamentais, direitos que abordem indiretamente a proteção de dados pessoais, como a inviolabilidade da vida privada e da intimidade (ar. 5º, X, CF/88), a igualdade (art. 5º, I, CF/88), liberdade (art. 5º, CF/88), privacidade (art. 5º, X, CF/88), ainda assim não há disposto explicitamente este direito (MENDES, 2008, p. 119).

Em que se pese haver entre esses dispositivos um contexto parecido, o direito à privacidade e o direito à proteção de dados pessoais não se confundem. Como versa David Lyon, o direito à privacidade tem uma importância limitada nos contextos em que vigilância

constante está implicada nos modos de reprodução social, determinando a classificação da população e efetuando a discriminação de cidadãos (MENDES, 2008, p. 28)

Além da proteção de dados exercer a função de tutelar uma demanda social emergente, que carece de atenção jurisdicional, também trabalha como meio garantir outros direitos já previstos na CF, como da liberdade e igualdade.

> Ademais, a disciplina da proteção de dados pessoais envolve outra questão, que em certa medida era ignorada pelo direito à privacidade: o problema da igualdade. A igualdade se apresenta como um tema para essa disciplina, na medida em que a vigilância realizada por organismos privados ou estatais, a partir de informações obtidas em bancos de dados, pode acarretar a seleção e a classificação dos indivíduos, de modo a afetar expressivamente as suas oportunidades de vida na sociedade51. Desse modo, a tutela jurídica dos dados pessoais tem como uma de suas funções combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados, buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias (MENDES, 2008, p. 27-28).

Tendo em vista esse cenário, nota-se que os direitos previstos pelo texto constitucional não são suficientes para garantir a proteção efetiva e direta, diante da vasta e notória abrangência da violação dos dados pessoais, uma vez que seus conceitos são limitados frente às novas demandas da sociedade da informação.

No Brasil, há de se ponderar também o direcionamento de recentes julgados brasileiros: a Ação Direta de Inconstitucionalidade n. 6.389/DF, de maio de 2020, demonstra o um posicionamento relevante dos magistrados do Supremo Tribunal Federal. Tal julgado reivindicava a suspensão da Medida Provisória (MP) 954/2020, que possibilitava o compartilhamento de dados por empresas de telecomunicação prestadoras de serviço de Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE).

A decisão monocrática, proferida pela relatora Ministra Rosa Weber, não desconsidera o cenário excepcional de urgência implementado em decorrência da pandemia do COVID-19, e nem a necessidade de criação de políticas públicas para o seu enfrentamento. Todavia, ela reconhece que as medidas para o combate desse cenário não podem legitimar o atropelo de garantias fundamentais consagradas na Constituição (ADI n. 6.387/DF).

Ainda em sede do julgado, vale ressaltar, o caminho interpretativo do voto da Relatora foi o de evocar um direito fundamental à proteção de dados pessoais, por via do artigo 5º, XII, CF/88, que se refere à inviolabilidade do sigilo da correspondência e das comunicações. Nesse

sentido, há o reconhecimento de que a jurisdição constitucional, no parâmetro da proteção dos direitos fundamentais, deve estar permanentemente suscetível à evolução tecnológica e, ainda, que "a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo" (ADI n. 6.387/DF).

Doneda (2011, p. 104) levanta um posicionamento interessante acerca do que ele diz ser uma consciência do direito brasileiro a possibilidade de tratar desse tema de forma satisfatória, por meio de uma série de categorizações generalistas e abstratas. Para tanto, ele eleva a discussão para o patamar da potencialidade da utilização abusiva das informações pessoais em bancos de dados. Nessa seara da volumosa sistematização de dados pessoais, há um risco que vai além da discussão do caráter público ou particular, sigiloso ou não de uma dada informação.

> A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a corrente mencionada, gozariam de uma proteção mais tênue. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados (DONEDA, p. 106, 2011)

A ponderações apresentadas por Doneda – ainda em 2011 – são até hoje muito relevantes e norteiam um caminho temeroso, nessa alçada da incorporação e reconhecimento da proteção de dados pessoais ao ordenamento jurídico brasileiro. Nesse contexto, em que o cenário jurisprudencial atual se faz tão necessário de ser colocado em questão, também se encontra a extrema relevância da decisão da ADI n. 6.387/DF. Todavia, em que se pese a grande relevância do reconhecimento implícito da proteção de dados como direito constitucional, por meio do julgado acima referido, é necessário que haja uniformidade legislativa sobre o tema, pois seria excessivamente morosa uma construção apenas jurisprudencial de um direito fundamental constitucional de proteção de dados pessoais. Esse cenário de atraso e possível descaso com a positivação desse direito provocaria, além de insegurança jurídica, decisões heterogêneas na jurisdição brasileira.

Nessa perspectiva, a LGPD e os demais dispositivos legislativos que tratam sobre a matéria, detêm diplomas legais que podem ocasionar em eventuais contrapontos jurisprudenciais. Esse desalinho pode ocorrer, por exemplo, em relação à Lei nº 12.965/2014,

o Marco Civil da Internet, que constituiu um marco normativo com caráter geral, em função de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. O mesmo se verifica com a Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011, que objetiva regulamentar a obrigatoriedade da divulgação e transparência de dados de interesse coletivo ou individual em sites oficiais desses órgãos na internet.

Entre esses três marcos regulatórios, há um hiato temporal significativo quanto a suas promulgações, em comparação à LGPD, sendo 04 (quatro) anos, em relação ao MCI, e 06 (seis) anos, em relação à LAI. Isso leva a ponderar três pontos: (i) como tais leis foram pensadas e formuladas em contextos diferentes, poderiam ocasionar pontos dissonantes entre si, o que deve ser observado pelo julgador no momento de avaliar o caso concreto; (i) quanto à aplicação lei no tempo, tem-se que aos fatos que ocorrerem anteriormente à vigência da LGPD, aplicar-se-á o texto normativo disposto no MCI, bem como o CDC, com relação ao caráter de consumo entre os agente de tratamento e titulares localizados no Brasil. (LIMA, PEROLI, 2020, p. 96); (iii) quanto ao conteúdo da LGPD e da LAI, a grosso modo, respectivamente, tem-se uma lei que visa à proteção dos dados pessoais, ao passo que a outra objetiva a publicidade de informações pelo poder público. Nesta última hipótese, tem-se duas leis que podem se complementar positivamente, fortificando o direito do titular quanto à finalidade e à transparência do tratamento de seus dados pelo Estado, ou agir em contramão, abrindo prerrogativa para que o Estado restrinja informações que devam ser públicas.

Essas são brechas que demonstram como as respectivas leis têm que dialogar entre si, ficando, ao final, a critério da interpretação do julgador quanto à forma de sua aplicação. Como esse é um cenário que dependerá da análise de cada caso concreto, com suas peculiaridades e pormenores, importa destacar aqui, frente a tais possibilidades de heterogeneidade jurisprudencial, que deve prevalecer a interpretação que esteja atrelada aos direitos de personalidade do titular de dados. E como forma de basilar as interpretações dos magistrados, bem como elevar a hierarquia de proteção dos direitos do titular, a constitucionalização da proteção de dados pessoais asseguraria e resguardaria essa prevalência.

Ainda nessa seara de necessidade e ausência de garantias efetivas a esse direito no nosso ordenamento, o Código Civil de 2002 também é omisso quanto a sua disciplina, que

apenas versa sobre a inviolabilidade da vida privada da pessoa natural, em seu art. 21[5]. Dessa garantia, dois pontos resolutos se extraem: (i) esse dispositivo não é passível de abranger a complexidade que advém de um cidadão hiperconectado na sociedade tecnológica; e, (ii) tal qual demonstrado anteriormente, o titular sofre sistemáticas violações em sua vida privada, seja por meio de vazamentos, de fraude ou até mesmo de manipulação comportamental. Seja qual for a forma de violação, a consequência é sempre a mesma: a vida privada do titular está sempre sendo exposta e/ou violada.

> O Código Civil de 2002, por sua vez, destinou apenas o artigo 21 à disciplina do direito à privacidade, ignorando por completo a noção de proteção de dados pessoais, suas restrições frente a outros direitos e liberdades (e. g., liberdade de expressão e comunicação), e toda a complexidade que é própria da contemporânea sociedade da informação, hiperconectada, com acesso cada vez mais difuso às tecnologias da informação e da comunicação. Nas palavras de Anderson Schreiber, "[a] mera observação da vida cotidiana revela que, ao contrário da assertiva retumbante do art. 21, a vida privada da pessoa humana é violada sistematicamente" (IRIS, 2019, p. 27).

Isso posto, tem-se que ressaltar o dever de zelar pela consistência constitucional do marco normativo, é imposto ao Estado, bem como versa SARLET (2020):

> De particular relevância no caso brasileiro – justamente pela existência, além da nova LGPD e de outras leis que versam sobre o tema, é ter sempre presente que, independentemente de sua inclusão no texto da CF, impõe-se ao Estado, por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD) no tocante aos diplomas legais isoladamente considerados, mas também de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade (SARLET, 2020).

Conclui-se, portanto, que no contexto em que estamos inseridos, não há o que se falar em dados ou informações irrelevantes, frente ao alto valor que se extrai deles, muito menos na ausência de importância em tutelar os dados pessoais, que são matéria prima da informação. Não há dúvidas que a matéria de proteção de dados se mostra tema de grandes discussões e preocupações pelos mais diversos seguimentos sociais, políticos e econômicos. Portanto, é

---

[5] O art. 21º do CC brasileiro (Lei n. 10.406, de 10 de janeiro de 2002) disciplina in verbis "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

imperativo constatar a sua relevância para o direito brasileiro, quanto a se assegurar os direitos fundamentais inerentes aos seus titulares.

4.2.2 A proteção de dados como um direito fundamental no Brasil

Inicialmente, cumpre salientar a função de uma norma fundamental:

> [...] qualificaremos como norma fundamental aquela norma que, numa determinada comunidade política, unifica e confere validade às suas normas jurídicas, as quais, em razão e a partir dela, se organizam e/ou se estruturam em sistema (Gilmar Mendes, Inocêncio Coelho e Paulo Gonet Branco, 2008, p. 1).

As normas fundamentais, portanto, servem de alicerce para o pluralismo das demais normas jurídicas, constituindo à elas verdadeira validade e eficácia. O crivo constitucional é o ponto de partida e o ponto final dos direitos basilares que compõe o Estado Democrático de Direito.

O atual contexto social, econômico e tecnológico qual estamos inseridos, demonstra cada vez mais a hipervulnerabilidade do usuário/titular de dados, e esse é apenas um dos pontos que reforçam a necessidade da constitucionalização desse direito, a fim de complementar a tutela constitucional à privacidade, intimidade, igualdade, e demais garantias constitucionais. Isso promoveria maior segurança jurídica, bem como atenuaria a distância entre o direito nominal positivo e as novas demandas complexas do mundo contemporâneo.

Nesse sentido, diversas jurisdições internacionais já atenderam a essa demanda. A União Europeia, com seus dispositivos que resguardam o processamento e tratamento do uso dos dados pessoais, vem atuando como um preceito seguido por muitos países, inclusive o Brasil, que agora trata do assunto com intenção de elevá-lo a um direito previsto na Constituição (PEC n. 17/2019), o que na UE, já consta na Carta de Direitos Fundamentais desde 2000. Mas qual seria a relevância de constitucionalizar um direito que já está previsto infraconstitucionalmente?

BARROSO (2012) discursa sobre a relevância da constitucionalização de uma norma infraconstitucional, abordando a importância da filtragem constitucional:

> (...) a Constituição figura hoje no centro do sistema jurídico, de onde irradia sua força normativa, dotada de supremacia formal e material. Funciona, assim, não apenas como parâmetro de validade para a ordem infraconstitucional, mas

> também como vetor de interpretação de todas as normas do sistema (BARROSO, 2012, pag. 43).

Ou seja, uma norma constitucional vai além de ser apenas um disposto normativista, é também um guia, um mentor de interpretação para demais normas em todo o sistema jurídico brasileiro.

> O sistema jurídico deve proteger determinados direitos e valores, não apenas pelo eventual proveito que possam trazer a uma ou a algumas pessoas, mas pelo interesse geral da sociedade na sua satisfação. Tais normas constitucionais condicionam a interpretação de todos os ramos do direito, público ou privado, e vinculam os Poderes estatais (BARROSO, 2012, pag. 35).

Como já exposto, a Constituição Federal não é um conjunto de normas completamente estáticas, mas que devem acompanhar as mudanças sociais. Todavia, o reconhecimento e a consolidação de um novo direito fundamental não é tarefa meramente relativizada e indeliberada. Para tanto, deve haver um equilibro:

> Os estudiosos dos direitos humanos normalmente concordam que "não há razões inerentes" que explicam por que os novos direitos humanos não devem ser reconhecidos no direito internacional. Não obstante, o reconhecimento de novos direitos humanos deve ser capaz de alcançar um equilíbrio entre, por um lado, 'a necessidade de manter a integridade e credibilidade da tradição dos direitos humanos', e por outro lado, 'a necessidade adotar uma abordagem dinâmica que reflita plenamente as necessidades e perspectivas em mudança e responda ao surgimento de novas ameaças à dignidade e ao bem-estar humanos (TZANOU, 2007, p. 18).

A integridade e a credibilidade da tradição dos direitos humanos já foram abordadas em tópico anterior, assim como o diálogo da proteção de dados com os demais direitos fundamentais. No entanto, as demais garantias dispostas na CF ainda não são suficientes para atender essa complexa demanda que surge com as possibilidades de violações e abusos na utilização indiscriminada desses dados. Preenche-se, assim, o segundo critério elencado por Tzanou, que dispõe sobre a necessidade de uma abordagem dinâmica que consiga espelhar as mudanças que ocorram na sociedade, a fim de apresentar uma saída frente aos novos desafios que ameacem a dignidade e o bem-estar de seus membros.

Tanto a LGPD, quanto a ADI n. 6387/DF, são instrumentos importantes na construção de uma cultura de proteção dos dados pessoais. Contudo, apesar de uma ampla rede protetiva, esses são marcos que carregam as determinações históricas e impressões valorativas próprias de seu tempo histórico, em especial a LGPD, que “apresenta alguns problemas e falhas que

podem ter o condão de desnaturar os nobres objetivos que o legislador pretendeu implementar" (COSTA, FERREIRA, 2020).

Devido à relevância nacional e internacional dessa nova demanda, bem como o rumo que se tem tomado de reconhecimento deste direito como um direito fundamental, serão abordados os efeitos da eventual constitucionalização deste direito, dispostos em três pressupostos: (a) expansão da hierarquia de proteção do titular de dados; (b) garantia de manutenção da democracia; e (c) vedação ao retrocesso.

(a) Expansão da hierarquia de proteção do titular de dados

Primeiramente, será analisado a consequente e necessária expansão da hierarquia de proteção ao titular de dados, como hipótese da previsão desse direito expressamente disposto no rol de direitos fundamentais.

Aqui, não se trata da mera propriedade do titular sobre seus dados pessoais, mas sim, da possibilidade de controle, transparência e limitação do uso desses dados, sempre com a máxima de respeitar o titular, que é a quem esses dados pertencem e a quem eles devem estar em função.

> No contexto da proteção de dados é importante referir a lição da decisão do censo de que não é adequado falar em propriedade por parte do indivíduo dos dados relativos a sua pessoa. Ainda segundo Roßnagel, a concepção do ordenamento jurídico relativo à proteção de dados não se coaduna com a ideia de propriedade sobre os dados pessoais. O mais adequado é que se considere os dados relacionados a uma pessoa como resultado de uma observação social ou de um processo de comunicação social multirrelacional. Como modelos da realidade, teriam os dados pessoais sempre um autor e um objeto. Os dados têm relação com um objeto, mas também com o autor. Não podem ser associados exclusivamente ao objeto (MENKE, 2021).

Isso se fortalece frente às instituições e empresas públicas e privadas que se valem cada vez mais do uso dos dados pessoais em suas tecnologias, tendo como pretexto uma certa inevitabilidade tecnológica, com intuito de expandir seu legado de capitalismo de vigilância, o que foi ampliado sob pretextos e justificativas de segurança pública com o advento da pandemia do COVID-19. Essa inevitabilidade do uso da tecnologia é, na verdade, uma forma de camuflar as verdadeiras intenções por trás das práticas que visam algo mais significativo, como fomento da economia de vigilância. Zuboff (2020), alerta: "a tecnologia não é – e nunca deve ser – um fim em si mesmo, isolado da economia e da sociedade. Isso significa que a inevitabilidade tecnológica não existe" (ZUBOFF, 2020, p. 27).

A Coalização Direitos Na Rede, que reúne uma série de organizações acadêmicas e da sociedade civil em defesa dos direitos digitais, noticia que, na *vacatio legis* da LGPD, decisões foram tomadas “usando tecnologias opacas ao grande público, sem transparência nos processos e qualquer controle da sociedade”, sem o devido respaldo jurídico que a lei exige, no que diz respeito aos direitos pessoais dos titulares (LOURENÇO, 2020).

O que se almeja é uma maior garantia de proteção dos direitos do titular frente a eventuais colisões de direitos, como por exemplo, a direitos protetivos de mercado, direito à livre economia de mercado, direitos das partes em contrato firmado. Buscando a equidade entre dois lados desproporcionais, qual seja, o titular e o detentor dos dados de seus dados, visando sempre a proteção a parte mais carente da relação (titular).

> Mas a importância da proteção de dados não se esgota na sua faceta de pressuposto funcional da comunicação democrática. Ao mesmo tempo é pressuposto de uma "autodeterminada decisão contratual" (selbstbestimmte Vertragsentscheidung) e, por conseguinte, pressuposto funcional de uma livre economia de mercado (Funktionsbedingung einer freien Marktwirtschaft), no sentido de que uma decisão livre dos contratantes de um modo geral, e dos consumidores em particular, uma decisão ausente de manipulações, só é possível quando o fornecedor em potencial só tenha conhecimento dos dados fornecidos pelo próprio consumidor, ou que, no mínimo, este conheça as informações relativas a sua pessoa que o fornecedor disponha (MENKE, 2021).

Sem a devida proteção, os titulares de dados estão a mercê da “boa vontade do mercado”, em utilizarem seus dados com a devida ética. No entanto, esse cenário utópico não condiz com a realidade. São cada vez mais recorrentes as notícias sobre vazamento de dados, em proporções igualmente maiores. Foi noticiado que em fevereiro de 2021, o Brasil teve o maior vazamento de dados da sua história, com dados de 220 milhões de brasileiros, contando com RG, CPF, título de eleitor, endereço, pontuação de crédito, escolaridade, renda, salário etc. Devido ao caráter de algumas das informações vazadas, como as pontuações de créditos e as classificações segundo modelos preditivos do comportamento do consumidor, suspeita-se a Serasa Experiance como a provável fonte desses dados, muito embora a empresa tenha negado tal alegação. Essa exposição carrega um grande potencial lesivo, ao colocar os titulares em risco de fraudes de identidade, até crimes como roubo e sequestro (RODRIGUES, 2021). Esse cenário corriqueiro e assombroso requer que o titular tenha como direito mínimo a máxima eficácia de proteção normativa possível no ordenamento brasileiro.

A constitucionalização da proteção de dados pessoais elevaria o patamar de proteção do titular, garantindo um sistema jurídico que o teria como pressuposto basilar para dirimir quaisquer controvérsias, bem como máxima eficácia frente a eventuais violações.

(b) Garantia de manutenção da democracia

O caso Cambridge Analytica expôs como processamento e tratamento de dados pessoais ocorre no contexto de estratégias eleitorais. A empresa angariou informações privadas de mais de 87 milhões de usuários, sem consentimento, por meio de uma aplicação acessória à plataforma do Facebook, que permitia o direcionamento de publicidade política especialmente adaptada, bem como a elaboração de informes detalhados acerca das preferências comportamentais de seus participantes. O objetivo foi o de promover anúncios especialmente direcionados e customizados, em benefício da campanha do ex-presidente eleito dos EUA, Donald Trump (ANJOS, 2018).

A coleta e o uso indiscriminado dos dados pessoais possibilitam a formação de um insumo informacional para que campanhas e candidatos conheçam os perfis comportamentais dos eleitorados. O poder dessas informações permite a seleção de nichos específicos de eleitores para que campanhas de candidatos planejem com mais eficiência os seus recursos, bem como construam um maior poder de convencimento sobre eles. Ao entender os comportamentos de seus eleitores, as campanhas podem tomar decisões mais assertivas sobre suas estratégias com objetivo ganhar a confiança e os votos do eleitorado. Tudo isso é realizado por meio da coleta e análise de dados como curtidas em redes sociais ou até endereço/localização do usuário, que permitem identificar as regiões em que estão, os seus interesses e as suas afinidades (MASSARO e col., 2020, p. 06).

> Além disso, a depender de como essas ferramentas e capacidades de uso de dados pessoais são incorporadas às estratégias de campanha, elas podem fomentar divisões e polarização no eleitorado, além de possibilitar que mensagens contraditórias sejam veiculadas de modo a enganar o eleitor e reduzir a transparência sobre a totalidade das campanhas (MASSARO e col., 2020, p. 06).

A LGPD se estende ao contexto eleitoral, agindo como uma importante mediadora frente a esse cenário, na medida em que fornece princípios para tratamento dos dados dos

titulares, garantindo que sejam esses processos sejam dotados de transparência, minimização, finalidade, entre outros.

No entanto, a criação de mecanismos que visem a uma maior proteção a esse contexto das eleições não deve se resumir a isso. A constitucionalização da proteção de dados forneceria um maior grau de segurança a esses processos eleitorais e garantiria uma elevada proteção a formação do processo democrático.

Em sede do recente julgado da ADI n. 6387/DF, o Ministro Fux destaca a importância da proteção de dados no âmbito da manutenção da democracia:

> Não por acaso, o Ministro Luiz Fux destacou a centralidade do tema da proteção de dados em face da manutenção da democracia, uma vez que dados aparentemente "insignificantes" podem ser utilizados até mesmo para distorcer processos eleitorais. "[o] recente escândalo envolvendo a Cambridge Analytica revelou como modelos de negócios são rentabilizados pela análise de dados e alertou como seu uso indevido pode lesar (...) a própria democracia (BIONI, col., 2020).

Apesar desse quadro de insegurança, cabe destacar que há um cenário em que, respeitados os princípios de proteção e uso ético do tratamento dos dados, abre-se a possibilidade de que esse tratamento seja usado em benefício dos processos eleitorais. Ao serem respeitadas as regras de proteção de dados pessoais, por meio de uma comunicação mais transparente, dirimiam-se eventuais discrepâncias de informações, possibilitando uma maior igualdade de chances entre candidaturas. (MASSARO e col., 2020, p. 7-8). Esse cenário só seria possível se fossem enfrentadas as brechas de violações, viabilizando uma real legitimidade para a proteção de dados.

Desta forma, os esforços em benefício do reconhecimento de um direito fundamental à proteção de dados pessoais, são também uma ponte para a consolidação do Estado democrático de direito.

(c) Vedação ao retrocesso

Por fim, outro eixo argumentativo desse cenário visa ao robustecimento de um direito que ainda está nos primórdios de seu desenvolvimento, e representa um arcabouço repleto de inseguranças jurídicas e de violações sistemáticas. Visa-se possibilitar ao titular a efetividade e a eficácia dos direitos que já lhe são assegurados pela ordem jurídica constitucional.

Completar o rol dos direitos fundamentais do cidadão com a proteção de dados pessoais, garantiria ao titular um crivo de controle de constitucionalidade de eventuais dispositivos legislativos que possam ofender a matéria. Esta, por sua vez, não engloba apenas os dados pessoais em si, mas também assegura que os demais subconceitos inseridos em sua interpretação sejam observados, como a minimização, a finalidade, a transparência, a autodeterminação informativa, e a demais repercussões intrínsecas à proteção dos dados pessoais.

Tendo em vista a vagância das proteções constitucionais ora vigentes, frente à complexidade das novas dinâmicas sociais, eficaz seria centralizar as atenções em fortificar os direitos fundamentais do titular. Para que isso ocorra, é necessária a complementação dessas garantias, prevendo a proteção de dados pessoais no rol de direitos fundamentais do cidadão. Essa seria uma forma de prevenir medidas de cunho retrocessivo, de condutas que conotem a supressão ou a redução dos direitos de personalidade, e de atuações que tenham como escopo a utilização tanto mercadológica indiscriminada dos dados pessoais, quanto abusiva pelo Estado e seus agentes.

A busca da vedação ao retrocesso diz respeito a ter um olhar para o futuro, sem esquecer do que já foi conquistado, fortificando os mecanismos de proteção ao indivíduo e a coletividade, tendo em vista as novas demandas que surgem. Além disso, esse conceito busca tutelar os espaços vazios que emergem, que possibilitam a invasão e violação de direitos já conquistados anteriormente, suprindo as vagâncias na lei através da tutela máxima do Estado, pois, dessa forma, as normas jurídicas que existem e possam vir a existir estarão sujeitas a um controle de constitucionalidade que assegure a prevalência da integralidade dos direitos fundamentais.

A autonomia desse direito constitucionalmente expresso e desvinculado apenas da interpretação limitante dos outras dispositivos fundamentais é um preceito essencial e mais que necessário para que se possam efetivar uma verdadeira garantia aos direitos de personalidade dos indivíduos titulares de dados pessoais.

5 CONCLUSÃO

Em um mundo cada vez mais informatizado, em que as barreiras territoriais já não são mais entraves ao desenvolvimento dos mais diversos mercados, há grande risco envolvendo tanto o tratamento dos dados pessoais em seu sentido mais pormenorizado, quanto com a sua crescente utilização massiva, sistematizada e indiscriminada.

São crescentes os episódios de violação e vazamento desses dados, materializando, portanto, a fragilidade do sistema em estamos inseridos, nessa relação entre dado pessoal e mercado (público ou privado).

Com a evolução da sociedade e a crescente digitalização das relações sociais, emergiu também a demanda de um novo direito: o da proteção de dados pessoais. Apesar de haver a possibilidade de uma interpretação extensiva de direitos constitucionais já garantidos, como a privacidade e a intimidade, este direito, por sua vez, deveria ser observado expressamente como uma norma fundamental, como é defendido neste trabalho.

A dimensão alcançada por essa nova demanda jurídica e social é revestida por uma escassez de precedentes. Há um progressivo movimento internacional em torno da construção normativa e cultural da proteção de dados pessoais, buscando harmonização e a segurança de um nível mínimo de proteção. O Brasil tem caminhado em conjunto com esse movimento legislativo, com o objetivo de se tornar um país com níveis mínimos de adequação à proteção de dados, segundo os padrões internacionais.

Nessa esfera da normatização da proteção de dados pessoais, a União Europeia tornou-se uma referência por ter implementando de maneira percursora em seu sistema jurídico garantias a essa matéria. A princípio, com a Diretiva 95/46/CE, foi substituída pela Regulamento Geral sobre a Proteção de Dados (GDPR), de 2016, bem como o bloco tem garantido a proteção de dados como um direito fundamental desde os anos 2000.

No Brasil, a Lei Geral de Proteção de Dados consiste em um marco normativo substancial, muito inspirado nos precedentes construídos pela União Europeia. Ela regula o tratamento de dados pessoais, tanto nos meios digitais quanto nos físicos, fornecendo uma proteção até então inédita em no nosso ordenamento, impondo princípios basilares para esses tratamentos, como o da finalidade, o da minimização, o da transparência, entre outros. Por fim, a LGPD também previu e possibilitou a criação da Autoridade Nacional de Proteção de Dados,

um importante órgão regulador que irá direcionar os rumos interpretativas e executivos dessa lei.

Ainda no sentido de caminhar para uma nação mais atenta aos direitos dos titulares de dados, tramita no Senado a PEC n. 17/2019, que prevê a inclusão da matéria da proteção de dados pessoais entre os direitos e garantias fundamentais do texto constitucional. A proposta também fixa a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais no país.

Em sede da ADI n. 6387/DF, a jurisprudência do Supremo Tribunal Federal já reconheceu a proteção de dados pessoais como um direito fundamental. Esse é um cenário de incorporação gradual da constitucionalização da proteção de dados no ordenamento jurídico brasileiro. Assim, estamos caminhando para uma chave interpretativa que busca a efetiva autonomia jurídica deste direito.

Toda a movimentação quanto a esse tema é extremamente necessária, frente às sistemáticas violações que titulares têm sofrido no país, seja de forma individual, por meio de fraudes, seja em um contexto maior, por meio do uso indiscriminado de informações para manipulações sociais, com objetivos econômicos, políticos, financeiros etc.

Em vista disso é que a constitucionalização da proteção de dados pessoais se faz cada vez mais inevitável. E a previsão desse direito no rol dos direitos fundamentais do cidadão brasileiro possibilitaria algumas ressalvas, entre elas, a expansão da hierarquia de proteção do titular de dados no ordenamento jurídico nacional, a garantia da manutenção da democracia, e a vedação ao retrocesso.

Por fim, reconhecer a proteção de dados pessoais como um direito fundamental expressamente positivado na Constituição Federal, representaria um subsídio hierárquico jurídico maior contra as violações que o titular de dados tem enfrentando, bem como demonstraria à sociedade uma preocupação em relação aos seus cidadãos, fomentando uma embrionária cultura da proteção de dados no país.

REFERÊNCIAS

ALBRECHT, Jan. P. **Como a GDPR vai mudar o mundo**. Proteção de Dados Europeia. Revisão, v. 2, n. 3, 2016.

ANJOS, Lucas. **Privacidade no Facebook: o que aprender com a Cambridge Analytica**. IRIS. 19 mar 2018. Disponível em < https://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/ >. Acesso em 03 de março de 2021.

ARANHA, E.; FERREIRA, L. M. T. **O direito fundamental à proteção de dados e a importância da proposta de emenda constitucional nº 17/2019**. 24 jan. 2020. Disponível em <https://politica.estadao.com.br/blogs/fausto-macedo/o-direito-fundamental-a-protecao-de-dados-e-a-importancia-da-proposta-de-emenda-constitucional-no-17-2019/> Acesso em 30 de julho de 2020

BARROSO, Luís Roberto. A constitucionalização do direito e suas repercussões no âmbito administrativo**.** In: ARAGÃO, Alexandre Santos de; MARQUES NETO, Floriano de Azevedo (Coord.). **Direito administrativo e seus novos paradigmas**. Belo Horizonte: Fórum, 2012. p. 31-63. ISBN 978-85-7700-186-6

BIONI, Bruno R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; JR, Otavio Luiz Rodrigues; SARLET, Wolfgang. **Tratado de Proteção de Dados Pessoais**. Editora Forense ltda. 2020. Edição do Kindle.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 23ª edição. Editora Malheiros. 2008.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 01 de fevereiro de 2021.

BRASIL**. Lei de Acesso a Informação, Lei nº. 12.2965**, de 18 novembro 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 01 fev. 2021.

BRASIL**. Lei Geral de Proteção de Dados, Lei nº. 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 01 fev. 2021.

BRASIL. **Lei n.º 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 01 de fevereiro de 2021.

BRASIL**. Marco Civil da Internet, Lei nº. 12.2965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <

http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 01 fev. 2021.

BRASÍLIA (DF). Senado Federal. **Proposta de Emenda Constitucional nº 17, de 2019.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Tramitação: Especial (Art. 202 c/c 191, I, RICD) Proposição Sujeita à Apreciação do Plenário. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2210757>. Acesso em 10 set 2020.

CARDOSO, Letycia. **Fraudes no Caixa Tem continuam, e beneficiários relatam roubo de FGTS emergencial**. Portal Extra. Globo. 17 out 2020. Disponível em <https://extra.globo.com/noticias/economia/fraudes-no-caixa-tem-continuam-beneficiarios-relatam-roubo-de-fgts-emergencial-rv1-1-24697212.html> Acesso em: 22 out. 2020.

CASTELLS, Manuel. **A sociedade em rede; a era da informação: economia, sociedade e cultura**; v.1. Tradução: Roneide Venâncio Majer; atualização para 6º edição: Jussara Simões. São Paulo: Paz e Terra, 1999.

CÉSAR, A. C. M; ASPIS, F. L.; CHAVES, L. F. P. **GDPR: 1 ano de vida. Lições aprendidas e influências da lei europeia**. 24 jun de 2019. Disponível em: <https://migalhas.uol.com.br/depeso/304735/gdpr-1-ano-de-vida>. Acesso em 02 de agos. de 2020.

CNN Brasil Business. **Roubo de dados bancários aumenta 80% durante pandemia; saiba como se proteger**. CNN Brasil. São Paulo. 21 out 2020. Disponível em: <https://www.cnnbrasil.com.br/business/2020/10/21/roubo-de-dados-bancarios-aumenta-80-durante-pandemia-saiba-como-se-proteger>. Acesso em 05 mar 2021.

COSTA, Leonardo P. S.; FERREIRA, Marcus Vinicius V.. **Lei Geral de Proteção de Dados: externalidades negativas não projetadas**. Consultor Jurídico. 6 de dezembro de 2020. Disponível em: <https://www.conjur.com.br/2020-dez-06/direito-consumidor-lgpd-externalidades-negativas >. Acesso em 24 fev 2021.

CUEVA, Ricardo Villas Bôas. **A insuficiente proteção de dados pessoais no Brasil**. Revista de Justiça e Cidadania. Ed. 231. Ano 20. Rio de Janeiro/RJ. Nov. 2019. ISBN 1807-779x

CUNHA, Paulo Ferreira da. **Do constitucionalismo global.** Revista Brasileira de Direito Constitucional. Vol. 15. p. 245-255. jan-jul. 2010. Disponível em: <http://www. esdc.com.br/RBDC/RBDC-15/RBDC-15-245-Paulo_Ferreira_da_Cunha_(Do_ Constitucionalismo_Global).pdf>.

DONEDA, Danilo. **A Proteção Dos Dados Pessoais Como Um Direito Fundamental.** Revista Espaço Jurídico. v. 12, n. 2, p. 91-108, jul./dez. 2011. Joaçaba/SC.

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

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

FERREIRA, Marcus Vinicius Vita; COSTA, Leonardo P. Santos. **Lei Geral de Proteção de Dados: externalidades negativas não projetadas**. In: Consultor Jurídico, em 06/12/2020.

Disponível em <https://www.conjur.com.br/2020-dez-06/direito-consumidor-lgpd-externalidades-negativas>. Acesso em 15 fev. 2021.

GARTNER GLOSSÁRIO. Disponível em: <http://www.gartner.com/it-glossary/bigdata/>. Acesso em 04 ago. 2020.

Koch, Richie. **LGPD: a versão brasileira do regulamento europeu.** SERPRO. GOV. 12 set 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais>. Acesso em 05 de agosto de 2020.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. **A aplicação da Lei Geral de Proteção de Dados do Brasil no tempo e no espaço**. In: LIMA, Cíntia Rosa Pereira de (org.). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 69-100.

LOUBAK, Ana Letícia. **Vazamento de dados expõe telefone e e-mail de 1,2 bilhão de pessoas**. TechTudo. Tecnologia. Globo. 27 nov 2019. Disponível em: <https://www.techtudo.com.br/noticias/2019/11/vazamento-de-dados-expoe-telefone-e-e-mail-de-12-bilhao-de-pessoas.ghtml>. Acesso em 05 mar 2021.

LOURENÇO, Enio. **A Vigilância Massiva Será O Legado Da Pandemia?.** Coalização Direitos na Rede. 23 DE SETEMBRO DE 2020. Disponível em: < https://direitosnarede.org.br/2020/09/23/a-vigilancia-massiva-sera-o-legado-da-pandemia/> Acesso em 23 de fev. de 2021.

MACIEL, R. **Bolsonaro sanciona e LGPD entra em vigor nesta sexta-feira. Mas com brechas**. CanalTech. 18 set. 2020. Disponível em: < https://canaltech.com.br/legislacao/lgpd-entra-em-vigor-brasil-171732/>. Acesso em 02 de agos. de 2020.

MATOS, Tiago Farina. **Comércio de dados pessoais, privacidade e Internet**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 9, n. 427, 7 set. 2004. Disponível em: https://jus.com.br/artigos/5667. Acesso em: 16 jul. 2020.

MCCLUSKEY, P. D. **À medida que os ataques cibernéticos aumentam, médicos e hospitais lutam para atualizar as medidas de segurança: o risco de ataques de malware pode estar aumentando durante a pandemia de coronavírus**. 19 abr. 2020. Disponível em: <https://www.bostonglobe.com/2020/04/19/business/cyber-attacks-grow-doctors-hospitals-struggle-update-security-measures/>. Acesso em 02 de agos. de 2020.

MEIRELLES, F. **Pesquisa anual do uso de TI**. 31ª Pesquisa Anual do FGVcia: Uso da TI nas Empresas. 2020. FGV/EAESP. Disponível em <https://eaesp.fgv.br/ensinoeconhecimento/centros/cia/pesquisa.> Acesso em 19 fev 2021.

MENDES, Gilmar; COLEHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2ª ed. São Paulo: Editora Saraiva, 2008.

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

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. MIGALHAS. 30 out 2020. Disponível em < https://migalhas.uol.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa>. Acesso em 10 fev 2021.

NICOLÁS, E. S. **O crime cibernético aumenta durante a pandemia de coronavírus**. 25 mar. 2020. Disponível em: <https://euobserver.com/coronavirus/147869>. Acesso em 02 de agos. de 2020.

OLIVEIRA, Gabriel Prado Souza de. **Sigilo de Dados no Brasil: da Previsão Constitucional à Nova Lei Geral De Proteção De Dados Pessoais**. Portal Âmbito Jurídico. 01 jan 2020. Disponível em <https://ambitojuridico.com.br/cadernos/direito-constitucional/sigilo-de-dados-no-brasil-da-previsao-constitucional-a-nova-lei-geral-de-protecao-de-dados-pessoais/>. Acesso em 31 ago 2020

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Assembleia Geral da ONU. 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 20 de out 2020..

PEIXOTO, G.; ADLER, M. **Golpistas usam aplicativo da Caixa para roubar FGTS emergencial**. 28 nov. 2020. Disponível em <https://www.em.com.br/app/noticia/economia/2020/09/28/internas_economia,1189404/golpistas-usam-aplicativo-da-caixa-para-roubar-fgts-emergencial.shtml> Acesso em: 22 out. 2020

PEIXOTO, G.; ADLER, M. **Ministério Público Federal analisa denúncia de fraude no FGTS emergencial em BH**. 02 out 2020. Disponível em (https://www.em.com.br/app/noticia/economia/2020/10/02/internas_economia,1191196/mpf-analisa-denuncia-de-fraude-no-fgts-emergencial-em-bh.shtml> Acesso em: 22 out. 2020

Pesquisa:"Right to privacy" em Constitute". Disponível em: <constituteproject.org>. Acessado em 05 de Agosto de 2020.

POLIDO, F.B. e col. **GDPR e suas Repercussões no Direito Brasileiro: primeiras impressões de análise comparativa**. Instituto de Referência em Internet e Sociedade. Belo Horizonte, 2018.

RIBAS, B. H. de O. & GUERRA, C. C.. **O Impacto Do Regulamento Geral De Proteção De Dados Pessoais Da União Europeia No Brasil**. Revista Governança e Direitos Fundamentais. Editora: Instituto Iberoamericano de Estudios Jurídicos. Espanha, 2020.

RODRIGUES, Gustavo.**O Brasil teve o maior vazamento de dados de sua história. E agora?.** IRIS. 9 fev 2021. Disponível em < https://irisbh.com.br/o-brasil-teve-o-maior-vazamento-de-dados-de-sua-historia-e-agora/#:~:text=No%20dia%2022%20de%20janeiro,vidas%20publicizadas%20para%20download%20na>. Acesso em 24 fev 2021.

ROHR, Altieres. **Vazamento de dados do Yahoo: veja o que você precisa saber.** Segurança Digita. G1. 23 set. 2016. Disponível em: <g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-de-dados-do-yahoo-veja-o-que-voce-precisa-saber.html>. Acesso em 05 de mar 2021.

SARINGER, Giuliana. **Fraudes no Caixa Tem continuam, e beneficiários relatam roubo de FGTS emergencial.** 17 out 2020. Disponível em < https://noticias.r7.com/economia/golpe-tira-saque-emergencial-do-fgts-da-conta-de-quem-tem-direito-17102020> Acesso em: 22 out. 2020

SARLET, I. W. **Precisamos da previsão de um direito fundamental à proteção de dados no texto da CF?**. 04 set. 2020. Disponível em: <https://www.conjur.com.br/2020-set-04/direitos-

fundamentais-precisamos-previsao-direito-fundamental-protecao-dados-cf>. Acesso em 17 jan. 2021.

SUPREMO TRIBUNAL FEDERAL. **ADI 6387/DF**. Relatora Ministra Rosa Weber. Disponível em < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em 20 fev 2021.

TZANOU , Maria. **O Direito Fundamental à Proteção de Dados: O Valor Normativo no Contexto da Vigilância Antiterrorismo (Estudos Modernos de Direito Europeu**). Portland, Oregon: Hart Publishing, 2017. v. 71.

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados, nº 2016/679** do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados**)**. Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/uri=CELEX:32016R0679&from=PT>. Acesso em: 01 fev. 2021.

VENTURA, Felipe. **Banco Inter paga R$ 1,5 milhão e encerra processo sobre vazamento de dados**. Techboblog. 19 dez 2018. Disponível em: <tecnoblog.net/272056/banco-inter-acordo-mpdft/>. Acesso em 05 mar 2021.

VIOLA, Mario. **Transferência de Dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira**. ITIS Rio. Rio de Janeiro. Novembro, 2019.

WARREN, Samuel D., BRANDEIS, Louis D. **O Direito a Privacidad**e. Revisão de Direito de Harvard, Vol. 4, no. 5. Dez., 1890. Disponível em: <https://bit.ly/2USNUNJ>. Acesso em 20 de julho de 2020.

ZUBOFF, S. A **Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira de poder**. Tradução: Goerge Schlesinger. 1º Ed. Intrínseca. Rio de Janeiro, 2020.