A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos: linhas introdutórias à dinâmica dos dados, do *Big Data*, da economia de dados e da discriminação algorítmica*

Mônia Clarissa Hennig LEAL**

Lucas Moreschi PAULO***

RESUMO: Por meio da revisão bibliográfica, utilizando-se do método dedutivo, trata-se de estudo acerca da tutela do usuário, complementada pela Lei Geral de Proteção de Dados, mas ainda deficitária a partir do renovado paradigma da discriminação algorítmica. Nesse contexto, busca-se estabelecer uma linha racional entre o construtivismo histórico da concretização de um direito à proteção dos dados, a estrutura da nova lei, bem como da atual realidade, para se conceber as atuais necessidades de tutela do ser-usuário-titular dos dados, enquanto sujeito de direitos e vulnerável. Assim, busca-se levantar questionamentos críticos para contribuir com a construção de respostas ao novo paradigma protetivo.

PALAVRAS-CHAVE: Discriminação algorítmica; direitos fundamentais; Lei Geral de Proteção de Dados; sociedade da informação; vulnerabilidade.

TITLE: *The General Data Protection Law, the Vulnerability of Internet Users, and the Protection of Rights: Introductory Lines to the Dynamics of Data, Big Data, Data Economy, and Algorithmic Discrimination*

* Este artigo é resultante das atividades do projeto de pesquisa "'Teoria da essencialidade' (Wesentlichkeitstheorie) e discriminação algorítmica: standards protetivos em face do Supremo Tribunal Federal e da Corte IDH – proposta de parâmetros de controle", financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq (Bolsa de Produtividade em Pesquisa – Processo 309115/2021-3). A pesquisa é vinculada ao Grupo de Pesquisa "Jurisdição Constitucional aberta" (CNPq) e desenvolvida junto ao Centro Integrado de Estudos e Pesquisas em Políticas Públicas – CIEPPP e ao Observatório da Jurisdição Constitucional Latino-Americana (ambos financiados pelo FINEP e ligados ao Programa de Pós-Graduação em Direito – Mestrado e Doutorado da Universidade de Santa Cruz do Sul – UNISC). Também se insere no âmbito do projeto de cooperação internacional "Observatório da Jurisdição Constitucional Latino-Americana: recepção da jurisprudência da Corte Interamericana de Direitos Humanos e sua utilização como parâmetro para o controle jurisdicional de Políticas Públicas pelos Tribunais Constitucionais", financiado pela Capes (Edital PGCI 02/2015 – Processo 88881.1375114/2017-1 e Processo 88887.137513/2017-00).

** Com Pós-Doutorado na Ruprecht-KarlsUniversität Heidelberg (Alemanha) e Doutorado em Direito pela Universidade do Vale do Rio dos Sinos – Unisinos (com pesquisas realizadas junto à Ruprecht-KarlsUniversität Heidelberg, na Alemanha). Professora do Programa de Pós-Graduação em Direito – Mestrado e Doutorado da Universidade de Santa Cruz do Sul – UNISC, onde ministra as disciplinas de Jurisdição Constitucional e de Controle Jurisdicional de Políticas Públicas, respectivamente. Coordenadora do Grupo de Pesquisa "Jurisdição Constitucional aberta", vinculado ao CNPq. Bolsista de produtividade em pesquisa do CNPq. Lattes: lattes.cnpq.br/6628165246247243. Orcid: orcid.org/0000-0002-3446-1302. *E-mail*: moniah@unisc.br.

*** Advogado. Doutorando em Direito no Programa de Pós-Graduação em Direito - Mestrado e Doutorado da UNISC, bolsista do Programa de Suporte à Pós-Graduação de Instituições Comunitárias de Educação Superior (PROSUC) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Mestre e graduado em Direito pela Fundação Escola Superior do Ministério Público (FMP). Integrante do Grupo de Pesquisa "Jurisdição Constitucional Aberta", coordenado pela Prof.ª Dr.ª Mônia Clarissa Hennig Leal, vinculado ao CNPq. Lattes: lattes.cnpq.br/4330914363996350. Orcid: orcid.org/0000-0003-4583-4853. *E-mail*: lucasmoreschipaulo@gmail.com.

ABSTRACT: Through a bibliographic review, using the deductive method, this study focuses on the protection of the user, complemented by the General Data Protection Law, but still deficient considering the renewed paradigm of algorithmic discrimination. In this context, the aim is to establish a rational line of thought that encompasses the historical constructivism of the right to data protection, the structure of the new law, and the current reality, in order to understand the current needs for the protection of the user as a data subject, who is both a rights holder and vulnerable. Therefore, critical questions are raised to contribute to the development of responses to the new protective paradigm.

KEYWORDS: Algorithmic discrimination; fundamental rights; General Data Protection Law; information society; vulnerability.

1. Introdução

A tecnologia de rede está cada vez mais integrada ao ser humano. O comodismo no uso da Internet pode levar à inconsciência dos riscos associados ao uso da rede. O exemplo não é ao acaso, uma das primeiras utilizações pró-usuário de um serviço a partir dos dados coletados por usuários de uma mesma plataforma foi o caso do Google Maps, e ele serve para o Aplicativo de mobilidade Waze. A partir de um complexo levantamento constante de informações recolhidas de todos os dispositivos celulares que habilitam a função de GPS, a comunidade que trafega se beneficia com maiores informações.

Essa simbiose é marca da sociedade da informação, uma sociedade que tem seu principal alicerce em algo intangível, a interconectividade informacional. Uma sociedade insaciável por informação, agilidade, instantaneidade e comodismo ao alcance de um *click*. É o universo do dataísmo, uma realidade bioquímico-digital que oferece poderes inéditos e imensos a todas as classes de homem.[1] Além disso, nesse intenso fluxo informacional, encontra-se o ser usuário da *web*, que se põe no meio de um turbilhão inconstante de mudanças paradigmáticas recorrentes, sem base jurisdicional unitária, sem barreiras para a aceleração ou alterações estruturais. O paradigma, para Castells,[2] é o da ação sobre a informação, centralizando a experiência humana na valorização do fluxo informacional, colocando o homem no centro da criação e do direcionamento de algoritmos que sabem mais de um indivíduo do que este sobre si próprio.[3]

---

[1] HARARI, Yuval Noah. *Homo Deus:* uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 2016, p. 370-371.
[2] CASTELLS, Manuel. *A Era da Informação:* economia, sociedade e cultura, v. 1: A sociedade em Rede, 4. ed., Lisboa: Fundação Calouste Gulbenkian, 2011, p. 87.
[3] HARARI, Yuval Noah. *Homo Deus:* uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 2016, p. 394.

A magnitude da importância da informação, sobretudo a das informações sobre pessoas, dos dados pessoais portanto, alavanca os dados a papel de destaque dentro da nova economia. Os dados são alçados ao novo petróleo (*data is the new oil*), com a vantagem de ser infindável, os veículos, contudo, são a própria economia fomentada pelas Big Techs. As estradas, no entanto, são os consumidores (fornecedores de dados, a matéria-prima). O paradigma da valorização de um bem intangível não é passível de assimilação tão-somente pela velha concepção mercadológica. O ganho associado ao conhecimento e direcionamento possível com os dados só é possível na nova concepção de economia digital de rede.

A Internet consegue ainda mais. Com a emergência da possibilidade de utilização dos dados para perfilização (formando perfis para análise comportamental, maior segurança de crédito e etc.), análise behaviorista de mercado (analisar o comportamento dos usuários-consumidores na Internet, para tentar manipular suas preferências a partir disso), e fluidez quanto a assertividade de ofertas de marketing (*micromarketing* e *microtargeting*) direcionadas para pessoas com o perfil de compra de um determinado produto, conseguiu promover um verdadeiro giro copernicano: transformou o consumidor-usuário em produto, e o fornecedor de produtos em consumidor de dados, o vulnerável da relação passa a ser o detentor da riqueza buscada na relação comercial. O usuário se torna fonte única e primária de insumo de dados.

Insta analisar o estado arte do usuário na internet, sendo ameaçado enquanto produto por uma realidade de marketing direcionado e ostensivo, que se vale de digital *fingerprints*, histórico de navegações e dados mais sensíveis, para direcionar ofertas de produtos e serviços através de complexos algoritmos, inclusive, discriminando pessoas para que produtos ou serviços não sejam disponibilizados, no que se cunhou os termos *geoblocking, geopricing* e discriminação algorítmica (viés). Calha refletir, nesse sentido, se a Lei Geral de Proteção de Dados, pensada para essa tutela, consegue desempenhar uma proteção material frente a nova realidade que se apresenta, e que em momento posterior à formatação final do presente já estará mais avançada. A ideia de resguardo dos dados, no âmbito digital, consubstancia-se na proteção das informações que podem ser coletadas, armazenadas, usadas e propagadas comercialmente no mundo virtual. Assim, insta analisar o estado arte desta nova relação, em que o ser é ameaçado enquanto um mero produto de uma ostensiva e direcionada realidade algorítmica.

Para esse efeito, a partir de metodologia bibliográfica e uma abordagem exploratória, primeiramente deve ser caracterizado o titular dos dados como um sujeito de direitos

que se encontra em vulnerabilidade de fato e diante o direito, que ainda não conta com um significativo arcabouço normativo suficiente. Isso significa que depende do direito para que tenha um escudo eficaz contra o vazamento e a má-utilização de seus dados, bem como que não será alvo de discriminações a partir de tomada de decisões automatizadas que não analisam outras questões a não ser aquele quantificável algebricamente. Após, diante do paradigma de que existem direitos fundamentais que tutelam os dados pessoais, deve-se analisar o papel da LGPD frente aos direitos dos portadores de dados, que são altamente vulneráveis pelo simples fato de estarem em rede, e podem ter sua vulnerabilidade social aumentada em ambiente virtual. A tutela destes, bem como a conservação de sua autodeterminação, são deveres que o direito deverá exigir das empresas, para que zelem pelos dados pessoais, efetuando um bom e íntegro tratamento, encaminhamento e utilização desses. Posteriormente, frente a todo o panorama desenhado, e estabelecendo alguns casos práticos recentes, e paradigmáticos, analisar-se-á o atual estágio da proteção dos dados dos usuários no ordenamento jurídico brasileiro, no chamado microssistema normativo de tutela aos dados, verificando em que premissas e lacunas caberá à jurisdição constitucional atuar assertivamente.

2. Da proteção de dados pessoais, entre o status de direito fundamental e sua efetiva proteção no texto constitucional

A Internet hoje é o grande meio de existência do ser humano. É o espaço não-físico da plataforma de relevante percentual do relacionamento humano. É na Internet que se negociam bens e serviços, que se encontram pessoas, profissionais e empresas, que se conhece até mesmo o verdadeiro amor. É na internet que a vida, de fato, vem acontecendo; isto é, sem a internet, a vida do lado de fora das telas seria completamente diferente. Esse protagonismo da Internet ainda ganhou um tempero maior em 2020, com a decretação da pandemia por conta da circulação do vírus Sars-Cov-2, e, com isso, o início das medidas de isolamento social.

Assim, mais do que nunca, a sociedade civil se comunicou pela Internet, participando de aulas de instituições públicas e privadas por plataformas como Google Meet e Zoom, vendo transmissões pelo Instagram, ou ainda pelo Youtube e Facebook, reunindo-se para reuniões de trabalho. Tudo isso dependente da criação de perfis com informações pessoais, como nome, e-mail, telefone, por vezes até cartão de crédito, nome da mãe, do pai, se tem filhos, qual a profissão e a faixa de remuneração etc. Tomemos como exemplo extremo o número de dados que as pessoas informam na rede quando se cadastram em

e-bankings ou quando preenchem cadastros de seleção de vagas de emprego. Até mesmo o Poder Judiciário, resistente acerca da expansão das audiências e instrução para o meio digital migrou completamente suas operações para o meio digital, vindo a exigir como regra geral a presencialidade apenas em 2023.

Dessa forma, nota-se uma complexização da vida. E, como sempre, o direito deve acompanhar. A mudança, contudo, e positivamente, veio dois anos antes desse novo boom no protagonismo da Internet na nova realidade que impôs a pandemia, e antes do segundo grande boom da década, o avanço e popularização do acesso às ferramentas de Inteligência Artificial. Naturalmente, o fluxo intenso de informações de dados pessoais não começou em 2020. Com efeito, a preocupação acerca da proteção desses dados pessoais, que já era existente, ganhou uma importância a mais e foi acelerada com o episódio da Cambridge Analytica ("CA"). Ao que se sabe, e o que uma parte ficou demonstrado no documentário *The Great Hack*, do Netflix, a CA era uma empresa britânica de análise de dados, contratada, dentre outros, pelo então candidato à presidência norte-americana Donald Trump, para influenciar eleitores indecisos em 2016. A estratégia era a de avaliar os dados existentes em redes sociais, como o Facebook, montando perfis de eleitores, os influenciando através do *micromarketing* e *microtargeting* dessas plataformas através de estratégias de postagens que cada perfil receberia, conquistando eleitores pelo perfil, ou fazendo com que opositores fracos não votassem. Segundo o que se sabe, a CA teria atuado também no *British Exit from EU* (BREXIT).

Assim, uma nova preocupação com a defesa das pessoas em rede, usuários de produtos e serviços na web, deu início à corrida legal por mecanismos de proteção normativa. Bem na verdade, a tutela era a do consumidor que tem uma vulnerabilidade expandida e acentuada em rede digital. Além disso, a proteção paradigmática do consumidor-usuário, que de sujeito de consumo, passou a sujeito fornecedor de dados a título semigratuito, precisava ser fortemente re-compassada. Essa preocupação faz a UE aprimorar a normativa anterior com a *General Data Protection Regulation* ("GDPR"). Dois anos mais tarde, com inspiração na GDPR, o Brasil promulga a Lei Geral de Proteção de Dados ("LGPD"). O escândalo da CA, que também envolveu, como se sabe, o Facebook, não foi a gênesis da preocupação com a proteção de dados, mas foi o combustível que faltava para o impulso final, ainda que não definitivo, desta proteção.

Até 2018, ano marcado pelo ato legiferante da LGPD, a proteção de dados era tratada apenas reflexamente pelo ordenamento jurídico pátrio, por leis esparsas que não

garantiam a tutela adequada desses novos *digital assets*, porquanto não eram legislações centradas nisso. Em linhas gerais, que serão densificadas posteriormente, o Brasil contava com proteção de dados em diversas leis, destacando-se o Código de Defesa do Consumidor, a Lei do Habeas Data, a Lei do Cadastro positivo, a Lei de Acesso à Informação e o Marco Civil da Internet.

Em termos de atualização normativa, pode-se dizer que o Brasil está atrás de países latino-americanos como o Chile, que tem legislação sobre proteção de dados pessoais desde 1999, a Argentina, desde o ano 2000, o Uruguai, desde o ano 2008, o México, desde 2010, o Peru, desde 2011, e a Colômbia, desde 2012. Além disso, a primeira normativa que tratou do tema data ainda do ano de 1970, quando a Alemanha, através da Lei do Estado de Hesse, começou a tutelar os direitos individuais frente ao tratamento de dados pessoais realizado pelo poder público e reconhecia, dentre outras disposições, um conjunto de princípios essenciais para nortear o tratamento de dados pessoais.[4]

Esse paradigma, que se pode chamar de paradigma alemão da proteção de dados, o qual tutelava relações eminentemente verticais (Estado-cidadão), serviu de base para o movimento internacional seguinte: os *Fair Information Practice Principles* (FIPPs). Os FIPPs são um conjunto de princípios desenvolvidos para servir de base para o tratamento de dados pessoais por todos os países. Os princípios dos FIPPs são a transparência, participação individual, especificação de propósito para o tratamento dos dados pessoais, minimização de dados pessoais utilizados, limitação de uso dos dados, controle de qualidade dos dados, integridade da atividade, segurança e uma dupla possibilidade-responsabilidade de que o tratamento seja auditável, e que se conduza o processo tendo-se em vista a necessidade de *accountability* da atividade. Nos EUA, esses princípios foram a base do *Privacy Act* de 1974. Também merece destaque a lei nacional de proteção de dados sueca, que foi o Estatuto para bancos de dados de 1973 (*Data Legen* ou *Datalag*).[5]

Afora essa questão, a partir da Lei do Estado de Hesse, foram confeccionadas diversas normas protetivas no mundo. Segundo Martins,[6] tais normas podem ser classificadas em gerações, de acordo com suas dimensões internacionais. A primeira geração é a da gênese

[4] MENDES, Laura Schertel; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: Mapeando Convergências na Direção de um Nível de Equivalência. *Revista de Direito do Consumidor*. São Paulo, Revista dos Tribunais, v. 124, p. 157-180, jul./ago. 2019, p. 164.
[5] *Ibidem*, p. 162-164.
[6] MARTINS, Fernando Rodrigues. Sociedade da informação e promoção à pessoa. *Revista de Direito do Consumidor*, São Paulo, Revista dos Tribunais, v. 96, p. 225-257, nov./dez. 2014, p. 231.

da década de 70, e tinha por objetivo a regulação do processo eletrônico de dados pessoais pelas administrações públicas, e algumas empresas privadas, e ganhou destaque, para além da Lei de Hesse, com Estatuto de Proteção de Dados do Estado Alemão e Lei Federal de Proteção de Dados da Alemanha. Posteriormente, a segunda geração diz respeito à preocupação com o consentimento e a liberdade de escolha do cidadão. A terceira geração, por sua vez, cuidou da questão relativa à autodeterminação informativa, pela qual o titular controla individualmente o processamento de seus dados pessoais. E, finalmente, a quarta geração se preocupou em melhorar o controle dos dados fornecidos pelo próprio titular, bem como "estabelecer temas de dados pessoais intangíveis a qualquer acesso e, por fim, partir de metodologia de formatação de normas gerais com complementação por normas setoriais".

Ainda em linhas históricas, há de se destacar o avanço que teve a proteção de dados pessoais enquanto um direito constitucional reconhecido na Constituição de Portugal, de 1976, no pós-Revolução dos Cravos.[7] E, igualmente, a Constituição da Espanha, de 1978, trouxe a ressalva que com o avanço da tecnologia, e a necessidade de proteção dos direitos fundamentais, como os dados pessoais, a constituição hispânica asseverou que o Estado deveria limitar o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos, bem como garantir o pleno gozo e exercício dos direitos.

Na Alemanha, embora já houvessem dispositivos constitucionais que tutelassem a privacidade e o livre desenvolvimento, o direito fundamental à proteção individual ao uso indiscriminado dos dados pessoais por terceiras pessoas, ou pelo Estado, veio através do caso BVERFGE 65, 1, 1983, conhecido como o caso da Lei do Censo Alemão (*Volkszählungsgesetz*), no qual pode-se dizer que houve o nascedouro forte da proteção de dados como um compromisso dos Estados nacionais, com assento de garantia constitucional, e, portanto, com status de direito fundamental. O caso discutia a constitucionalidade da lei que determinava o recenseamento geral da população, com o levantamento de dados sobre a profissão, moradia e local de trabalho para fins estatísticos, e foi levado à Corte máxima alemã por conta do §9º, que previa, dentre outras questões, a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa.[8]

[7] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, Santa Cruz do Sul, p. 138-160, jul. 2008, p. 141.
[8] SCHWABE, Jürgen. *Cinquenta anos de jurisprudência do tribunal constitucional federal alemão*. Trad. Beatriz Henning e Leonardo Martins. Montevideo: Fundación Konrad-Adenauer, 2005, p. 233-234.

As alegações nas reclamações constitucionais recebidas pelo Tribunal Constitucional Alemão (*Bundesverfassungsgericht*) ("BVerfG") eram de violação direta a alguns direitos individuais da Constituição da Alemanha (*Grundgesetz*) ("GG"), sobretudo ao direito ao livre desenvolvimento da personalidade (art. 2, I, da GG). Ao final, no mérito, o BVerfG julgou as reclamações no sentido de confirmar a constitucionalidade da Lei do Censo, contudo declarando nulos os dispositivos sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa. Assim, o que o BVerfG asseverou na oportunidade foi o direito individual contra o levantamento, armazenagem, uso e transmissão irrestrito de dados pessoais, porquanto o indivíduo é credor de um direito geral de personalidade (art. 2, I, e 11, ambos da GG) e, por isso, tem o poder de decidir sobre a exibição de seus dados pessoais.[9]

Além disso, Schwabe[10] assevera que a partir desse caso ficou consignado no direito alemão que as restrições ao direito à autodeterminação sobre a informação pessoal são permitidas apenas em casos de interesse predominante da coletividade, e mesmo nesses é necessária a observância à existência de uma legislação específica para aquela finalidade, bem como base constitucional para a lei, e que seja observada a proporcionalidade, devendo ser tomadas todas as precauções organizacionais e processuais necessárias para que riscos de violação aos direitos de personalidade sejam evitados. O Tribunal ainda distinguiu os dados levantados anonimamente dos dados individuais, determinando que acerca dos dados levantados para propósitos estatísticos (anonimamente), não se pode exigir uma vinculação estrita e concreta de propósito dos dados. Ainda assim, dentro do sistema de informação devem existir barreiras para compensação, em contraposição ao levantamento e uso da informação.

Posteriormente, a União Europeia preocupou-se em tutelar de forma uniforme a matéria, tutelando adequadamente os dados pessoais dos indivíduos em sua macro jurisdição, habilitando-os para exercerem suas liberdades e seus direitos da personalidade, assim como para facilitar a transferência internacional de dados. Para tanto, em 1995, o Parlamento Europeu e o Conselho Europeu lançaram a Diretiva nº 46, disciplinando o tratamento e a proteção de dados das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados no continente. Essa diretiva viria a ser substituída pela GDPR em 2016.

Na Espanha, a Diretiva nº 46/95 deu origem à Lei Orgânica de Proteção de Dados

[9] *Ibidem*, p. 234.
[10] *Ibidem*, p. 235.

("LOPD"). A LOPD ampliou a proteção ofertada pelo texto constitucional de 1978, trazendo inovações quanto ao âmbito de proteção legal, ampliando-o para que alcançasse todos os bancos de dados, informatizados ou não, bem como que houvesse proteção aos dados pessoais com o escopo de garantir liberdades públicas e direitos fundamentais individuais.[11] Assim, a proteção de dados caminhava já para ser reconhecida, pelo menos em alguns ordenamentos, a tutela com assento constitucional alcançado.

Contudo, o ano de 2000 tem especial importância para o avançar transcontinental da proteção dos dados pessoais. Com efeito, é nesse ano que a Carta dos Direitos Fundamentais da União Europeia é organizada. No capítulo II – Liberdade, no art. 8º, consta que a União Europeia terá proteção de dados, sendo todas as pessoas credoras do direito à proteção dos dados que lhes digam respeito, que os dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, e que por isso todas os indivíduos têm o direito de acessar os dados que lhes digam respeito, obtendo a respectiva retificação. E, por último, que o cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente.

Em 2016 a Diretiva nº 46/95 foi substituída pelo Regulamento nº 679 de 2016, a GDPR, do Parlamento Europeu e do Conselho Europeu, entrando em vigor no ano de 2018. Assim, com o avanço da legislação europeia, bem como o reconhecimento da proteção dos dados pessoais, ou da autodeterminação dos dados pessoais, em nível continental, a matéria está sendo delineada e desenvolvida a partir das decisões do Tribunal de Justiça da União Europeia, que influenciam a matéria em nível mundial, e fortemente no Brasil.

No Brasil, em 2018 foi aprovada a LGPD, que entrou em vigor em 2020, com disposições valendo apenas a partir de agosto de 2021. A Lei traz disposições acerca do tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O dever de proteção (*Schutzpflicht*) aqui aparece e, com ele, podemos entender que o Brasil não estava desprotegido na matéria, visto que a partir de elementos normativos constitucionais e infraconstitucionais legislador e judiciário poderiam intervir para salvaguarda deste direito fundamental. Ainda assim, formalmente não havia proteção em assento constitucional até a EC nº 115/2022, oriunda da Proposta de Emenda à

[11] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, Santa Cruz do Sul, p. 138-160, jul. 2008, p. 145.

Constituição (PEC nº 17/03/2019), alterando o texto constitucional para que conste no artigo 5º, inciso LXXIX, que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais", no artigo 21, inciso XXVI, que compete à União "organizar e fiscalizar a proteção e o tratamento de dados pessoais", bem como que o artigo 22, inciso XXX, passe a constar que compete privativamente à União legislar sobre "proteção e tratamento de dados pessoais".

Ainda assim, já era possível compreender que, desde antes, do art. 5º, *caput*, da Constituição, decorre a liberdade individual, do inciso X decorre a inviolabilidade da intimidade e da vida privada e do inciso XII decorre o livre desenvolvimento, a autodeterminação individual e, portanto, os dados pessoais – o ponto não é mais controverso; felizmente. Pode-se afirmar que seja pela alteração constitucional, seja pela soma interpretativo-construtivista que resultava no reconhecimento do direito implícito à inviolabilidade dos dados pessoais, vê-se que ela não é suficientemente adequada para tutelar integralmente os dados pessoais. É que a tutela de algo não depende unicamente da CF.[12]

Como aludido, o Brasil já contava com legislação que resguardava os dados pessoais. Leis como o Código de Defesa do Consumidor, a Lei do Habeas Data, a Lei do Cadastro positivo, a Lei de Acesso à Informação, o próprio Código Civil e o Marco Civil da Internet formavam uma espécie de microssistema protetivo aos dados pessoais. Ainda que, como mostra Santos,[13] a tentativa de formatação de uma lei de proteção aos bancos de dados remonte ao ano de 1999 no Brasil, apenas em 2018 teve-se a aprovação da LGPD.

O Código Civil, por exemplo, determinava que 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, conforme inteligência do seu art. 21. Uma lei mais específica, a do Cadastro Positivo (nº 12.414/2011), já disciplinava a formação e consulta a bancos de dados com informações de pessoas naturais ou jurídicas, com o fito exclusivo de formar seu histórico de crédito. Essa lei trouxe questões importantes, como o princípio da qualidade dos dados (art. 3º) e os direitos de acesso, retificação e cancelamento de dados (art. 5º). Ainda, a lei delimita as finalidades para as quais os dados podem ser coletados (art. 7º). Por todas essas disposições, Mendes entende que a referida lei consolida a evolução de um conceito de autodeterminação

[12] MENDES, Laura Schertel. O Direito Fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*. São Paulo, Revista dos Tribunais, v. 79, p. 45-81, jul./set. 2011.
[13] SANTOS, Ana Luiza Liz dos. Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. *Revista dos Tribunais,* São Paulo, v. 1013, p. 105-126, mar., 2020.

informativa no ordenamento pátrio.[14]

Pouco tempo depois, em 2012, a Lei Carolina Dickmann (nº 12.737) criminalizou as condutas de invadir dispositivo alheio com o fim de adulterar, obter ou destruir dados ou informações sem a autorização do titular dos dados, bem como, no presente escopo, criminaliza a conduta do desenvolvedor de software capaz de facilitar as práticas supra. Ainda, A Lei do Marco Civil da Internet (nº 12.965, de 2014) ("MCI") prevê, em seu art. 3º, que o princípio da proteção dos dados pessoais integra o rol dos princípios que disciplinam o uso da Internet no Brasil, juntamente com o princípio da proteção da privacidade e outros. Do mesmo modo, dispõe, o art. 11 diz que os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros deverão ser obrigatoriamente respeitados em qualquer operação de coleta, armazenamento, guarda e tratamento de dados, desde que pelo menos um ato ocorra em território nacional. Os princípios da finalidade e da adequação dos dados pessoas também já estavam presentes no MCI. A lei traz expressa vedação, no art. 16, à guarda dos "registros de acesso a outras aplicações de Internet sem que o titular dos dados tenha consentido previamente" e à guarda de "dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular".[15]

Tais leis, ainda que juntas, se mostraram insuficientes para o trato e proteção dos dados pessoais nas relações que ocorrem na Internet, sobretudo no espectro do direito do consumidor. Nesse sentido, o Código de Defesa do Consumidor (nº 8.078, de 1990) ("CDC") já demonstrava uma ampla proteção aos dados pessoais dos consumidores. E não só isso, mas o direito do consumidor engloba, em seu escopo interpretativo, um viés aberto e mais amplo de proteção dos consumidores, porquanto aplicado como uma política de Estado. O CDC já previa que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre suas respectivas fontes (art. 43, *caput*), prevendo que as informações devem ser verdadeiras, claras e objetivas (art. 43,§1º); que a abertura do cadastro ou registro deve ser comunicado por escrito ao consumidor quando não solicitada por ele (art. 43, §2º); que o consumidor poderá exigir a correção de informação inexata. Assim, com o acréscimo da LGPD, que surgiu para regulamentar de forma abrangente o tratamento de dados pessoais, ampliou-se o já composto o microssistema protetivo de dados.

---

[14] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.
[15] MACIEL, Rafael. *Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:* Atualizado com a Medida Provisória nº 869/18. Goiânia: RM Digital, 2019.

Todo esse aparato normativo, que já vinha fortalecido e cristalizado pela LGPD, foi respaldado pela Emenda Constitucional nº 115/2022, que fez constar explicitamente a proteção dos dados pessoais como um direito fundamental. Mesmo quando não havia a EC 115/2022, já se ventilava a possibilidade do reconhecimento do direito fundamental implícito à proteção de dados e à autodeterminação na CF/88, isto é, um direito fundamental associado.[16] Advogando a existência desde antes da tutela constitucional, Doneda[17] defendeu nos autos da ADI 6.389, que a Carta da República deve ser interpretada à luz de novos desafios, buscando o reconhecimento da constitucionalidade da proteção dos dados, de modo a garantir privacidade, liberdade e autodeterminação ao cidadão. Essa preocupação é reflexo do atual contexto tecnológico, que ceifará, se não houver zelo, a própria esfera cidadã e democrática da liberdade de conduzir a sua própria vida. É por isso, assevera Doneda, que a interpretação constitucional deverá ser apontada a solução dos problemas dos novos desafios que estão por vir.

Assim, ao menos, foi reconhecido pelo Supremo Tribunal Federal ao julgamento conjunto das Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393.[18] Na hipótese, o STF reconheceu o direito à proteção de dados como direito fundamental implícito ao suspender a Medida Provisória n. 954, que determinava o compartilhamento dos dados pessoais dos usuários de telefonia pelas empresas do ramo ao Instituto Brasileiro de Geografia e Estatística (IBGE). A MP 954, como se sabe, foi justificada por conta da pandemia da COVID-19, para que o governo tivesse uma base epistêmica mais sólida para acompanhar o avanço da pandemia.[19]

Para além dessas questões, insta referir que o conceito de dado adotado pela legislação brasileira abarca um conceito expansionista e dinâmico de dado pessoal, a norma brasileira tutela os dados referentes a pessoas naturais, identificadas ou identificáveis, ainda que anonimizados em algumas circunstâncias, tratados por bancos de dados públicos ou privados.[20] Dessa forma, abrange não somente os dados pessoais que se

[16] Segundo Gavião Filho e Freitas (Direitos fundamentais estatuídos não diretamente ou implícitos. Revista Direitos Fundamentais & Democracia, Curitiba, v. 25, n. 3, p. 232-257, set./out. 2020, p. 240-241), os direitos fundamentais implícitos são aqueles que não estão expressamente dispostos no constitucional, mas dependem de uma formulação interpretativo-argumentativa para existir. O que parece ser o caso, pelo menos diante da atual situação.
[17] DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, *caput* e §§1º e 3º da MP 954/2020. *Civilistica.com*, a. 9, n. 1, 2020, p. 8.
[18] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6387. Relatora: Ministra Rosa Weber, 06 maio 2020.
[19] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. *Revista de Direito do Consumidor*. São Paulo, Revista dos Tribunais, v. 130, p. 471-478, jul./ago., 2020.
[20] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: A função e os limites do consentimento. São Paulo: Forense, 2019, p. 74.

associam à pessoa natural, como também os que permitem à identificação, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.

Assim, a LGPD define marcos para utilização dos dados, com foco em garantir os direitos da personalidade, notadamente o direito à privacidade e à autodeterminação informativa. A LGPD amplia, densifica e concretiza a tutela dos dados pessoais que não era inexistente, mas era, no mínimo, desordenada. E, ainda que talvez não inove em questões protetivas, operacionaliza um sistema protetivo que o Brasil era carente.[21] Além disso, após os escândalos da Cambridge Analytica, a LGPD, como a GDPR, encontrou meios para oferecer caminhos adequados entre um não cerceamento dos direitos comunicativos e um oferecimento de bases adequadas para o desenvolvimento da economia da informação, baseada nos vetores da confiança e da segurança.[22] Adicionalmente, sobretudo pelo rápido avanço das tecnologias algorítmicas mais avançadas, a base de novos direitos estabelecida pelo movimento da LGPD dá raízes fortes para uma nova tutela especializada acerca das decisões automatizadas, resguardando-se, de modo mais direto, direitos como o da vedação à discriminação injustificada, o direito à transparência e à explicabilidade dos algoritmos e o itinerário lógico que seguiu para a tomada de decisão. Tais são desafios que já existiam, que foram tutelados, mas que diante do rápido avanço já começam a ficar a descoberto novamente. Para além da tutela dos dados, agora se faz necessária uma tutela também sobre Inteligência Artificial, problemas que de nenhum modo são isolados, mas com implícito nascedouro na relação Estado/Mercado e Sociedade Civil, que é uma relação iminentemente constitucional, na qual em atualização, o Mercado passa a ter igual poderio para com os cidadãos como era tal poderio outrora de monopólio do Estado.

3. A tutela da lei geral de proteção de dados em ação: a tutela da vulnerabilidade do ser-usuário em rede

A LGPD inaugura no Brasil um regime geral de proteção de dados pessoais. Ainda que não implemente grandes mudanças fáticas no quesito proteção aos dados dos usuários, porquanto esses já vinham sendo tutelados, como visto, pelo microssistema existente em 2018, a LGPD consolida-se enquanto um importante marco normativo-protetivo, reacendendo a importância estratégica dos dados para as maiores empresas do mundo, como a Apple, o Facebook, o Google, Amazon etc. O Facebook em especial preocupa,

[21] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: A função e os limites do consentimento. São Paulo: Forense, 2019, p. 110.
[22] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 469-483, nov./dez., 2018, p. 470.

sobretudo desde a aquisição de apps como WhatsApp e Instagram.[23] Proteger o usuário de virar objeto de consumo das empresas de Big Data, marketing e que se baseiam em behaviorismo virou, portanto, um compromisso que assume esferas comerciais, constitucionais, negociais e, também, do direito do consumidor.[24] Segundo Doneda,[25] a vigência da LGPD, a parte de tudo que trouxe, serviu como organizadora de toda a fenomenologia do direito acerca da proteção de dados, servindo como elemento introdutor da retomada da preocupação acerca da proteção dos dados pessoais, ainda que ela estivesse presente há algum tempo.

A LGPD visa a tutela e a proteção, dentre outros, da autodeterminação, ao desenvolvimento da personalidade e, também, ajudar a promover a defesa do usuário, que pode sofrer discriminações de múltiplas origens e de diversos modos. A proteção de dados tem por objetivo a proteção dos direitos fundamentais de liberdade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural e a igualdade na dimensão de sua não-discriminação, e a sua regulação, segundo o texto legal da LGPD, consiste em proporcionar ao cidadão garantias em relação ao uso dos seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esses dados, dentro de parâmetros e limites.

Extrai-se, portanto, a partir da análise do caput do art. 1º da Lei 13.709/18, a intenção do legislador infraconstitucional em preservar não só o direito fundamental à privacidade e à intimidade dos titulares de dados pessoais, consagrado expressamente no art. 5º, X, da CF/88, mas igualmente fortalecendo a autodeterminação informativa individual. Assim, o direito à autodeterminação firma-se na possibilidade de decisão pessoal sobre os dados que lhe é de titularidade, sejam eles sensíveis ou não. Além disso, a lei possibilita o tratamento desses dados pessoais por terceiros, ressalvadas as hipóteses do art. 4º da LGPD.

Para os fins da LGPD, o tratamento de dados pessoais compreende toda a operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

---

[23] CARUGATI, Christophe. The 2017 Facebook Saga: A Competition, Consumer and Data Protection Story. *European Competition and Regulatory Law Review*, v. 2, n; 1, p. 4-10, 2018, p. 5.
[24] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 469-483, nov./dez., 2018.
[25] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; e RODRIGUES JÚNIOR, Otavio. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração dos dados pessoais. A inteligência é da disposição do art. 5º, X, da LGPD.

A informação de dados, na sociedade da informação, é o ativo mais valioso, uma vez que influencia, prevê e manipula o comportamento do próprio indivíduo titular dos dados, que perde controle de si mesmo, por causa do mal uso de seus dados.[26] O fortalecimento da proteção de dados é indispensável para a adequada consolidação da proteção dos direitos fundamentais, portanto.[27] Para que isso seja de fato assegurado, é necessária uma estrutura principiológica densa. Veja-se, os dados pessoais são monetizados, e são utilizados para determinar a vida de bilhões de indivíduos ao redor do globo. Assim, não apenas normas protetivas devem ser asseguradas e fielmente cumpridas, mas o escopo interpretativo que serve de guia em casos não claros, deve ser fortemente asseverada. Nesse sentido, a LGPD ostenta uma estrutura principiológica densa, e até repetitiva. Desta forma, traz consigo um rol de princípios que precisam ser observados, na sua aplicação, por ocasião do tratamento de dados.[28]

O art. 2º, inciso VII, da LGPD disciplina a proteção dos dados pessoais a partir do fundamento dos "direitos humanos, do livre desenvolvimento da personalidade, da dignidade e o exercício da cidadania pelas pessoas naturais". O art. 6º da LGPD, dedicado aos princípios, colaciona os princípios da boa-fé, da finalidade, da necessidade, da adequação, do livre acesso, da qualidade dos dados, da prevenção, da transparência, da não discriminação, da segurança e da responsabilidade e da prestação de contas. Individualmente, o princípio da boa-fé é importante porquanto determina a adoção de condutas corretas e adequadas que todos os participantes da cadeia de tratamento dos dados deverão obedecer. De certa forma, os demais princípios são decorrências lógicas e especificadas do princípio da boa-fé. O princípio da boa-fé, nesse sentido, impõe um valor ético-moral substancial ao trato com os dados pessoais, de modo a coibir conceitualmente condutas contrárias ao escopo de proteção da norma; o qual pode-se colocar como o da prevenção da mercantilização dos dados pessoais, com o fim de garantir a autodeterminação informativa individual.[29]

---

[26] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. 2. Ed. São Paulo: Revista dos Tribunais, 2019, p. 169.
[27] RODOTÀ, Stefano. *A vida na sociedade de vigilância: privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 21.
[28] PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n.13.709/2018 (LGPD)*. São Paulo: Saraiva, 2018, p. 24.
[29] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, n.p., nov., 2019.

Pulando-se aos pontos chaves, o princípio da finalidade específica dos dados significa que o tratamento precisa ter um resultado único, específico e legítimo que deve ser alcançado, e que o mesmo deve ser o motivo primário para a solicitação dos dados, evitando-se desvirtuações. Também deverá garantir o livre acesso do titular dos dados a eles, tendo poderes de portabilidade, exclusão, retificação ou inclusão de seus dados, mantendo a qualidade dos dados, que devem ser transmitidos de modo claro e exato entre o titular e o operador, da transparência no tratamento de dados, para que se garantam informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, de segurança na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados, isto é, à integridade dos dados. Também deverá atender aos princípios de prevenção através da tomada de medidas que previnam a ocorrência de danos em virtude do tratamento de dados pessoais.

Segundo a LGPD, não poderá haver discriminações ilícitas ou abusivas dos dados coletados, com as técnicas de perfilização, p.e., utilizadas para restringir crédito, mesmo com os CPFs não negativados nas listas de proteção ao crédito. Sobre essa análise de risco, a LGPD traz em seu art. 11, §5º, que os planos de saúde estão proibidos de prever o risco do usuário para a contratação ou exclusão, e o mesmo aplica-se aos bancos de dados de proteção ao crédito, que avançam na questão da perfilização do risco individual (*profiling*). E, ainda, há a preocupação acerca da responsabilização e prestação de contas (*accountability*), de modo que o agente de tratamento adote medidas eficazes de comprovar a observância e o cumprimento das normas de proteção de dados, inclusive as de segurança da informação, demonstrando a eficácia das medidas.[30] Nesse sentido, o titular tem o direito de solicitar a revisão de decisões automatizadas que afetem seus interesses, conforme previsto na LGPD, visando a transparência no tratamento de dados. Embora a lei reconheça o direito ao sigilo comercial e industrial, a ANPD pode realizar auditorias para verificar discriminações em tratamentos automatizados, buscando a compatibilização entre essas preocupações.

Uma questão premente, de ordem mais técnico-jurídica, se relaciona a necessária ponderação que deverá ser feita a partir da colisão do direito difuso à publicidade, quando aplicável, sobretudo nos casos de informações públicas, como as processuais ou sobre saúde pública, e o direito individual à proteção de dados pessoais. Veja-se o caso do IBGE (RmCADI 6.389), no qual os dados levantados eram de enorme interesse

[30] *Ibidem*.

público, porquanto poderiam auxiliar na prevenção da doença COVID-19, o que atende ao interesse público. A LGPD inclusive traz a questão do interesse público enquanto escopo interpretativo para a indisponibilização dos dados, no art. 4, §1º, art. 7, §3º, art. 15, III e, na seara pública, no art. 23. Assim, a lei traz possibilidades previstas para a relativização da proteção máxima aos dados.

Soares[31] traz que, por serem os direitos fundamentais organizados sob a estrutura de princípios, devendo ser aplicados por otimização em casos, e, sendo o direito à privacidade, à proteção de dados ou à autodeterminação informativa, direitos fundamentais, admitiram relativização frente a outros que, por algumas questões, apresentassem grau satisfativo em maior importância. Para solucionar esse entrave deve ser tomada a utilização da estrutura do teste da proporcionalidade de Alexy. Com lucidez, Soares[32] traz ainda que aqui, deve-se ter a cautela de diferenciar entre o interesse público genuíno e a utilização do fundamento do "bem comum" como forma de mascarar outros interesses estatais oportunistas.

Nesse sentido, o Tribunal de Justiça da União Europeia, no caso Digital Rights Ireland (C-293/12), destacou a existência do direito fundamental à proteção dos dados, assentando que qualquer medida legislativa promulgada para fornecer uma base legal para o tema deve atender à proporcionalidade, de modo que só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

No Brasil, ainda sobre o caso do IBGE e da MP nº 954, o STF, considerando a violação ao postulado da proporcionalidade, destacou que, *in verbis*:

> (...) as leis que tratam de coleta e processamento de dados devem (i) atender a propósitos legítimos, específicos, explícitos e informados; (iii) limitar a coleta ao mínimo necessário para a realização das finalidades normativas; (iv) prever medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados e (v) prevenir a ocorrência de danos, consoante os parâmetros desenhados no direito comparado e no art. 6º da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In casu*, a Medida Provisória 954/2020 não atende ao direito à proteção de dados e ao

[31] SOARES, Carolina Borges. Direito à autodeterminação informativa e proteção de dados em tempos de pandemia: análise do atual contexto jurídico brasileiro. In: FERRAZ, Miriam Olivia Knopik; VETTORAZI, Karlo Messa (org.). *Direitos fundamentais e a era tecnológica - Law Experience*. Curitiba: FAE/Bom Jesus, 2020, p. 31
[32] *Ibidem*.

> postulado da proporcionalidade, máxime porque (i) não especifica para quais finalidades os dados serão utilizados; (ii) incorre em excesso ao determinar o compartilhamento de dados de milhões de brasileiros, quando pesquisas amostrais realizadas pelo IBGE em geral envolvem apenas cerca de 70 (setenta) mil domicílios por mês; (iii) não detalha métodos de segurança para a proteção dos dados contra riscos de vazamento; (iv) determina que o relatório de impacto à proteção de dados seja elaborado somente após já efetivado o compartilhamento, e não antes; e (v) pode gerar um nível preocupante de precisão na identificação dos usuários (...)[33]

Assim, como escopo interpretativo, para os parâmetros decisórios do STF, sabe-se desde logo que a LGPD deve guiar sua aplicação atendendo propósitos legítimos, específicos, explícitos e informados, com coleta do mínimo necessário, adotando medidas de prevenção de vazamentos e danos. Por isso, no caso do IBGE, foi entendido que a MP nº 954/2020 não atendia ao direito à proteção de dados e ao postulado da proporcionalidade pelos fatos de não especificar as finalidades para as quais os dados seriam utilizados, causando um excesso na coleta e no compartilhamento de dados. Além disso, a MP não trazia os métodos de segurança para a proteção dos dados contra riscos de vazamento que seriam adotadas etc.

Contudo, ainda fica em aberto, não por qualquer descrédito da decisão do STF ou do próprio STF, a questão da possibilidade de relativização da proteção de dados, porquanto tem estrutura de direito fundamental, para a satisfação de outros direitos fundamentais. O STF aplicando a proporcionalidade chegou em resultado de maior peso relativo à proteção de dados. O que é especialmente bom em tempos de direito da crise, isto é, quando o Estado derruba garantias individuais para satisfazer projeto de governo, muitas vezes influenciados pelo medo, sem gestão de crise das autoridades. Nesse sentido, Long[34] ensina que uma vez estabelecidos mecanismos de coleta de dados indiscriminados, é improvável que poderes governamentais de vigilância e coleta de dados retrocedam voluntariamente. A linha entre a materialização do *Big Brother* de Orwell e o direito fundamental à proteção dados é tênue.[35] A história também tem ensinado que uma vez que dados são coletados para um propósito é difícil evitar que sejam usados para outros fins não relacionados. Long argumenta ainda que sempre haverá uma próxima pandemia, senão de COVID-19 de outro agente infeccioso, e que

---

33 BRASIL. Supremo Tribunal Federal. Referendo na Medida Cautelar na *Ação Direta de Inconstitucionalidade 6.389*. Relatora: Ministra Rosa Weber, 07 maio 2020, p. 62.
34 LONG, Clarissa. Privacy and Pandemics. In PISTOR, Katharina. *Law in the time of COVID-19*. Columbia Law School Books, 2020, p. 92-94.
35 SARTORI, Ellen Carina Mattias; BAHIA, Cláudio José Amaral. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. *Revista de Direitos e Garantias Fundamentais,* v. 20, n. 3, p. 225-248, 2019, p. 231.

esses momentos não podem servir de desculpa para o abandono das garantias fundamentais. Os desafios que as pandemias apresentam para a privacidade, mais do que para a liberdade, não irão embora nem se atenuarão com brevidade.

A pandemia ocasionada pelo temor em torno da propagação da SARS-COV-2, além de ter ocasionada medidas restritivas da liberdade, postergando muito da vida presencial, e acelerando muito o desenvolvimento da vida através da Internet, como a expansão da educação EAD, do e-Commerce etc., significou uma postergação da vigência da própria LGPD. A *vacatio legis* da LGPD, originalmente composta para 24 meses (art. 65, II), foi prorrogada pelo Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia do coronavírus e pela MP nº 959/2020. Em 18/09/2020, contudo, e finalmente, a LGPD começou a surtir efeitos a partir da sanção presidencial.[36]

Diante de todo esse paradigma, resta analisar como se dará a tutela dos dados pessoais dos usuários frente à realidade algorítmica, que impõe novos desafios à LGPD, bem como as práticas que devem ser tomadas como mais atentas, os principais desafios no dia a dia dos usuários, bem como sobre o trato de alguns dos pilares de aplicação da LGPD no e-commerce, no mercado comum e no principal mercado de todos: o *Big Market* dos dados pessoais.

4. Da proteção dos dados à realidade algorítmica

O fascinante mundo dos dados, e de seu potencial transformador da realidade humana, ganha especial notoriedade quando os estudos de defesa do usuário e de proteção de dados pessoais se relacionam. Segundo os estudos de *behavioral economics* (economia comportamental), que se estabelece a partir de análises das capacidades cognitivas pessoais quando da tomada de decisão sobre amplos aspectos da vida, há questões psicológicas, bioquímicas e econômicas relacionadas quanto o comportamento humano, sobretudo com foco no *homo economicus*, isto é, o homem inserido em uma sociedade mercadológica.[37]

Um case famoso de análise comportamental é a da empresa Target. A empresa queria

[36] SANTOS, Ana Luiza Liz dos. Lei Geral de Proteção de Dados: os caminhos percorridos até sua vigência no contexto da sociedade da informação. In VASCONCELOS, Adaylson Wagner Souza de (Org.). *A (não)efetividade das ciências jurídicas no Brasil 3*. Ponta Grossa: Atena, 2021, p. 254.
[37] DAURA, Samir Alves. Behavioral Economics and Consumer Law: New Perspectives to Confront the Overindebtedness. *Revista Brasileira de Políticas Públicas*, v. 8, n.2, p. 568-599, ago., 2018, p. 569-570.

atingir o público dos novos pais e, para isso, começou a cruzar milhões de dados de padrão de consumo, via Big Data, que pudessem identificar possíveis grávidas, a partir da compra de produtos não diretamente relacionados à gravidez, mas frequentemente comprado por grávidas. O caso virou famoso quando uma adolescente recebeu anúncios de produtos de bebê, achou estranho, e descobriu que estava de fato grávida, isto é, o estudo da Target conseguiu descobrir que ela estava grávida mesmo sem ela ou seus pais terem se dado conta. Esse é o poder da análise comportamental e o paradigma econômico-tecnológico atual.

A proteção de dados na realidade algorítmica é um tema cada vez mais relevante e desafiador para a sociedade contemporânea. Com o avanço das tecnologias algorítmicas, a coleta e o processamento de dados pessoais se tornaram cada vez mais complexos e difíceis de serem controlados. A realidade algorítmica impõe novos desafios à proteção dos dados pessoais dos usuários, especialmente no que diz respeito à discriminação injustificada e à transparência dos algoritmos. A LGPD estabelece diretrizes importantes para a proteção dos dados pessoais na realidade algorítmica, incluindo a vedação à discriminação injustificada e o direito à transparência e explicabilidade dos algoritmos. No entanto, ainda há muito a ser feito para garantir uma proteção efetiva dos dados pessoais na era do big data. Para garantir a proteção dos dados pessoais na realidade algorítmica, é necessário estabelecer mecanismos eficazes de controle e fiscalização da coleta e do uso desses dados pelas empresas. Além disso, é importante que os usuários tenham acesso às informações sobre como seus dados estão sendo coletados e usados pelos algoritmos.

Um dos principais desafios enfrentados na proteção dos dados pessoais na realidade algorítmica é a discriminação injustificada. Os algoritmos podem perpetuar preconceitos e estereótipos ao tomar decisões com base em dados pessoais, como raça, gênero e orientação sexual. Isso pode levar a uma discriminação injusta e prejudicar a vida das pessoas afetadas. Outro desafio importante é a falta de transparência dos algoritmos. Muitas vezes, os usuários não têm acesso às informações sobre como seus dados estão sendo coletados e usados pelos algoritmos. Isso pode levar a uma falta de confiança nos serviços que utilizam esses algoritmos e prejudicar a privacidade dos usuários.[38] A discriminação algorítmica é uma ameaça cada vez mais preocupante para a proteção dos dados pessoais na sociedade contemporânea. À medida que as tecnologias algorítmicas avançam, torna-se mais difícil controlar a coleta e o processamento de informações

[38] PARANHOS, Mário C. Oliveira. *Viés algorítmico:* uma análise sobre discriminações automatizadas. Rio de Janeiro: Lúmens Juris, 2022.

pessoais, o que pode levar a uma discriminação injustificada e prejudicar vidas e dignidades. É fundamental que a proteção dos dados pessoais seja fortalecida para impedir que os algoritmos perpetuem preconceitos e estereótipos com base em informações como raça, gênero e orientação sexual. Para garantir uma proteção efetiva dos dados pessoais na era do big data, é necessário que as empresas estabeleçam mecanismos eficazes de controle e fiscalização da coleta e do uso dessas informações. Os usuários também devem ter acesso a informações claras sobre como seus dados estão sendo coletados e usados pelos algoritmos, a fim de garantir a transparência e a responsabilidade das empresas. Ações efetivas devem ser tomadas para garantir que as empresas cumpram suas obrigações legais e éticas de proteção dos dados pessoais dos usuários, sem discriminação ou violação de seus direitos fundamentais.

Para enfrentar esses desafios, é necessário desenvolver novas tecnologias que garantam a transparência e explicabilidade dos algoritmos. Isso pode incluir o uso de técnicas de explicabilidade, que permitem aos usuários entender como os algoritmos tomam decisões com base em seus dados pessoais. Além disso, é importante fortalecer as leis e regulamentações existentes para garantir uma proteção efetiva dos dados pessoais na realidade algorítmica. A LGPD é um exemplo importante de legislação que estabelece diretrizes claras para a proteção dos dados pessoais no Brasil. No entanto, ainda há muito a ser feito para garantir que essas diretrizes sejam efetivamente implementadas pelas empresas e fiscalizadas pelos órgãos reguladores.

Portanto, é imperioso analisar a relação dos dados no universo da defesa do usuário, que é vulnerável conceitualmente e pela própria essência de uma política de proteção.[39] Alguns casos são extremamente pertinentes de serem abordados para desenhar o estado da arte e o risco de vazamento de dados. Um caso de vazamento de dados foi protagonizados pelo Serasa. O Procon-SP notificou a Serasa Experian pedindo explicações sobre notícias acerca de um suposto vazamento de 220 milhões de dados pessoais de cidadãos brasileiros. Após explicações, o Procon-SP entendeu que a empresa não teria conseguido implementar medidas para cumprimento do CDC e da LGPD. O entendimento veio apoiado no fato de que a empresa não detalhou a finalidade e base legal para o tratamento de dados pessoais, a necessidade do consentimento para a coleta de dados, medidas para o atendimento da LGPD, e a segurança desses dados, tampouco uma política de armazenamento e descarte dos dados coletados. Esse caso de São Paulo aguarda desfecho, contudo a Serasa S.A. também foi ré em Brasília.

[39] MARQUES, Cláudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. 2. ed. São Paulo: Revista dos Tribunais, 2014, p. 160.

Nos autos da Ação Civil Pública nº 0736634-81.2020.8.07.0001, o Ministério Público do Distrito Federal e dos Territórios identificou, através da Unidade Especial de Proteção de Dados e Inteligência Artificial, a indevida e maciça comercialização de dados pessoais de brasileiros por meio de serviços como "Lista Online" e "Prospecção de Clientes", oferecidos pela Serasa Experian. O TJDFT julgou procedente a ACP, no sentido de condenar a ré Serasa S.A. a se abster de comercializar dados pessoais dos titulares por meio dos produtos denominados "Lista Online" e "Prospecção de Clientes", sob pena de imposição das medidas indutivas, coercitivas etc. No dispêndio argumentativo, os desembargadores entenderam que a comercialização das listas viola o art. 5º, X, da Constituição Federal, bem como os correspondentes incisos I e IV do art. 2 da LGPD, todos os dispositivos tratando sobre a inviolabilidade da intimidade, da honra e da imagem dos titulares dos dados. Mas há considerações do caso a serem consideradas mais aprofundadamente.

Os dados comercializados não tratavam de dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, como conceitua o art. 5º, II, da LGPD. Para o tratamento desses, o art. 11, I, dispõe que o tratamento somente é cabível com o consentimento do titular ou responsável, manifestado de forma específica e destacada, ressalvadas hipóteses em que os dados forem indispensáveis para questões legais (art. 11, II, da LGPD). No entanto, os dados comercializados não eram sensíveis. Ainda assim, mereciam tutela. O Serasa argumentou que por não serem dados sensíveis, não haveria ilegalidade na prática, visto que haveria dispensa do consentimento do titular, uma vez que o controlador teria interesse legítimo (art. 7º, IX, da LGPD) ou que o compartilhamento dos dados tenha finalidade de proteção do crédito (art. 7º, X, da LGPD). E de fato, há interesse legítimo e atende as finalidades da Serasa, porquanto no seu estatuto social estão delineados os objetos sociais de coleta, o armazenamento e o gerenciamento de dados, organização, análise, desenvolvimento, operação e comercialização de informações e soluções para apoiar decisões, o gerenciamento de risco de crédito e de negócios, a administração de finanças pessoais e para promover educação financeira etc.

Ainda assim, o TJDFT entendeu que o art. 7º da LGPD dispõe que o consentimento do titular é a regra maior a ser observada para o tratamento de dados pessoais, tanto é que o § 4º, daquele dispositivo, prescreve a dispensa do consentimento apenas para os dados tornados manifestamente públicos pelo titular. De modo que mesmo para os dados não sensíveis, o controlador deve obter o consentimento, exceto quando os dados foram

tornados manifestamente públicos pelo próprio titular. Além disso, o cerne da LGPD é a tutela à autodeterminação do indivíduo em relação à veiculação de suas informações, de modo que apenas pelo consentimento inequívoco que o titular dos dados consegue controlar o nível de proteção e os fluxos de seus dados, permitindo ou não que suas informações sejam processadas, utilizadas, repassadas e assim por diante. É direito dos titulares dos dados, portanto, dar anuência. E a maior preocupação com o consentimento valoriza a pessoa no mundo digitalizado.[40]

Sobre comercialização de dados, o Ministério Público do Distrito Federal e dos Territórios também litigou com o Mercado Livre, que oferecia banco de dados e cadastro em geral pela plataforma. O Vendedor era EMARKETING011ERICAVIRTUAL, que vendia bancos de dados digitais por R$ 500,00. O Mercado Livre, nos autos da Ação nº 0733785-39.2020.8.07.0001, da 17ª Vara Cível de Brasília, teve que suspender o anúncio, em liminar, e em sentença ficou condicionada a multa de R$ 2 mil por operação desse tipo realizada novamente pelo Mercado Livre. No caso não parecia haver anuência dos titulares de dados com a comercialização do produto, portanto essa era ilegal.

Interessante notar que em uma cadeia de e-commerce os dados podem transitar por muitas empresas, sobretudo para a viabilização de meios de pagamento. Com efeito, entre a loja virtual e o usuário há empresas de gateway, antifraudes, adquirentes, subadquirentes, bandeiras de cartão de crédito, emissores de cartões, bancos e intermediários. Assim, há muito fluxo informacional envolvido, o que redobra o grau de seriedade com a tutela dos dados pessoais, tratamento e demais direitos estabelecidos pelo microssistema protetivo, foco especial no CDC, e na LGPD. Uma palavra é essencial para toda a cadeia comercial: confiança.

A relação comercial que ocorre na Internet precisa ter a mesma confiança, segurança e informação que a clássica, isto é, deve atender aos mesmos requisitos e ainda a outros mais específicos. O complexo normativo protetivo dos dados tem, também, esse desafio, o de transformar o ambiente virtual em um ambiente seguro, confiável e tutelado, que não promova a discriminação ou o predatismo potencializado por esses dados ilicitamente comercializados.

O Código de Defesa do Consumidor encampa essa proteção desde 1990, sobretudo com o art. 43, que estabelece uma série de direitos e garantias para o usuário em relação às

[40] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, a. 9, n. 1, 2020, p. 6-7.

suas informações pessoais presentes em bancos de dados e cadastros. Com base tão somente nesse dispositivo destacam-se os direitos de acesso aos dados, de retificação dos dados e de cancelamento deles. Além disso, o §1º determina que os cadastros e dados de usuários devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos, atendendo aos princípios trazidos na LGPD como qualidade dos dados, livre acesso e transparência. Além disso, o limite legal de 5 anos beneficia muito os usuários. Nesse sentido, Bioni,[41] destaca que o CDC já trazia a preocupação com a autodeterminação informacional.

Uma prática abusiva, nesse sentido de proteção ao crédito, é a da perfilização (*profiling*), que consiste na elaboração de perfis de comportamento de uma pessoa (ou de um grupo de pessoas) a partir de dados pessoais, disponibilizados por ela ou colhidos. Para Clarke,[42] o "*profiling is a technique whereby a set of characteristics of a particular class of person is inferred from past experience*". Assim, através de algoritmos aliados à ciência da economia comportamental, é possível prever condições, decisões ou comportamentos futuros de uma pessoa. Isso certamente beneficia as empresas que trabalham com risco, ou que querem evitar o risco demasiado, com a técnica do *Credit Scoring*, conhecida dos brasileiros, e julgada lícita pelo STJ nos autos do RESP nº 1.419.697/RS, afetado para julgamento pelo rito dos recursos repetitivos. Outro uso é para o direcionamento do marketing ostensivo e pessoalizado, esse uso até pode ocorrer, mas deve ser feito mediante consentimento adequado do usuário.

Ainda sobre a questão a questão da oferta de crédito, insta comentar que a nova Lei nº 14.181/2021, promulgada em 1º de julho de 2021, inseriu o art. 54-D no CDC, determinando, no inciso II, que o fornecedor ou intermediário da oferta de crédito avalie, de forma responsável as condições de crédito do usuário, mediante análise das informações disponíveis em bancos de dados de proteção ao crédito, observado o disposto no CDC e nas demais leis do sistema normativo de proteção de dados.

Sobre o consentimento, que guarda relação com a autodeterminação, tem-se que a formação de bancos de dados de usuários, pela incidência em comum da LGPD e do CDC exige o consentimento expresso do usuário-titular. Esse deve ser dado a partir de uma manifestação livre de vontade, voltado a uma finalidade específica e que tenha sido

[41] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* A função e os limites do consentimento. São Paulo: Forense, 2019, p. 126.
[42] CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law & Information Science*, v. 4, p. 403-419, 1993, p. 403.

informado sobre o processamento e utilização dos dados, bem como da possibilidade de não consentir e ainda assim utilizar a plataforma ou ferramenta. Há, contudo, uma grave crise de consentimento de dados. E isso pode ser facilmente explicado pelo fato de que as pessoas não leem as políticas de privacidade, e, mesmo que se lessem, talvez não as entendessem completamente, por lhes faltar conhecimento técnico. De forma que o consentimento informado pode ser uma doce ilusão[43]. Mendes[44] comenta que há uma situação de extrema vulnerabilidade para os usuários-consumidores, que enfrentam dificuldades para sequer controlar seus dados disponibilizados por *clicks* em *pop-ups* que surgem no meio da navegação na rede. Uma marca da modernidade é a aceleração da ansiedade, da ânsia pelo serviço, pelo bem, pela informação, e os *pop-ups* de consentimento estão no caminho e a um *click* em "aceitar" de distância.

Essas coletas podem ser chamadas de quase não consentidas. Mas há um caso interessante sobre a coleta não consentida de dados, mediante a utilização de scanners corporais pela empresa ViaQuatro de SP. O caso desenrolou a partir de um scanner de reconhecimento facial implantado para coletar registros biométricos de passageiros, e a ideia era na utilização das telas, que eram capazes de contar quantas pessoas passaram em sua frente e de analisar as emoções a partir da expressão facial, para a finalidade de passar anúncios publicitários em uma modalidade chamada *pay-per-face*, isto é, pague de acordo com a quantidade de pessoas que olharam para a tela. Na justiça de São Paulo, nos autos da Ação Civil Pública nº 1090663-42.2018.8.26.0100, movida pelo IDEC, a empresa foi condenada a pagar R$ 100 mil de multa, e se abster de utilizar a tecnologia, porquanto os usuários sequer foram advertidos da utilização do totem, e muito menos foi solicitado qualquer consentimento para os usuários dos serviços de metrô da ViaQuatro. Após o caso, a empresa se comprometeu a reforçar a transparência e se adequar à LGPD.

Contudo, o caso tem mais uma agravante, por assim dizer. Dentre a coletividade dos usuários da ViaQuatro, poderiam, obviamente, existir crianças e adolescentes. O Código de Defesa do Consumidor destaca, em seu art. 39, IV, que é uma prática abusiva prevalecer-se da fraqueza ou ignorância do usuário, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços. Além disso, a LGPD, em seu art. 14, estabelece uma proteção especial às crianças e

---

43 SCHERMER, Bart Willem; CUSTERS, Bart; VAN DER HOF, Simone. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology, The Crisis of Consent:* How Stronger Legal Protection may lead to Weaker Consent in Data Protection, 2014. Disponível em papers.ssrn.com/. Acesso em 07 jul. 2021.

44 MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 23.

adolescentes, trazendo que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. No mesmo sentido, o ECA, em seu art. 17, garante o direito ao respeito à imagem de crianças e adolescentes, preservando-as. No caso da ViaQuatro, a juíza da 37ª Vara Cível entendeu que os dados coletados eram sensíveis, além de que a violação aos direitos básicos do usuário é amplificada em termos de seus dados, sobretudo na moderna sociedade da informação. O resguardo do usuário enquanto um produto, e maior ainda quando o usuário que pode ser objetificado em seus dados é uma criança ou um adolescente. Há vulnerabilidade dos usuários, e hipervulnerabilidade agravada quando esses são crianças ou adolescentes.

Os dados são os maiores ativos de certos ramos empresariais e esse só fato acarreta riscos à privacidade dos consumidores. A partir da capacidade de contenção e operacionalização do turbilhão informativo, através do Big Data, torna-se perigosa a questão dos consentimentos. A partir de simples "consentimentos" por parte dos titulares de dados pessoais é possível criar um banco de dados com informações pessoais desses e, até mesmo, traçar perfis de consumo com a seleção de ofertas que, possivelmente, irão interessar ao titular. No que diz respeito aos dados coletados de crianças e adolescentes, frequentadores assíduos da Internet, o cuidado deve ser maior. A solução encontrada pela LGPD foi, pela inteligência do art. 14, §1º, o de condicionar o consentimento do infante, por substituição, ao de pelo menos um dos pais ou pelo responsável legal. Das duas uma, portanto: ou há um poder parental ativo e presente, cuidando da navegação da web dos filhos, que são muitas vezes mais hábeis em rede do que os pais ou responsáveis, ou deverá ser reformulada a política de proteção de dados para crianças e adolescentes, fortalecendo-a.

Como aludido, o descumprimento desses deveres poderá ensejar em responsabilização dos controladores. Atentando-se à necessidade de tutelar, de maneira efetiva, os interesses dos titulares, a LGPD traz nos arts. 42, 43 e 44, as regras atinentes à responsabilidade civil, na hipótese de violação de proteção de dados, pelos agentes de tratamento. E, apesar de trazer a previsão, a lei não indicou expressamente se o dever de indenizar decorre da culpa do agente que, ao praticar uma conduta ilícita, enseja o dano ou se a responsabilidade decorre do risco inerente à atividade praticada. Têm-se, contudo, que a responsabilidade é objetiva.

O art. 42 da LGPD, dispõe que, havendo indícios de tratamento irregular, ou, então, violação à legislação de proteção de dados, de modo a ocasionar, a outrem, dano patrimonial, moral, individual ou coletivo, incumbirá, aos agentes de tratamento, a

obrigação repará-lo. Como regra geral, a responsabilidade por danos causados ao titular não é solidária, contudo, se o operador descumprir as obrigações da legislação de dados, ou quando não tiver seguido as instruções lícitas do controlador, equiparam-se e a responsabilização recaí solidariamente. A responsabilidade só será excluída, segundo o art. 43, quando controlador e operador não realizarem tratamento de dados que lhes é atribuído, quando realizado o tratamento, não houver tido violação à legislação de proteção de dados, ou quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.[45]

Após a denúncia, a ANPD, segundo o art. 52 da LGPD, poderá aplicar as penas de advertência, com a adoção de medidas corretivas, multa de até 2% do faturamento da PJ, com o limite em R$ 50 milhões por infração, publicação da infração cometida, bloqueio e eliminação dos dados em questão, multa diária na modalidade *astreinte* e a indenização ao titular dos dados na medida do dano causado. Naturalmente as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da defesa, de acordo com as peculiaridades do caso concreto e considerados os parâmetros e critérios da gravidade e da natureza das infrações e dos direitos afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, o grau do dano, a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado dos dados, a adoção de política de boas práticas e governança, a pronta adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Tudo isso para que se garanta a tutela dos dados dos usuários. Se não pelo temor às altas sanções, pelo caráter pedagógico que adota a legislação protetiva. Usuários são pessoas, dotados de direitos fundamentais, e não podem ser coisificados ou precificados por seu valor de mercado inerente aos dados pessoais que detêm. Não são barris de petróleo, mas sujeitos vulneráveis de direitos.

5. Conclusões

A crescente e recente preocupação com a proteção de dados tem justificativa. O temor pela coisificação é uma realidade, atinge a todos e é lucrativo para empresas de certos

[45] DRESCH, Rafael de Freitas Valle; FALEIROS JUNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (lei 13.709/2018). In: ROSENVALD, Nelson; WESENDONCK, Tula; DRESCH, Rafael. (Org.). *Responsabilidade civil: novos riscos*. Indaiatuba: Editora Foco Jurídico Ltda., 2019, p. 82.

ramos apoiados na inovação tecnológica. A proteção de dados, assim, assume papel de escudo aos direitos e garantias individuais. A concretização do direito fundamental específico à proteção dos dados pessoais viria como decorrência lógica das movimentações normativo-constitucionais brasileiras, e mundiais, acabou sendo concretizada via Emenda Constitucional. Na verdade, bastava a constatação, por parte do Supremo Tribunal Federal, uma vez que a organização protetiva já era de estrutura jusfundamental.

Alicerçou-se, ao longo do texto, que a LGPD não inovou em proteger dados pessoais, sensíveis ou não, em terras brasileiras. O seu mérito é o da consolidação de uma ordem jurídica de proteção de dados, bem como de um retorno da preocupação acerca desse tema, fruto dos incidentes que assolavam a Internet e seus usuários na última década. Viu-se também que a LGPD, além de organizar a tutela protetiva dos dados, lança bases gerais à nova legislação que deverá vir à efetividade para regular o uso e a existência da Inteligência Artificial no Brasil.

No específico, delineou-se os usuários-consumidores, ou usuários-titulares, como o grupo majoritário visado pela lei. Desse modo, nota-se a importância da discussão acerca da temática da proteção de dados na tutela da dignidade do usuário, que se torna verdadeiro fornecedor de dados, que posteriormente são utilizados para influenciá-lo, sem transparência.

Foi possível notar, também, mediante o emprego de alguns casos práticos, que a realidade de vazamento de dados e desrespeito da legislação vigente existe, acarreta danos e consolida situações. Além disso, e de modo mais acentuado, viu-se como vícios na coleta, armazenamento e uso dos dados pode ferir gravemente direitos fundamentais como o princípio da igualdade, em sua vertente de vedação à discriminação. A discriminação algorítmica, que merece estudo detido em outras oportunidades, não pode ser um sintoma apenas lateral das práticas comerciais. O custo social do enviesamento algorítmico é alto, e seu nascedouro está no modo como se tutelam os dados pessoais. O Estado Democrático Brasileiro, tanto por seu corpo político, como por sua jurisdição constitucional, tem o dever de tutelar o consumidor em rede, prevenindo-o de ser tratado como um barril de petróleo, como uma mercadoria.

Referências

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* A função e os limites do consentimento. São Paulo: Forense, 2019.

CARUGATI, Christophe. The 2017 Facebook Saga: A Competition, Consumer and Data Protection Story. *European Competition and Regulatory L. Review*, v. 2, n; 1, p. 4-10, 2018.

CASTELLS, Manuel. *A Era da Informação:* economia, sociedade e cultura, v. 1: A sociedade em Rede, 4. ed., Lisboa: Fundação Calouste Gulbenkian, 2011.

CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law & Information Science*, v. 4, p. 403-419, 1993.

DAURA, Samir Alves. Behavioral Economics and Consumer Law: New Perspectives to Confront the Overindebtedness. *RBPP*, v. 8, n.2, p. 568-599, ago., 2018.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, *caput* e §§1º e 3º da MP 954/2020. *Civilistica.com*, a. 9, n. 1, 2020.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; e RODRIGUES JÚNIOR, Otavio. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

DRESCH, Rafael de Freitas Valle; FALEIROS JUNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (lei 13.709/2018). In: ROSENVALD, Nelson; WESENDONCK, Tula; DRESCH, Rafael. (Org.). *Responsabilidade civil:* novos riscos. Indaiatuba: Editora Foco Jurídico Ltda., 2019.

GAVIÃO FILHO, Anizio Pires; FREITAS, Luiz Fernando Calil de. Direitos fundamentais estatuídos não diretamente ou implícitos. *Revista Direitos Fundamentais & Democracia*, Curitiba, v. 25, n. 3, p. 232-257, set./out. 2020.

HARARI, Yuval Noah. *Homo Deus:* uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 2016.

LEAL, Mônia Clarissa Hennig; MAAS, Rosana Helena. *Dever de proteção estatal, proibição de proteção insuficiente e controle jurisdicional de Políticas Públicas*. Rio de Janeiro: Lumen Juris, 2020.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, Santa Cruz do Sul, p. 138-160, jul. 2008.

LONG, Clarissa. Privacy and Pandemics. In PISTOR, Katharina. *Law in the time of COVID-19*. Columbia Law School Books, 2020.

MACIEL, Rafael. *Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:* Atualizado com a Medida Provisória nº 869/18. Goiânia: RM Digital, 2019.

MARTINS, Fernando Rodrigues. Sociedade da informação e promoção à pessoa. *Revista de Direito do Consumidor*, São Paulo, Revista dos Tribunais, v. 96, p. 225-257, nov./dez. 2014.

MARQUES, Cláudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. 2. ed. São Paulo: Revista dos Tribunais, 2014.

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

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

MENDES, Laura S.; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: Mapeando Convergências na Direção de um Nível de Equivalência. *Revista de Direito do Consumidor*. São Paulo, Revista dos Tribunais, v. 124, p. 157-180, jul./ago. 2019.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. *Revista de Direito do Consumidor*. São Paulo, Revista dos Tribunais, v. 130, p. 471-478, jul./ago., 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. *RDC*, São Paulo, v. 120, p. 469-483, nov./dez., 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, n.p., nov. 2019.

PARANHOS, Mário C. Oliveira. *Viés algorítmico:* uma análise sobre discriminações automatizadas. Rio de Janeiro: Lúmens Juris, 2022.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n.13.709/2018 (LGPD)*. São Paulo: Saraiva, 2018.

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

SANTOS, Ana Luiza L. Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais. *RT*, São Paulo, v. 1013, p. 105-126, mar., 2020.

SANTOS, Ana Luiza L. Lei Geral de Proteção de Dados: os caminhos percorridos até sua vigência no contexto da sociedade da informação. In VASCONCELOS, Adaylson W. Souza de (Org.). *A (não)efetividade das ciências jurídicas no Brasil 3*. Ponta Grossa: Atena, 2021.

SARTORI, Ellen Carina Mattias; BAHIA, Cláudio José Amaral. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. *Revista de Direitos e Garantias Fundamentais,* v. 20, n. 3, p. 225-248, 2019.

SCHERMER, Bart Willem; CUSTERS, Bart; VAN DER HOF, Simone. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. *Ethics and Information Technology, The Crisis of Consent:* How Stronger Legal Protection may lead to Weaker Consent in Data Protection, 2014. Disponível em papers.ssrn.com/.

SCHWABE, Jürgen. *Cinquenta anos de jurisprudência do tribunal constitucional federal alemão*. Trad. B. Henning e L. Martins. Montevideo: Fundación Konrad-Adenauer, 2005.

SOARES, Carolina Borges. Direito à autodeterminação informativa e proteção de dados em tempos de pandemia: análise do atual contexto jurídico brasileiro. In: FERRAZ, Miriam Olivia Knopik; VETTORAZI, Karlo Messa (org.). *Direitos fundamentais e a era tecnológica - Law Experience*. Curitiba: FAE/Bom Jesus, 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, a. 9, n. 1, 2020.

Como citar:

LEAL, Mônia Clarissa Hennig; PAULO, Lucas Moreschi. A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos: linhas introdutórias à dinâmica dos dados, do Big Data, da economia de dados e da discriminação algorítmica. **Civilistica.com**. Rio de Janeiro, a. 12, n. 3, 2023. Disponível em: <https://civilistica.emnuvens.com.br/redc>. Data de acesso.

civilistica.com
Recebido em:
28.5.2023
Aprovado em:
11.12.2023