CONPEDI LAW REVIEW

e-ISSN: 2448-3931
Received on 05 December, 2023
Approved on 17 December, 2023
Evaluation Process: Double Blind Review pelo SEER/OJS

O VAZAMENTO DE DADOS POR UMA INSTITUIÇÃO FINANCEIRA: A INSUFICIÊNCIA DE RESPOSTA JURISDICIONAL AOS CONFLITOS EMERGENTES DE UMA SOCIEDADE DE MASSA

Nara Suzana Stainr Pires [*]
Wedner Costodio Lima [*]
Wiliam Costodio Lima [*]

RESUMO: O presente estudo analisa um caso de vazamento de dados ocorrido em uma instituição financeira e a resposta do Poder Judiciário, colocando em relevo o desafio da proteção de dados diante dos fluxos informacionais. Nesse contexto, discute-se a vulnerabilidade dos dados pessoais diante de novas e sofisticadas formas de tratamento, o que aponta para a necessidade de tutela diferenciada. O Brasil aprovou a sua primeira lei de proteção de dados apenas no ano de 2018, e diante do caso concreto se suscita: em que medida a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), pode contribuir para a efetivação do direito humano à liberdade informática, permitindo a autodeterminação informativa? Na tentativa de oferecer uma resposta optou-se por abordagem indutiva ao partir de uma análise de um caso concreto para uma mais geral sobre o tema. Concluiu-se que os conflitos emergentes de uma sociedade de massa exigem uma adaptação das estruturas clássicas do direito com foco maior na prevenção do que na reparação.

Palavras-chave: Autoridade Nacional de Proteção de Dados; Fluxos informacionais; Liberdade informática; Proteção de dados; Vazamento de dados.

DATA LEAKAGE BY A FINANCIAL INSTITUTION: THE INSUFFICIENCY OF JURISDICTIONAL RESPONSE TO THE EMERGING CONFLICTS OF A MASS SOCIETY

ABSTRACT: This study analyzes a case of data leakage that occurred in a financial institution and the Judiciary's response, highlighting the challenge of data protection in the face of information flows. In this context, the vulnerability of personal data in the face of new and sophisticated forms of processing is discussed, which points to the need for differentiated protection. Brazil approved its first data protection law only in 2018, and in view of the specific case it arises: to what extent can Law No. 13,709/2018, called the General Data Protection Law (LGPD), can contribute to the enforcement of the human right to computer freedom, allowing informational self-determination? In an attempt to offer an answer, an inductive approach was chosen, starting from an analysis of a specific case to a more general one on the topic. It was concluded that conflicts emerging from a mass

[*] Pós doutora pela Universidade de Passo Fundo com bolsa CAPES. Doutora em Direito pela Universidade Federal de Santa Catarina – UFSC. Mestre em Direito Constitucional Contemporâneo pela Universidade de Santa Cruz do Sul – RS (UNISC). Graduada no Curso de Direito pelo Centro Universtitário Franciscano (UNIFRA).
[*] Mestre em Direito, UNISC. (2017) Pós-graduado em Direito Penal e Processo Penal pela Faculdade de Direito Damásio de Jesus (2014). Graduado em Direito pela Universidade Luterana do Brasil (2011). Advogado Criminalista. Professor universitário. Email: advwednerlima@hotmail.com.
[*] Mestre pelo Programa de Pós-Graduação em Direito pela Universidade de Santa Maria. Professor da UNISM – Faculdade de Ciências Jurídicas de Santa Maria. Advogado. Email: wiliamadv3@gmail.com.

society require an adaptation of classical legal structures with a greater focus on prevention than reparation.

Keywords: National Data Protection Authority; Information flows; Computer freedom; Data protection; Data leak.

1. INTRODUÇÃO

A proteção de dados pessoais é um novo direito que surge do desenvolvimento das novas tecnologias, especialmente após o término da segunda guerra mundial em 1945 e o surgimento da informática. Desde aquela época a sociedade civil já mostrava preocupação com os riscos decorrentes da sociedade de massa, como nas relações de consumo, nos desafios de viver em um ambiente ecologicamente saudável, e no caso da informatização, das possibilidades de tratamento de dados pessoais.

O fluxo informacional é uma característica marcante das sociedades de massa diante da disseminação das novas tecnologias, sendo cada vez mais intenso a proliferação de dados pessoais nas atividades laborais, de ensino e econômicas. Diante disto, amplia-se a exposição de dados pessoais, e, por consequência, a necessidade de sua proteção, devido ao seu tratamento poder causar sérios riscos aos direitos fundamentais como a liberdade, a intimidade e a igualdade, o que justifica a apresentação do presente artigo, cujo objetivo é analisar se a Lei 13.853/2019 (Lei Geral de Proteção de Dados) pode contribuir para a garantia do direito humano à liberdade informática, conceito empregado a partir das lições de Pérez Luño (2013, p. 173). Tal análise se mostra adequada e pertinente em face das novas e sofisticadas técnicas de coleta, armazenamento, tratamento e transferência de dados pessoais, direito que somente pode se completar e ser efetivado a partir de uma lei geral de proteção de dados e a atuação de uma autoridade nacional independente.

O Brasil aprovou sua primeira legislação específica sobre o tema no ano de 2018, a Lei Federal nº. 13.709, com sua entrada em vigência se deu em setembro de 2020. Portanto, são 05 (cinco) anos de aprovação da lei e 03 (três) anos que ela esta em vigor. Neste passo, o país busca a consolidação de uma cultura de proteção de dados, fator que leva a que se questione se Lei Geral de Proteção de Dados possui condições de realizar as medidas preventivas, educativas e punitivas que se fizerem necessárias, em respeito aos direitos fundamentais dos titulares, caso suas medidas eventualmente contrariarem interesses econômicos ou políticos em voga.

Para enfrentar esse questionamento optou-se por utilizar o método de abordagem indutivo, partindo-se de um caso de vazamento de dados por uma instituição financeira julgado pelo Tribunal

de Justiça do Rio Grande do Sul no ano de 2023, para um panorama geral sobre a liberdade informática e o surgimento de leis de proteção de dados e suas formas de tutela.

O artigo está articulado em três capítulos: em um primeiro momento, analisa-se os fundamentos da decisão exarada pelo Tribunal e a tutela jurídica ao direito à proteção de dados pessoais. No segundo capítulo, explora-se a liberdade informática, destacando sua importância e o desenvolvimento normativo das leis de proteção de dados pessoais, com ênfase para o tratamento do tema na União Europeia, com foco principalmente no papel das autoridades nacionais de proteção de dados. Na última parte é discutida a atuação do Brasil no segmento de proteção de dados, na tentativa de responder ao problema de pesquisa.

2. O CASO DE UM VAZAMENTO DE DADOS POR UMA INSTITUIÇÃO FINANCEIRA: A resposta jurisdicional

O caso a ser analisado se trata de um recurso de apelação cível, que tramitou sob nº 5009366-06.2021.8.21.0026/RS, interposto por uma pessoa física contra uma instituição financeira[2], julgado no ano de 2023. Na ocasião, se tratava de uma ação que buscava uma indenização decorrente de uma suposta falha na prestação de serviços pelo réu diante de vazamento de seus dados pessoais. O autor alegou, em um breve resumo, que o aplicativo da instituição financeira ré expõe aos seus usuários o número de conta e agência de todos os seus clientes.

[2] BRASIL. Tribunal de Justiça do Rio Grande do Sul (TJRS). Apelação Cível nº 5009366-06.2021.8.21.0026/RS. APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO INDENIZATÓRIA. VAZAMENTO DE DADOS PESSOAIS. AUSÊNCIADE VIOLAÇÃO DALEI GERAL DE PROTEÇÃO DE DADOS (LGPD). DANOS MORAIS NÃO CONFIGURADOS. 1. A inversão do ônus da prova prevista no Diploma Consumerista (art. 6o, inc. VIII) não instituiu nova "distribuição estática" do ônus probatório, agora sempre em desfavor do fornecedor – o que sequer "distribuição" seria –, possuindo, ao contrário, natureza relativa. A partir de uma leitura contemporânea acerca da Teoria da Prova, cujo estudo conduz para uma distribuição dinâmica do ônus probatório, a prova incumbe a quem tem melhores condições de produzi-la, à luz das circunstâncias do caso concreto. 2. Informações como agência e conta do consumidor são considerados de natureza comum, não se enquadrando nas características de dados sensíveis, os quais abarcam informações de cunho sexual, político, étnicas, entre outros. 3. O vazamento de dados pessoais não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações (AREsp n. 2.130.619/SP). 4. Competia ao demandante comprovar minimante as violações à sua honra proveniente da disponibilização dos dados no aplicativo do demandado, fato constitutivo do seu direito, nos termos do art. 373, inc. I, do CPC, ônus do qual não se desincumbiu.. **APELAÇÃO DESPROVIDA.** jul. 2023. Disponível em: < https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa >. Acesso em: 10 ago. 2023.

Antes de analisar o caso concreto, oportuno consignar o conceito de proteção de dados de Danilo Doneda (2006, p. 205):

> Westin nos faz notar que, no seu aspecto informacional, a privacidade passa a desempenhar funções essenciais, seja para o indivíduo como para a sociedade a garantia da tolerância e da liberdade de opinião, de associação e de religião; a garantia da livre pesquisa científica; garantia da lisura do próprio processo eleitoral, e tantos outros quanto possamos descrever em uma sucessão de hipóteses, nas quais o que realmente interessa é precisar o contexto no qual encontramos hoje a privacidade.

Como dito, a Lei Geral de Proteção de Dados brasileira (LGPD) entrou em vigor já faz quase 03 (três) anos, e as consequências para o Poder Judiciário, como o ajuizamento de várias ações que se baseiam nela já era algo esperado. Ademais, a Autoridade Nacional de Proteção de Dados, órgão da sociedade civil responsável pela fiscalização e cumprimento da lei, foi instituída em momento posterior à aprovação da LGPD, através da Lei 13.853/2019, e somente foi criada em 06 de novembro de 2020 com a nomeação pelo chefe do Poder executivo do seu primeiro corpo diretivo.

Entre os direitos garantidos pela LGPD aos titulares dos dados pessoais, esta o dever de o controlador dos dados comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano aos mesmos, ou seja, deve comunicar imediatamente a ambos a ocorrência de vazamento de dados. É o que dispõe o art. 48 da Lei:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Como leciona Patrícia Peck Pinheiro (2023, p. 169-170):

> Como reflexo da boa-fé, transparência e responsabilização dos agentes, a comunicação pelo controlador da ocorrência de incidentes de segurança durante o processo de tratamento de dados é essencial. Embora o dispositivo não tenha definido um prazo, indicando apenas que este dever ser razoável, a Autoridade Nacional de Proteção de Dados recomenda um prazo, indicando apenas que este dever ser razoável, a Autoridade nacional de Proteção de Dados recomenda um prazo de 2 dias úteis, contados da data de conhecimento do incidente, bem como indica que a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização. Ainda, a ANPD disponibilizou em seu *site* um formulário modelo para a comunicação de incidentes à autoridade.

Contudo, o caso em análise não havia a comunicação ao titular dos dados pessoais sobre o suposto vazamento, tampouco à ANPD. O que ocorreu foi que os dados bancários do Autor ficam visíveis através do conhecimento anterior do seu CPF pela pessoa que tem a intenção de realizar o pagamento por meio de Pix em sua conta, o que o tribunal não considerou quebra de sigilo de dados pessoais. Como ressaltado na decisão, o procedimento apenas confere uma maior segurança para aquele que quiser fazer o pagamento evitando o risco de enviar dinheiro à terceiros.

Embora se possa discutir a fundamentação do acórdão no que tange à classificação dos dados bancários como não-sensíveis, fato é que o tratamento utilizado pela instituição financeira, em princípio, atende aos princípios da boa-fé e necessidade do uso dos dados pessoais possibilitando as transações financeira com maior segurança para todos os envolvidos. Ademais, outra possibilidade seria a formalização do autor de reclamação junto a ANPD, o que poderia acarretar na revisão e aperfeiçoamento do procedimento pela instituição financeira, de modo a conferir uma maior proteção de dados à toda a sociedade e não apenas ao autor da ação.

Diante do caso concreto e algumas observações atinentes, passa-se a discorrer sobre o direito à proteção de dados na lição de Pérez Luño e a liberdade informática, de modo a enfatizar o riscos do tratamento de dados pessoais e as formas inovadoras de tutela que surgem deste novo direito.

2 A LIBERDADE INFORMÁTICA: um debate sempre atual.

A segunda guerra mundial ocorrida no século XX, momento histórico que evidenciou a "banalidade do mal" e revelou situações de barbárie sem precedentes deixou como legado à comunidade internacional a convicção da necessidade de que fossem firmados compromissos internacionais voltados à prevenção e proteção dos Direitos Humanos, reconhecendo a dignidade que cada ser, independentemente de sua raça, credo ou nacionalidade.

A importância desses compromissos ficou ainda mais clara com a intensificação da globalização, pois o deslocamento físico de pessoas exige uma proteção mínima, a observância de um mínimo ético que acompanhe a pessoa onde quer que esteja independentemente de ser originária daquele Estado ou não. E se nesse momento histórico a preocupação com a vida, a integridade física e a preservação dos direitos mais básicos se sobressaía, o processo tecnológico desencadeado no final do século XX aportou novos temas para a pauta de proteção de direitos, como os direitos relacionados à privacidade, proteção de dados e liberdade informacional.

Em que pese sua importância, os casos de violação a esses direitos nem sempre são percebidos, pois enquanto os ataques à vida e à integridade física produzem marcas evidentes e deixam um triste rastro de sangue e destruição, os ataques aos direitos decorrentes do uso das tecnologias são mais sutis e sofisticados, o que amplia e agrava o problema. Dentre os direitos recorrentemente violados pela utilização das tecnologias da informação e comunicação estão a privacidade e os dados pessoais, frequentemente atingidos pela ação dos Estados, agentes econômicos e pelos próprios particulares (outros usuários), num sistema de vigilância em escala global que não encontra precedentes.

Diante disso e considerando os fluxos de pessoas e de informações, com amparo em Negri, Oliveira e Costa (2020, p. 91) pode-se dizer que "[...] a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana", pois existe um leque vasto de liberdades individuais relacionadas à proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade [...]". Logo, fica evidente que na sociedade em rede não é suficiente a tutela da privacidade, o que impulsionou a tratar de um novo e autônomo direito.

Com efeito, se na modernidade era possível pensar que para a satisfação do direito à privacidade bastava a abstenção de intromissões indevidas do Estado e de particulares na esfera jurídica de seu titular, associando-o ao direito de estar só, os impactos do desenvolvimento tecnológico, por outro lado, evidenciaram não só o esgotamento dessa concepção, como também apontaram a necessidade de ampliar a carta de direitos. Isso fez com que a visão individualista do Direito à privacidade fosse revisitada, como em Pérez Luño (2013, p. 168), ao sustentar que o desenvolvimento tecnológico edificou as bases de uma nova geração de direitos humanos, que são complementares aos de primeira e segunda geração.

Através de pautas de reinvindicação do direito à paz, dos consumidores, decorrentes das biotecnologias e da manipulação genética, ao um meio ambiente saudável e à liberdade informática, estes direitos, ao contrário das gerações anteriores que se caracterizavam pela liberdade e igualdade respectivamente, são denominados direitos de fraternidade e de solidariedade, por serem direitos coletivos ou difusos.

Tal ampliação conduz naturalmente a que se chegue ao direito à proteção de dados pessoais, o que significa dizer a partir de Sarlet e Saavedra (2020, p. 37) que "O caminho da privacidade à proteção de dados pessoais é mais uma prova de que a dimensão individual da construção da personalidade depende de as condições de seu desenvolvimento estejam protegidas", ou seja, só tem sentido tratar desses direitos no âmbito relacional e sua satisfação exige seu reconhecimento pelos demais atores sociais, tendo em conta sempre as inúmeras variáveis e interesses postos em causa, fatores que dão complexidade ao tema.

O reconhecimento de todos os fatores e atores que atuam na sociedade em rede, cujas interações sociais e fluxos informacionais não respeitam as fronteiras dos Estados-nação evidenciam as insuficiências das soluções jurídicas desenhadas pelo Estado de direito moderno para solucionar conflitos advindos do uso das tecnologias. Os novos problemas e demandas ultrapassam o modelo construído na modernidade e exigem uma concepção interdisciplinar e solidária do direito, na qual a regulação não pode encontrar no Estado a fonte principal, já que não se pode prescindir da colaboração da academia, das empresas, dos representantes dos usuários, dos experts em informática, ampliando-se os partícipes do processo de construção normativa, num sistema denominado co-regulação.

Essa participação ampliada e multidisciplinar mostra-se essencial, pois uma das grandes dificuldades em tratar o tema decorre da sofisticação do sistema, a exigir conhecimento especializado dos usuários para a melhor compreensão do que ocorre com seus dados pessoais. Sem perceber os

riscos, o usuário se entrega às vantagens do uso das tecnologias da informação e comunicação, sendo seduzido por elas.

É lógico que tais vantagens não podem ser esquecidas, dentre elas as novas possibilidades de participação e engajamento político, tal qual anunciado por Pérez Luño (2003, p. 100) ao tratar da *cibercidadania*, apontada como um novo horizonte para o exercício dos direitos políticos. Atualmente, o distanciamento temporal e todos os fatos políticos desencadeados no período que medeia a produção do autor e os dias que correm estão a evidenciar que até mesmo essa vantagem também carrega consigo o seu contrário, ou seja, o uso das tecnologias pode oferecer riscos para o exercício da cidadania e para a própria manutenção das democracias.

Ao fazer uma digressão histórica o autor refere que nas primeiras versões do Estado liberal o conceito de cidadania não se estendia a todos, pois havia a exclusão das mulheres, crianças e adolescentes, analfabetos e indigentes, não partícipes da vida da *polis*. Posteriormente, cidadania significava o desfrute de direitos sociais, econômicos e culturais, que também não eram estendidos a todos. A evolução política ocorrida permitiu a inclusão de novos atores na arena pública, bem como o uso das tecnologias ampliou o conceito de cidadania para além do momento estanque do voto para a eleição dos seus representantes políticos. Tais possibilidades levaram o referido autor a sustentar a emergência de uma nova espécie de cidadania e a anunciar que o uso correto de tecnologias poderia apontar um novo caminho rumo ao que chamou de teledemocracia em sua versão forte (PÉREZ LUÑO, 2003, p. 73).

Não se pode desprezar essa contribuição, pois é inegável que o uso das tecnologias possibilita acesso a informações públicas como em nenhum outro tempo, especialmente pelo potencial de pesquisa, de verificação e cruzamento dos dados disponíveis em fontes diversas. De igual forma, a incorporação de tecnologias pelo próprio poder público e as consequentes leis de acesso à informação pública, editadas sobretudo na última parte do Século XX, impuseram não só um novo ritmo na prestação de serviços, como também novos deveres de transparência aos órgãos públicos. Com mais informação é possível diminuir a discricionariedade administrativa, forçando a transparência ativa e passiva o que, em tese, fortalece a democracia (LAMBERTY, GOMES, SILVA, 2020, p. 160).

Entretanto, ainda que não se possam negar suas potencialidades emancipatórias, as novas tecnologias não escapam seus riscos e podem tornar o cidadão um ávido consumidor de informações, nem todas verdadeiras, tornando-o refém de armadilhas tecnológicas, algoritmos e robôs que podem, a partir da coleta de seus dados pessoais, direcionar suas escolhas, reduzindo-se o potencial cívico ao que Pérez Luño (2003, p. 100) chama de *cidadania.com:*

> A complexidade da vida moderna, as imensas possibilidades que nas grandes sociedades de nosso tempo se oferecem para deixar no anonimato ou na impunidade condutas antissociais ou delitivas exigem impor o funcionamento de meios de informação e controle. Porém estas observações não pretendem conduzir a falsa afirmação de que seriam inertes o Estado e a sociedade, e os cidadãos deveriam aceitar a existência de um colossal aparato informático e de controle, não se sabendo ao certo o nível de informação possuído, quem pode utilizar essas informações e com que finalidade irão fazê-lo. (PÉREZ LUÑO, 2003, p. 105, tradução nossa.).

E nessa perspectiva negativa, o uso das tecnologias ao invés de promover os direitos fundamentais os reduziria e colocaria em risco, não só pelo direcionamento das escolhas políticas, mas pela exclusão de milhões de pessoas do debate público, restringindo as participações àqueles com acesso às tecnologias. Em um breve resumo, Pérez Luño (2003, p. 84) demonstra que esses riscos podem ser classificados como políticos, morais e jurídicos. Os primeiros representariam uma verticalização da política, uma mercantilização da esfera pública e a apatia política. Os riscos morais apontam para uma carência da realidade. Os riscos jurídicos, por sua vez, seriam evidenciados pela degradação do processo legislativo, com aumento da criminalidade informática e invasão da intimidade. Nesse sentido parece que os temores do autor são fundados e acabaram de certa forma se confirmando, o que pode ser constatado no atual cenário brasileiro.

Esse estado de coisas alimenta a discussão sobre a necessidade de os usuários manterem-se sempre atentos à proteção da liberdade informática, como sustentado por Pérez Luño (2013, p. 178), preocupação que motivou a elaboração das primeiras leis de proteção de dados e se mantém atual. Nesse sentido, deve-se compreender a importância da liberdade informática tanto para o exercício de direitos individuais quanto para os sociais e tem forte imbricação com a participação política, pois ambos podem ser afetados pelas novas e sofisticadas formas de vigilância postas em funcionamento com o auxílio de tecnologias da informação e comunicação.

O recolhimento de dados pessoais e o tratamento dessas informações para a construção de perfis permite estratégias de direcionamento de conteúdo sem precedentes, pois pelo falseamento ou distorção da verdade são reforçadas convicções ideológicas propagadas por determinados grupos, que com isso obtêm a aceitação absoluta e radical de suas ideias, acirrando as polarizações. E o cidadão, num emaranhado de informações e capturado entre redes e filtros imagina exercer sua liberdade

informativa, quando em realidade é uma presa fácil de um sistema de vigilância muito bem engendrado que verdadeiramente lhe retira o direito de escolha política esclarecida.

Como consequência, as promessas de fortalecimento da própria democracia podem perder fôlego até serem totalmente tragadas por processos totalitários que, de maneira insidiosa, retiram a liberdade de escolha do cidadão e manobram sua vontade, num perverso processo de assujeitamento que nada tem de democrático. A complexidade desse fenômeno exige uma visão alargada sobre a proteção que deve ser estendida aos dados pessoais nessa quadra histórica, o que não se limita a uma ou outra informação pessoal, já que o cruzamento de dados aparentemente inofensivos pode ser bastante revelador da personalidade do titular e direcionar suas escolhas. A proteção desses dados deve se dar tanto em face do Estado quanto de particulares, cuja vinculação aos direitos fundamentais é incontestável, pois do contrário será uma proteção insuficiente.

Com base nessas constatações e considerando a complexidade que o tema suscita, indaga-se se as leis de proteção de dados, em especial a brasileira, seriam suficientes para orientar os comportamentos e garantir a preservação de direitos dos usuários e em que medida essa proteção poderia ser ampliada pela atuação das Autoridades Nacionais de Proteção de Dados, tema que será abordado na sequência.

3 A PROTEÇÃO DE DADOS NO BRASIL: a necessidade de uma tutela coletiva conferida pela ANPD

Como se sabe, até 2018, o ordenamento jurídico brasileiro não dispunha de uma legislação unitária e específica sobre a proteção de dados, contendo apenas uma série de dispositivos decorrentes dos direitos fundamentais e de personalidade, com destaque para o direito à privacidade (inviolabilidade da vida privada e intimidade).

Quanto ao acesso às informações pessoais em poder do Estado o titular dispunha do *habeas data*, previsto no art. 5º, inciso LXXII, da Constituição Federal de 1988 e no que concerne às relações com os particulares que fossem de consumo era possível aplicar os artigos 43 e 44 do Código de Defesa do Consumidor, referente ao banco de dados e cadastro dos consumidores (DONEDA, 2006, p. 340).

Embora no direito brasileiro o Código de Defesa do Consumidor tenha sido reconhecido por muito tempo como a norma que mais diretamente abordava a proteção de dados, servindo de subsídio para a resolução de problemas que por vezes escapavam de seu escopo de abrangência, sua proteção era insuficiente diante das operações realizadas na internet (DONEDA, 2015, p. 381). Nos últimos

anos até se observou a produção de outras leis que evidenciavam a preocupação com os dados pessoais, tais como a Lei de Cadastro Positivo (Lei nº. 12.414/11), Lei de Acesso à Informação (Lei nº. 12.527/11) e o Marco Civil da Internet (Lei nº. 12.965/14), no entanto o Brasil ainda carecia de uma legislação específica sobre a proteção de dados, somente tangenciada no Marco Civil da Internet.

Sobre as normas de proteção de dados no Marco Civil da Internet vale anotar de início, a distinção prevista no artigo 3º, incisos II e III, que trata dos princípios do uso da internet no Brasil, entre a proteção da privacidade e a proteção dos dados pessoais, tal qual acontece na Carta de Direitos Fundamentais da União Europeia (artigo 7º e 8º). No entanto, a proteção de dados no Marco Civil da Internet, além de ter redação mais genérica, era definida apenas como direito e destituída de mecanismos para a adequada proteção e fiscalização do cumprimento das previsões legais (ZANATTA, 2015, p. 463).

Somente após a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (Regulamento EU nº 2016/679) que o tema ganhou força no Brasil, motivado muito mais por interesses comerciais em termos de adequação do país às normas previstas pelos países que já contavam com legislação sobre esse tema do que preocupação com a tutela de direitos fundamentais dos titulares. Embalados por essa preocupação de se adequar ao contexto internacional foi que em 2018 foi editada a Lei nº 13.709/18, que dispõe sobre a proteção de dados pessoais, cuja previsão originária era de entrada em vigor em agosto de 2020.

Uma das surpresas negativas foi contemporânea a sua produção e se manifestou no veto presidencial à criação da Autoridade Nacional de Proteção de Dados (ANPD), vetada pelo então presidente da República, Michel Temer. Tal decisão foi embasada no fato de não haver orçamento previsto para dar amparo à estrutura necessária para a criação do órgão. Essa dificuldade foi posteriormente contornada por meio da Medida Provisória nº 869/2018 (BRASIL, 2018), mas ainda que a autoridade tenha sido criada, esse arranjo sofreu alterações posteriores, a revelar fragilidades não somente no instrumento jurídico utilizado (Medida Provisória), quanto no seu conteúdo.

Com efeito, segundo narram Copetti e Cella (2019, p. 54), o Projeto de Lei 5726/2016 previa a criação da autoridade Nacional de Proteção de Dados, que adotaria o regime de autarquia especial integrante da administração pública indireta, devendo observar, portanto, os termos da Lei nº 9.986, de 18 de julho de 2000 sobre gestão de recursos humanos das Agências Reguladoras. Com essa configuração incialmente prevista, "Foi dada a natureza de autarquia especial conferida à ANPD, caracterizando-a por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira".

As atribuições claramente definidas no projeto de lei originário, bem como a autonomia administrativa e financeira visavam a garantir que tal órgão tivesse condições de fiscalizar o cumprimento da Lei de Proteção de Dados.

O desdobramento histórico que se seguiu, no entanto, contrariou o projeto inicial, pois a Autoridade Nacional de Proteção de Dados, de acordo com o art. 55-A passou a integrar a Presidência da República, sendo-lhe assegurada a autonomia técnica (art. 55-B). Em que pese essa previsão, a submissão à Presidência da República, como destacam Copetti e Cella (2019, p. 58), deixa "[...] evidenciada a dependência e a submissão da ANPD à chefia do Executivo Federal, retirando-se características primordiais a um órgão de proteção de dados pessoais.".

Na sequência a Medida Provisória nº 869/2018 é convertida na Lei nº 13.853, de 08 de julho de 2019 (BRASIL, 2019), cuja análise dos dispositivos quanto à Autoridade Nacional de Proteção de Dados permite verificar sua falta de independência, o que se evidencia em vários pontos, a saber: a) previsão de que o órgão seja integrante da Presidência da República (art. 55-A); b) natureza transitória que *poderá* ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, sem que fiquem claras as condições para isso e mesmo que seja feita essa transformação, ficará vinculada à Presidência da República (art. 55, § 1º); c) segundo o disposto no art. 55 – D, § 1º os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República, os quais não serão submetidos a nenhuma consulta ou posterior aprovação por parte do Congresso Nacional, ou seja, trata-se de escolha do chefe do Executivo; d) a estrutura regimental da Autoridade Nacional será definida por ato do Presidente da República, assim como os cargos de comissão e de confiança serão remanejados de outros órgãos e entidades do Executivo Federal, o que demonstra a clara subordinação que tais membros terão ao Presidente da República, e) até a entrada em vigor da ANPD, receberá apoio técnico e administrativo da Casa Civil da Presidência da República (Art. 55- G).

Não bastasse o engessamento e controle da ANPD pela Presidência da República, a Lei nº 13.853/2019 também criou o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e, em seu, em seu art. 58-A dispôs sobre sua composição, percebendo-se que cinco membros serão do Poder Executivo Federal e, segundo o disposto no § 1º, do art. em comento, "Os representantes serão designados por ato do Presidente da República, permitida a delegação".

As previsões de sanções a serem aplicadas pela Autoridade Nacional de Proteção de Dados também sofreram enfraquecimentos, o que ocorreu em legislações posteriores, a demonstrar certo esvaziamento da atuação do órgão, antes mesmo de sua efetivação. Com efeito, a publicação originária da Lei nº 13.853/2019 ocorreu na edição do Diário Oficial de 09 de julho de 2019, mas em

20 de dezembro do mesmo ano há nova publicação, com acréscimo das partes vetadas quando da publicação originária. Tais vetos tratavam justamente das sanções aplicáveis aos controladores.

> Já os Ministérios da Economia, da Saúde, a Controladoria-Geral da União e o Banco Central do Brasil manifestaram-se pelo veto aos seguintes dispositivos:
> *Incisos X, XI e XII, §§ 3º e 6º do art. 52 da Lei nº 13.709, de 14 de agosto de 2018, alterados pelo art. 2º do projeto de lei de conversão*.
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados."
> "§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011."
> "§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:
> I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e
> II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos."
> *Razões dos vetos*
> A propositura legislativa, ao prever as sanções administrativas de suspensão ou proibição do funcionamento/exercício da atividade relacionada ao tratamento de dados, gera insegurança aos responsáveis por essas informações, bem como impossibilita a utilização e tratamento de bancos de dados essenciais a diversas atividades privadas, a exemplo das aproveitadas pelas instituições financeiras, podendo acarretar prejuízo à estabilidade do sistema financeiro nacional, bem como a entes públicos, com potencial de afetar a continuidade de serviços públicos. [grifos no original].

As razões do veto, acima explicitadas, demonstram claramente que a preocupação do Brasil, longe de ser com a proteção de dados pessoais dos titulares, é com a segurança jurídica dos controladores e visam ao incremento de suas atividades econômicas, mencionando-se especificamente um segmento, já bastante privilegiado, que são as instituições financeiras.

Ademais, ainda que a Autoridade Nacional de Proteção de Dados identifique uma violação não poderá impor a sanção de suspensão parcial do funcionamento do banco de dados, mesmo que este contrarie o escopo da LGPD, pois conforme previsto nos dois novos incisos agregados no § 6º ao art. 52, para aplicar as sanções mais gravosas é necessário que o controlador tenha reincidido, ou seja, tem que lhe ter sido aplicado antes, para o mesmo caso concreto, uma medida inicial mais branda. E não para por aí, pois se o controlador estiver submetido a outro órgão ou entidade que

também tenha poder sancionador, este órgão precisará ser ouvido para a aplicação da sanção por parte da ANPD.

Logo, quer seja pela nova configuração dada a este órgão, por sua composição depender da Presidência da República, pelo esvaziamento de suas funções e competências, quer seja pelo abrandamento de suas sanções, todos esses elementos indicam um verdadeiro abismo entre as promessas iniciais de proteção de dados e o que se desenha para o futuro. Esse descompasso está a revelar que o Brasil se afasta do modelo Europeu não só hipostasiamento do Poder Executivo, o que representa, entre outras coisas, a tutela dos interesses do mercado em detrimento da proteção dos direitos dos usuários, o que apartará o Brasil dos Estados mais desenvolvimentos tecnologicamente que tentam, ao menos, conciliar os dois interesses.

Atualmente, o Brasil incorporou o direito á proteção de dados como direito fundamental através da 115/2022, e conferiu á ANPD a forma de autarquia de natureza especial, através da Lei 14.460/2022, o que em tese, lhe confere maior independência administrativa e técnica, requisito fundamental para a proteção dos dados pessoais dos cidadãos, já que incumbe a mesma a fiscalização da LGPD por parte do mercado como pelo ESTADO.

5. CONCLUSÃO

A aprovação recente da LGPD pelo Brasil tem tido impacto nas demandas judiciais no já abarrotado Poder Judiciário brasileiro, o que por si só não é um fator negativo, haja vista a importância deste novo direito fundamental na vida em sociedade e os riscos aos demais direitos fundamentais que o tratamento de dados pessoais pode ocasionar. Ocorre que estes novos direitos fundamentais, como a proteção de dados, exigem formas inovadoras de tutela, eis que os danos causados são de difícil dimensionamento e, logo, praticamente impossíveis de serem reparados, uma vez que estando estes dados na rede, será tecnicamente impossível impossibilitar seu fluxo.

Por tal razão, se não gera surpresa o ajuizamento de ações indenizatórias por vazamento de dados, tampouco causa espanto que um país que esta implementando uma cultura de proteção de dados ainda não tenha a conscientização na importância da prevenção dos danos ocasionados pelo tratamento de dados e a necessidade de utilização da ANPD como um importante instrumento da sociedade civil neste objetivo, ao orientar, receber reclamações, aplicar sanções e educar.

Este papel desejado pela ANPD é fundamental para a disseminação de uma cultura de proteção de dados, e finalmente, na prevenção dos riscos ocasionados pelo necessário tratamento de dados na sociedade de massa.

6. REFERÊNCIAS

BRASIL. **Lei nº 13853, de 08 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 09 jul. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 9 ago. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 9 ago. 2023.

BRASIL. Congresso Nacional. **Medida Provisória nº 869**, de 27 de dezembro de 2018. Disponível em: http://planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 24 jul. 2023.

BRASIL. Tribunal de Justiça do Rio Grande do Sul (TJRS). Apelação Cível nº 5009366-06.2021.8.21.0026/RS. APELAÇÃO CÍVEL. NEGÓCIOS JURÍDICOS BANCÁRIOS. AÇÃO INDENIZATÓRIA. VAZAMENTO DE DADOS PESSOAIS. AUSÊNCIADE VIOLAÇÃO DALEI GERAL DE PROTEÇÃO DE DADOS (LGPD). DANOS MORAIS NÃO CONFIGURADOS. 1. A inversão do ônus da prova prevista no Diploma Consumerista (art. 6o, inc. VIII) não instituiu nova "distribuição estática" do ônus probatório, agora sempre em desfavor do fornecedor – o que sequer "distribuição" seria –, possuindo, ao contrário, natureza relativa. A partir de uma leitura contemporânea acerca da Teoria da Prova, cujo estudo conduz para uma distribuição dinâmica do ônus probatório, a prova incumbe a quem tem melhores condições de produzi-la, à luz das circunstâncias do caso concreto. 2. Informações como agência e conta do consumidor são considerados de natureza comum, não se enquadrando nas características de dados sensíveis, os quais abarcam informações de cunho sexual, político, étnicas, entre outros. 3. O vazamento de dados pessoais não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações (AREsp n. 2.130.619/SP). 4. Competia ao demandante comprovar minimante as violações à sua honra proveniente da disponibilização dos dados no aplicativo do demandado, fato constitutivo do seu direito, nos termos do art. 373, inc. I, do CPC, ônus do qual não se desincumbiu.. **APELAÇÃO DESPROVIDA.** jul. 2023. Disponível em: < https://www.tjrs.jus.br/novo/buscas-solr/?aba=jurisprudencia&q=&conteudo_busca=ementa_completa >. Acesso em: 10 ago. 2023.

COPETTI, Rafael; CELLA, José Renato Graziero. A salvaguarda da privacidade e a Autoridade Nacional de Proteção de Dados. **Revista de Direito, Governança e Novas Tecnologias**. Goiânia. v. 5, n. 1, p. 44-62. Jan/Jun. 2019. Disponível em: https://core.ac.uk/download/pdf/232939759.pdf. Acesso em: 24 jul. 2023.

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

DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 369-384.

LAMBERTY, Andrey oliveira; GOMES, Thais Bonato; SILVA, Rosane Leal da. Direito de acesso à informação pública e governo eletrônico: a transparência nos portais do Poder Executivo da Argentina e do Brasil. **Revista da Faculdade de Direito UFPR,** Curitiba, p. 157-184, 2020. Disponível em: https: //revistas.ufpr.br/direito/article/view/67912. Acesso em: 15 jul. 2023.

NEGRI, Sergio Marcos Carvalho de Ávila; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL BASEADAS EM INTELIGÊNCIA ARTIFICIAL E O DIREITO À PROTEÇÃO DE DADOS. **Direito Público**, [S.l.], v. 17, n. 93, jul. 2020. ISSN 2236-1766. Disponível em: https://portal.idp.emnuvens.com.br/direitopublico/article/view/3740. Acesso em: 7 ago. 2023.

PÉREZ LUÑO, Antonio-Enrique. **¿Ciberciudadani@ o ciudadani@.com?** Barcelona: Gedisa, 2003.

PÉREZ LUÑO, Antonio-Enrique. Las generaciones de derechos humanos. **Revista Direitos Emergentes na Sociedade Global**, Santa Maria, v. 2, n. 1, p.136-196, 2013. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/10183/pdf_1#.XUpquuhKjIU. Acesso em: 07 ago. 2023.

PINHEIRO, Patricia Peck. Proteção de dados pessoais. Comentários à Lei 13.709/2018. 4ª ed. São Paulo: Saraiva, 2023.

UNIÃO EUROPEIA. **Regulamento nº 2016/679, de 27 de abril de 2016. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt. Acesso em: 06 ago. 2023.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? **I Encontro da rede de Pesquisa em Governança da Internet – REDE 2017.** São Paulo, 2018. p. 175. Disponível em: http://redegovernanca.net.br/public/conferences/1/anais/Anais_REDE_2017-1.pdf. Acesso em: 23 mar. 2023.

WOLFGANG SARLET, Ingo; AGOSTINI SAAVEDRA, Giovani. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. **Direito Público**, [S.l.], v. 17, n. 93, jul. 2020, P. 33-57. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 24 jul. 2023.