ISSN 2238-9121

6 CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE
EDIÇÃO 2022
MÍDIAS E DIREITOS DA SOCIEDADE EM REDE

Dias 24, 25 e 26 de outubro de 2022 - Santa Maria / RS UFSM - Universidade Federal de Santa Maria

NÍVEL DE PROTEÇÃO DE DADOS NO BRASIL: UMA ANÁLISE SOB A ÓTICA DA ATUAÇÃO DA AUTORIDADE NACIONAL

LEVEL OF DATA PROTECTION IN BRAZIL: AN ANALYSIS FROM THE PERFORMANCE OF THE NATIONAL AUTHORITY

Wiliam Costodio Lima [1]
Wedner Costodio Lima [2]

RESUMO

O Brasil aprovou em 2018 e 2022, respectivamente, uma lei geral para a proteção de dados e a previsão constitucional deste novo direito. Assim o país se alinha aos demais que países que vem legislando sobre a matéria e possuem um sistema de proteção de dados. Tendo em vista a adoção do modelo europeu, é essencial para esta proteção a atuação de uma autoridade nacional independente. Do ponto de vista do cidadão, a preocupação com a proteção dos dados pessoais passa pelos riscos aos direitos fundamentais decorrentes de seu tratamento. O objetivo do presente artigo é contribuir para o debate e efetivação do direito fundamental à proteção de dados. Para isso, foi adotado o seguinte problema de pesquisa: qual o nível de proteção de dados no Brasil analisando sob a ótica da autoridade nacional? O método utilizado é o dedutivo, o procedimento é monográfico e as técnicas de pesquisas são bibliográfica e documental. Ao final conclui-se que a atuação da autoridade nacional de proteção de dados no Brasil tem contribuindo para a efetivação de direitos fundamentais.

Palavras-chave: autoridade nacional; direitos fundamentais; proteção de dados.

ABSTRACT

Brazil approved in 2018 and 2022, respectively, a general law for data protection and the constitutional provision of this new right. Thus, the country aligns itself with other countries that have been legislating on the matter and have a data protection system. In view of the adoption of the European model, the performance of an independent national authority is essential for this protection. From the citizen's point of view, the concern with the protection of personal data involves the risks to fundamental rights arising from its treatment. The purpose of this article is to contribute to the debate and realization of the fundamental right to data protection. For this, the following research problem was adopted: what is the level of data protection in Brazil, analyzing from the perspective of the national authority? The method used is deductive, the procedure is monographic and the research techniques are bibliographic and documentary. In the end, it is concluded that the performance of the national data protection authority in Brazil has contributed to the realization of fundamental rights.
Keywords: national authority; fundamental rights; data protection

[1] Mestre em Direito pela Universidade Federal de Santa Maria - UFSM (2020). Especialista em Ciências Penais e Criminologia (2016). Graduado em Direito pela Universidade Luterana do Brasil (2010). Advogado. Email: wiliamadv3@gmail.com. Currículo lattes disponível em: http://lattes.cnpq.br/8837991522983105. OAB/RS 80015.
[2] 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. Currículo lattes disponível em: http://lattes.cnpq.br/5598503195183947. OAB/RS 84271.

ISSN 2238-9121

INTRODUÇÃO

O presente estudo analisa o nível de proteção de dados no Brasil através da atuação da Autoridade Nacional de Proteção de Dados. O país recentemente aprovou sua primeira Lei Geral de Proteção de Dados, e passou a prever este novo direito na Constituição Federal. Ao contrário do que ocorre com a Carta de Direito Fundamentais da União Europeia de 2000, não consta que este deve ser garantido pela atuação de uma autoridade administrativa. Por outro lado, a efetiva proteção de dados decorre de atuação de uma autoridade independente de proteção.

O debate sobre a proteção de dados pessoais no Brasil tem crescido a cada dia. Na perspectiva do cidadão, há a preocupação com a vulnerabilidade dos dados pessoais e riscos aos direitos fundamentais. Desse modo, surge o seguinte questionamento, ao qual se pretende contribuir: qual o nível de proteção da proteção de dados no Brasil analisando sob a ótica da atuação da Autoridade Nacional de Proteção?

Assim, com o emprego do método dedutivo, de técnicas de pesquisa documental e bibliográfica, partindo da necessidade de assegurar uma liberdade informática, se analisa o surgimento destas formas de tutela inovadora de direitos fundamentais, para então, verificar a atuação na proteção de dados pela autoridade independente de proteção.

1 NOVOS DIREITOS E NOVAS FORMAS DE TUTELA: O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

O Brasil, ao aprovar no ano de 2018 sua primeira Lei Geral de Proteção de Dados[3], criou, em 2019, a Autoridade Nacional de Proteção, encarregada de fiscalizar o cumprimento da lei. A proteção de dados é garantida, portanto, com a atuação de uma autoridade fiscalizadora[4], a Autoridade Nacional de Proteção de Dados. As primeiras leis de

[3] A LGPD dispõe sobre o 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.

[4] A Autoridade Nacional de Proteção de Dados do Brasil possui competência para zelar pela proteção dos dados pessoais nos termos da legislação.

ISSN 2238-9121

proteção de dados surgiram em outros países, no entanto, por volta dos anos 1970, principalmente no continente Europeu e nos EUA.

Há dois modelos predominantes de proteção de dados. O modelo europeu, que tem como característica a existência de uma lei geral para regular a matéria, e o modelo americano, que aposta em uma fragmentação da regulação através de normas setoriais específicas para cada situação. Logo, o Brasil, ao adotar uma lei geral de proteção de dados, seguiu o modelo europeu.

O modelo europeu foi se modificando ao longo dos anos. Em 2016, houve a aprovação do Regulamento Geral de Dados Pessoais da União Europeia. Válido em todos os países-membros da União Europeia, revogou a Diretiva de 1995, um instrumento normativo que não era vinculativo mas que representava já a quarta geração de leis de proteção de dados na Europa.

Para compreender o nível de proteção de dados no Brasil se opta por abordar primeiro, o surgimento da necessidade de proteção de dados pessoais e a elaboração de leis para a tutela deste novo direito. Finalmente, o enfoque é a atuação das autoridades independentes de proteção, em especial a brasileira, para averiguar-se o nível de proteção de dados no Brasil.

Como afirma Pérez-Luño[5], as pessoas possuem uma ilusão de que os direitos sempre existiram. Os direitos seriam estáticos. Quando se trata de proteção de dados, ser percebe a força do dinamismo. Fruto de disputas sociais e políticas nos seus respectivos contextos, o direito à proteção de dados pessoais surge com o desenvolvimento da informática.

Neste sentido se fala em gerações de direitos humanos para caracterizar os momentos históricos de seu reconhecimento. A primeira geração de direitos humanos seria referente ao período do Iluminismo, por volta do começo do século XIX, com os direitos civis e políticos. Estes direitos representam as liberdades e possuem cunho negativo em relação ao Estado, ao limitar o seu poder atuação quando envolvido direitos como a vida, a liberdade, a liberdade de expressão, a propriedade, entre outros. São considerados assim direitos e garantias individuais.

[5] 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: 23 fev. 2021.

ISSN 2238-9121

Já por volta do início do século XX, começam a ocorrer movimentos operários de reivindicação como a proibição de utilização de crianças nas fábricas, limitação de horas diárias, possuindo um sentido mais coletivo de proteção, sendo denominados como direitos sociais. Por sua vez, os direitos sociais exigem uma atuação positiva do Estado de modo a atuar para a tutela destes direitos. Também possuem um sentido de complemento aos direitos de primeira geração, como se observa, por exemplo, do direito à saúde em relação ao direito à vida. É por isso que não se devem confundir as gerações de direitos humanos com a substituição de uma geração pela outra, havendo autores que preferem adotar o termo 'dimensões' para abordar os direitos humanos[6].

No entanto, posteriormente, outros direitos passaram a ser reivindicados, como o direito à paz entre os povos, como condição para o exercício das demais gerações de direitos humanos, os individuais e coletivos, principalmente, com o fim da segunda guerra mundial em 1945. Do mesmo modo, viver em um meio ambiente saudável, com a globalização e industrialização, passou a ser determinante para o exercício de demais direitos. Assim como, os direitos do consumidor.

O surgimento da informática possibilitou o armazenamento de grandes quantidades de dados pessoais, assim como uma combinação mais ampla diante das possibilidades matemáticas dos computadores. O receio em relação aos possíveis danos à liberdade e à privacidade das pessoas enseja a criação das primeiras leis de proteção de dados, como já mencionado, por volta dos anos 1970 em países mais desenvolvidos. Fala-se aqui de um direito à liberdade informática, retratando a discussão na doutrina jurídica e na própria jurisprudência, como ocorreu com o julgamento pela inconstitucionalidade da Lei do Censo alemão em 1983 pela Suprema Corte daquele país.

Alguns autores irão denominar estes novos direitos como de terceira geração, que devido à sua complexidade e seu grau de alcance de degradação exigem esforços em escala planetária. São considerados direitos de solidariedade. Mas, independentemente da discussão doutrinária acerca dos direitos de terceira geração, o que importa aqui refletir são as novas formas de tutela de direitos fundamentais que exigem estes novos direitos. E como afirma Pérez-Luño[7], as autoridades independentes de proteção, que surgem juntamente com as primeiras leis de proteção de dados, são um dos exemplos de destaca

[6] SARLET, Ingo. **Curso de direito constitucional.** São Paulo: Saraiva, 2015, p. 322.
[7] PÉREZ LUÑO, Antonio-Enrique. La tutela de la libertad informática en la sociedad globalizada. **Isegoría**, [s.l.], n. 22, p.59-68, 30 set. 2000. Editorial CSIC. Disponível em: http://isegoria.revistas.csic.es/index.php/isegoria/article/view/521/521. Acesso em: 16 mai. 2021.

da necessidade de criação de novas formas de tutela de direitos fundamentais dos direitos de terceira geração.

Cumpre aqui apontar os principais aspectos da evolução conceitual do direito à privacidade, para então encontrar o papel da autoridade independente de proteção para o direito à proteção de dados pessoais. O direito à privacidade nasce da discussão de um famoso artigo escrito por dois juristas americanos em 1890. A preocupação gerada pelos meios de comunicação de massa que começam a se estabelecer naquela época por possíveis publicações que pudessem afetar a tranquilidade psíquica das pessoas originou no que se denominou de direito à privacidade.

Este direito ganhou reconhecimento internacional em Convenções como a Declaração Universal dos Direitos Humanos de 1948 da ONU[8]. No entanto, com o desenvolvimento da informática e a possibilidade de tratamento de dados superior a capacidade humana, passou-se a discutir a privacidade de um ângulo não apenas individualista, mas coletivo, diante da possibilidade de discriminação de grupos de pessoas através destes bancos de dados.

Apesar da síntese da evolução conceitual do direito à privacidade, desde seu surgimento à proteção de dados pessoais decorrente do surgimento da informática, é possível afirmar que a indeterminação do conceito é uma característica intrínseca da matéria[9]. Pode-se apontar a tradição norte-americana sobre o conceito de privacidade, como uma situação complexa que envolve uma ampla gama de direitos decorrentes de diferentes situações envolvendo o livre desenvolvimento da pessoa humana, a privacidade e a democracia.

Portanto, a informática possibilitou o desenvolvimento de bancos de dados que podem atingir a liberdade, a privacidade e a igualdade das pessoas. A ideia de evolução do conceito de privacidade para o de proteção de dados encontra consonância na visão de geração de direitos humanos, e o direito aqui em questão, a liberdade informática. O direito à proteção de dados e a liberdade informática possuem relevância na medida em que são condições necessárias para o exercício de outros direitos.

[8] "Artigo 12 Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.". ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. PARIS, 10 dez. 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 15 fev. 2020..

[9] LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011, p. 51.

Pérez-Luño[10] irá afirmar que este seria o lado perverso das novas tecnologias, e que para o desfrute de seus benefícios seria necessário a regulação. No caso da informática, as leis de proteção de dados pessoais. Neste momento, a preocupação era com a vigilância por parte do Estado, que já era fruto de experiências totalitárias durante a segunda guerra mundial. No entanto, era reconhecido que este mesmo Estado necessitava de informações para governar, como se podia perceber na elaboração de pesquisas como censos demográficos.

Os debates públicos neste sentido chegaram ao ápice quando do julgamento pela Suprema Corte alemã da lei do censo em 1983, onde diante da possibilidade de que informações colhidas nestas pesquisas pudessem ser utilizadas com outras finalidades como a retificação de registros públicos e certidões de nascimento, ou mesmo a revogação de algum benefício assistencial, fez com que houvesse um boicote da população para não responder aos questionários. Nascia ali o conceito da autodeterminação informativa.

De outro lado, com a expansão das novas tecnologias na economia fez-se com que houvesse uma descentralização dos bancos de dados. Logo, uma segunda geração de leis de proteção de dados visou não apenas criar um órgão para autorizar o funcionamento destes bancos informatizados, como conferiu aos cidadãos direitos e que caso se sentissem prejudicados poderiam procurar uma autoridade de proteção para registrar suas reclamações.

Foram criados princípios para o tratamento lícito dos dados pessoais[11], como a finalidade, a segurança, o consentimento, a transparência, entre outros, que passaram a

[10] "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, Antonio-Enrique. **? Ciberciudadani@ o ciudadani@.com?** Barcelona: Gedisa, 2003. P. 105.

[11] Doneda elabora uma síntese destes princípios: 1 – *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos. 2 – *Princípio da exatidão:* Os dados armazenados deve ser fieis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade. 3 – *Princípio da finalidade,* pelo qual toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes de sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a utilização de determinados

fazer parte de Convenções Internacionais que passaram a padronizar as regras. Como destaque se tem a Convenção de Estrasburgo de 1981[12] assinada por vários países. Embora este padrão internacional das regras sobre proteção de dados conferisse uma maior possibilidade de cumprimento e de respeitos aos direitos nele envolvidos, também se discutiu a efetividade da autodeterminação informativa principalmente em casos em que o cidadão ao não aceitar fornecer seus dados pessoais acabava por ser tolhido de algum serviço ou possibilidade no comércio. Ademais, também foram criadas categorias especiais de proteção como os dados sensíveis, procurando limitar o seu tratamento diante dos riscos maiores de discriminação.

A Diretiva da União Europeia em 1995, como uma quarta geração de leis de proteção de dados engloba todo este desenvolvimento. No entanto, a Internet naquele período apenas iniciava sua trajetória na economia. Foi em 2013 que se passou a discutir a necessidade de reformulação e elaboração de uma nova lei de proteção de dados na União Europeia diante do escândalo público das revelações de Edward Snowden[13] e o desrespeito

dados para uma certa finalidade (fora da qual haveria abusividade). 4 - *Princípio do livre acesso,* pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias destes registos com a consequente possibilidade de controle destes dados, após este acesso de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou ainda pode-se proceder a eventuais acréscimos. 5 – *Princípio da segurança física e lógica,* pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. 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.

[12]**Artigo 1º - Objetivos e finalidades.** A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»). **Artigo 2º - Definições.** Para os fins da presente Convenção: **a)** «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados») [...]. CONSELHO DA EUROPA. Convenção nº Convenção 108 - 1981, de 20 de janeiro de 1981. **CONVENÇÃO PARA A PROTECÇÃO DAS PESSOAS RELATIVAMENTE AO TRATAMENTO AUTOMATIZADO DE DADOS DE CARÁCTER PESSOAL**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 23 fev. 2021.

[13] "As práticas de vigilância reveladas por Snowden mostra claramente, se não completamente, que os governos - especialmente americano, britânico, canadense e possivelmente outras agências - participe de uma escala surpreendentemente grande monitoramento das populações e também como elas o fazem. Por um lado, a NSA envolve contratados para compartilham o ônus de seu trabalho e também reúne e extrai dados de usuários coletados por outras empresas, empresas de telefonia, internet e web. E em por outro, esse tipo de vigilância também significa que o a NSA e agências similares observam cookies e fazem login em formação. Assim, eles usam dados derivados do uso de dispositivos como telefones celulares ou mídias sociais e localização geográfica. O que os usuários inadvertidamente divulgam nessas plataformas - como Facebook ou Twitter - ou ao usar

dos Estados com as leis de proteção, a vigilância de chefes de Estado e de pessoas comuns. Esta discussão culminou na aprovação do RGDP em 2016 e na LGPD brasileira em 2018.

As principais mudanças percebidas nestas novas leis de proteção de dados é uma preocupação maior com a prevenção de danos antes que eles ocorram. Isso se percebe claramente na previsão legal do conceito de privacidade no *design*, ou seja, a ideia de construir aparelhos tecnológicos que respeitem os limites e as formas de tratamento de dados pessoais. Também se nota na exigência de relatórios de impacto de privacidade em casos específicos de tratamento de dados sensíveis, o dever dos responsáveis pelo tratamento de comunicar o titular dos dados pessoais de eventuais danos ocorridos com possíveis vazamentos de dados, e a exigência dos agentes de tratamento de comprovar o tratamento lícito dos dados pessoais em qualquer momento.

Todas estas situações, e outras, demonstram uma mudança de paradigma na proteção de dados pessoais, que vai desde a autodeterminação informativa e o princípio do consentimento para o tratamento de dados pessoais, para uma regulação dos seus riscos. Esta regulação do risco na proteção de dados pessoais irá depender fundamentalmente da atuação das autoridades independentes de proteção, que deverão fiscalizar o cumprimento da lei tanto do setor privado como do setor público.

As autoridades nacionais de proteção de dados são um exemplo de destaque de tutela inovadora de novos direitos, como o direito à liberdade informática, e suas principais funções, além da fiscalização do cumprimento da lei, é no sentido preventivo, através do dever de disseminação de uma cultura de proteção de dados pessoais na sociedade com campanhas de conscientização, assim como uma maior expertise técnica capaz de agir com maior dinamismo exigido pelo avanço tecnológico que se faz presente tanto na elaboração de pareceres consultivos em projetos de lei como na elaboração de normas administrativas.

Além disto, são o ponto crucial para o desenvolvimento de um novo paradigma de proteção de dados pessoais, perceptível na evolução legislativa, no qual busca-se ao lado

seus telefones, são dados utilizáveis para " segurança nacional " e fins de policiamento. Mas o mais importante de uma grande perspectiva de dados, metadados (veja a discussão abaixo) relacionados aos usuários que são recolhidos sem o conhecimento deles pelo simples uso dessas máquinas. Existem assim pelo menos três atores significativos nesse drama, agências de fomento, empresas privadas e, ainda que surpreendentemente, usuários comuns.". LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, [s.l.], v. 1, n. 2, p.205395171454186-13, 9 jul. 2014. SAGE Publications. http://dx.doi.org/10.1177/2053951714541861. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951714541861. Acesso em: 15 fev. 2020. P. 02.

do consentimento conferir uma maior proteção através de uma regulação que consiga prevenir os danos antes que eles ocorram, eis que estes são de difícil reparação e mensuração. O Brasil, ao aprovar sua primeira LGPD, e criar sua Autoridade Nacional de Proteção de Dados se alinha a este modelo de regulação que é difundido em vários países[14].

Recentemente, em em 25 de outubro de 2022, o Brasil aprovou a transformação da ANPD em autarquia, já que criada vinculada diretamente ao Poder Executivo, o que lhe conferiria uma maior autonomia orçamentária e técnica. Embora se reconheça que ainda se o Brasil se encontra em um momento de transição na cultura de proteção de dados pessoais, deve-se advertir que a atuação de uma autoridade independente de proteção é fundamental para a tutela dos direitos envolvidos, e que ainda, confere uma maior segurança jurídica para o desenvolvimento tecnológico no país e a possibilidade de um reconhecimento de padrão internacional de proteção o que facilitaria a expansão econômica nacional.

Estas são, portanto, as características principais do direito à proteção de dados pessoais, e a atuação da autoridade independente de proteção como forma inovadora de tutela. O próximo capítulo debate sobre o nível de proteção de dados no Brasil.

2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: UMA CONDIÇÃO EXIGIDA PARA ASSEGURAR O CUMPRIMENTO DA LEI

O Brasil aprovou sua primeira lei geral de proteção de dados apenas no ano 2018 e constitucionalmente a previsão expressa do direito à proteção de dados ocorreu somente em 2022.

[14]Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.". 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: 21 mai. 2021.

O ano de 2020 é marcado pela chegada da pandemia da Covid-19. Em março do mesmo ano, o poder executivo federal elaborou uma medida provisória[15] que visava obrigar as empresas de telecomunicações fornecerem os dados pessoais de seus consumidores e clientes para o governo que teria o propósito de elaborar um censo populacional. A medida foi alvo de ação direta de inconstitucionalidade que teve deferida medida liminar para a sua suspensão imediata, devido seus vícios e violações de normas de proteção de dados pessoais.

A situação guarda grande semelhança com a decisão de 1983 da Suprema Corte alemã sobre a inconstitucionalidade da lei do censo local. No Brasil, contudo, a grande questão advinda do julgamento foi o reconhecimento da existência do direito à autodeterminação informativa e proteção de dados pessoais em diversos países e diplomas legais, bem como a aprovação no Brasil da própria LGDP, mas de forma implícita na Constituição Federal, através da conjugação de outros direitos relacionados com a proteção de dados pessoais.

Logo, a medida liminar ao declarar a inconstitucionalidade da medida provisória[16] editada pelo governo brasileiro no ano de 2020, referente ao compartilhamento de dados pelo setor de telefonia com o governo federal se baseou na afronta ao direito à proteção de dados pessoais que está previsto de forma implícita na Constituição Federal. E o entendimento jurídico que sustentou esta posição é de grande plausibilidade, pois, como visto, a proteção de dados pessoais passa a ser uma condição para o exercício de outros direitos e liberdades, bem como para assegurar condições de isonomia e igualdade na

[15]A legislação, disposta em 05 (cinco) artigos, aduz que as empresas de telecomunicações deverão disponibilizar ao IBGE dados pessoais de seus consumidores. A finalidade é disposta no seu art. 2º: Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. § 1º Os dados de que trata o **caput** serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. § 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o **caput**. § 3º Os dados deverão ser disponibilizados no prazo de: I - sete dias, contado da data de publicação do ato de que trata o § 2º; e II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes. BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. . Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 30 maio 2020.

[16] Presente no sítio eletrônico do Supremo Tribunal Federal (Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal). A sessão de julgamento pelo plenário, ocorrida de forma virtual, que confirmou a medida cautelar, em decisão por maioria, encontra-se disponível no seu canal no Youtube.

sociedade. Se estes demais direitos estão previstos constitucionalmente, pois considerados direitos humanos de primeira e segunda geração, a violação à proteção de dados pessoais significa na prática a violação de outros direitos fundamentais.

Este entendimento foi adotado, por exemplo, no reconhecimento do Uruguai pela União Europeia de mesmo nível de proteção de dados pessoais, no ano de 2016[17]. Na decisão, foi citado que o Uruguai não reconhece expressamente o direito à proteção de dados pessoais, embora possua instrumentos jurídicos como o habeas data, e a atuação de uma autoridade independente de proteção. A situação constitucional da proteção de dados pessoais na constituição uruguaia, logo, é similar a brasileira.

No ano de 2022, uma emenda à constituição federal[18], reconheceu o direito à proteção de dados pessoais. A justificativa foi a evolução conceitual deste considerado novo direito, que decorre inicialmente do direito à privacidade, mas que vai ganhando outros contornos de modo a ser considerado dele independente. Além da previsão do direito à proteção de dados pessoais, há a previsão de exclusividade de competência da União para legislar sobre o tema.

[17] "[...] (5) A Constituição da República Oriental do Uruguai, aprovada em 1967, não reconhece expressamente o direito ao respeito pela vida privada e à proteção dos dados pessoais. Contudo, a enumeração dos direitos fundamentais não constitui uma lista fechada, dado que o artigo 72.o da Constituição determina que a lista de direitos, obrigações e garantias previstos na Constituição não exclui outros que sejam inerentes à personalidade humana ou que derivem da forma republicana de governo. O artigo 1.o da Lei n.o 18.331 de proteção de dados pessoais e ação de habeas data, de 11 de agosto de 2008 (Ley n.o 18.331 de protección de datos personales y acción de habeas data) prevê expressamente que «o direito à proteção dos dados pessoais é inerente ao ser humano, pelo que se encontra abrangido pelo artigo 72.o da Constituição da República». [...] (10) A aplicação das normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de habeas data, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento dos dados, a fim de exercer o direito de acesso, retificação e supressão, e por um controlo independente efetuado pela Unidade Reguladora e de Controlo de Dados Pessoais (Unidad Reguladora y de Control de Datos Personales – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28.o da Diretiva 95/46/CE, e que atua de forma totalmente independente.". COMISSÃO EUROPEIA. **C (2012) 5704**: DECISÃO DE EXECUÇÃO DA COMISSÃO de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Bruxelas, 2012. Disponível em: https://op.europa.eu/et/publication-detail/-/publication/d3dd96fc-ee04-11e1-8e28-01aa75ed71a1/language-pt. Acesso em: 21 mai. 2021.

[18] Acrescenta o inciso XII-A, ao art. 5º e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria, e ainda q eu compete a União organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.

Deste modo, em comparação com a Carta de Direitos Fundamentais da União Europeia de 2000[19], há também esta distinção entre o direito à privacidade, previsto no seu art. 7º, e o direito à proteção de dados pessoais, previsto no art. 8º. Ocorre que no item 3 deste, é expresso que o direito fica assegurado pela atuação de uma autoridade independente de proteção. Em outros termos, isto significa na prática dizer que o direito à proteção de dados pessoais somente pode existir com a atuação desta autoridade administrativa.

Como visto no primeiro capítulo, as autoridades independentes de proteção são exemplos de destaque de novas formas de tutela de direitos fundamentais. Mas todas suas funções, além de sua atuação, exigem antes sua independência. Por isso sua previsão expressa no diploma jurídico europeu. E, há ainda de se considerar que estas autoridades passaram a ser ponto crucial no sistema de proteção de dados, devido às novas formas de regulação com foco nas formas preventivas de proteção enfatizadas pelos avanços legislativos da matéria.

Na prática, a LGPD e o sistema de proteção de dados pessoais no Brasil adotam esta tendência e cria a autoridade nacional de proteção[20]. O Brasil possui normativamente as

[19] "*Artigo 7.º* **Respeito pela vida privada e familiar.** Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. *Artigo 8.º* **Proteção de dados pessoais.** Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses 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. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.". UNIÃO EUROPEIA. Carta nº (2000/C 364/01), de 18 de dezembro de 2000. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 mai. 2021.

[20] A competência da Autoridade Nacional de Proteção de dados brasileira está disposta no artigo 55-J "Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou

mesmas condições constitucionais em relação ao Uruguai[21], por exemplo, que tem reconhecido o mesmo nível de proteção aos dos países europeus.

O reconhecimento formal do direito à proteção de dados pessoais na constituição acresce a competência privativa da União para legislar sobre a matéria. A diferença com o texto europeu de direitos fundamentais é que neste esta expressamente reconhecida que a

transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.". 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. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 23 fev. 2021.

[21] Aponta neste sentido a dissertação de Martin Marks Szinvelski (2021) "O direito à proteção de dados na sociedade em rede: a perspectiva comparada entre a Autoridade Nacional de Proteção de Dados (ANPD) e a Unidade Reguladora e Controladora dos Dados Pessoais (URCDP) do Uruguai.". Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=10987301. Acesso 16 nov. 2022.

proteção de dados pessoais é assegurada pela atuação de uma autoridade administrativa[22]. Na constituição brasileira, nada há em relação a autoridade nacional de proteção de dados pessoais.

O dilema deste estudo, que não pode ser resolvido apenas com a reflexão e acerto conceitual sobre o tema, mas com a contribuição para o debate sobre a proteção de dados

[22] *Artigo 57.º*. **Atribuições.** Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controlo, no território respectivo: a) Controla e executa a aplicação do presente regulamento; b) Promove a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial; c) Aconselha, em conformidade com o direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento; d) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento; e) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito; f) Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.o, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo; g) Coopera, incluindo partilhando informações e prestando assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento; h) Conduz investigações sobre a aplicação do presente regulamento, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública; i) Acompanha fatos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações e das práticas comerciais; j) Adota as cláusulas contratuais-tipo previstas no artigo 28.o, n.o 8, e no artigo 46.o, n.o 2, alínea d); k) Elabora e conserva uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35.o, n.o 4; l) Dá orientações sobre as operações de tratamento previstas no artigo 36.o, n.o 2; m) Incentiva a elaboração de códigos de conduta nos termos do artigo 40º, nº 1, dá parecer sobre eles e aprova os que preveem garantias suficientes, nos termos do artigo 40.º, nº 5; n) Incentiva o estabelecimento de procedimentos de certificação de proteção de dados, e de selos e marcas de proteção de dados, nos termos do artigo 42.o, n.o 1, e aprova os critérios de certificação nos termos do artigo 42.o, n.o 5; o) Se necessário, proceder a uma revisão periódica das certificações emitidas, nos termos do artigo 42.o, n.o 7; p) Redige e publicar os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43; q) Conduz o processo de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43.o ; r) Autoriza as cláusulas contratuais e disposições previstas no artigo 46.o, n.o 3; s) Aprova as regras vinculativas aplicáveis às empresas nos termos do artigo 47.o , t) Contribui para as atividades do Comité; u) Conserva registos internos de violações do presente regulamento e das medidas tomadas nos termos do artigo 58.o, n.o 2; e, v) Desempenha quaisquer outras tarefas relacionadas com a proteção de dados pessoais. ”. 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: 23 fev. 2021.

pessoais no Brasil, é na discussão do próprio papel destas autoridades. O Brasil aprovou sua primeira lei geral de proteção de dados pessoais apenas no ano de 2018. É verdade que na última década o debate tem crescido no país, com a realização anual do Seminário Internacional de Proteção de Dados Pessoais desde 2010, com a aprovação do Marco Civil da Internet em 2014 e toda a discussão sobre a aprovação da lei geral. Esta, pode-se dizer, fruto de um grande movimento de diversos segmentos sociais que lutaram pela aprovação desta lei.

Antes mesmo da aprovação da primeira lei geral, era possível perceber a atuação de organizações não governamentais na defesa judicial de interesses coletivos relacionados à proteção de dados pessoais, como no caso de uma empresa de metrô de São Paulo que coletava as reações das pessoas aos anúncios publicitários sem o consentimento dos usuários do metrô. O fato demonstra que o direito à proteção de dados pessoais exige estes esforços e novas formas de tutela, se complementando justamente em razão destas atuações.

Porém, esta cultura jurídica da proteção de dados pessoais talvez não encontre eco em uma forma positivista de ver o direito, e por isso também se faz importante e oportuno mencionar que apenas a existência de uma lei ou sua previsão constitucional não é o suficiente para solucionar uma lesão ou ameaça a um direito. A própria legislação foi evoluindo em gerações que apostaram primeiramente na elaboração de princípios e no consentimento do cidadão para o tratamento dos dados. Com o passar do tempo e as novas formas de tratamento e novas exigências sociais, além de apostar neste mesmo caminho de regulação, também aponta na direção da prevenção dos riscos apostando na atuação independente de uma autoridade de proteção.

Este modelo de regulação corresponde em maior escala a países de tradição não romano-germânica, ao contrário do Brasil, que aposta na lei e não na construção de precedentes de julgamentos como o modelo anglo-saxão. Esta nova forma de atuação do Estado através das agências reguladoras tem sido usual na maioria dos países devido ás exigências da globalização. Tendo em vista que o Brasil não pode ser considerado ainda um país de economia avançada, também neste sentido tem sofrido mais com estas novas formas de regulação.

O que se deve afirmar categoricamente em relação a isto é a importância fundamental da independência destas agências reguladoras, o que lhe irá emprestar credibilidade técnica e autonomia financeira para executar suas funções e assim contribuir

para a preservação de direitos. No campo de proteção de dados, tem sido imprescindível, tanto que prevista expressamente em textos legais relacionados à proteção de dados pessoais[23].

Deste modo, considerando o momento de transição brasileiro em direção ao fortalecimento de uma cultura de proteção de dados pessoais, e a transformação em agência reguladora, se espera a consolidação da ANPD como instrumento importante na proteção de direitos fundamentais. Apesar da ausência expressa na Constituição, a autoridade de proteção brasileira tem expedido normativas, guias de orientação e possui canais para reclamações *on line,* o que acaba prevenindo riscos.

.

CONCLUSÃO

A atuação da Autoridade Nacional de Proteção de Dados emerge de novos desafios regulatórios e legislativos referente à temática que envolve uma ampla e variada gama de direitos. É reflexo de uma sociedade complexa e globalizada que exigem diálogo entre diferentes campos do saber de modo a aproveitar os potenciais emancipatório das novas tecnologias e prevenir suas ameaças, com ensina Pérez-Luño.

O desafio jurídico de regulação é imposto por esta dinâmica, e o Brasil, ainda que tenha levado muito tempo para a aprovação da primeira lei geral de proteção de dados, tem respondido juridicamente no sentido de acompanhamento das tendências e padrões internacionais. No entanto, diante da impossibilidade de eliminação total de riscos aos direitos, é preciso pensar em regulação, espaço estes das autoridades independentes de proteção. A independência é fundamental para a atuação de forma a efetivamente tutelar estes direitos.

O Brasil deve seguir o rumo das transformações regulatórias e legais sobre a proteção de dados, e, finalmente, após este período transitório, conferida a Autoridade

[23] Veja-se, a título de argumentação, o que dispõe o Tratado que estabelece uma Constituição para a Europa: "Artigo I-51°. **Proteção de dados pessoais.** 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. A lei ou lei-quadro europeia estabelece as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controle de autoridades independentes.". UNIÃO EUROPEIA. **Tratado que Estabelece Uma Constituição para a Europa**. 2004. Disponível em: https://europa.eu/europeanunion/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf. Acesso em: 15 fev. 2020.

Nacional de Proteção de Dados o caráter autarquia, seguir ainda mais no caminho da proteção de dados. A previsão constitucional do direito à proteção de dados no Brasil deve reforçar este entendimento, e desta maneira, realçar os potenciais emancipatórios do tratamento de dados pessoais.

REFERÊNCIAS

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: 06 ago. 2022.

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. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 06 ago. 2022.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020.** Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 30 maio 2022.

COMISSÃO EUROPEIA. **C(2012) 5704**: DECISÃO DE EXECUÇÃO DA COMISSÃO de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Bruxelas, 2012. Disponível em: https://op.europa.eu/et/publication-detail/-/publication/d3dd96fc-ee04-11e1-8e28-01aa75ed71a1/language-pt. Acesso em: 10 mar. 2022.

CONSELHO DA EUROPA. Convenção nº Convenção 108 - 1981, de 20 de janeiro de 1981. **CONVENÇÃO PARA A PROTECÇÃO DAS PESSOAS RELATIVAMENTE AO TRATAMENTO AUTOMATIZADO DE DADOS DE CARÁCTER PESSOAL**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 06 ago. 2022.

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.

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. 2022.

PÉREZ LUÑO, Antonio Enrique Pérez. La tutela de la libertad informática en la sociedad globalizada. **Isegoría**, [s.l.], n. 22, p.59-68, 30 set. 2000. Editorial CSIC. http://dx.doi.org/10.3989/isegoria.2000.i22.521. Disponível em: http://isegoria.revistas.csic.es/index.php/isegoria/article/view/521/521. Acesso em: 18 dez. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, [s.l.], v. 1, n. 2, p.205395171454186-13, 9 jul. 2014. SAGE Publications. http://dx.doi.org/10.1177/2053951714541861. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951714541861. Acesso em: 15 fev. 2022.

SARLET, Ingo. **Curso de direito constitucional.** São Paulo: Saraiva, 2015.

SZINVELSKI, Martin Marks. **O direito à proteção de dados na sociedade em rede: a perspectiva comparada entre a Autoridade Nacional de Proteção de Dados (ANPD) e a Unidade Reguladora e Controladora (URCDP) do Uruguai.** Disponível em : https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=10987301. Acesso 16 nov. 2022.

UNIÃO EUROPEIA. Carta nº (2000/C 364/01), de 18 de dezembro de 2000. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf. Acesso em: 06 ago. 2022.

UNIÃO EUROPEIA. **Tratado sobre o Funcionamento da União Europeia**. 2009. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 15 fev. 2022.