6

DOI: 10.5281/zenodo.13172066

Como citar este artigo
(ABNT NBR 6023/2018):

MIRANDA, Alexandra Cavalcante; MELO, João Pedro Pinto. Proteção de dados pessoais como direito fundamental na união europeia e no Brasil e a cooperação jurídica internacional. **Revista Insigne de Humanidades**, Natal, v. 1, n. 2, p. 96-119, maio/ago. 2024.

Recebido em: 02/05/2024
Aprovado em: 12/05/2024

Proteção de dados pessoais como direito fundamental na união europeia e no Brasil e a cooperação jurídica internacional

Personal Data Protection as a Fundamental Right in the European Union and Brazil and International Legal Cooperation

Alexandra Cavalcante Miranda[1]
Universidade Federal do Rio Grande do Norte (UFRN).
Lattes: http://lattes.cnpq.br/2945170359078147.
E-mail: alexandra.miranda.871@ufrn.edu.br.

João Pedro Pinto do Monte[2]
Universidade Federal do Rio Grande do Norte (UFRN).
Lattes: http://lattes.cnpq.br/2114142584821001.
E-mail: joao.pedro.monte.072@ufrn.edu.br.

SUMÁRIO

[1] Graduanda em Direito pela Universidade Federal do Rio Grande do Norte (UFRN). Técnica em Administração (INTEGRAR/RS). Pesquisadora do Instituto Nacional de Ciência e Tecnologia, Violência, Poder e Segurança Pública (INVIPS/CNPQ). Estagiária do Ministério Público do Rio Grande do Norte (MPRN). Lattes: http://lattes.cnpq.br/2945170359078147. E-mail: alexandra.miranda.871@ufrn.edu.br.

[2] Graduando em Direito pela Universidade Federal do Rio Grande do Norte (UFRN). Cursista em Técnico em Serviços Jurídicos pelo Instituto Federal do Norte de Minas Gerais (IFNMG). Técnico em Informática pelo Instituto Federal do Pará (IFPA). Estagiário do Sindicato dos Auditores Fiscais do Rio Grande do Norte (SINDIFERN). Lattes: http://lattes.cnpq.br/2114142584821001. E-mail: joao.pedro.monte.072@ufrn.edu.br

RESUMO:
A proteção de dados pessoais é reconhecida como um direito fundamental tanto na União Europeia quanto no Brasil, refletindo a importância de proteger a privacidade e os direitos individuais em um cenário globalizado. Este estudo analisa a evolução das legislações, destacando o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. Ambos os marcos legais estabelecem princípios fundamentais para o tratamento de dados pessoais, incluindo a necessidade de consentimento informado, a transparência, e a segurança dos dados. A pesquisa aborda os desafios contemporâneos, como a violação de dados transnacionais, e a necessidade de cooperação jurídica internacional para garantir a efetiva proteção dos dados pessoais. A comparação entre GDPR e LGPD revela semelhanças e diferenças nas abordagens de proteção de dados, evidenciando a necessidade de harmonização e colaboração internacional. Conclui-se que a cooperação jurídica internacional é essencial para enfrentar os desafios transnacionais e proteger os direitos fundamentais à privacidade e à segurança dos dados pessoais em um mundo digitalmente interconectado.

Palavras-chave:
Proteção de dados pessoais. Direito fundamental. GDPR. LGPD. Cooperação jurídica internacional.

ABSTRACT:
Personal data protection is recognized as a fundamental right in both the European Union and Brazil, reflecting the importance of safeguarding privacy and individual rights in a globalized context. This study analyzes the evolution of legislation, highlighting the General Data Protection Regulation (GDPR) in the European Union and the General Data Protection Law (LGPD) in Brazil. Both legal frameworks establish fundamental principles for the processing of personal data, including the necessity of informed consent, transparency, and data security. The research addresses contemporary challenges, such as transnational data breaches, and the need for international legal cooperation to ensure effective data protection. The comparison between GDPR and LGPD reveals similarities and differences in data protection approaches, emphasizing the need for harmonization and international collaboration. It concludes that international legal cooperation is essential to tackle transnational challenges and protect fundamental rights to privacy and data security in a digitally interconnected world.

Keywords:
Personal data protection. Fundamental right. GDPR. LGPD. International legal cooperation.

1 INTRODUÇÃO

Na era da informação, os avanços tecnológicos informacionais trazem inúmeros benefícios para a sociedade em âmbito nacional e internacional. No entanto, a proteção dos direitos fundamentais encontra novos desafios inerentes ao cenário tecnológico contemporâneo, principalmente no que tange à proteção de dados pessoais, direito que foi elevado à categoria dos direitos fundamentais, primeiramente, na União Europeia e, posteriormente, no Brasil. Para isso, é primordial a regulamentação da proteção a esse direito fundamental por meio de legislações, como a Regulação Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) do Brasil, e soluções por meio da cooperação jurídica internacional.

Este estudo delimita-se à uma análise comparativa entre o GDPR da União Europeia e a LGPD brasileira, tendo em vista que ambos compartilham o enfoque no direito fundamental à proteção de dados pessoais em âmbito transnacional e nacional, respectivamente.

Assim, surge a seguinte problemática central: como promover a efetivação do direito fundamental à proteção de dados pessoais em casos de violação de dados pessoais transnacionais na União Europeia e no Brasil, diante do cenário tecnológico globalizado contemporâneo?

Nesse sentido, este estudo se justifica em razão da importância do direito fundamental à proteção de dados pessoais na era da globalização tecnológica contemporânea, diante da transnacionalidade desses dados e das lacunas jurídicas e legislativas que dificultam a proteção a eles e facilitam a atuação de agentes que violam o referido direito fundamental na União Europeia e no Brasil, assim como em outros ordenamentos jurídicos também.

O presente estudo tem como objetivo geral mostrar os aspectos, características e principais desafios do direito fundamental à proteção de dados pessoais na União Europeia e no Brasil. Para isso, os objetivos específicos elencados visam: a) evidenciar o processo de elevação do direito à proteção de dados pessoais à categoria dos direitos fundamentais; b) discutir sobre as principais legislações regulatórias que versam sobre a proteção de dados pessoais na União Europeia e no Brasil, quais sejam: o GDPR e a LGPD, respectivamente; c) analisar a importância da cooperação jurídica internacional para a efetivação do direito fundamental à proteção de dados pessoais; e d) apontar a necessidade de se fortalecer a proteção do referido direito fundamental e a responsabilização adequada aos agentes que violarem tal direito, ou seja, promover o enfrentamento aos desafios contemporâneos transnacionais por meio da cooperação jurídica internacional.

Metodologicamente, o presente estudo foi produzido por meio de pesquisa bibliográfica baseada em dados qualitativos e fundamentada em diversos doutrinadores que discutem o referido tema em variados livros e artigos. Assim, tendo como base a pesquisa bibliográfica, utilizou-se a pesquisa qualitativa para discutir e argumentar os resultados a partir

de percepções da realidade jurídico-social europeia e brasileira, trazendo fontes de pesquisa que refletem o referido tema a partir de uma abordagem hipotético-dedutiva.

No que concerne à estruturação, o presente estudo, em primeiro lugar, após a introdução, desenvolve-se a partir de uma digressão histórica à proteção de dados pessoais como direito fundamental na União Europeia e no Brasil (Seção 2). Em segundo, faz-se uma análise da regulamentação da proteção de dados na União Europeia e no Brasil (Seção 3). Em terceiro, traz-se os desafios contemporâneos e possíveis soluções por meio da cooperação jurídica internacional em casos de violação de dados pessoais (Seção 4). Em quarto, é abordada a cooperação jurídica internacional na busca pela efetivação do direito fundamental à proteção de dados pessoais (Seção 5) e encerra-se com as considerações finais.

Espera-se, à vista disso, incentivar e promover a discussão e pesquisa jurídica, acadêmica e social sobre o presente tema, ao mostrar a proteção de dados pessoais como direito fundamental e a importância da cooperação jurídica internacional como solução para os desafios contemporâneos transnacionais, diante da era tecnológica vigente. Sendo assim, começa-se então essa análise.

2 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA UNIÃO EUROPEIA E NO BRASIL

Os direitos fundamentais, a partir de concepções diversas, como a histórica, filosófica e sociológica, consistem em prerrogativas que concretizam as exigências de liberdade, igualdade e dignidade humana, assegurando uma sociedade livre, justa e isonômica. Isto é, eles constituem o núcleo inviolável de uma sociedade política, com o intuito de garantir a dignidade da pessoa humana, razão pela qual devem ser reconhecidos formal e materialmente e de forma contínua pelo Estado (Alexy, 2024). Logo, os direitos fundamentais são aqueles direitos do ser humano reconhecidos e positivados na esfera do direito constitucional de determinado Estado e, também, das legislações regionais e internacionais (Sarlet, 2006).

2.1 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA UNIÃO EUROPEIA

No decorrer da história, os direitos fundamentais emergiram inicialmente nas declarações de direitos, na forma de proclamações solenes, onde eram enunciados os direitos, e, posteriormente, passaram a compor o preâmbulo das constituições, como na França, por exemplo. Atualmente, nos ordenamentos nacionais integram as constituições, adquirindo o caráter de normas jurídicas positivas constitucionais. Em razão disso, subjetivando-se em direito particular de cada povo, configuram declarações constitucionais de direito, o que tem consequência jurídica em âmbito nacional, regional e internacional (Silva, 2012).

Nesse sentido, além dos direitos fundamentais clássicos, leis e diretrizes foram sendo criadas com uma certa atenção aos dados sensíveis das pessoas e todo seu entorno, já

mostrando uma preocupação com a era tecnológica informacional, como a Declaração Universal de Direitos Humanos (DUDH) de 1948. Em seu artigo 12, ela dispõe que ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem no ataque à sua honra e reputação (ONU, 1948).

Diante desse contexto, a proteção de dados pessoais como direito fundamental na União Europeia foi consolidada a partir de diversas experiências legislativas no âmbito do continente europeu. Segundo Viktor Mayer-Scönberger, há uma classificação evolutiva das leis de proteção de dados pessoais na Europa com quatro gerações distintas (Doneda, 2011).

A primeira geração era formada por normas que refletiam a tecnologia à época, no intuito de regular um ambiente no qual centros elaboradores de dados concentrariam a coleta, o manuseio e a gestão dos dados pessoais. Assim, os núcleos dessas normas tratavam de autorizações para a criação de bancos de dados e do seu controle ulterior por órgãos públicos (Doneda, 2011). Esta primeira geração persiste até a lei federal sobre proteção de dados pessoais da Alemanha, de 1977. Em seguida, a segunda geração de leis surgiu no final da década de 1970, já na era dos bancos de dados informatizados, tendo como seu primeiro grande exemplo a lei de proteção de dados pessoais da França, de 1978 (Doneda, 2011).

A terceira geração de leis, surgida na década de 1980, buscou ampliar a tutela dos dados pessoais, que passou a abarcar mais do que a liberdade sobre os próprios dados pessoais, mas também a garantia da efetividade desta liberdade (Doneda, 2011). Por último, a quarta geração de leis de proteção de dados pessoais caracterizou-se por procurar suprir as desvantagens do enfoque individual, buscando o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais na escolha individual, isto é, são necessários instrumentos que elevem o padrão coletivo de proteção (Doneda, 2011).

Em face disso, é possível considerar que a Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, a convenção de Strasbourg, de 1981, é o principal marco da matéria pela visão dos direitos fundamentais. Em seu preâmbulo, a convenção estabelece que a proteção de dados pessoais está ligada à proteção dos direitos humanos e das liberdades fundamentais, sendo entendida como pressuposto do estado democrático, evidenciando sua aceitação ao artigo 8º da Convenção Europeia para os Direitos do Homem (CEDH) (Doneda, 2011).

Na supracitada convenção de Strasbourg, “o direito à proteção de dados finalmente alçou à condição de direito fundamental de natureza autônoma, mas vinculando, como tal, apenas os estados integrantes da União Europeia (UE), o que se deu apenas com a entrada em vigor do Tratado de Lisboa, em 2009” (Sarlet, 2020, p. 183).

Posteriormente, o direito fundamental à proteção de dados pessoais é consagrado na Diretiva 95/46/CE, de 24 de outubro de 1995, diretiva sobre proteção de dados pessoais da União Europeia (UE), que viria a ser substituída pelo GDPR futuramente. Em seu artigo 1º, que trata do *objetivo da diretiva*, afirma que os Estados-membros assegurarão a proteção das liberdades e dos direitos fundamentais das pessoas singulares, como o direito à vida privada, no que tange ao tratamento de dados pessoais. Dessa forma, a proteção de dados pessoais

como direito fundamental é consagrada na UE, assim como, posteriormente e a seu modo, é consagrada no Brasil, conforme o exposto a seguir.

2.2 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NO BRASIL

Para Paulo Bonavides, é possível observar no decorrer da história dos direitos fundamentais, um desenvolvimento que se dá em cinco gerações. Na primeira estão os direitos de liberdade, ou seja, os direitos civis e políticos, surgidos no século XVIII em meio à fase inicial do constitucionalismo. Na segunda estão os que surgiram com o constitucionalismo social-democrático do século XX, como os direitos sociais, econômicos e culturais. Na terceira estão aqueles cuja principal característica reside em sua universalidade, tendo como destinatário não o indivíduo, mas o gênero humano, como o direito ao desenvolvimento, ao meio-ambiente e a proteção ao patrimônio comum da humanidade. Por fim, na quarta geração estão os direitos à democracia, à informação e ao pluralismo, e como direito fundamental de quinta geração está o direito à paz (Bonavides, 2020).

A Constituição da República Federativa do Brasil de 1988 (CRFB/1988), de acordo com seu artigo 5º, dispõe que todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, além da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente da violação desses direitos fundamentais (Brasil, 1988). No entanto, a CRFB/1988 não reconhece expressamente em seu texto originário o direito à proteção de dados pessoais como sendo um direito fundamental, conforme Sarlet (2020, p. 183):

> No caso do Brasil, como já antecipado, a Constituição Federal de 1988 (CF), embora faça referência, no art. 5º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não contempla expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira.

Nas últimas décadas, foram elaborados diversos diplomas legais que, direta ou indiretamente, garantem a proteção de dados pessoais, o que mostra a importância dessa matéria para o legislador, como reflexo dos anseios sociais. Aqui, cabe destacar a Lei nº 8.078/1990, o Código de Defesa do Consumidor (CDC/1990), que assegura ao consumidor, em seu artigo 43, o acesso a suas informações pessoais e de consumo constante em cadastros, registros e suas fontes. Outro exemplo é a Lei Complementar nº 105/2001, a Lei do Sigilo Bancário, que protege as operações (ativas e passivas) e serviços entre uma instituição

financeira e seu cliente, garantindo o sigilo e preservando a vida privada do cidadão no âmbito bancário e financeiro.

Nesse sentido, em 2002, o Código Civil (CC/2002) destacou a privacidade e a intimidade do cidadão, alinhando-se aos direitos da personalidade. Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) surgiu como referência para proteção de dados e privacidade online (Cots; Oliveira, 2019). Anos mais tarde, a promulgação da Lei nº 13.709, de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), introduziu novos contornos e perspectivas à realidade jurídica e social.

Segundo o artigo 1º da LGPD, o seu foco é 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 (Brasil, 2018).

Mesmo diante de todo esse arcabouço normativo, ainda se fazia necessário a positivação expressa do direito à proteção de dados pessoais à nível constitucional, tendo em vista a sua importância para a sociedade, especialmente na era da tecnologia da informação. Nessa perspectiva, o Supremo Tribunal Federal (STF), em julgamento ocorrido em maio de 2020, reconheceu a proteção de dados pessoais como um direito fundamental autônomo, por meio da Ação Direta de Inconstitucionalidade (ADI) nº 6.387 MC-Ref/DF, na qual:

> Cuida-se de pedido de medida cautelar em ação direta de inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil contra o inteiro teor da Medida Provisória nº 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020" (STF, 2020).

Em face da referida decisão do STF, ascendeu o debate em torno da necessidade de se incorporar a proteção de dados pessoais à CRFB/1988 como um direito fundamental, para que não houvesse mais nenhuma margem a interpretações que violassem ou negassem tal direito. Dessa forma, a proteção de dados pessoais alçaria a posição de direito fundamental de caráter geral e especial, como a dignidade da pessoa humana, por exemplo.

Nesse contexto, e em virtude de a CRFB/1988 cuidar da garantia da privacidade e da intimidade como faces da própria garantia da individualidade, foi promulgada em fevereiro de 2022 a Emenda Constitucional (EC) nº 115/2022[1], que adicionou o inciso LXXIX ao artigo 5º,

[1] A referida Emenda é decorrente da Proposta de Emenda à Constituição (PEC) nº 17, de 2019, que buscava alterar a redação do inciso XII do art. 5º, do §3º do art. 37 e do §4º do art. 225 da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para atualizar as competências dos órgãos públicos. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 2 jan. 2024.

dispondo que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 1988).

Com isso, a proteção de dados pessoais foi positivada expressamente na CRFB/1988, trazendo segurança jurídica ao assumir a condição de limite material à reforma constitucional, conforme o seu artigo 60, que trata das cláusulas pétreas, além de proporcionar soluções mais efetivas no combate às violações desse direito, assim como é possível constatar em outros ordenamentos jurídicos, como o exposto a seguir.

3 REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA E NO BRASIL

A Europa é reconhecida por sua atenção aos direitos fundamentais, incluindo a proteção de dados pessoais. Essa ênfase é resultado de fatores históricos, políticos e sociais, levando os países europeus a elevarem a proteção de dados pessoais à categoria de direito fundamental. Assim, o papel proeminente da Europa na definição do quadro global para a proteção de dados influenciou significativamente o Brasil, refletindo-se na elaboração de sua legislação sobre o tema, que incorporou princípios e conceitos europeus.

3.1 REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA – GDPR: PRINCÍPIOS E CARACTERÍSTICAS

Em 27 de abril de 2016 foi aprovado o Regulamento nº 2016/679 do Parlamento e do Conselho Europeu, denominado de Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*), ou GDPR, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O GDPR abrange todas as organizações que processam dados pessoais de residentes na UE, independentemente de sua localização, fazendo com que empresas globais que coletam e processam dados de cidadãos em sua jurisdição sejam obrigadas a aderir ao GDPR. Este revogou a já citada Diretiva nº 95/46/CE, antigo regulamento geral sobre a matéria, mas preservou seus objetivos e princípios basilares.

A Diretiva nº 95/46/CE, que regulamentou a proteção de dados pessoais na Europa até o ano de 2016, definiu, em seu artigo 2º, que dados pessoais são:

> [...] qualquer informação relativa a uma pessoa singular identificada ou identificável (“pessoa em causa”); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social (UE, 1995).

Nessa perspectiva, o GDPR visa harmonizar a defesa dos direitos fundamentais das pessoas singulares em relação ao tratamento de seus dados pessoais e assegurar a livre

circulação desses dados entre os Estados-membros da UE, fazendo com que empresas globais que trabalham com a matéria na UE respeitem alguns limites estabelecidos pelo Regulamento (UE, 2016). No entanto, tal regulamento não deve ser entendido como um obstáculo às operações empresariais, apesar da certa complexidade do processo de adaptação, o que pode impactar, às vezes, nas atividades das empresas. Assim, faz-se necessário compreender que o propósito central do GDPR é o direito dos indivíduos de terem seus dados pessoais sendo utilizados de maneira segura, sob o escudo protetor dos direitos fundamentais (Abade, 2013).

Para elucidar a importância do GDPR, é fundamental explorar os três pilares que alicerçam suas regras. O primeiro é a *governança de dados*, que implica na criação de um sistema pré-definido para gerenciar informações, envolvendo pessoas, tecnologias, políticas e processos, visando a transparência e facilitação na tomada de decisões. O segundo é a *gestão de dados*, que representa a execução prática da governança, incluindo regras práticas do GDPR, como a obrigação de manter registros internos de todas as atividades de processamento de dados. Por último, o terceiro é a *transparência de dados*, que aborda o consentimento do usuário e a necessidade de as empresas comprovarem a autorização para utilizar os dados armazenados, o que envolve a divulgação clara e acessível das políticas de privacidade (UE, 2016).

Diante disso, o GDPR foi criado a partir de três motivações principais. Primeiramente, ele busca harmonizar as leis de privacidade de dados pessoais em toda a UE. Em segundo lugar, visa proteger a privacidade de dados pessoais dos cidadãos da UE. Por fim, propõe uma reformulação das práticas organizacionais em relação à privacidade de dados, incentivando uma postura responsável na gestão desses dados e informações sensíveis, alçando proteger os cidadãos contra as violações de privacidade em um mundo globalizado como o atual, conforme os seus princípios e características.

O GDPR representa uma resposta robusta e sistematizada a respeito do direito fundamental à proteção de dados pessoais, em face das mudanças no cenário tecnológico e de hiperconectividade no âmbito europeu. Estruturalmente, o regulamento em questão divide-se em duas seções, sendo a primeira composta por 173 considerações, que fundamentam e direcionam o regulamento. Em seguida, a segunda seção é formada por 11 capítulos, com 99 artigos ordenando os princípios e requisitos que devem ser obedecidos pelas pessoas (naturais ou jurídicas) que tratem de dados pessoais.

Sistematicamente, o GDPR traz como principais elementos: o direito ao esquecimento; a proteção específica para crianças no universo *online*; a necessidade de permissão explícita para uso de dados; a portabilidade de dados; a notificação imediata em caso de invasão e vazamento de dados, e a figura essencial do controlador de dados. Este regulamento possui também a aplicabilidade extraterritorial, sendo a única lei da UE válida para países e grupos empresariais externos ao acordo de integração, consolidando assim um conjunto sistemático de regras para promover uma gestão ética de dados pessoais no continente europeu (UE, 2016).

Em seu artigo 5º, a referida norma traz os seus princípios norteadores, sendo os alicerces que sustentam a proteção de dados pessoais, elevando-os ao patamar dos direitos fundamentais. Tais princípios são os seguintes: licitude; lealdade; transparência; limitação de finalidade; minimização dos dados; limitação de armazenamento; exatidão; integridade e confidencialidade (UE, 2016). Estes princípios terão suas aplicações fiscalizadas pelo Conselho Europeu de Proteção de Dados (EDPB, na sigla em inglês), que atua com o intuito de fiscalizar e monitorar a aplicação da lei referente à proteção de dados pessoais (UE, 2016).

Sinteticamente, o princípio da licitude, que destaca que os dados pessoais somente podem ser tratados com permissão legal; o princípio da lealdade, que aponta para o senso de justiça que deve nortear todos os tratamentos de dados pessoais; o princípio da transparência, que traz a concisão, exigindo uma linguagem simples e compreensível com a identificação do responsável pelo tratamento e a sua finalidade, e o princípio da limitação de finalidade, que determina que o tratamento de dados pessoais deve ser feito de forma específica, explícita, legítima e alicerçada em base jurídica (Maldonado; Blum, 2019).

Em mesmo sentido, o princípio da minimização dos dados pessoais, que ordena que os dados devem ser congruentes e limitados ao que é necessário para atingir suas finalidades; o princípio da limitação do armazenamento, que prescreve que os dados devem ser armazenados de maneira que se permita identificar os seus titulares durante o seu tratamento; o princípio da exatidão, que determina que os dados pessoais devem ser exatos e atuais, evidenciando um compromisso com a identidade do titular, e, por fim, os princípios da integridade e confidencialidade, que estabelecem que os dados pessoais devem ser tratados de modo que promovam a sua segurança, a proteção contra o seu tratamento ilícito e contra a sua perda, destruição ou danificação (Maldonado; Blum, 2019).

Quanto à sua implementação, faz-se necessário esclarecer o que é uma diretiva, instrumento jurídico utilizado para a criação do GDPR. A diretiva é um instrumento normativo da UE, que constitui uma fonte secundária no sistema de fontes do direito comunitário, tendo como função básica a uniformização legislativa (Doneda, 2006). Sendo assim, com a aprovação de uma diretiva, cada país-membro da UE tem um determinado período para adaptar seu ordenamento jurídico aos novos moldes estabelecidos, por meio do processo de transposição.

Neste processo, a falha de um país-membro a transpô-la de forma tempestiva acarreta um certo grau de eficácia direta da diretiva, levando o país a responder pela mora perante o Tribunal de Justiça da União Europeia (TJUE) (Doneda, 2006). Segundo o artigo 288 do Estatuto do TJUE, o regulamento detém um alcance geral, sendo obrigatório para todos os seus membros, isto é, as diretrizes vinculam os Estados destinatários quanto ao resultado almejado, ao passo que as recomendações não possuem esse caráter vinculativo (Carreau; Bichara, 2021).

Entre 1995 e os dias atuais, a hiperconectividade e o surgimento de soluções tecnológicas transformaram a obtenção e utilização de dados dos usuários, dando origem a novos e complexos dilemas éticos e normativos. Ao entrar em vigor, o GDPR respondeu a esses desafios emergentes, estabelecendo um marco regulatório mais abrangente e adaptado à era

digital, visando garantir a privacidade e segurança dos dados pessoais dos cidadãos europeus, exigindo que as companhias expliquem de forma clara e compreensiva às pessoas como usam seus dados pessoais e informações, e que haja consentimento explícito para tal uso.

Em relação ao consentimento exigido, o GDPR dispõe que:

> O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. [...]. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido (UE, 2016, item 32).

Nesse sentido, o artigo 4º, em seu item 11, preceitua que o consentimento do titular dos dados consiste em uma manifestação de vontade, livre, específica e expressa, pela qual a pessoa titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito se tornem objeto de tratamento (UE, 2016). Em face disso, e de outras características que não foram esgotadas neste estudo, o GDPR é de suma importância para a UE e, também, para outros ordenamentos jurídicos que se inspiraram nele, como o Brasil, conforme será observado a seguir.

3.2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS DO BRASIL – LGPD: PRINCÍPIOS E CARACTERÍSTICAS

No dia 14 de agosto de 2018 foi promulgada a LGPD, lei originária do Projeto de Lei Complementar (PLC) nº 53/2018, que surgiu como “uma legislação extremamente técnica, que reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humanos” (Pinheiro, 2020, p. 15). Esta lei, como já antecipado, teve bastante influência do GDPR da UE, trazendo parte de suas teorias, além de outras características pertinentes que serão abordadas abaixo.

Segundo o seu artigo 1º, 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, em consonância com a CRFB/1988 (Brasil, 2018). Esta lei deve ser observada pela União, Estados, Distrito Federal e Municípios, devendo ser aplicada a todos os atores estatais, ou seja:

> No direito constitucional e na dogmática dos direitos fundamentais brasileira é absolutamente majoritário o entendimento de que os direitos fundamentais, o que, à evidência, se aplica ao direito à proteção de dados, vinculam diretamente, na condição de normas imediatamente aplicáveis, todos os atores (órgãos, funções, agentes, atos) estatais, aqui considerados em sentido amplo, de modo a assegurar uma proteção sem lacunas (Sarlet, 2018, p. 272).

Em seu artigo 6º, a referida norma traz os seus princípios norteadores, sendo os alicerces que sustentam a proteção de dados pessoais de pessoas naturais, elevando-os ao patamar dos direitos fundamentais. Tais princípios são os seguintes: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação e responsabilização e prestação de contas (Brasil, 2018). Estes princípios terão suas aplicações fiscalizadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (Brasil, 2018).

Sinteticamente, o princípio da finalidade, que impõe que o tratamento de dados deve visar um resultado único e legítimo; o princípio da adequação, que estabelece que o tratamento de dados deve ser coerente com a finalidade do tratamento informada ao titular dos dados coletados, e o princípio da necessidade, que define que o tratamento deve se restringir aos dados necessários para ao fim colimado (Cots; Oliveira, 2019). Em mesma linha, o princípio do livre acesso, que garante ao titular dos dados informação acerca do propósito e da duração do tratamento; o princípio da qualidade, que visa garantir ao titular dos dados a sua exatidão e atualização, e o princípio da transparência, que enfatiza a ideia de privacidade, pois garante que as informações coletadas devem ser acessíveis aos seus titulares (Cots; Oliveira, 2019).

Por fim, o princípio da segurança, que garante ao titular dos dados a ser tratados que o responsável pelo tratamento adotará medidas para proteger os dados coletados; o princípio da prevenção, que diz respeito as medidas que o responsável pelo tratamento dos dados deve tomar para prevenir a ocorrência de qualquer tipo de danos às informações coletadas; o princípio da não discriminação, que garante que os dados coletados não sejam utilizados para fins discriminatórios, e o princípio da responsabilidade que garante que os responsáveis pelo tratamento de dados cumpram com as exigências da LGPD (Cots; Oliveira, 2019).

De acordo com o artigo 5º da LGPD, considera-se dado pessoal informação relacionada a pessoa natural identificada ou identificável, sendo sensível quando versar sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018). Tais dados só poderão ser tratados mediante o consentimento pelo titular (salvo exceções

previstas na lei), ou seja, pela manifestação livre e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Brasil, 2018).

Quanto à sua implementação, a LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Brasil, 2018).

No entanto, esta lei não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos ou acadêmicos, e para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais (Brasil, 2018). Em face disso, a LGPD é de suma importância para o ordenamento jurídico brasileiro, sendo essencial para o combate à violação do direito fundamental à proteção de dados pessoais em âmbito nacional e, também, contribuindo para soluções de caráter transnacional por meio da cooperação jurídica internacional, conforme será visto a seguir.

4 DESAFIOS CONTEMPORÂNEOS E POSSÍVEIS SOLUÇÕES POR MEIO DA COOPERAÇÃO JURÍDICA INTERNACIONAL EM CASOS DE VIOLAÇÃO DE DADOS PESSOAIS

Em uma análise comparativa, é possível traçar paralelos entre o GDPR da União Europeia e a LGPD brasileira, tendo em vista que ambos compartilham o enfoque na proteção da privacidade dos indivíduos e buscam estabelecer normas compreensíveis para o tratamento de dados pessoais. Embora tenham origens distintas, tanto o GDPR quanto a LGPD refletem uma tendência global em fortalecer a proteção do direito fundamental à proteção de dados pessoais e promover a responsabilidade por parte das organizações que tratam esses dados, fortalecendo o enfrentamento aos desafios contemporâneos e transnacionais por meio da cooperação jurídica internacional, conforme será abordado nesta seção.

4.1 DESAFIOS CONTEMPORÂNEOS EM CASOS DE VIOLAÇÃO DE DADOS PESSOAIS E A COOPERAÇÃO JURÍDICA INTERNACIONAL

É válido ressaltar que a LGPD é uma das legislações mais recentes e alinhadas ao GDPR, conferindo responsabilidades específicas às organizações no tocante à proteção de dados, apesar de algumas diferenças entre ambas. Por exemplo, o GDPR estipula a obrigatoriedade de designar um Encarregado de Proteção de Dados (DPO), para assegurar a conformidade com a regulamentação. Em contrapartida, a LGPD não impõe a nomeação obrigatória de um DPO para as empresas, permitindo a isenção para empresas de pequeno

porte que atendam aos requisitos legais, exigindo apenas que as organizações designem um encarregado pelo tratamento de dados como sinal de boa fé (Brasil, 2018).

Entretanto, apesar de compartilharem o objetivo central de resguardar a privacidade e segurança dos indivíduos em relação aos seus dados pessoais, destacam-se algumas diferenças notáveis no escopo de aplicação, definições, bases legais, hipóteses de tratamento, penalidades e nas funções atribuídas às organizações. Sendo assim, cada um dos diplomas legais em análise desfruta de suas próprias particularidades, que decorrem de seus aspectos territoriais, jurídicos e sociais, sem prejuízo de apresentarem semelhanças, especialmente no que tange ao enfrentamento de desafios da contemporaneidade (Paulo, 2021).

Nessa conjuntura, quando há casos de violação de dados pessoais, tais violações fragilizam a segurança jurídica nacional, regional e/ou mundial. Isto é, além das dificuldades em se estabelecer a jurisdição competente e aplicação da lei correta, a obtenção de provas e a responsabilização dos infratores relacionados à infração se torna um outro problema, em razão do fator territorial, visto que a vítima da violação pode não estar no mesmo local em que o crime ocorreu. Assim, os processos e julgamentos na presente matéria enfrentam dificuldades desde a identificação dos responsáveis até às sanções dos infratores ou pagamentos indenizatórios às vítimas, tendo a maioria desses problemas o mesmo fundamento: a dificuldade de se estabelecer uma jurisdição competente e qual a lei a se aplicar (Paulo, 2021).

Contudo, existem soluções jurídicas aplicáveis aos problemas supracitados, sendo a cooperação jurídica internacional a principal delas. A cooperação jurídica internacional constitui-se em um conjunto de normas internacionais e nacionais que rege a colaboração mútua entre os membros da sociedade internacional, principalmente os Estados e organizações internacionais, com o objetivo de facilitar o acesso à justiça e a concretização dos objetivos universais (Abade, 2013).

A cooperação jurídica internacional é composta de alguns instrumentos, como o Acordo de Assistência Mútua (MLAT), que consiste em um acordo entre autoridades de diferentes países objetivando a assistência na coleta de provas e condução de investigações, sendo esse dispositivo um dos mais úteis e efetivos em casos de violação de dados, pois facilitam o acesso a dados armazenados em outros países. Além disso, as Cartas Rogatórias também são uma ferramenta utilizada porque possibilitam o cumprimento de decisões judiciais em outras jurisdições, superando assim os desafios extraterritoriais na proteção do direito fundamental à proteção de dados pessoais.

Na esfera jurídica, o ambiente virtual (ciberespaço) é uma área emblemática porque seu aspecto transnacional desafia os conceitos jurídicos acerca de jurisdição e soberania. Isto significa que o ciberespaço não se atém a fronteiras físicas, fazendo com que a aplicação de leis exija esforços conjuntos de autoridades jurídicas de diferentes localidades/nacionalidades para a garantia de direitos, especialmente a proteção de dados pessoais.

Nesse sentido, o 17º Relatório de Riscos Globais do Fórum Econômico Mundial (*The World Economic Forum*)[2] incluiu as ameaças cibernéticas como uma de suas categorias de risco e frisou a necessidade do fortalecimento de ações que assegurem a proteção dos cidadãos no ciberespaço. Diante disso, resta evidente a necessidade de se fortalecer os instrumentos jurídicos e legislativos que versam sobre essa matéria, com a missão de sanar as lacunas que dificultam a responsabilização judicial em casos de violação de dados pessoais e, assim, superar os desafios jurídicos contemporâneos (Lemos Filho, 2018).

Tendo em vista que a harmonização das leis internacionais e nacionais acerca da matéria, apesar de ser desafiadora (uma vez que cada Estado possui sua soberania e seus próprios costumes jurídicos), é essencial para o enfrentamento à crimes dessa natureza (Kuner, 2013). Logo, a proteção do direito fundamental em comento exige rigor e efetividade, com o uso de instrumentos jurídicos eficientes e eficazes, como o já mencionado MLAT, que será explicado a seguir.

4.2 ACORDO DE ASSISTÊNCIA MÚTUA COMO INSTRUMENTO DE COOPERAÇÃO JURÍDICA INTERNACIONAL NO COMBATE À VIOLAÇÃO DE DADOS PESSOAIS

Como já mencionado, o Acordo de Assistência Mútua (*Mutual Legal Assitance Treaties*), ou MLAT, tornou-se um dos principais instrumentos jurídicos no que concerne ao enfrentamento nos casos de violação de dados pessoais, especialmente em situações transfronteiriças, pois ele facilita o acesso a dados armazenados no exterior, em outras jurisdições. No ordenamento jurídico brasileiro, a LGPD estabelece as bases legais para a transferência internacional de dados, conforme ordena o seu artigo 33:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> [...]
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> [...] (Brasil, 2018, art. 33).

Nessa perspectiva, o GPDR também versa sobre o MLAT, descrevendo o procedimento de cooperação jurídica internacional entre as autoridades de controle. Em específico, ele estabelece que uma autoridade de controle que recebe uma queixa ou detecta uma possível infração deve notificar e solicitar assistência de outras autoridades de controle pertinentes ao caso. Assim, pode-se incluir também, além do compartilhamento de

2 Ver a íntegra do relatório em: https://www3.weforum.org/docs/WEF_GRR22_Press_Release_Brazil.pdf. Acesso em: 20 abr. 2024.

informações, a realização de investigações conjuntas, conforme a primeira parte do artigo 61 do Regulamento:

> 1. As autoridades de controlo prestam entre si informações úteis e assistência mútua a fim de executar e aplicar o presente regulamento de forma coerente, e tomam as medidas para cooperar eficazmente entre si. A assistência mútua abrange, em especial, os pedidos de informação e as medidas de controlo, tais como os pedidos de autorização prévia e de consulta prévia, bem como de inspeção e de investigação.
> 2. As autoridades de controlo tomam todas as medidas adequadas que forem necessárias para responder a um pedido de outra autoridade de controlo sem demora injustificada e, o mais tardar, um mês após a receção do pedido. Essas medidas podem incluir, particularmente, a transmissão de informações úteis sobre a condução de uma investigação.
> 3. Os pedidos de assistência incluem todas as informações necessárias, nomeadamente a finalidade e os motivos do pedido. As informações trocadas só podem ser utilizadas para a finalidade para que tiverem sido solicitadas.
> [...] (UE, 2016, art. 61).

No entanto, a morosidade dos procedimentos processuais atrelados aos acordos de cooperação diminui a eficácia desses instrumentos. Isso se dá por razões como as diferenças legais e regulatórias, visto que cada jurisdição possui seus próprios instrumentos jurídicos sobre proteção de dados e requisitos processuais, tornando a cooperação jurídica algo desafiador, porém, possível. Como exemplo do uso do MLAT, é pertinente comentar o caso *Microsoft Inc. (Irlanda) vs. U.S. Department of Justice*[3], que evidenciou com maestria as dificuldades que a comunidade jurídica internacional enfrenta no que tange a cooperação bilateral em prol da proteção de dados pessoais.

Em 2013, a *Microsoft* contestou um mandado judicial dos EUA para entregar dados eletrônicos de *e-mails* hospedados em seu centro de dados na Irlanda, argumentando que violaria os princípios de soberania e territorialidade. Assim, a empresa propôs o uso do MLAT como meio adequado para obter os dados, enfatizando a necessidade de cooperação jurídica internacional. Em contraposição, o governo dos EUA defendeu que a coleta não tinha efeitos extraterritoriais, pois os dados poderiam ser obtidos remotamente no território americano.

Contudo, a Corte Distrital dos EUA rejeitou a argumentação da *Microsoft*, considerando a falta de efeitos extraterritoriais na decisão. O Governo da Irlanda e o Parlamento Europeu expressaram preocupação com a atuação unilateral dos EUA e

[3] Ver a íntegra do caso em: https://supreme.justia.com/cases/federal/us/584/17-2/. Acesso em: 20 abr. 2024.

defenderam a utilização do MLAT para garantir a cooperação jurídica internacional e o respeito ao direito fundamental à proteção de dados pessoais. Por fim, o caso foi submetido à Suprema Corte norte-americana. Entretanto, com a entrada em vigor do *Cloud Act*[4], em 2018, responsável por autorizar a coleta de dados armazenados em outra jurisdição, foi declarada a impossibilidade da lide, e a devolução do processo à Corte de origem.

Diante disso, resta evidente a importância da cooperação jurídica internacional, principalmente quando se trata da proteção de dados pessoais em questões emblemáticas no cenário transnacional, com a vantagem de que as próprias leis sobre proteção de dados pessoais, como o GDPR e a LGPD, já possuírem instrumentos que garantem essa cooperação, possibilitando respostas eficazes em casos de violação de dados pessoais e efetivando o direito fundamental em questão, conforme será aprofundado na próxima seção.

5 COOPERAÇÃO JURÍDICA INTERNACIONAL NA BUSCA PELA EFETIVAÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Nessa incursão, é importante frisar que a cooperação jurídica internacional é fundamental para a viabilidade de qualquer lei de proteção de dados pessoais, justamente por que os dados são transmissíveis livremente por meio da *internet*. Sendo assim, a necessidade de integração política e econômica em um contexto globalizado implica na regulamentação das relações jurídicas para além das fronteiras, desafiando a concepção tradicional de soberania como um limite à jurisdição. Logo, a cooperação jurídica internacional assume um papel crucial ao se desenvolver sem a presença de uma jurisdição transnacional, mas sim através de relacionamentos pautados no compromisso de assistência mútua entre os Estados.

5.1 COOPERAÇÃO JURÍDICA INTERNACIONAL E TRANSNACIONALIDADE: UM NOVO PARADIGMA PARA A PROTEÇÃO DE DADOS PESSOAIS

No que tange à cooperação jurídica internacional, torna-se imperativo enfatizar um elemento de grande relevância: a transnacionalidade. Esta transcende a noção de Estado nacional, assim como os dados pessoais contemporâneos ultrapassam as fronteiras nacionais, configurando-se, assim, como transnacionais. Neste ponto, faz-se necessária a compreensão do conceito de transnacionalidade a partir da visão do direito internacional contemporâneo.

Na atualidade, o direito internacional ordena as relações entre todos os membros da sociedade internacional (Estados, organizações e organismos internacionais e pessoas privadas, incluindo os indivíduos), o que o faz ser caracterizado como direito transnacional

4 Os Estados Unidos promulgaram a Lei de Esclarhizante, lei sobre Negócios Estrangeiros (CLOUD) Act, em março de 2018 para acelerar o acesso a informações eletrônicas detidas por provedores globais com sede nos EUA que são críticas para as investigações de crimes graves de nossos parceiros estrangeiros, desde terrorismo e crimes violentos até exploração sexual de crianças e crimes cibernéticos. Disponível em: https://www.justice.gov/criminal/cloud-act-resources. Acesso em: 20 abr. 2024.

(Carreau; Bichara, 2021). Tal concepção é oriunda do jurista americano Philip Caryl Jessup, que define esse direito transnacional como sendo o direito que regulamenta as ações e/ou os acontecimentos que transcendem as fronteiras nacionais (Carreau; Bichara, 2021).

Em mesma linha, a transnacionalidade pode ser entendida como sendo os novos espaços públicos não vinculados a um território específico, que perpassam a ideia clássica de nação jurídica, aceitam a pluralidade como premissa maior e possibilitam o exercício de poder a partir de uma pauta axiológica consensual destinada a viabilizar a proposição de um novo pacto de civilização. Essa perspectiva ressalta a natureza para além das fronteiras nacionais, destacando a essência da colaboração entre nações no cenário global (Cruz; Bodnar, 2009). Isto é, na atualidade, em razão de um processo de pluralização na estrutura do direito internacional, este deixa de ser um Direito apenas estatal para repercutir além da figura do Estado, na vida das pessoas e em uma realidade plural de direitos e sujeitos, como instrumento de invocação de direitos sociais fundamentais (Menezes; Marcos, 2020).

Nesse ínterim, a essência da cooperação jurídica internacional não se limita à concepção de Estados conectados por normas derivadas de valores moldados por uma realidade jurídica, econômica e social que os orienta nessa interação (Menski, 2006). Na medida em que a jurisdição estatal encontra limites atrelados ao seu território, surge a necessidade do Estado contar com a colaboração dos demais para fazer valer suas decisões sobre pessoas, bens e condutas localizados ou realizados no âmbito extraterritorial, o que é denominado de cooperação jurídica internacional.

Ao lidar com a cooperação jurídica internacional, é imperativo reconhecer que a integração entre nações não está isenta de desafios e controvérsias, e a segurança dos dados pessoais emerge como uma preocupação significativa. A violação de dados pessoais representa uma problemática intrínseca a esse ambiente globalizado. Isto significa que tal abordagem requer um espírito de diálogo, negociação e cooperação, respeitando a pluralidade e diversidade, em vez de lutar contra visões distintas que buscam excluir totalmente outras perspectivas (Menski, 2006).

Dessa forma, a cooperação jurídica internacional não apenas viabiliza a resolução pacífica de conflitos, mas também desafia os Estados a desenvolverem estratégias conjuntas para protegerem seus cidadãos contra as ameaças modernas, como a violação de dados pessoais no cenário transnacional decorrentes dos avanços tecnológicos informacionais. Tais avanços ultrapassam os limites de segurança e dificultam a percepção e o controle dessas tecnologias, como a inteligência artificial, por exemplo, assunto que merece um estudo específico, tendo em vista a gama de elementos que a compõe e seus inúmeros dilemas. Além disso, outros desafios transnacionais merecem discussão, como os elencados a seguir.

5.2 DESAFIOS TRANSNACIONAIS À PROTEÇÃO DE DADOS PESSOAIS E AVANÇOS REGULATÓRIOS NA AMÉRICA LATINA

À exemplo de casos que transcendem as fronteiras nacionais, destaca-se o contencioso entre a empresa de tecnologia americana Meta e a UE, um embate que lançou luz sobre a inovação tecnológica, proteção da privacidade e a busca por soluções eficazes em um ambiente globalizado. Em janeiro de 2023, a Comissão de Proteção de Dados da Irlanda, órgão regulador de privacidade da UE, emitiu uma penalidade à Meta, conglomerado que controla as plataformas *Facebook*, *Instagram*, dentre outras, relacionada à violação de serviços das redes sociais, no valor de 390 milhões de euros, por ferir as normas de proteção de dados pessoais estabelecidas no GDPR (Halpin, 2023).

No caso, o veredito da referida Comissão revelou que a Meta foi considerada responsável por armazenar e transferir de forma ilícita dados pessoais de usuários europeus para servidores localizados nos EUA, prática proibida pela legislação regulatória europeia. Este caso ilustra os desafios enfrentados por grandes corporações globais ao operar em conformidade com as rigorosas diretrizes de proteção de dados da UE (Halpin, 2023).

Ao final, a decisão proferida pela Corte Europeia representou um marco significativo e sublinhou não apenas a complexidade das questões envolvidas na proteção de dados pessoais em um contexto transnacional, mas também enfatizou a necessidade de se estabelecer diretrizes internacionais coerentes para a harmonização das legislações nacionais e a garantia da privacidade digital em escala global (Halpin, 2023).

No âmbito da América Latina, destaca-se a Rede Iberoamericana de Proteção de Dados (RIPD), um mecanismo regional para cooperação na esfera da privacidade e proteção de dados pessoais. A RIPD envolve organizações de diversos setores, desempenhando um papel significativo na promoção do direito à proteção de dados pessoais na região iberoamericana, que compreende os territórios, no continente americano, onde o português ou espanhol são as línguas predominantes.

Outrossim, um marco significativo evidenciou-se nas Diretrizes de Proteção de Dados Pessoais para Estados Iberoamericanos, aprovadas no XVI Encontro Iberoamericano de Santiago do Chile, em junho de 2017. Insta salientar que essas diretrizes foram elaboradas com o apoio da Comissão Europeia, consolidando-se como um modelo regional de referência para o direito de proteção de dados pessoais. Tais diretrizes fornecem uma base jurídica para a revisão das normas existentes e orientam a formulação de normas futuras (Aguiar, 2022).

Diante dessa repercussão, a referida Rede estabeleceu-se como o principal catalisador do diálogo e das iniciativas de proteção de dados pessoais na região ibero-americana. Em termos de impacto, os benefícios alcançaram mais de 350 milhões de cidadãos latino-americanos que agora contam com leis de proteção de dados pessoais e autoridades locais empenhadas em assegurá-las. No Brasil, semelhante à UE, em incidentes de segurança, mesmo com a implementação de todas as medidas previstas na legislação para evitá-lo, os responsáveis devem comunicá-lo imediatamente à ANPD, autoridade fiscalizadora

competente. A comunicação à ANPD deve incluir a descrição dos dados afetados, informações sobre os titulares, medidas de segurança adotadas, riscos do incidente, motivos da demora, se houver, e medidas para reverter ou mitigar danos (Brasil, 2018).

Em face disso, a cooperação jurídica internacional revela-se como elemento essencial na dinâmica da proteção de dados pessoais na contemporaneidade. A transnacionalidade desafia a concepção tradicional de soberania, demandando colaboração entre Estados e os demais membros da sociedade internacional, para efetivar a proteção de dados pessoais.

Logo, são essenciais as redes de integração, como a RIPD, e a comunicação imediata à autoridade fiscalizadora competente em casos de incidentes de segurança, reforçando a necessidade de respostas cooperativas no enfrentamento aos desafios jurídicos transnacionais da contemporaneidade, que implicam na efetivação (ou não) do direito fundamental à proteção de dados pessoais.

6 CONSIDERAÇÕES FINAIS

Em síntese, o presente estudo mostrou que a proteção dos direitos fundamentais encontra novos desafios inerentes ao cenário tecnológico globalizado contemporâneo, principalmente no que tange à proteção de dados pessoais, direito que foi elevado à categoria dos direitos fundamentais tanto na União Europeia quanto no Brasil. Nessa perspectiva, evidenciou-se a regulamentação da proteção a esse direito fundamental por meio de legislações, como o GDPR da União Europeia e a LGPD do Brasil, e foi discutido soluções para a presente problemática por meio da cooperação jurídica internacional.

Analisou-se, de forma comparativa, a importância do GDPR da União Europeia e da LGPD brasileira, tendo em vista que ambas as regulamentações compartilham o enfoque no direito fundamental à proteção de dados pessoais em âmbito transnacional e nacional, respectivamente. Com isso, chegou-se à resposta para a problemática central, ou seja, é necessário promover o uso da cooperação jurídica internacional, como um instrumento de efetivação do direito fundamental à proteção de dados pessoais em casos de violação transnacionais na União Europeia e no Brasil, diante do cenário atual versado.

Portanto, conforme foi apontado, este estudo trouxe à tona a importância do direito fundamental à proteção de dados pessoais no cenário tecnológico globalizado contemporâneo, diante da transnacionalidade desses dados e das lacunas jurídicas e legislativas que dificultam a proteção a eles e facilitam a atuação de agentes que violam o referido direito fundamental na União Europeia e no Brasil, assim como em outros ordenamentos jurídicos também.

Por fim, espera-se que este estudo possa impulsionar a discussão e pesquisa jurídica, acadêmica e social sobre o tema em questão, promovendo o avanço dos mecanismos de proteção de dados pessoais como direito fundamental. Ademais, busca-se fomentar uma

maior cooperação jurídica internacional como resposta aos desafios transnacionais atuais, em meio ao contexto da globalização tecnológica.

REFERÊNCIAS

ABADE, Denise Neves. **Direitos fundamentais na cooperação jurídica internacional**. São Paulo: Saraiva, 2013.

AGUIAR, Thaís. Cooperação internacional em proteção de dados: conhecendo a Rede Iberoamericana de Proteção de Dados e seu Fórum da Sociedade Civil. **DataPrivacyBR Research**, 23 ago. 2022. Disponível em: https://www.dataprivacybr.org/cooperacao-internacional-em-protecao-de-dados-conhecendo-a-rede-iberoamericana-de-protecao-de-dados-e-seu-forum-da-sociedade-civil. Acesso em: 7 dez. 2023.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. de Virgílio Afonso da Silva. 3. ed. São Paulo: JusPodivm; Malheiros, 2024.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 fev. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018 /lei/l13709.htm. Acesso em: 25 abr. 2024.

BRASIL. **Proposta de Emenda à Constituição nº 17, de 2019**. Altera a redação do inciso XII do art. 5º, do §3º do art. 37 e do §4º do art. 225 da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para atualizar as competências dos órgãos públicos. Diário Oficial da União. Brasília, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 2 dez. 2023.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 35. ed. São Paulo: JusPodivm; Malheiros, 2020.

CARREAU, Dominique; BICHARA, Jahir-Philippe. **Direito internacional**. Paris: A. Pedone, 2021.

CARVALHO RAMOS, André de; MENEZES, Wagner (orgs.). **Direito Internacional Privado e a nova cooperação jurídica internacional**. 1.ed. São Paulo: Arraes, 2015.

CARVALHO RAMOS, André de. Obtenção de provas no exterior: para além da Lex fori e lex diligentiae. **Revista de Direito Internacional**, Brasília, n. 2, p. 685, 2015, v. 12.

COTS, Márcio; OLIVEIRA, Ricardo**. LGPD:** Lei Geral de Proteção de Dados comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

CRUZ, Paulo Márcio; BODNAR, Zenildo. A transnacionalidade e a emergência do Estado e do Direito transnacionais. **Revista eletrônica do CEJUR**, n. 4, 2009, v. 1. Disponível em: https://revistas.ufpr.br/cejur/article/download/15054/11488. Acesso em 5 dez. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico**, n. 2, p. 91-108, jul./dez. 2011.

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

LEMOS FILHO, Tarcísio Germano de. **A Cooperação Jurídica Internacional no Código de Processo Civil Brasileiro e a Exigência de Jurisprudência Íntegra, Estável e Coerente**. Tese (Doutorado em Ciência Jurídica) - Universidade do Vale do Itajaí, [S. L.], 2018.

HALPIN, Padraic. **Meta told to reassess legal basis for EU personalised ad**s. Reuters, 2023. Disponível em: https://www.reuters.com/technology/irish-privacy-regulator -fines-meta-more-than-400-mln-2023-01-04/. Acesso em: 10 fev. 2024.

KUNER, Christopher. **Transborder Data Flow Regulation and Data Privacy Law**. 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2274387. Acesso em: 10 fev. 2024.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Comentários ao GDPR**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MENEZES, Wagner; MARCOS, Henrique. O Direito Internacional e a Pandemia: Reflexões Sistêmico-Deontológicas. **Revista da Faculdade de Direito da UFU**, n. 2, p. 43-78, Uberlândia, 2020, v. 48.

MENSKI, Werner. **Comparative law in a global context:** The legal systems of Asia and Africa. 2 ed. Cambridge: Cambridge University, 2006.

PAULO, Matheus Adriano. **Análise Comparativa da Cooperação Internacional, das Sanções Administrativas e do Controle Judicial na Proteção de Dados na União Europeia e no Brasil**. Dissertação (Mestrado em Ciência Jurídica) - Universidade do Vale do Itajaí, [S. L.], 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei nº 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista Direitos Fundamentais & Justiça**, a. 14, n. 42, p. 179-218, jan./jun. 2020. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 20 abr. 2024.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 6. ed. Porto Alegre: Livraria do Advogado, 2006.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2012.

SUPREMO TRIBUNAL FEDERAL [STF]. **Ação Direta de Inconstitucionalidade (ADI) nº 6.387 MC-Ref/DF**. Disponível em: https://portal.stf.jus.br/. Acesso em: 25 abr. 2024.

UNIÃO EUROPEIA [UE]. **Regulamento nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - GDPR.** 2016. Disponível em: https://gdpr-info.eu/art-61-gdpr/. Acesso em: 25 jan. 2024.

UNIÃO EUROPEIA [UE]. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.** 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046/. Acesso em: 25 jan. 2024.