DOI: 10.5433/1980-511X.2024.v19.n3.p253-274

PROTEÇÃO DE DADOS PESSOAIS E AUTODETERMINAÇÃO INFORMATIVA: A EXTRATERRITORIALIDADE DA LEI 13.709/2018 E AS IMPLICAÇÕES À SOBERANIA

PERSONAL DATA PROTECTION AND INFORMATIONAL SELF-DETERMINATION: THE EXTRATERRITORIALITY OF LAW NO. 13.709/2018 AND ITS IMPLICATIONS FOR SOVEREIGNTY

André Pedroso Kasemirski*

Clodomiro José Bannwart Júnior**

Arthur Lustosa Strozzi***

*Doutorando e Mestre em Direito Negocial pela Universidade Estadual de Londrina (UEL), com bolsa CAPES. Advogado e Professor de Direito. E-mail: andre.kasemirski@uel.br. ORCID: https://orcid.org/0000-0001-6760-3680.

**Doutor e Mestre em Filosofia, com Pós-doutoramento pela Universidade Estadual de Campinas. Especialista em Direito Eleitoral. Professor de Filosofia e do Programa de Doutorado em Direito Negocial da UEL. ORCID: https://orcid.org/0000-0003-2897-6809.

*** Doutorando e Mestre em Direito Negocial pela Universidade Estadual de Londrina (UEL). Bolsista CAPES-Consolidação. Advogado e Professor de Direito. ORCID: https://orcid.org/0000-0002-9302-0339.

Resumo: Por intermédio do método dedutivo, corresponde à extração discursiva do conhecimento a partir de premissas gerais aplicáveis a hipóteses concretas, e a partir das técnicas de levantamento de bibliografias e legislações acerca da categoria analítica inerente à abrangência do tema proteção de dados, investiga-se e procura estabelecer reflexões acerca da eficácia da Lei 13.709/2018, fora dos limites do Estado, inclusive se sobrepondo as regras do Estado estrangeiro, de modo a implicar na violação do princípio da soberania. Estende-se como hipótese que, a aplicação da Lei 13.709/2018 fora dos limites do Estado, não desrespeita à soberania do Estado estrangeiro, mas redimensiona seus contornos, especialmente no que concerne aos direitos humanos fundamentais.

Palavras-chave: direitos humanos fundamentais; proteção de dados pessoais; autodeterminação informativa; extraterritorialidade; soberania.

Abstract: Using the deductive method, which involves extracting knowledge from general premises applicable to concrete hypotheses and employing techniques for bibliographic and legislative surveys concerning the analytical category related to data protection, this study investigates and reflects on the effectiveness of Law No. 13.709/2018 beyond state borders. This includes instances where it overlaps with foreign state rules, potentially violating the principle of sovereignty. The hypothesis is that the application of Law No. 13.709/2018 beyond state borders does not disrespect the sovereignty of the foreign state but redefines its contours, especially concerning fundamental human rights.

Keywords: fundamental human rights; protection of personal data; informative self-determination; extraterritoriality; sovereignty.

INTRODUÇÃO

A Lei Geral de Proteção de Dados projeta-se no campo constitucional dos direitos fundamentais e tem suas primeiras raízes na doutrina internacional dos direitos humanos. Nesse sentido, tanto a Lei 13.709/2018, art. 2, inciso VII[1], quanto a legislação europeia Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (*General Data Protection Regulation)*, considerando 104[2], têm como fundamento os direitos humanos para a proteção dos dados pessoais.

Assim, mediante a aplicação do processo dedutivo, explora e busca delinear ponderações sobre a efetividade da Lei Geral de Proteção de Dados além das fronteiras estatais, até mesmo ultrapassando as regulamentações do Estado estrangeiro. Como suposição, considera-se que a utilização da Lei nº. 13.709/2018 fora das fronteiras do Estado não viola a soberania do Estado estrangeiro, mas reconfigura seus parâmetros.

Para tanto, diante do método empregado, na primeira seção inicialmente discorre sobre a conexão dos direitos fundamentais com a doutrina dos direitos humanos, apontando as semelhanças e diferenças da doutrina quanto às terminologias adotadas, entre elas "direitos humanos", "direitos do homem" e "direitos fundamentais", tomando como referencial teórico, entre outras obras, os estudos de Ingo Wolfgang Sarlet e Manoel Gonçalves Ferreira Filho.

Em seguida, estabelecido o conceito de direitos humanos, no qual a proteção de dados tem seu primeiro fundamento, a partir dos estudos de J. J. Gomes Canotilho e Stefano Rodotà, procura estabelecer na segunda seção os desdobramentos internacionais da autodeterminação informativa do titular. Nesse ponto, a autodeterminação informativa, correspondente ao controle conferido ao titular, não se restringe às barreiras do Estado, mas se estende dentro da rede e por todo o globo, independentemente do local de tratamento ou do local em que se situem controlador e titular.

Isto posto, reconhecida a importância da autodeterminação informativa no ambiente virtual, especialmente no que tange à proteção dos dados em ambiente internacional, na terceira seção passa a refletir acerta da aplicação da Lei 13.709/2018 em âmbito extraterritorial, inclusive se sobrepondo às normas de proteção de dados pessoais do país estrangeiro. Outrossim, discorre se, ao sobrepor

1 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

2 (104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial (European Union, 2016).

a Lei 13.709/2018 à legislação de país estrangeiro, que não fornece proteção em mesmo patamar, não se estaria a infringir o princípio da soberania.

Assim, inegável que a extraterritorialidade da lei é tema relevante e de suma importância, tendo em vista que alguns agentes de tratamento de dados (controladores e operadores) estão localizados fisicamente ou virtualmente em outros países.

É verdade que, assim como o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, a Lei nº. 13.709/2018 possui aplicação para qualquer operação de tratamento realizada pelos controladores, independentemente do país de sua sede e do país em que estejam localizados os dados. Para tanto, é necessário o enquadramento em alguma das hipóteses previstas no art. 3 da Lei nº. 13.709/2018[3], como por exemplo, que a operação de tratamento seja realizada no Brasil, ainda que os agentes de tratamento estejam localizados no exterior (inciso I).

Por outro lado, não se aplica a Lei nº. 13.709/2018 ao tratamento de dados provenientes de fora do território nacional e que não seja objeto de comunicação com agentes de tratamento brasileiro, desde que o país de proveniência proporcione grau de proteção adequado, conforme art. 4, inciso IV da Lei nº. 13.709/2018[4]. Ou seja, inexistindo grau de proteção adequado, aplicar-se-á a Lei nº. 13.709/2018 em face do Estado estrangeiro proveniente, ainda que esse possua legislação sobre a temática, porém com grau protetivo inferior.

Desse modo, ainda que discutível eventual existência de violação à soberania do Estado estrangeiro, há de se reconhecer que a Lei nº. 13.709/2018 poderá ser invocada, sem qualquer afronta, visto a ausência de proteção em grau adequado quanto à tutela dos dados pessoais. Nesses termos, a extensão extraterritorial da Lei nº. 13.709/2018 não implica na diminuição do conceito de soberania, mas no redimensionamento dos seus contornos, de modo a abranger a tutela dos direitos humanos. Logo, interferir na dignidade humana é função do Estado e a violação dos direitos humanos pelo ente Estatal implica em afronta ao poder soberano, que não está acima da lei.

3 Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - 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;
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Brasil, 2018).

4 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...]
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018).

1 A TUTELA DOS DADOS PESSOAIS ENQUANTO DIREITO HUMANO FUNDAMENTAL

A Lei Geral de Proteção de Dados, nº 13.709/18, projetada no campo constitucional dos direitos fundamentais, tem seu primeiro fundamento na doutrina internacional dos direitos humanos, motivo pelo qual é indispensável traçar um conceito claro de direitos humanos e em que medida são equivalentes ou se distinguem dos direitos fundamentais.

É verdade que a carta de 1988 é a primeira Constituição brasileira a elencar o princípio da prevalência dos direitos humanos como princípio fundamental a reger o Estado nas relações internacionais (Brasil, 1988). Nesse sentido, a Constituição Federal de 1988 inova ao trazer uma orientação internacionalista jamais vista até então na história do direito constitucional, uma vez que o Império, na experiência brasileira, cuidou da independência e da preservação da unidade nacional, enquanto que a República consolidou as fronteiras nacionais, bem como afirmou a vocação pacífica do país, de modo a reconhecer paulatinamente a importância da cooperação internacional para a preservação da paz (Piovesan, 2018, p. 117).

A expressão "direitos humanos" é um termo intrinsecamente ligado ao direito internacional público, tratando-se de um desdobramento, haja vista que quando se utiliza o termo "direitos humanos" está afirmando-se que há direitos garantidos por normas de índole internacional, ou seja, por tratados, declarações ou outros, celebrados entre Estados.

Para Valério Mazzuoli (2019, p. 25) os direitos humanos são aqueles direitos protegidos pela ordem internacional, entre os quais se encontram os tratados multilaterais, globais ou regionais, contra as violações e arbitrariedades do Estado. Mais ainda, os direitos humanos são indispensáveis a uma vida digna e, por isso, estabelecem um nível protetivo mínimo que todos os Estados devem respeitar.

Muito embora, sob a ótica internacional, a proteção dos dados pessoais já pudesse ser deduzida da Declaração Universal dos Direitos Humanos de 1948[5] e da Convenção Europeia de Direitos do Homem de 1950[6], foi na Convenção 108 para a para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais de 1981[7], conhecida como Convenção de Estrasburgo, que passou a regular o tratamento de dados pessoais. Por sua vez, somente no ano 2000 com

5 Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques (ONU, 1948).

6 Artigo 8º - 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência (European Union, 1950)

7 Artigo 1º - 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") (European Union, 1981).

a Carta de Direitos Fundamentais da União Europeia[8], CDFUE, que a proteção de dados pessoais passou a adquirir patamar de direito fundamental (Sarlet, 2021, p. 23).

Destarte, a expressão "direitos do homem" possui cunho jusnaturalista, e por sua vez remete aos direitos naturais, e podem ser compreendidos como aqueles que não foram positivados pelos ordenamentos de forma inequívoca para proteção global. Esses direitos, em tese, não se encontram nos textos das Constituições ou nos tratados internacionais, sendo raros, atualmente, a sua existência.

Já a expressão "direitos fundamentais" diz respeito à afetação da proteção em um sistema interno, ligado à matriz constitucional, na medida em que se encontrem positivados. Nesse sentido, são direitos garantidos e limitados no tempo e espaço, objetivamente vigentes em uma ordem jurídica em concreto. Isto posto, quando se utiliza a expressão "direitos humanos", está-se referindo aos direitos positivados em tratados e declarações ou previstos em costumes internacionais (Mazzuoli, 2019, p. 26).

É inquestionável que os direitos essenciais, de alguma maneira, são igualmente sempre direitos da pessoa, no sentido de que seu detentor será sempre um ser humano, mesmo que representado por coletividades (grupos, comunidades, nações, Estado).

É verdade que, no âmbito da União Europeia, convencionou-se utilizar a expressão "direitos fundamentais" de forma genérica, a exemplo da "Carta dos Direitos Fundamentais da União Europeia", mesmo não sendo essa o termo utilizado pela ONU, que utiliza a expressão para se referir aos direitos garantidos pela ordem interna.

Destarte, parte da doutrina, entre eles Manoel Gonçalves Ferreira Filho (2005, p. 46), adota e tem preferido a expressão "direitos humanos fundamentais", com o intuito de significar a união material da proteção da matriz constitucional com a expressão de direito internacional.

Nesse sentido, ao que indica a expressão "direitos humanos fundamentais" é mais adequada do que a visão em que os direitos humanos possuem uma maior amplitude. Dentro dessa acepção, os direitos fundamentais, são, por consequência, direitos humanos. Logo, os direitos fundamentais não são espécies do gênero direitos humanos, mas estariam circunscritos por eles.

É verdade que a preferência pelo termo "direitos fundamentais" dá-se pelos seguintes motivos: a) é esta a que se encontra positivada na Constituição Federal de 1988, em seu Título II; b) a tendência majoritária na doutrina moderna constitucional em rechaçar expressões como "direitos naturais", "direitos civis", "direitos individuais", "liberdades públicas", "liberdades fundamentais", porque anacrônicos (em desacordo com o atual estágio dos direitos fundamentais, notadamente na perspectiva de um Estado Democrático e Social de Direito) e insuficientes para abarcar a abrangência do assunto.

8 Art. 8º - 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. [...] (European Union, 2000).

Ao estabelecer o conceito de direitos fundamentais, Ingo W. Sarlet (2012, p. 16-18), propõe que sejam inseridos no mesmo rol todos aqueles direitos que, explicita ou implicitamente, são positivados pela Constituição Federal, assim como as posições jurídicas que possam ser a elas equiparadas por seu conteúdo ou significado.

Desse modo, o ordenamento jurídico abarcaria dois grupos: a) os direitos expressamente positivados na Constituição ou diplomas correlatos, b) direitos implicitamente positivados, os quais são compreendidos como aqueles decorrentes de princípios constitucionais ou de direitos subtendidos nas normas de direito fundamentais expressamente positivadas.

Outrossim, no primeiro grupo se encontram os direitos dispostos entre art. 5 ao art. 17 da Constituição Federal e os demais esparsos pela Constituição. Já no segundo grupo, estariam aqueles positivados na legislação infraconstitucional, porém decorrentes de princípios consagrados na Constituição Federal.

Muito embora a proteção de dados pessoais seja dotada de autonomia no que diz respeito ao seu âmbito de proteção próprio, guarda também conexão com outros direitos e princípios de matriz constitucional, assim como com o direito internacional dos direitos humanos.

É verdade que a proteção de dados pessoais não se encontrava positivada de forma autônoma no texto Constitucional, até a Emenda Constitucional nº. 115 de 2022, que incluiu o inciso LXXIX no art. 5º. No entanto, também não há dúvidas que o direito da proteção de dados pessoais já decorria do princípio da dignidade humana e do direito fundamental do livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, como é o caso da privacidade e intimidade (Sarlet, 2021, p. 36).

Nessa via, ainda que antes da EC. 115/2022 a proteção de dados não estivesse inserida no rol explícito de direitos fundamentais, inegável que se trata de norma fundamental, até porque a legislação infraconstitucional assim o dispôs expressamente. Assim, a tutela dos dados pessoais visa proteger os direitos fundamentais de liberdade e livre desenvolvimento da personalidade da pessoa natural, tendo como fundamento o respeito à privacidade, aos direitos humanos e à dignidade, conforme art. 1, caput[9] e art. 2, incisos I, II e VII[10] da Lei 13.709/2018.

O direito ao livre desenvolvimento da personalidade, ao que tudo indica, é o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados, haja vista que se trata de cláusula geral de proteção de todas as dimensões da personalidade humana (Sarlet, 2021, p. 36). Logo, inegável que a proteção de dados pessoais se encontra implicitamente positiva-

9 Art. 1º Esta Lei 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 (Brasil, 2018).

10 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...]
I - o respeito à privacidade;
II - a autodeterminação informativa; [...]
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

da enquanto um direito fundamental. Outrossim, independentemente da Emenda Constitucional 115/2022 (PEC nº. /17/2019), o qual alterou o art. 5, inciso XII para inserir a proteção de dados pessoais de forma explícita, sua proteção já decorria implicitamente da Constituição, tanto que na Ação Direta de Inconstitucionalidade – ADI nº. 6387, o Plenário do STF confirmou, em 07.05.2020, a decisão monocrática da relatora Ministra Rosa Weber, que dispôs que a proteção de dados pessoais "representa direito fundamental" e "autônomo" (Brasil, 2020).

Ademais, ainda que se possa tecer críticas ao legislador, que pretendeu ser "engenheiro de obra pronta" na PEC nº. 17/2019, atual Emenda Constitucional nº 115, de 2022, que incluiu a proteção de dados no art. 5º da CF[11], reconhecendo-a enquanto um direito fundamental, há de se identificar que a positivação formal carrega consigo uma carga positiva e agrega valor substancial ao dar destaque para a tutela dos dados pessoais.

No que diz respeito à extensão da proteção de dados, também enquanto um direito de personalidade, há de se reconhecer que as normas de direito de personalidade dispostas no Código Civil também são consideradas como direitos deduzidos de uma cláusula geral, ancorada no direito fundamental de liberdade e no princípio da dignidade da pessoa humana, conforme art. 1, inciso III, da Constituição Federal.

Nesses termos, além de compreender que a proteção de dados pessoais guarda referência e fundamento na doutrina dos direitos humanos fundamentais, há de se reconhecer que sua tutela perpassa os direitos de personalidade.

Assim, para Carlos Alberto Bittar (1999, p. 10) os direitos de personalidade devem ser compreendidos como: a) os próprios da pessoa em si (ou originários), existentes por sua natureza, como ente humano, com o nascimento; b) e os referentes às suas projeções para o mundo exterior (a pessoa como ente moral e social, ou seja, em seu relacionamento com a sociedade).

Se não bastasse, não se pode perder de vista que a proteção de dados tem tanto como "fundamento", quanto tem como objetivo "proteger" o desenvolvimento da personalidade, conforme respectivamente art. 2, inciso VII e art. 1, caput da Lei 13.709/2018.

2 A AUTODETERMINAÇÃO INFORMATIVA PARA ALÉM DOS LIMITES DO ESTADO

Estabelecido os fundamentos pelos quais a Lei Geral de Proteção de Dados nº. 13.709/18 projeta-se no campo dos direitos humanos fundamentais, passa a apresentar algumas considerações acerca do princípio da autodeterminação informativa, controle esse conferido ao titular e que merece proteção em um cenário internacional.

11 LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022) (Brasil, 2022).

O direito à privacidade, como aponta Ricardo Villas Bôas Cueva (2017, p. 62), foi primeiramente definido no clássico artigo de 1890 de Samuel Warren e Lois Brandeis, como o direito de ser deixado só, no qual se identificou a partir de precedentes do *common law.*

Além disso, ganhou relevância a teoria dos círculos concêntricos da esfera da vida privada ou teoria das esferas da personalidade elaborada mais detalhadamente pelo alemão Heinrich Hubmann em 1953, de modo que foi revisitada por Heinrich Henkel em 1957 (Mota; Tena, 2020, p. 538-576). Heinrich Henkel deu forma tripartida à teoria dos círculos concêntricos, de modo que dividiu a vida privada em sentido *lato sensu* em: o círculo da vida privada em sentido estrito, em que se insere o círculo da intimidade e, por sua vez, que se encontra adentrado o círculo do segredo (Szaniawski, 2005, p. 127).

A Constituição Federal protege a privacidade (gênero) ao reconhecer como invioláveis a vida privada, a intimidade, a honra e a imagem da pessoa (espécies). Ademais, para Tulio Lima Vianna (2004, p. 344) a privacidade decorre do direito de não ser registrado, não ser reconhecido e não ser monitorado.

Ora, na era do *big data*, a privacidade física ou clássica pode versar sobre uma invasão física na residência alheia ou, ainda, sobre o monitoramento de câmeras, enquanto que a privacidade informacional ultrapassa os limites físicos e afeta a proteção de dados pessoais, uma vez que tratados. Com isso, a privacidade informacional se concentra em resguardar o titular contra abusos no tratamento de dados pessoais, seja na coleta, classificação, utilização, acesso, reprodução, transmissão, distribuição, armazenamento, comunicação, transferência, difusão ou extração, como, por exemplo, informações relacionadas às convicções políticas e religiosas.

Nesse cenário, insere-se o conceito de autodeterminação informativa, o qual tem suas raízes no Tribunal Constitucional Federal Alemão, que, em 1983, diante da célebre sentença da Lei do Censo (*Volkszählungsurteil*) – como ficou conhecida mundialmente – elucida a relação conceitual existente entre a privacidade e a tutela de dados pessoais, sem deixar de ancorá-las aos valores fundamentais que assumem proteger.

Desse modo, o Estado alemão pretendia finalizar um censo geral em 1983, que tinha como objetivo principal realizar perguntas e confrontar os dados fornecidos com os dos registros públicos existentes. Diante do sentimento de insegurança, temendo-se a criação de um Estado "superinformado", houve questionamentos quanto à violação de direitos fundamentais, entre eles o livre desenvolvimento da personalidade e a dignidade da pessoa humana, protegidos pelos artigos 1º e 2º da Lei Fundamental da Alemanha. Como resultado, o Tribunal Constitucional Federal Alemão declarou nulos os dispositivos que versavam sobre a trocam de dados e competências para sua transmissão (Schwabe, 2005, p. 234).

Caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos, estaria caracterizada a diversidade de finalidades, o que impediria o cidadão de conhecer o efetivo uso de suas informações, em verdadeiro desatendimento das normas fundamentais.

O Tribunal entendeu que o livre desenvolvimento da personalidade pressupõe, sob as modernas condições de processamento de dados, a proteção do indivíduo contra o levantamento, a armazenagem, o uso e a transmissão irrestrita.

No mesmo sentido da decisão indicada percorre o pensamento de Canotilho (2007, p. 550):

> [...] o direito ao conhecimento dos dados pessoais desdobra-se em vários direitos: 'a) o direito de acesso, ou seja, o direito de conhecer os dados constantes de registros informáticos, quaisquer que eles sejam (públicos ou privados), b) o direito ao conhecimento da identidade dos responsáveis, bem como o direito ao esclarecimento sobre a finalidade dos dados; c) o direito de contestação, ou seja, direito à retificação dos dados e sobre identidade e endereço do responsável; d) o direito de atualização (cujo escopo fundamental é a correção do conteúdo dos dados em caso de desatualização); e) finalmente, o direito à eliminação dos dados cujo registro é interdito.

A decisão apontada é considerada como o marco oficial de surgimento do direito à autodeterminação informativa, de modo que consiste, segundo a sentença, no direito dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados. Dito isso, o sujeito passa a poder decidir quando e sob que circunstâncias poderão se dar conhecimento de seus dados pessoais.

Para Stefano Rodotà (2008, p. 7), a autodeterminação informativa concede a cada um de nós um real poder sobre nossas próprias informações, nossos próprios dados. Percebe-se aqui, segundo Rodotà (2008, p. 7), um ponto de chegada na longa evolução do conceito de privacidade, da originária definição, *the rigth to be let alone*, ao direito de manter o controle sobre suas próprias informações e de determinar as modalidades de construção da própria esfera privada.

Quando se pensa em autodeterminação informativa, ou seja, no controle conferido ao titular sobre suas informações, no caso da Lei nº 13.709/2018, art. 2, inciso II, não se pode perder de vista o dilema que existente entre privacidade *versus* segurança. De plano, é enganosa a receita que menos privacidade aos indivíduos implicará em maior segurança a esses. Ora, nessa linha, Stefano Rodotà remete à metáfora do homem de vidro de matriz nazista:

> [...] A ideia do homem de vidro é totalitária porque sobre ela baseia a pretensão do Estado de conhecer tudo, até os aspectos mais íntimos da vida dos cidadãos, transformando automaticamente em suspeito todo aquele que quiser salvaguardar sua vida privada. Ao argumento de que quem não ter nada a esconder, nada deve temer, o autor não se cansa de admoestar que o emprego das tecnologias da informação coloca justamente o cidadão que nada tem a temer em uma situação de risco, de discriminação. Menos cidadãos, mais suspeitos é a expressão estigmatizante do momento (Rodotà, 2008, p. 7-8).

Outrossim, se assiste na atualidade à uma progressiva extensão das formas de controle social, motivadas sobretudo por razões de segurança, no entanto, o respeito à privacidade, à autodeterminação informativa, à inviolabilidade da intimidade, da honra e da imagem deve ser preservado, sendo inclusive um dos fundamentos da Lei Geral de Proteção de Dados Pessoais, conforme art. 2.

Para Ingo Sarlet, a autodeterminação informativa consiste em um direito individual de decisão:

> A relação do direito à autodeterminação informativa com o princípio da dignidade da pessoa humana, portanto, é, em certo sentido, dúplice, pois se manifesta, tanto pela sua vinculação com a noção de autonomia, quanto com o do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento, para o qual a garantia de uma esfera privada e intima indispensável (Sarlet, 2021, p. 31).

Dessa forma, a fim de assegurar efetividade ao princípio da autodeterminação informativa, a Lei nº 13.709/2018 elenca uma série de direitos ao titular, conforme art. 18. Assim, tanto o direito de requerer acesso, correção ou eliminação dos dados pessoais, entre outros insculpidos na lei, decorrem do princípio da autodeterminação informativa e proporcionam efetivo controle das informações pelo titular.

Além disso, limitar dentro dos territórios estatais a aplicação da Lei 13.709/2018 e, por conseguinte, o princípio da autodeterminação informativa no contexto da internet, equivale a enfraquecer a proteção do detentor de informações pessoais na rede mundial, uma vez que a transferência de dados não se sujeita às tradicionais delimitações do Estado soberano.

3 EXTRATERRITORIALIDADE DA LEI 13.709/2018 E A SOBERANIA DO ESTADO FRENTE A TUTELA DOS DIREITOS HUMANOS

Um dos maiores desafios para a aplicação efetiva de uma legislação de proteção de dados pessoais é a extraterritorialidade. Outrossim, há de se questionar se há uma insuficiência protetiva da LGPD diante do fluxo internacional de dados ou, ainda, uma ineficácia diante da aplicação extraterritorial da Lei 13.709/2018.

A aplicação extraterritorial da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), se refere à capacidade da lei brasileira de regular o tratamento de dados pessoais além das fronteiras nacionais. Isso significa que, em certas circunstâncias, a LGPD pode ser aplicada a operações de tratamento de dados realizadas fora do Brasil, desde que essas operações envolvam dados de indivíduos localizados no Brasil ou que os responsáveis pelo tratamento ofereçam bens ou serviços no Brasil, conforme disposto no art. 3º da lei.

Essa aplicação internacional visa garantir que os direitos dos titulares de dados sejam protegidos de forma adequada, independentemente de onde o tratamento dos dados ocorra. A lógica por trás dessa abordagem é assegurar que os dados pessoais de cidadãos brasileiros recebam o mesmo nível de proteção, mesmo quando são tratados por entidades estrangeiras. Isso pode envolver, por exemplo, empresas de tecnologia que coletam dados através de suas plataformas online usadas por brasileiros.

É verdade que a circulação de dados transfronteiriços já estava na agenda de 1980 da Organização para a Cooperação e Desenvolvimento Econômico – OCDE, que elaborou "Diretrizes sobre a proteção de privacidade e circulação transfronteiriça de dados pessoais" *(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).* Trata-se, segundo Cíntia Rosa Pereira de Lima e Kelvin Peroli (2020, p. 70), de uma *soft law* precursora do tema, a qual foi revisitada em 2013, em razão dos constantes avanços da informática e que colocam em xeque a eficácia de leis de proteção de dados pessoais.

Nesse sentido, a extraterritorialidade e a transferência internacional de dados pessoais são temas relevantes e de suma importância, e que se entrelaçam diante do cenário interconectado, tendo em vista que alguns agentes de tratamento de dados (controladores e operadores) estão localizados fisicamente ou virtualmente em outros países. Ou seja, embora os dados tenham sido coletados no território nacional, são tratados em âmbito internacional.

Assim, o sistema normativo de proteção de dados pessoais emerge no âmbito da sociedade da informação como forma de proteger a personalidade do indivíduo contra os potenciais riscos a serem causados pelo tratamento de dados pessoais (Bioni; Mendes, 2019, p. 818).

É verdade que, assim como o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, a Lei 13.709/2018 possui aplicação para qualquer operação de tratamento realizada pelos controladores, independentemente do país de sua sede, ou ainda, independentemente do país em que estejam localizados os dados. Para tanto, é necessário que o tratamento tenha sido realizado no território nacional, conforme art. 3[12]. Nesses termos, pode-se perceber que o inciso I do art. 3 é amplo, envolve qualquer atividade de tratamento e abrange inclusive as situações do inciso II e III, que foram especificadas em razão do grau de importância.

Percebe-se, assim, que as hipóteses dos incisos I e III, do art. 3 são comunicáveis, pois a coleta de dados, no território nacional, já configura hipótese de tratamento para aplicação da Lei 13.709/2018. Assim, um estrangeiro não residente no país, mas de passagem no aeroporto brasileiro, será tutelado pela Lei 13.709/2018, no que tange ao tratamento de dados que eventualmente forneceu para utilização dos serviços de *wi-fi* da concessionária do aeroporto.

O art. 3 da Lei 13.709/2018 possui correspondência no Regulamento (UE) 2016/679. Assim o art. 3º (2) do Regulamento (UE) 2016/679[13] prevê que haverá aplicação da norma ainda que o responsável pelo tratamento ou subcontratante não esteja estabelecido na União Europeia, quando:

12 Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - 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;
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Brasil, 2018).

13 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

alínea a) a atividade de tratamento estiver relacionada à oferta de bens ou serviços a esses titulares da União Europeia; alínea b) quando tratar-se de tratamento de dados para fins de monitoramento do comportamento do titular. Assim, para determinar a incidência do Regulamento (UE) 2016/679:

> [...] são irrelevantes a cidadania do titular dos dados (isto é, o GDPR não protege apenas cidadãos europeus) e o país de residência dele (assim, o fato de o titular se encontrar no território da União pode trazer a incidência do GDPR, mesmo que lá ele não tenha a sua residência).
>
> A incidência do GPDR, pois, não será imediata em qualquer situação, sendo necessário identificar em qual medida há intenção de efetivamente se oferecer bens ou serviços a pessoas que se encontrem fisicamente no território da União [...] (Lima, 2018, p. 31).

Apesar de aplicável a Lei 13.709/2018 para qualquer operação de tratamento realizada pelos controladores, independentemente do país de sua sede, ou ainda, independentemente do país em que estejam localizados os dados, o art. 4 da Lei 13.709/2018 disciplina situações em que não haverá aplicação da norma.

Desse modo, não se aplica a Lei 13.709/2018 ao tratamento de dados "provenientes de fora do território nacional" e que não sejam objeto de comunicação com agentes de tratamento brasileiro ou objeto de transferência internacional, desde que o país de proveniência proporcione grau de proteção adequado, conforme art. 4, inciso IV da Lei 13.709/2018[14]. Ou seja, inexistindo grau de proteção adequado, aplicar-se-á a Lei 13.709/2018 em face do Estado proveniente, ainda que esse possua legislação sobre a temática, porém com grau protetivo inferior.

Dessa forma, no tratamento de dados pessoais ocorrido em território estrangeiro, que não possua comunicação com o Brasil, ou seja, objeto de transferência internacional, aplicar-se-á a norma do país estrangeiro, desde que esse forneça grau de proteção adequado ao titular brasileiro.

Até o fim da *Privacy Shield15,* poderia ser considerado país com "grau de proteção adequado" aquele com capacidade de receber fluxo de dados pessoais da União Europeia, entre eles:

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União (European Union, 2016).

14 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...]
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018).

15 O *Privacy Shield* foi um acordo entre a UE e os EUA, de adoção voluntária de interessados, que tinha como objetivo fornecer às "empresas de ambos os lados do Atlântico um mecanismo para cumprir os requisitos de proteção de dados em apoio ao comércio transatlântico". Por sua vez, recentemente o Tribunal de Justiça da União Europeia (ECJ) em inglês concluiu que o *Privacy Shield* falhou em proteger a privacidade das pessoas cujos dados estavam sendo transferidos para os EUA. O órgão constatou que os programas de vigilância dos EUA não se limitavam a coletar somente o que era necessário, e que os titulares dos dados não tinham recursos legais nos EUA em caso de reclamações. No final, o ECJ anulou o acordo *Privacy Shield*, o que deixa o futuro das transferências de dados entre a UE e os EUA preso em um limbo jurídico.

Andorra, Argentina, Canadá, Ilhas Faroe, Guesney, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos (Gutierrez, 2018, p. 218).

Por sua vez, no atual cenário, há de se indagar quais serão os critérios adotados pela Autoridade Nacional de Proteção de Dados para estabelecer quais os países estão no mesmo patamar protetivo, até porque a Lei 13.709/2018 utiliza a expressão "grau adequado" e não "grau equivalente".

É verdade que a redação contida no art. 33, inciso I, do Projeto de Lei - PL nº. 5.276 e da Lei 13.709/2018 reflete o chamado "modelo geográfico". Isso porque no anteprojeto de lei, a redação do inciso permitia a transferência de dados apenas para países que possuíssem nível de proteção "ao menos equiparável". Desse modo, na redação do Projeto de Lei houve mudança para que a transferência fosse permitida para países com nível de proteção "adequado" (Marques; Aquino, 2021, p. 306).

Nesses termos, em tese não será necessário que a norma do país estrangeiro proporcione sanção nos exatos valores da Lei 13.709/2018, mas que possua previsão sancionatória em grau aproximado e compatível com a Lei 13.709/2018. Não obstante, enquanto a Lei 13.709/2018 não estiver plenamente vigente com uma Autoridade Nacional de Proteção de Dados estruturada e atuante o debate público permanecerá parcialmente inconclusivo.

Ademais, para fins de transferência internacional de dados, pode-se citar o art. 33 da Lei 13.709/2018, com correspondência ao art. 46 do Regulamento (UE) 2016/679, que dispõe sobre a necessidade ou de: I – grau de proteção de dados pessoais adequado previsto em lei ao pais de transferência; ou ainda a comprovação de garantias de cumprimento de princípios previstos em lei, na forma de: a) cláusulas contratuais específicas; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos.

Dito isso, pode-se extrair da Lei 13.709/2018 duas situações distintas para a aplicação extraterritorial: I – Será aplicada inclusive aos agentes de tratamento situados em território internacional, quando qualquer atividade de tratamento (coleta, transmissão, comunicação, dentre outras) ocorrer no Brasil, conforme art. 3 da Lei 13.709/2018; II – Ou quando o tratamento de dados pessoais ocorrer fora do território nacional (coleta, utilização, acesso, reprodução, transmissão dentre outros) e que não for objeto de comunicação com agentes de tratamento brasileiro ou objeto de transferência internacional, porém o país de proveniência não proporcionar grau de proteção adequado, conforme art. 4, inciso IV da Lei 13.709/2018.

Nesses termos, a Lei 13.709/2018 deve seguir um propósito certo e funcional, mas que não supere a soberania e a defesa do próprio Estado. Em outras palavras, a Lei 13.709/2018 limita-se, por esse dispositivo, aos efeitos extraterritoriais da lei, que serão somente admitidos caso o país de proveniência dos dados não proporcione grau de proteção adequado aos mesmos (Pinheiro, 2018).

Assim, a aplicação extraterritorial da LGPD levanta questões sobre a soberania dos estados estrangeiros. A lei prevê que, na ausência de um nível de proteção adequado no país onde os dados estão sendo tratados, as normas da LGPD podem prevalecer. Isso pode ser visto como uma interferência na legislação local do país estrangeiro, desafiando o princípio da soberania. No entanto,

argumenta-se que a proteção dos direitos humanos, incluindo o direito à privacidade e à proteção de dados pessoais, transcende as fronteiras nacionais e deve ser garantida de maneira uniforme.

Para mitigar possíveis conflitos de soberania, a LGPD incorpora o conceito de adequação, permitindo a transferência de dados pessoais para países que proporcionem um grau de proteção similar ao brasileiro. Este mecanismo está alinhado com práticas internacionais, como as previstas pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, promovendo um equilíbrio entre a proteção dos dados pessoais e o respeito à soberania dos estados.

Entre as características da visão clássica de soberania, pode-se elencar as seguintes: absoluta, perpétua, indivisível, inalienável, imprescritível. Assim, trata-se no poder de dar a todos em geral e a cada um o direito. Já em uma visão contemporânea internacional, a soberania também se reveste na ideia de interdependência e do funcionalismo que limitam o alcance da soberania por força da construtiva reciprocidade de interesses comuns (Lafer, 1995, p. 139). Sob essa ótica, compreende o autor que sua expressão se encontra:

> [...] nas diversas formas de cooperação internacional e, num nível mais profundo, na União Europeia, experiência de integração econômica que, baseando-se na delegação de competências das soberanias a instituições supranacionais, pode ser vista como um novo fenômeno das relações internacionais.
>
> Outro modelo clássico de convivência internacional é o de Kant, que procura transcender o subjetivismo das soberanias e dos seus interesses, introduzindo a razão abrangente do ponto de vista da humanidade e do indivíduo como fim e não meio, tendo como horizonte a possibilidade de uma paz perpétua. O desdobramento contemporâneo da visão de Kant são os assim chamados temas globais, cuja primeira grande afirmação jurídica é o artigo 11 do Pacto da Sociedade das Nações. Este artigo postula a indivisibilidade da paz, explicitando que a guerra ou ameaça de guerra diz respeito não apenas às partes diretamente envolvidas – aos interesses de suas soberanias – mas a toda a sociedade internacional (Lafer, 1995, p. 139).

Dito isso, é verdade que a justificativa do art. 4, inciso IV da Lei 13.709/2018 encontra correspondência no art. 45 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[16]. Outrossim, o Regulamento Europeu procura estabelecer a partir dos pilares elencados nas alíneas

16 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e

"a", "b" e "c" quais países conferem "grau de proteção adequado". Logo, espera-se que o contido nas mencionadas alíneas seja material de análise pela Autoridade Nacional de Proteção de Dados brasileira para fins de adequação (Carvalho, 2019, p. 626).

A dificuldade a ser enfrentada pela Autoridade Nacional de Proteção de Dados - ANPD, por sua vez, reside na fixação da técnica e jurídica do significado desses "níveis de proteção adequado". Até porque, em 1999, com o advento da Diretiva 95/46/CE, Joel R. Reidenberg (1996, p. 911-930) entendia que o *Safe Harbor Agreement* era uma medida plausível a fim de conferir adequação, o que veio a desmoronar com a recente decisão no ano de 2020 do Tribunal de Justiça da União Europeia de considerá-lo inválido[17].

Além da correspondência com o Regulamento (UE) 2016/679, o art. 4, inciso IV, da Lei 13.709/2018 está em harmonia com os princípios do direito internacional, entre eles o princípio da máxima efetividade e o princípio da primazia da norma mais favorável.

O princípio da máxima efetividade no Direito Internacional dos Direitos Humanos consiste em assegurar às disposições convencionais seus efeitos próprios, evitando-se que sejam consideradas meramente pragmáticas (Ramos, 2015, p. 173). Assim, a interpretação dos tratados internacionais deve contribuir para o aumento da proteção dada ao ser humano.

Já o princípio da primazia da norma mais favorável consiste em técnica que visa evitar o conflito aparente entre diversas normas de proteção de direitos humanos. Logo, para se evitar normas que estabeleçam menor proteção, utiliza-se o princípio, pois nenhuma norma de direitos humanos pode ser invocada para limitar o exercício de qualquer direito ou liberdade já reconhecida por outra norma internacional ou nacional. Isto posto, impõe-se que seja utilizada a norma mais favorável ao indivíduo.

Neste contexto, é preciso destacar a interligação entre a jurisdição global e o sistema legal nacional, bem como a dependência do direito internacional, que se manifesta na aceitação da responsabilidade principal do Estado em adotar medidas para prevenir quaisquer infrações aos direitos humanos, ou ao menos, reparar o dano causado às vítimas. Nesse sentido, discorre Régio Taiar (2009, p. 303):

> [...] o ser humano adquiriu a condição de sujeito de direitos, não apenas nos limites territoriais de seu Estado, mas frente a toda a comunidade internacional, e desse modo, os Estados não mais podem justificar a violação de direitos humanos em seu espaço interno sob o argumento do exercício da soberania [...].

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais (European Union, 2016).

17 Deste modo, Facebook, Google, Oracle e empresas de tecnologia dos EUA passam a ser obrigadas a rever os seus acordos de transferência de dados com o Reino Unido e a Europa, conforme decisão do Tribunal de Justiça da União Europeia de 16 jul. 2020 (pedido de decisão prejudicial apresentado pela High Court – Irlanda – em 9 de maio de 2018 – *Data Protection Commissioner / Facebook Ireland Limited,* Maximillian Scherems – processo C-311/18) (European Union, 2020).

De igual forma, a tutela dos direitos humanos, na qual se insere a proteção de dados pessoais, não se trata de uma limitação do poder soberano do Estado, mas da inserção da proteção dos direitos humanos como característica do conceito de soberania. O descortino do tema leva à constatação de que os conceitos de soberania e de direitos humanos não são antagônicos, antes disso, são fundamentos que se apresentam necessariamente interligados. Logo, interferir na dignidade humana é função do Estado e a violação de direitos humanos pelo ente Estatal implica em afronta ao poder soberano, que não está acima da lei.

Seguindo o mesmo raciocínio, o autor conclui que a proteção dos direitos humanos que implica em intervenção no plano nacional não afronta o princípio da soberania dos Estados, ao contrário, fortalece-o. Assim, não pode mais ser questionada com fundamento numa pretensa soberania estatual. É uma conquista conceitual. Não há que se falar em diminuição da importância da soberania, mas sim do redimensionamento dos seus contornos a partir de uma coexistência harmoniosa (Taiar, 2009, p. 307).

Portanto, se o processamento realizado no país estrangeiro for ilegal ou ultrapassar seus propósitos e não houver comunicação com o Brasil ou transferência internacional, é necessário avaliar se o país estrangeiro dispõe de legislação que ofereça um nível adequado de proteção. Na ausência disso, a Lei 13.709/2018 será aplicada ao titular de nacionalidade brasileira, uma vez que tem como base a salvaguarda dos direitos humanos.

Por outro lado, a interferência e a sobreposição de normas de países estrangeiros devem ser vista com cautela, especialmente quando se trata de interferência de países centrais desenvolvidos em países ditos como periféricos ou subdesenvolvidos, de modo que não se utilize da proteção aos direitos humanos como pretexto para se atingir outros interesses.

Nesse sentido, alguns autores são críticos quanto à pretensão do direito da União Europeia fixar regimes transnacionais de proteção de dados pessoais, baseados na extraterritorialidade de aplicação do Regulamento (UE) 2016/679 (Collona, 2014, p. 203-211), por outro lado, alguns autores entendem como positivo que a União Europeia aja como motor de difusão de padrões disponíveis, o que pode possibilitar que países em desenvolvimento possam fruir da oportunidade de também fixar padrões de proteção de dados pessoais (Veronese, 2021, p. 719).

Além disso, sob a ótica do poder fácil aos países centrais desenvolvidos impor suas normas frente aos países periféricos e em desenvolvimento, porém o caminho contrário se torna mais difícil. Assim, imagine um brasileiro, de passagem no aeroporto da França para assistir às Olimpíadas que teve seus dados violados ou tratados de forma irregular. Mesmo que não ocorra qualquer hipótese de compartilhamento ou transferência internacional, a LGPD deveria ser aplicada, caso o país estrangeiro não possuísse um grau protetivo adequado nos termos da LGPD. A questão que se coloca é: conseguiria o Brasil, um país periférico, impor sua legislação sobre a França, um país central e desenvolvido?

Ora, não é o caso, pois a França segue as normas do GDPR (General Data Protection Regulation), que estabelecem um nível de proteção de dados pessoais compatível com a LGPD. No entanto, se esse mesmo exemplo ocorresse em outro país, como os EUA ou a China, a situação seria diferente. A capacidade do Brasil de fazer valer sua legislação sobre esses países se depararia com desafios significativos.

Os EUA, por exemplo, não possuem uma legislação federal de proteção de dados tão abrangente quanto a LGPD ou o GDPR, o que poderia abrir espaço para a aplicação da LGPD em casos específicos de tratamento irregular de dados de cidadãos brasileiros. No entanto, a imposição efetiva da LGPD sobre empresas americanas seria uma tarefa árdua, dada a influência econômica e política dos EUA e sua postura geralmente resistente a regulamentações extraterritoriais de outros países.

Já no caso da China, apesar de ter uma legislação de proteção de dados emergente, conhecida como a Lei de Proteção de Informações Pessoais (PIPL), a aplicação da LGPD encontraria obstáculos tanto legais quanto diplomáticos. A China possui uma abordagem rigorosa e centralizada sobre a governança de dados, o que dificultaria a aceitação de uma intervenção externa como a da LGPD.

Portanto, o Brasil teria grandes dificuldades em fazer prevalecer e aplicar sua legislação de proteção de dados em países como os EUA ou a China. As barreiras não são apenas legais, mas também práticas e diplomáticas, refletindo as desigualdades de poder entre países periféricos e centrais no cenário global. Este exemplo ilustra os desafios de implementação extraterritorial da LGPD e destaca a necessidade de cooperação internacional e harmonização de normas para a proteção efetiva dos dados pessoais.

Outrossim, a realidade dos fatos subverte a tentativa de um direito fundamental de proteção de dados no contexto internacional, motivo pelo qual é medida que se impõe o debate efetivo em nível global sobre os direitos do titular na internet, especialmente no que concerne à privacidade, propondo Stefano Rodotà (2015, p. 1-8) “uma Carta de Direitos das Internet”, de modo a abarcar a tutela de dados pessoais em nível global. Assim, a privacidade não evoca apenas uma necessidade de intimidade, mas sintetiza as liberdades que pertencem ao sujeito no mundo global e interconectado, motivo pelo qual o debate deve envolver uma multiplicidade de atores.

CONCLUSÃO

Diante da problemática estabelecida e dos objetivos traçados, utilizando-se do método dedutivo e das técnicas de levantamento de bibliografias e legislações, confirma-se a hipótese de que a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) fora dos limites do Brasil enfrenta desafios significativos, especialmente frente a países centrais e desenvolvidos ou aqueles com os quais o Brasil possui relações diplomáticas.

Na primeira seção, estabeleceu os fundamentos teóricos da proteção de dados pessoais enquanto direito humano fundamental. Este alicerce teórico é essencial para compreender a inter-

conexão entre a proteção de dados e os direitos fundamentais, como a dignidade humana e o livre desenvolvimento da personalidade. A partir dessa base, foi possível explorar na segunda seção a autodeterminação informativa e suas implicações internacionais.

A segunda seção focou na extensão do princípio da autodeterminação informativa além das fronteiras nacionais. Foi demonstrado que a proteção dos dados pessoais não se limita ao território brasileiro, mas se estende globalmente, independentemente do local de tratamento dos dados ou da localização do controlador e do titular. Essa perspectiva é fundamental para entender os desafios da aplicação extraterritorial da LGPD, explorados na terceira seção.

Na terceira seção, foi analisada a aplicação extraterritorial da LGPD e suas implicações à soberania dos Estados. Utilizando de exemplos práticos, como o de um brasileiro em trânsito no aeroporto estrangeiro (francês ou estadunidense), fica claro que, na prática, é difícil fazer valer a LGPD frente a países centrais e desenvolvidos, como França, EUA ou China. A França, por seguir o GDPR, possui um nível de proteção adequado, mas em países como os EUA e China, a imposição da LGPD seria desafiadora. As barreiras legais, diplomáticas e práticas refletem as desigualdades de poder no cenário global, evidenciando as limitações da aplicação da LGPD em âmbito internacional.

Em suma, a aplicação extraterritorial da LGPD enfrenta desafios significativos, especialmente quando confrontada com países desenvolvidos ou aqueles com fortes laços diplomáticos com o Brasil. A proteção dos direitos humanos, como o direito à privacidade e à autodeterminação informativa, transcende fronteiras, mas sua efetiva implementação depende de cooperação internacional e harmonização de normas. Deste modo, pode-se reconhecer e reafirmar a importância da LGPD, mas também reconhecer suas limitações práticas e a necessidade de um diálogo contínuo para fortalecer a proteção de dados pessoais globalmente.

REFERÊNCIAS

BIONI, Bruno; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando convergências na direção de um nível se equivalência. *In*: FRAZÃO, A.; TEPEDIDNO, G.; OLIVA, M. D. (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 3. ed. Rio de Janeiro: Forense, 1999.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República,1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 06 ago. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 06 ago. 2023.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 6 ago. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Brasília, DF: Presidência da República, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06 ago. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 ago. 2023.

BRASIL. **Proposta de Emenda à Constituição 17, de 2019.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0s7lrinhunwf01sy9eyzoc5s4q13527531.node0?codteor=1773684&filename=PEC+17/2019. Acesso em: 06 ago. 2023.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **ADI nº. 6387**. Requerente: Conselho Federal da Ordem dos Advogados Do Brasil - CFOAB. Intimado: Presidente da República. Rel. Ministro Rosa Weber, julgado em 07/05/2020, DJe, 2 de junho 2020. Disponível em: http://portal.stf.jus.br/processos/downloadTexto.asp?id=5078529&ext=RTF20. Acesso em: 06 ago. 2023.

CANOTILHO, José Joaquim Gomes. **Constituição da República Portuguesa anotada**. São Paulo: RT, 2007. v. 1.

CARVALHO, Angelo Gamba Prata de. Transferência internacional de dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 621-647.

COLLONA, Liane. Article 4 of the EU Data Protection Directive and the irrelevance of the UE--US Safe Harbor program? **International Data Privacy Law**, Oxford, v. 4, n. 3, p. 203-221, 2014.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, São Paulo: RT, v. 4, p. 59-67, 2017.

EUROPEAN UNION. Carta dos direitos fundamentais da União Europeia, de 7 de dezembro de 2000. **Jornal Oficial das Comunidades Europeias**: C 364/3, [*s.l.*], 18 dez. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 6 ago. 2023.

EUROPEAN UNION. **Convenção 108:** Convenção para a proteção de indivíduos com Respeito ao processamento automatizado de dados pessoais, de 28 de janeiro de 1981. European Union: Council of Europe, 1981. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 6 ago. 2023.

EUROPEAN UNION. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 4 de novembro de 1950**. Paris: European Court of Human Rights, 1950. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 6 ago. 2023.

EUROPEAN UNION. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial da União Europeia**: L 119/1, Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT-EN-FR/TXT/?from=PT&uri=CELEX%3A32016R0679&qid=1615924045194. Acesso em: 06 ago. 2023.

EUROPEAN UNION. Tribunal de Justiça. **Document 62018CJ0311**. Acórdão do Tribunal de Justiça (Grande Seção), de 16 jul. 2020. Pedido de decisão prejudicial apresentado pela High Court (Irlanda) em 9 de maio de 2018. Contra: Facebook Ireland Limited, Maximillian Scherems (processo C-311/18). EUR-Lex, European Union, 16 jul. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62018CJ0311. Acesso em: 6 ago. 2023.

FERREIRA FILHO, Manoel Gonçalves. **Direitos humanos fundamentais**. São Paulo: Saraiva, 2005.

GUTIERREZ, Andriei. Transferência internacional de dados & estratégias de desenvolvimento nacional. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Comentários ao GDPR**: regulamento geral de proteção de dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 213-228.

LAFER, Celso. A soberania e os direitos humanos. **Lua Nova: Revista de Cultura e Política**, São Paulo, n. 35, p. 137-148, 1995.

LIMA, Caio César Carvalho. Objeto, aplicação material e aplicação territorial. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Comentários ao GDPR**: Regulamento geral de proteção de dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 23-37.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. A aplicação da Lei Geral de Proteção de Dados do Brasil no tempo e no espaço. *In*: LIMA, Cíntia Rosa Pereira de Lima (coord.). **Comentários à lei geral de proteção de dados**. São Paulo: Almedina, 2020. p. 69–100.

MARQUES, Fernanda Mascarenhas; AQUINO, Theófilo Miguel de. O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES JR., O. L.; BIONI, B. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 299-319.

MAZZUOLI, Valério de Oliveira. **Curso de direitos humanos**. 6. ed. Rio de Janeiro: Forense. 2019.

MOTA, Ivan; TENA, Lucimara Plaza. Fundamentos da LGPD: círculos concêntricos e sociedade de informação no contexto de direitos da personalidade. **Revista Jurídica**, Curitiba, v. 2, n. 59, p. 538-576, 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/download/4330/371372603. Acesso em: 6 ago. 2023.

ONU - ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1948**. Genebra: ONU, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 6 ago. 2023.

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

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 18. ed. São Paulo: Saraiva Educação. 2018.

RAMOS, André de Carvalho. **Teoria geral dos direitos humanos na ordem internacional**. 5. ed. São Paulo: Saraiva Educação. 2015.

REIDENBERG, Joel R. Governing networks and rule-making in Cyberspace. **Emory Law Journal**, New York, v. 45, p. 911-930, 1996. Disponível em: https://ir.lawnet.fordham.edu/faculty_scholarship/29/. Acesso em: 6 ago. 2023.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet? Tradução de Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**, Rio de Janeiro, ano 4, n. 2, jul./dez. 2015. Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/. Acesso em: 6 ago. 2023.

RODOTÀ, Stefano. Tecnologias e direito. *In*: MORAES, Maria Celina Bodin (org.). **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado. 2012.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES JR., O. L.; BIONI, B. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense. 2021. p. 22-61.

SCHWABE, Jürgen; MARTINS, Leonardo (org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Berlim: Konrad-Adenauer-Stiftung E.V., 2005.

SZANIAWSKI, Elimar. **Direitos da personalidade e sua tutela**. 2. ed. São Paulo: Revista dos Tribunais, 2005.

TAIAR, Rogério. **Direito internacional dos direitos humanos**: uma discussão sobre a relativização da soberania face a efetivação da proteção internacional dos direitos humanos. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2009.

VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, L. S.; DONEDA, D.; SARLET, I. W.; RODRIGUES JUNIOR, O. L.; BIONI, B. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense. 2021. p. 689-727.

VIANNA, Túlio Lima. A era do controle: introdução crítica ao direito penal cibernético. **Direito e Justiça – Revista da Faculdade de Direito da Universidade Católica Portuguesa**, Lisboa, v. 18, p. 344, 2004. Disponível em: https://www.researchgate.net/profile/Tulio_Vianna/publication/28769889_A_era_do_Controle_introducao_critica_ao_direito_penal_cibernetico/links/54353c430cf2dc341daf b3c6/A-era-do-Controle-introducao-critica-ao-direito-penal-cibernetico.pdf. Acesso em: 6 ago. 2023.