UNIVERSIDADE D
COIMBRA

Natalia Mendes Melo

A EXTRATERRITORIALIDADE DO RGPD: DA INFLUÊNCIA NO ORDENAMENTO JURÍDICO BRASILEIRO À ESTIPULAÇÃO DO NÍVEL MÍNIMO ADEQUADO DE PROTEÇÃO DOS DADOS PESSOAIS

Dissertação no âmbito do Mestrado em Ciências Jurídico-Políticas com menção em Direito Internacional Público e Europeu, orientada pela Professora Doutora Dulce Margarida de Jesus Lopes e apresentada à Faculdade de Direito da Universidade de Coimbra

Julho de 2023

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Natalia Mendes Melo

A extraterritorialidade do RGPD: da influência no ordenamento jurídico brasileiro à estipulação do nível mínimo adequado de proteção dos dados pessoais

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º. Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Políticas com menção em Direito Internacional Público e Europeu.

Orientadora: Professora Doutora Dulce Margarida de Jesus Lopes.

COIMBRA
2023

Não sei quantas almas tenho.
Cada momento mudei.
Continuamente me estranho.
Nunca me vi nem achei.
Fernando Pessoa, em Não sei quantas almas tenho.

AGRADECIMENTOS

Reconheço o risco de incorrer em um clichê literário, mas tamanha é minha admiração por Clarice Lispector que assumo esse risco e inauguro estes agradecimentos com a sua célebre sentença “quem caminha sozinho pode até chegar mais rápido, mas aquele que vai acompanhado, com certeza vai mais longe”. Decerto, eu fui longe – afinal, eu cheguei até aqui – e muito bem acompanhada:

Pelas minhas convicções religiosas, que materializaram uma confiança em algo superior – a quem eu intitulo de Deus –, permitindo-me confiar no processo e superar os percalços que surgiram. Pelos meus pais e pela minha irmã, que me lembravam, incessantemente, da magnitude da evolução pessoal e profissional e que o conhecimento precisa extrapolar fronteiras geográficas, encorajando-me a vivenciar a vida académica em um outro país. Pelo meu grande amor e companheiro, o maior entusiasta e incentivador de tudo o que eu me proponho a realizar. Pela minha orientadora, Dra. Dulce Lopes, que tanto me inspirou e ensinou, revelando-se uma exímia condutora desta árdua trajetória investigativa.

E agora, que cá estou, compreendo o real valor deste projeto. Muito mais valioso do que o título acadêmico a ser por ele conferido é o percurso percorrido para elaborá-lo, durante o qual colecionei experiências ímpares e me conectei, genuinamente, a algumas pessoas – por sorte, hoje as tenho como amigos(as).

Então, a todos vocês: muito obrigada.

RESUMO

A sociedade contemporânea vem experimentando, há algumas décadas, uma acelerada (r)evolução tecnológica, caracterizada por inúmeros (e facilmente disponíveis) dispositivos de tecnologia da informação e comunicação que propiciam a circulação imediata e indiscriminada de dados pessoais no ecossistema digital – o qual, a propósito, não encontra limites territoriais, desvinculando-se de fronteiras geográficas. Um marco regulatório para a proteção desses dados e dos seus titulares mostrou-se, portanto, medida de urgência e de interesse global. Nesse contexto, é escopo do presente trabalho analisar o desenvolvimento do direito à proteção de dados pessoais na União Europeia – precursora do assunto – em conjunto com o desenvolvimento desse direito no Brasil, de modo a explicar a influência e os reflexos que as normas europeias exerceram (e exercem) sobre as brasileiras. A partir de uma pesquisa bibliográfica e documental, em obras especializadas que circundam o tema, e de uma pesquisa nas principais jurisprudências correlatas, o trabalho se propõe a compreender as características da jurisdição na Internet; as particularidades do Regulamento Geral sobre a Proteção de Dados (RGPD), com ênfase nas suas formas de extraterritorialidade – seja por meio da sua aplicação direta, seja indiretamente por meio da sua influência –; bem como a compreender as particularidades do arcabouço legal brasileiro em matéria de proteção de dados, em especial, a Lei Geral de Proteção de Dados Pessoais (LGPD). Pretende-se, ainda, à luz das regras estabelecidas no RGPD acerca das transferências internacionais de dados pessoais, avaliar se o Brasil assegura um nível adequado de proteção de dados.

PALAVRAS-CHAVE: Direito da União Europeia; Direito à proteção de dados pessoais; Extraterritorialidade; Jurisdição na Internet; Transferências internacionais de dados pessoais; Nível adequado de proteção de dados pessoais.

ABSTRACT

For the last few decades, contemporary society has been experiencing an accelerated technological (r)evolution, characterized by countless (and easily available) information and communication technology devices that enable the immediate and indiscriminate circulation of personal data in the digital ecosystem – which, by the way, knows no territorial limits, freeing itself from geographical boundaries. A regulatory framework for the protection of these data and their holders is, therefore, a measure of urgency and global interest. In this context, the scope of this project is to analyze the development of the right to the protection of personal data in the European Union – a precursor of the theme – along with the development of this right in Brazil, in order to explain the influence and the reflexes that European norms have exerted (and still do) on Brazilian ones. Based on a bibliographic and documentary research, in specialized works on the subject, and a survey of the main related case law, the project aims to understand the characteristics of Internet jurisdiction; the particularities of the General Data Protection Regulation (GDPR), with emphasis on its extraterritorial reach – either through its direct application, or indirectly, through its influence – as well as to understand the particularities of the Brazilian legal framework on data protection, especially the LGPD. It is also intended, considering the rules established in the GDPR on international transfers of personal data, to assess whether Brazil ensures an adequate level of data protection.

KEYWORDS: European Union law; Right to protection of personal data; Extraterritoriality; Jurisdiction on the Internet; International transfers of personal data; Adequate level of protection of personal data.

LISTA DE SIGLAS E ABREVIATURAS

AEPD	Agência Espanhola de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
CADE	Conselho Administrativo de Defesa Econômica
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CEPD	Comité Europeu para a Proteção de Dados
CNPD	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
CPJI	Corte Permanente de Justiça Internacional
EUA	Estados Unidos da América
IBGE	Instituto Brasileiro de Geografia e Estatística
LGPD	Lei Geral de Proteção de Dados Pessoais
PEC	Proposta de Emenda à Constituição
PII	*Personally Identifiable Information*
RGPD	Regulamento Geral sobre a Proteção de Dados
R2P	*Responsibility to Protect*
STF	Supremo Tribunal Federal
TFUE	Tratado de Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
TSE	Tribunal Superior Eleitoral
UE	União Europeia

ÍNDICE

INTRODUÇÃO

Na atual sociedade tecnológica, o direito à privacidade ganha novos contornos, deitando raízes em solo dos direitos da personalidade, de modo a compreender não apenas o direito a uma vida privada, como também o direito ao controlo de acesso aos dados pessoais. Pioneira em constatar tal circunstância, a União Europeia desenvolveu normas que, sem dúvidas, foram um "divisor de águas" na abordagem da tutela dos dados pessoais e da circulação desses dados no meio digital.

Sem a pretensão de esgotar o tema do direito à proteção de dados pessoais, o trabalho tem o escopo de demonstrar que, a despeito de terem sido discutidas no âmbito da União Europeia e de seus Estados-Membros, tais normas exercem influência global, na medida em que podem ser legitimadas por certas obrigações de direitos fundamentais e apresentam diretrizes mínimas para uma jurisdição protetora de dados pessoais a ser seguida por todos os Estados, além de o tratamento desses dados está cada vez mais interconectado e dotado de um caráter transfronteiriço, o que torna a sua regulação incompatível com parâmetros estrita e puramente territoriais.

Para tanto, ao amparo dos próprios objeto e objetivos em que o direito à proteção de dados pessoais se funda, bem como dos contornos delineativos que o configuram, o trabalho foi dividido em quatro capítulos. O primeiro capítulo aborda, a partir dos elementos que compõem o Estado, a soberania, com suas características e particularidades mutáveis ao longo dos séculos, bem como os corolários provenientes do seu exercício, especialmente, a jurisdição. Sem desprezar a estreita relação entre território e jurisdição, evidencia-se a problemática jurisdicional intrínseca da Era Digital: as atividades na Internet, por sua própria natureza, não são geograficamente delimitadas, tampouco atreladas a um único Estado, o que faz emergir a necessidade de tornar operáveis entre si os diversos sistemas jurídicos existentes.

Complementando essas informações propedêuticas, no segundo capítulo apresentam-se os direitos, cuja tutela ganhou (ainda mais) magnitude na Era Digital. A começar pelo direito à privacidade, o capítulo percorre os desdobramentos desse direito até chegar no direito à proteção de dados pessoais e no direito à autodeterminação informativa.

Em matéria de proteção de dados pessoais, é impensável não abordar o precursor e expoente máximo do assunto: o Regulamento (UE) 2016/679, o qual, visto através da lente

do direito internacional público, evidencia como uma regulamentação local está a se tornar global. Dada tamanha relevância, todo o terceiro capítulo é destinado a tratar das particularidades desse regulamento, das suas principais disposições e das suas interfaces extraterritoriais, consubstanciadas na sua aplicação extraterritorial (direta) por força dos critérios jurisdicionais previstos no artigo 3º e na sua aplicação extraterritorial (indireta) por meio da robusta influência exercida no ordenamento jurídico brasileiro.

Sob essa ótica de que os dados pessoais circulam para além das fronteiras geográficas dos Estados-Membros e que, por consequência, a tutela desses dados deve se dar globalmente, não apenas no âmbito europeu, o quarto e último capítulo objetiva abordar as disposições do RGPD acerca das transferências de dados pessoais para países terceiros e organizações internacionais – disposições essas que são aplicadas de forma a assegurar que o nível de proteção das pessoas singulares garantido pelo regulamento não será comprometido.

Nesse contexto, a partir da análise conjunta de tais disposições e do arcabouço legal brasileiro em matéria de proteção de dados, o capítulo se destina, ao final, a tratar dos mecanismos de transferências de dados pessoais entre Estados-Membros e o Brasil, com ênfase na ponderação do nível de proteção de dados garantido pelo Brasil – se essencialmente equivalente ao assegurado pela União ou não – para efeitos de decisão de adequação, na aceção do artigo 45º do RGPD; bem como na apresentação de garantias adequadas, nos termos do artigo 46º.

Para a realização do trabalho foi empreendida uma pesquisa, básica, observacional, qualitativa e exploratória[1], valendo-se da busca por material teórico-bibliográfico, a partir da análise de artigos e livros científicos pertinentes aos diversos assuntos que circundam a temática da soberania, da jurisdição, dos direitos fundamentais e, principalmente, do direito à proteção de dados pessoais.

Além disso, também se empregou pesquisa jurisprudencial, sobretudo nas decisões do Tribunal de Justiça da União Europeia e do Supremo Tribunal Federal do Brasil. O objetivo da pesquisa jurisprudencial foi precipuamente verificar como as legislações

[1] FONTELLES, Mauro José *et al*. *Metodologia da pesquisa científica: diretrizes para a elaboração de um protocolo de pesquisa*, *in* Rev. para. med, 2009.

brasileira e europeia no campo do direito à proteção de dados pessoais estão a ser aplicadas na prática. E a par de tais informações, tornou-se possível a construção de um cenário comparativo entre Brasil e União Europeia no que diz respeito à proteção de dados pessoais.

1 (EXTRA)TERRITORIALIDADE

1.1 SOBERANIA

Na condição de autor e destinatário de normas jurídicas internacionais, o Estado reúne em si elementos constitutivos, a saber: o agrupamento de pessoas (população), um mínimo de base territorial (território), órgãos governativos que o representam e exprimam a sua vontade (governo) e uma característica fundamental: a soberania. É patente a estreita relação e simbiose entre esses quatro elementos, sublinhando-se, em especial, a relação entre território e soberania.

Ainda que imperfeitamente, são as fronteiras naturais e artificiais que delimitam o território de um Estado, do qual fazem parte o domínio terrestre, o domínio fluvial, o domínio marítimo, o domínio lacustre e o domínio aéreo. Como afirma Almeida, é nesse "espaço compreendido pelo território que o Estado exerce os poderes que decorrem da soberania"[2].

E o que vem a ser a soberania? Dotado de dinamismo, o conceito está a se transformar através dos contextos históricos e políticos, revelando um caráter essencialmente polissêmico. Afinal, como destaca Besson ao citar Richard Falk, "diferentes períodos na história geraram diferentes dificuldades, as quais, por sua vez, influenciaram as respostas legais aos problemas políticos e condicionaram a função atribuída à soberania em qualquer tempo e espaço"[3].

Sem menosprezar a complexidade do termo e as controvérsias que o circundam, a soberania traduz-se, nos dias atuais, na discricionariedade de que gozam os Estados em exercer os atos de autoridade necessários ao desenvolvimento de todo o tipo de atividade em seu território, em prol dos valores constitutivos de um "bom" Estado (democracia, justiça, direitos humanos). Há, portanto, uma relação conceitual entre soberania e território.

Contudo, nem sempre foi assim. Até a Idade Média – período em que os indivíduos se identificavam pelas suas características humanas comuns e era forte o pertencimento à comunidade –, "o exercício de autoridade era essencialmente vinculado a determinados

[2]ALMEIDA, Francisco Ferreira de. *Direito internacional público*, 2ª ed. Coimbra: Coimbra Editora, 2003, p. 208.
[3]BESSON, Samantha. *Sovereignity.* Oxford Public International Law, Oxford University Press, 2011, p. 3. Disponível em <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL>. Acesso em 3 de novembro de 2022. Tradução livre.

grupos de pessoas e não necessariamente ao território que ocupavam"[4]. Conforme explica Andrade:

> "(...) Mesmo nas civilizações da Antiguidade que alcançaram um maior grau de complexidade social, como os babilónios, egípcios e gregos, aqueles que não pertencessem à comunidade não eram diretamente submetidos à autoridade que as regia, já que não havia identificação do escopo de aplicação da lei com o território. Pelo contrário, o senso de que a autoridade era ligada ao pertencimento à comunidade era tão forte que, entre os babilónios, por exemplo, entendia-se que os estrangeiros não eram sequer dignos de serem regidos pelas suas leis sagradas. (...)"[5].

Após o fim da Idade Média, a Europa experimentou um renascimento urbano e comercial, marcado pelo incremento significativo das rotas comerciais. Com isso, além do crescimento do comércio, houve também um aumento na circulação de moedas e no convívio de pessoas de diversas origens, o que tornou as relações sociais e econômicas muito mais complexas.

A complexidade dessas relações revelou ser insuficiente arraigar o exercício de autoridade na noção de pessoalidade e fez emergir a premissa de que cada Estado exerce de forma exclusiva os atos de autoridade sobre o seu território (e não mais sobre um determinado grupo de pessoas), transformando, assim, a soberania pessoal em territorial.

Grande expoente da época, Jean Bodin definiu o poder soberano como uma característica essencial do Estado, propondo como regra jurídico-política a tríplice: Estado, soberania e monarca. Os monarcas comportavam-se como proprietários do Estado e gozavam das mais absolutas prerrogativas, o que, no âmbito interestatal, conduziu à noção da superioridade da vontade do Estado soberano.

Diz-se que essa conceção de soberania remonta à sua consagração oficial nos Tratados de Vestefália, em 1648, os quais os autores Daillier, Dinh e Pellet consideram "como o ponto de partida de toda a evolução do direito internacional contemporâneo"[6], na medida em que assentaram o princípio da igualdade soberana dos Estados e o princípio da não-intervenção. No plano externo, à luz das relações mútuas entre os Estados, portanto, a

---

[4]ANDRADE, Caio Delgado de. *Soberania, jurisdição e territorialidade: passado, presente e futuro,* Revista de Direito Constitucional e Internacional, Vol. 117, Ano 28, p. 151-174, São Paulo: Editora RT, 2020, p. 153.
[5] *Ibid.*, p. 153.
[6] DAILLIER, Patrick; DINH, Nguyen; PELLET, Alain. *Direito internacional público*, 2ª ed. Lisboa: Fundação Calouste Gulbenkian, 2003, p. 53.

soberania encontrava limites exclusivamente na vontade monárquica, uma vez que esse cenário orientado pelo absolutismo, em que predominava a atitude individualista de Estados igualmente soberanos, era incompatível com qualquer ordem jurídica comum.

Nos séculos seguintes, a noção de soberania começou a se difundir nas práticas domésticas (internas) no mundo todo, sendo, então, atrelada a uma função do Estado-nação e não mais à qualidade do monarca, de uma pessoa em particular. "Assim, já não é mais o Estado senhorial e patrimonial, torna-se o Estado nacional e, como tal, está a serviço da nação, cujas aspirações deve realizar e cujas necessidades deve satisfazer"[7].

Consequentemente, reformulou-se a ideia primitiva de autoridade soberana, passando-se a conceber um soberano limitado e vinculado pelas suas próprias leis. Ademais, com a difusão dos ideais de Jean-Jacques Rousseau, emergiu o vínculo entre soberania e democracia, na medida em que, como explicou o filósofo, o exercício da soberania das instituições políticas deve ser submetido ao respeito da vontade geral, sob pena da autoridade soberana perder suas atribuições.

A ideia do Estado enquanto modelo de unidade política, a exercer soberania plena no seu território e em relação aos seus assuntos internos foi, por muito tempo, o cerne dos debates da época. Isso começou a mudar, contudo, a partir do século XIX, quando a ideia de Estado passou a ser acompanhada pelo desenvolvimento de ordens políticas e jurídicas, as quais, apesar de centralizadas e territorialmente determinadas, partilhavam interesses comuns, a despertar um sentimento de interdependência. As tensões e os conflitos entre Estados não desapareceram; pelo contrário, até se agravaram muitas vezes. A novidade é o que Daillier, Dinh e Pellet chamaram de "tomada de consciência da solidariedade internacional"[8], que trouxe gradualmente para o centro dos debates a questão da soberania do Estado nas suas relações internacionais.

Intensificou-se, então, a necessidade de elaborar regras jurídicas internacionais, a fim de responder aos imperativos da solidariedade internacional e de garantir o respeito recíproco da soberania e das promessas mútuas entre Estados soberanos. Eis que floresce, assim, o direito internacional – considerado a lei que permitiu a coexistência internacional

[7] DAILLIER, *Direito internacional público*. *op. cit.*, p. 63.
[8] *Ibid.*, p. 62.

entre Estados heterogéneos, mas igualmente soberanos. Nos termos dos ensinamentos de Besson:

> "Para ser plenamente responsável pelas suas relações com outros Estados em uma sociedade de Estados igualmente soberanos e ser externamente soberano; e por conseguinte, para proteger a sua soberania interna, um Estado precisava se submeter ao direito internacional público. No entanto, para que o direito internacional público surgisse, era necessário que os Estados soberanos e independentes consentissem livremente nas obrigações e direitos mútuos e na sua regulação.
> Consequentemente, uma vez que a soberania implica a existência do direito internacional público, tornou-se evidente que ela é intrinsecamente limitada. Mesmo que, por definição, um Estado soberano não possa ser limitado pelas leis de outro Estado, ele pode ser limitado quando essas leis resultam da vontade coletiva de todos os Estados".[9]

Sejam elas consuetudinárias ou convencionais, as normas internacionais às quais se reconheça valor imperativo sinalizam um exercício da soberania intrinsecamente limitado, na medida em que impõem balizas ao próprio poder constituinte originário e derivado. Além do mais, com a conjuntura pós-Segunda Guerra Mundial, marcada pela influência da globalização, da regionalização e da fragmentação, avultou-se a "incapacidade de os governos controlarem, por si sós, a economia, os fluxos migratórios, o crime transnacional, o terrorismo, as catástrofes ambientais, etc." [10], o que, por óbvio, esmoreceu aquela noção de soberania absoluta e resplandeceu a imprescindibilidade do direito internacional.

Em uma conceção moderna, a relação é quase simbiótica: dentro de seu território e em relação aos indivíduos que engloba, o Estado é a mais alta autoridade (desde que esteja em conformidade com os preceitos de direito internacional); porém, paralelamente, no plano externo e à luz das relações entre os diferentes Estados – todos eles igualmente soberanos –, o direito internacional exige uma relação de coordenação e independência entre eles. Afinal, como bem definido por Besson "*If States were to remain ultimate authorities on the inside, they needed to be independent on the outside"*[11].

---

[9] BESSON, *Sovereignity. op. cit*., p. 6.
[10] ALMEIDA, Francisco António de M. L. Ferreira de. *Mutações sistémicas e normativas no direito internacional em face de novos desafios*, *in* Scientia Ivridica: Revista de Direito Comparado Português e Brasileiro, Vol. 326, 2011, pág. 227.
[11] Para que os Estados continuem a ser a autoridade máxima no interior, é necessário que sejam independentes no exterior. BESSON, *Sovereignity. op. cit*., p. 6. Tradução livre.

Sob o prisma de sua incidência, pondera-se a soberania em duas dimensões: interna e externamente. Umbilicalmente ligadas, as soberanias interna e externa podem ser compreendidas como duas faces necessárias da mesma moeda: para que haja soberania externa, tem de haver soberania interna e vice-versa[12].

Ou, como ensina Kelsen, o direito internacional e as diversas ordens estatais integram o mesmo sistema jurídico, de modo que é o direito internacional quem delega aos Estados o poder de serem ordens jurídicas parciais e soberanas. Complementam Daillier, Dinh e Pellet que "a soberania não implica de maneira nenhuma que o Estado possa libertar-se das regras do direito internacional. Pelo contrário, o Estado só é soberano se estiver submetido direta e imediatamente ao direito internacional"[13]. Assim, os Estados são internamente soberanos, na medida em que impõem a si mesmo suas leis, e são externamente soberanos, na medida em que coexistem com outros sujeitos na ordem jurídica internacional, estabelecendo relações entre si.

A soberania é, simultaneamente, um princípio (do) e (sobre) o direito internacional, sendo fundamental para a ordem jurídica internacional como um todo. Muitas vezes, é vista como poder, competência ou imunidade, hábil a englobar direitos e deveres (há quem prefira conceber a soberania em termos dos componentes da independência dos Estados soberanos e das correspondentes restrições aos outros Estados). Em sua maioria, esses direitos e deveres derivam do princípio da igualdade soberana e foram abordados na Carta das Nações Unidas.

É ao amparo desses direitos e deveres que os Estados modernos não são orgânica e juridicamente subordinados a nenhum outro membro da comunidade internacional, contudo, deles se exige o respeito pelo direito internacional. Em outras palavras, a despeito da ausência de subordinação face a outros sujeitos, os Estados estão sujeitos ao ordenamento jurídico internacional e ao cumprimento de determinadas obrigações internacionais, as quais, frisa-se, não comprometem a independência do Estado, tampouco violam a sua soberania.

A autonomia constitucional e política dos Estados é também um direito da soberania, na medida em que pouco importa ao direito internacional o regime político, económico e social que o Estado instituiu. Sob essa mesma lógica de independência estatal,

[12] *Ibid.*, p. 7.
[13] DAILLIER, *Direito internacional público*. *op. cit.*, p. 435.

emerge um importante dever decorrente da soberania: a proibição de intervenção nos assuntos internos de outros Estados.

É claro que tanto a autonomia constitucional e política e o dever de não ingerência nos assuntos internos de outros Estados não são absolutos, encontrando limites edificados, especialmente, pelo desenvolvimento das normas internacionais sobre direitos humanos. Lançado a partir do compromisso firmado pelos Estados membros das Nações Unidas na Cúpula Mundial de 2005, o ideal da "responsabilidade de proteger" (R2P), por exemplo, é um princípio orientador que se traduz na responsabilidade de cada Estado de agir diante de violações dos direitos humanos e de proteger sua população do genocídio, dos crimes de guerra, da limpeza étnica e dos crimes contra a humanidade.

Desse modo, um regime político baseado na discriminação racial certamente será condenado pela comunidade internacional, assim como, por questões humanitárias e para obter soluções pacíficas em conflitos internacionais, a intervenção em assuntos internos de um Estado é medida que se impõe à comunidade internacional.

A atenção da segurança internacional foi, então, redirecionada ao bem-estar do ser humano em detrimento do Estado soberano, legitimando uma noção mais "humanizada" da soberania, cujo exercício implica não apenas direitos, mas também responsabilidades. Um Estado soberano tem de ser capaz de garantir a proteção dos direitos humanos fundamentais para além dos meios de "abstenção de interferência", de "respeitar e fazer respeitar". É preciso uma atuação positiva estatal para prevenir e combater as ameaças e violações aos direitos humanos[14].

Por fim, não se pode olvidar que, apesar de juridicamente iguais e independentes, os Estados não apenas coexistem na comunidade internacional, mas devem, sobretudo, satisfazer as necessidades e os interesses comuns, razão pela qual a eles se impõem o dever de cooperação entre si e com outros sujeitos do direito internacional. A partir desse dever, extrai-se um duplo interesse: contrapor a soberania nos domínios em que esta é definida de maneira muito enérgica – em particular em matéria económica – e estimular os Estados a

[14] PETERS, Anne. *Humanity as the A and Ω of sovereignty*, *in* The European Journal of International Law, Vol. 20, nº 3, 2009, p. 525. Disponível em <https://academic.oup.com/ejil/article/20/3/513/402328>. Acesso em 20 de fevereiro de 2023.

encontrar fórmulas jurídicas adaptadas à diversidade dos seus sistemas económicos e políticos[15].

1.2 JURISDIÇÃO

Outro importante corolário proveniente da soberania é o direito concedido aos Estados de legislar, executar e aplicar as leis sobre tudo e todos que se encontrem em seu território, exercendo a chamada jurisdição. No contexto internacional, a jurisdição refere-se à competência ou poder regulamentar de um Estado face a outros e, sob a ótica desse sentido mais amplo, as regras jurisdicionais são sobre a partilha do espaço regulamentar entre os Estados.

A jurisdição pode ter, ainda, outros dois sentidos – mais restritos –, conforme pontuado por Kohl:

> "Por vezes é também utilizado para se referir ao território físico de um Estado. Portanto, não é tautologia dizer que um Estado tem jurisdição (o direito de regular) dentro da sua jurisdição (no seu território) e por vezes sobre assuntos fora dele. Os advogados internacionais privados utilizam o termo de forma muito mais restrita, referindo-se à questão de saber se um tribunal tem o direito de julgar um litígio transnacional".[16]

Em razão dessa partilha do espaço regulamentar entre os Estados, nasce uma preocupação no campo do direito internacional: quando um Estado, na ânsia de promover os seus interesses soberanos no estrangeiro, adota leis que regem assuntos que não são de interesse puramente interno[17].

Nesse cenário, duas abordagens podem ser ponderadas: uma permite que os Estados exerçam a jurisdição como bem entenderem, a menos que haja uma regra proibitiva de direito internacional em sentido contrário. Essa abordagem foi consagrada pela Corte Permanente de Justiça Internacional no paradigmático caso *Lotus* e será

---

[15] DAILLIER, *Direito internacional público*. *op. cit.*, p. 446.
[16] KOHL, Uta. *Jurisdiction and the Internet – Regulatory Competence over Online Activity, in* Cambridge University Press, 2007, p. 11.
[17] CEDRIC, Ryngaert. *Jurisdiction in International Law*, 2ª ed., Oxford, Oxford University Press, 2015, p. 5.

pormenorizadamente esboçada nos parágrafos adiante. A outra abordagem, por sua vez, reflete o direito internacional consuetudinário e proíbe os Estados de exercerem sua jurisdição como bem entenderem, a menos que possam se amparar em regras permissivas, como os princípios da territorialidade, da personalidade, da universalidade e da proteção.

Não se pode afirmar categoricamente qual abordagem prevalece, uma vez que, na prática, os Estados que afirmam a sua jurisdição tendem a se amparar no caso *Lotus*, ao passo que os Estados que se opõem às afirmações jurisdicionais de outros Estados tendem a confiar na abordagem restritiva – das regras permissivas de direito internacional.

Certo é que o exercício da jurisdição deve ser razoável. Na tradicional conceção do direito internacional, na qual esse direito era visto como um direito de coexistência, a razoabilidade tinha um viés negativo, ou seja, era um princípio de restrição, de modo a proibir os Estados de usurparem a soberania uns dos outros. Todavia, na moderna conceção de direito internacional, esse direito é visto como um direito de cooperação e a razoabilidade manifesta-se positivamente, como um "dever de agir", de modo que os Estados têm, em certas circunstâncias e hipóteses, a responsabilidade de afirmar positivamente a jurisdição[18].

Para tanto, além de observar os princípios da territorialidade, da personalidade, da proteção e da universalidade – princípios jurisdicionais basilares do direito internacional –, o Estado que pretende exercer a jurisdição deve ter uma conexão genuína e relevante com a situação[19].

1.2.1 A abordagem ampliativa à luz do Caso *Lótus*

A jurisprudência internacional caminha para o alargamento da jurisdição estadual, de maneira a conferir aos Estados um amplo poder discricionário – apenas limitado em certos casos por regras proibitivas específicas prescritas pelo direito internacional – para definir a aplicação de suas leis e a jurisdição de seus tribunais sobre atos, pessoas e bens fora do seu próprio território.

[18] CEDRIC, *Jurisdiction in International Law*. *op. cit.,* p. 43.
[19] A exigência de um *link* (de uma conexão genuína) foi apresentada pela Corte Internacional de Justiça no caso *Nottebohm* em 1955.

Foi exatamente nesse sentido que decidiu a CPJI em setembro de 1927 no caso *Lotus*[20]*,* o qual envolvia o abalroamento, em alto-mar, do navio turco *Boz-Kourt* pelo navio francês *Lotus*, resultando na morte de oito tripulantes turcos. Após o acidente, o navio *Lotus* atracou em Istambul, onde um de seus oficiais foi detido, processado e condenado pelas autoridades turcas a oitenta dias de prisão e ao pagamento de multa.

Irresignada com julgamento, a França protestou formalmente junto à Turquia, tendo ambos os Estados acordado em submeter o caso à CPJI. O cerne da controvérsia residia, portanto, em determinar se a Turquia podia (ou não), à luz do direito internacional, processar e julgar o oficial da embarcação francesa em razão de fatos ocorridos em alto-mar.

Como principal fundamento de sua pretensão, a França alegou que a sua competência para penalizar seus nacionais estava assegurada pelos princípios de direito internacional segundo os quais o direito que vigora é o da bandeira do navio e o alto-mar não pertence a nenhum Estado, sendo um patrimônio comum da humanidade. No mais, para os franceses, a Turquia havia afrontado os preceitos do direito internacional, na medida em que não demonstrou nenhum elemento que justificasse o exercício da sua jurisdição.

A Turquia, por sua vez, argumentou no sentido de que a sua jurisdição poderia ser exercida sempre que não conflitasse com princípios do direito internacional, o que entendia ser o caso; ainda mais se tratando de uma situação na qual turcos morreram em um acidente envolvendo uma embarcação turca.

Em outras palavras, sintetizou Andrade que:

> "Para a França a jurisdição estava limitada ao território turco e a atos e fatos lá ocorridos, de modo que somente por autorização expressa do Direito Internacional poderia ser exercida pelo país fora de seus limites; para a Turquia, por outro lado, a jurisdição sobre fatos externos ao território seria preexistente e apenas limitada pelo Direito Internacional"[21].

Nesse contexto, ao decidir que a Turquia não agiu em conflito com os princípios do direito internacional, a CPJI estabeleceu uma relevante distinção entre a jurisdição como efetivo exercício de poder e o objeto do exercício da jurisdição, a saber:

---

[20] Corte Permanente de Justiça Internacional. Acórdão de 7 de setembro de 1927, *The Case of the S.S. LOTUS*, série A, nº 10. Disponível em https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf. Acesso em 9 de novembro de 2022.
[21] ANDRADE, *Soberania, jurisdição e territorialidade: passado, presente e futuro. op. cit.,* p. 160.

> "[A] primeira e principal restrição imposta pelo direito internacional a um Estado é que – não existindo regra permissiva em contrário – ele não pode exercer o seu poder sob qualquer forma no território de outro Estado. Neste sentido, a jurisdição é certamente territorial; não pode ser exercida por um Estado fora do seu território.
> Isso não significa, contudo, que o direito internacional proíba um Estado de exercer jurisdição no seu próprio território relativamente a um caso que diga respeito a atos que tenham ocorrido no estrangeiro e para o qual não se possa invocar uma regra permissiva de direito internacional. Tal entendimento só seria aceitável se o direito internacional previsse uma proibição geral aos Estados de estender a aplicação de suas leis e a jurisdição dos seus tribunais a pessoas, bens e atos fora do seu território e se, como exceção a essa proibição geral, permitisse que os Estados assim o fizessem em certos casos específicos. Mas esse certamente não é o caso do direito internacional atualmente. Longe de estabelecer uma proibição geral no sentido de que os Estados não podem estender a aplicação de suas leis e a jurisdição dos seus tribunais a pessoas, bens e atos fora do seu território, deixa-lhes uma ampla margem de discricionariedade que só é limitada em certos casos por regras proibitivas(...)"[22].

Portanto, sob a ótica dos direitos da soberania, no efetivo exercício do poder estatal, a jurisdição é "certamente territorial", não podendo um Estado exercer poder sob qualquer forma no território de outro Estado. No entanto, sob a ótica dos atos e relações que podem ser objeto desse direito, o direito internacional dá ampla liberdade aos Estados para definirem a aplicação de suas leis e a jurisdição dos seus tribunais a pessoas, bens e atos fora do seu território, liberdade essa que só encontra limites por regras proibitivas específicas.

Debruçando-se sobre a noção de soberania interna, a jurisdição engloba, especialmente nos países anglo-americanos, atos de comando dos três poderes do Estado: Legislativo, Judiciário e Executivo. Nesse cenário, apenas dentro do seu território um Estado tem jurisdição plena, exercendo seu direito de prescrever leis, de julgar litígios e de fazer cumprir as regras.

Esse foi outro emblemático contributo do caso *Lotus*: trazer à tona a distinção entre as ramificações da jurisdição – a jurisdição legislativa, a adjudicativa e a executiva. A jurisdição legislativa (*jurisdiction to prescribe*) é a jurisdição para prescrever, manifestando-se, portanto, na criação do Direito – no poder de regulamentar juridicamente uma determinada matéria por meio da criação de normas de conduta. A jurisdição adjudicativa (*jurisdiction to adjudicate*) é entendida como a função de julgar, traduzindo-se na

[22] CPJI, *The Case of the S.S. LOTUS. op. cit.,* p. 18-19. Tradução livre.

interpretação de determinada situação e na sua subsunção às normas vigentes pelo Judiciário. Por fim, mas não menos importante, a jurisdição executiva é a jurisdição para executar as leis e as decisões (*jurisdiction to enforce*).

A identificação com a territorialidade se manifesta de forma distinta nas três ramificações da jurisdição. Dentre elas, a mais desprendida de raízes territoriais é a jurisdição prescritiva. O exercício da extraterritorialidade legislativa está cada vez mais recorrente e encontra respaldo nas situações com múltiplos contatos e dotadas de um caráter transfronteiriço, as chamadas situações *cross border*. Tais situações se consubstanciam sobretudo em "hipóteses que envolvem direitos fundamentais, preocupações ambientais ou interesses políticos considerados essenciais"[23] e que, por razões lógicas, ultrapassam a base territorial e populacional dos Estados isoladamente considerados, alargando os limites territoriais jurisdicionais.

Caso a competência para legislar não pudesse ser exercida fora das fronteiras do Estado, correr-se-ia o risco de não definir juridicamente regras para regular situações como as acima mencionadas ou de tornar inócuas e/ou insuficientes as regras já prescritas. Nesses casos, é de suma importância que a escolha da lei de regência leve em consideração a proximidade, o vínculo e a intimidade com a hipótese.

No meio-termo, a jurisdição adjudicatória encontra-se mais arraigada à territorialidade, muito embora o seu exercício extraterritorialmente também esteja em notória ascensão; ao passo que a manifestação da territorialidade é essencialmente mais intensa na jurisdição de execução. Alega Andrade que:

> "Em todo caso, embora a jurisdição legislativa permita mil possibilidades – afinal, como ensina a sabedoria popular, o papel aceita tudo –, a pretensão de aplicação extraterritorial de leis pelo Estado é ofuscada pelas demais ramificações da jurisdição: tanto a função adjudicatória como a função executiva, que, em última análise, dão concretude à jurisdição legislativa, estão muito mais arraigadas à territorialidade e acabam servindo de freio a eventual ímpeto universalista de incidência da lei."[24]

[23] LOPES, Dulce. *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista, in* Direito Internacional e Comparado: trajetória e perspectivas. Homenagem aos 70 anos do professor catedrático Rui Manoel Moura Ramos, Vol. I. São Paulo: Editora Quartier Latin do Brasil, 2021, pág. 209.
[24] ANDRADE, *Soberania, jurisdição e territorialidade: passado, presente e futuro. op. cit.,* p. 165.

A par das particularidades, a execução de leis e decisões é eminentemente territorial. É vedado à entidade do foro praticar indiscriminadamente um ato de coerção material no território da entidade *ad quem* sem o seu consentimento, ou seja, um Estado não pode enviar seus agentes para o território de outro Estado para fazer valer suas reivindicações, sob pena de violar a igualdade soberana e o princípio da não intervenção. Como muito bem destacado por Colangelo, "não obstante a evolução que se verificou ao nível da extraterritorialidade, a jurisdição executiva manteve-se dominantemente estática, fiel a uma nota de estrita territorialidade"[25].

Há de se frisar que o caráter essencialmente estadual da jurisdição para executar não tem o condão de obstaculizar o espírito de cooperação internacional entre os Estados, a qual se traduz nas inúmeras e recorrentes solicitações de reconhecimento e execução de atos estrangeiros. Em outras palavras, em algumas situações – por exemplo, em matéria de forças armadas e Internet –, os Estados aplicam o direito em um caso concreto ou dão efeitos a pedidos de reconhecimento e execução de atos estrangeiros sem que tenham jurisdição prescritiva ou adjudicativa para tanto[26].

1.2.2 A abordagem restritiva à luz do direito internacional

As regras jurisdicionais são regras que determinam a competência e estabelecem o liame necessário entre o Estado e a atividade/pessoa/bem a ser regulada. Tais regras não dizem propriamente qual será o resultado, mas tão somente como e onde procurar para encontrá-lo[27]. Na abordagem mais restritiva, enfatizam-se os princípios da territorialidade, da personalidade, da proteção e da universalidade – princípios jurisdicionais basilares do direito internacional –, bem como a exigência de que o Estado que pretende exercer a jurisdição tenha uma conexão genuína e relevante com a situação.

Estando intimamente ligada à soberania, a jurisdição lhe toma emprestada a forte identificação territorial, sendo por vezes considerada "um aspecto, um ingrediente ou uma

[25] COLANGELO, Anthony J. *What is Extraterritorial Jurisdication?, in* Cornell Law Review, Vol. 99, 2014, p. 1311-1312. Tradução livre.
[26] LOPES, Dulce Margarida de Jesus. *Eficácia, reconhecimento e execução de actos administrativos estrangeiros.* Tese de Doutoramento, Faculdade de Direito da Universidade de Coimbra, 2017, p. 61. Disponível em <http://hdl.handle.net/10316/79669. Acesso em 30 de outubro de 2022.
[27] KOHL, *Jurisdiction and the Internet – Regulatory Competence over Online Activity. op. cit.*

consequência da soberania (ou da territorialidade ou do princípio da não intervenção – a diferença é meramente terminológica)"[28].

A despeito de ser o princípio básico da jurisdição no direito internacional, o princípio da territorialidade não é tão óbvio quanto parece, visto que a jurisdição não é um conceito estático e restrito a recortes geográficos. Na verdade, a questão surge no sentido de saber quais são os laços decisivos (territorialidade, nacionalidade, proteção, etc.) quando uma situação jurídica tem ligação com vários Estados.

Nada obstante a robusta ligação entre a jurisdição e o elemento territorial, sabe-se que, em algumas situações, o exercício da jurisdição não toma por referência apenas as fronteiras geográficas, de modo que, a depender do caso concreto, outros elementos ganham maior relevância, dando espaço, assim, a uma jurisdição extraterritorial do (e no) Estado – uma vez que um Estado pode ser titular e destinatário do exercício da extraterritorialidade[29].

A princípio, a discussão entre a territorialidade e a extraterritorialidade pode despontar uma (aparente) ambiguidade. Porém, diz-se aparente, pois na realidade, seja em maior ou menor intensidade, a jurisdição se associará a um elemento territorial, razão pela qual esses conceitos não podem ser tratados como opostos e, sim, como complementares. Ou como ensina Lopes, territorialidade e extraterritorialidade devem ser vistas como "verso e reverso de uma moeda, que não se compreendem uma sem a outra em situações com vínculos internacionais"[30].

Há, inclusive, quem conteste o termo extraterritorial. Ryngaery, por exemplo, apesar de entender que o termo já se consolidou, questiona a sua utilização por trazer indícios "de que o critério para a assunção de jurisdição não é, de todo, assente num nexo territorial, quando nas mais das vezes o é, ainda que parcialmente", propondo, em contrapartida, a utilização do termo *"não exclusivamente territorial"*[31].

A discussão é, portanto, terminológica. Uma mesma situação pode ser vista como uma manifestação territorial ou extraterritorial a depender do ponto de vista adotado e dos

[28]MANN, Frederick. *The Doctrine of Jurisdiction in International Law*, *in* Recueil des cours, t.111, 1964, p. 20; *apud* TIBURCIO, Carmen. *The current practice of international co-operation in civil matters*. Recueil des cours, t. 393, 2018, p. 54.
[29] O Estado que pretende exercer jurisdição fora do seu território será nomeado de Estado de foro.
[30] LOPES, *Eficácia, reconhecimento e execução de actos administrativos estrangeiros. op. cit.,* p. 34.
[31] CEDRIC, *Jurisdiction in International Law*. *op. cit.*, p. 7-8.

elementos de conexão considerados, assim como é possível – e muito comum hodiernamente – que uma situação "não tenha uma inicial vocação extraterritorial, mas venha a adquiri-la em virtude da mobilidade da concretização dos elementos de conexão"[32].

Para além do âmbito legal, mostra-se importante uma análise do termo extraterritorialidade sob o âmbito linguístico. O prefixo extra- (do latim *extra*) exprime a ideia de fora de, além de, para fora[33]; de maneira que, acrescido ao substantivo territorialidade, designa a noção de para fora de um determinado território. Nesse sentido, Zalucki aduz que a extraterritorialidade significa ou um processo que decorre "para além", independentemente dos limites de um território, ou ainda determina um sujeito ou objeto localizado fora de um território[34].

A noção de extraterritorialidade consubstancia-se, então, em assuntos, situações, pessoas e itens localizados fora das fronteiras não apenas geográficas, mas também legais de um determinado território. É o que o aludido doutrinador intitula como "*legal relations with a foreign element"*[35] – relações jurídicas com elemento estrangeiro.

Sem pretensões exaustivas – até porque a extraterritorialidade é marcada por uma pluralidade de definições doutrinárias –, sob o âmbito legal, uma jurisdição estatal extraterritorial é, conforme os ensinamentos de Lopes, "o conjunto de situações em que o Estado está habilitado, usualmente por via unilateral, a dizer o direito aplicável a situações internacionais"[36]. Ou, ainda, segundo a Comissão de Direito Internacional Público das Nações Unidas, "o exercício de jurisdição extraterritorial por um Estado é uma tentativa de regular, através de atos legislativos, judiciais ou executivos, a conduta de pessoas, bens ou atos, além das suas fronteiras, que afetam os seus interesses"[37].

---

[32] LOPES, *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista. op. cit.*
[33] Conforme conceito disponível em <https://www.infopedia.pt/dicionarios/lingua-portuguesa/extra->. Acesso em 3 de novembro de 2022.
[34] "*Extraterritoriality means either a process taking place beyond, regardless of a territory or determines a subject or object located outside a territory"*. Załucki, K. *Extraterritorial Jurisdiction in International Law*, *in* International Community Law Review, V. 17(4-5), 2015, p. 407. Disponível em <https://doi.org/10.1163/18719732-12341312>. Acesso em 2 de dezembro de 2022. Tradução livre.
[35] *Ibid.*
[36]LOPES, *Eficácia, reconhecimento e execução de actos administrativos estrangeiros*. *op. cit.,* p. 35.
[37] CDI. *Report on the Work of its Fifty-Eight Session*, 1 May-9 June and 3 July-11 August 2006, UN Doc. A/61/10, Annex E, nº 2. Disponível em <http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf>. Acesso em 10 de dezembro de 2022.

Uma reivindicação jurisdicional territorial se distingue de uma reivindicação extraterritorial em razão do exercício da jurisdição por um Estado sobre atividades que ocorrem fora (ou dentro) das suas fronteiras. Contudo, essa distinção é muitas vezes pouco clara, pois simplesmente não é possível traçar linhas tão delimitadas acerca do que é territorial e do que é extraterritorial.

A ideia de territorialidade e extraterritorialidade fica ainda mais turva quando se trata de atividades da Internet, onde não há quaisquer fronteiras físicas, e essas atividades acabam por não se restringirem ao território de um único país. Nesses casos em que as atividades têm natureza transfronteiriça, as reivindicações jurisdicionais com efeito extraterritorial são uma consequência natural, de maneira que as leis e os regulamentos editados por um Estado podem afetar atividades *online* fora de seu território.

O que se exige de um Estado é que ele não ultrapasse os limites impostos pelo direito internacional à sua jurisdição, de maneira que, dentro desses limites, a titularidade para exercer a jurisdição repousa na soberania. Arrisca-se dizer que o principal limite à assunção da jurisdição extraterritorial consiste na presença de um vínculo suficientemente estreito (uma conexão genuína) entre a Entidade que assume a jurisdição e a situação que propõe regular e apreciar.

Busca-se não apenas um vínculo *per se*, mas sim o que é um vínculo substancial no contexto, a partir de uma análise da situação concreta. A definição de vínculo substancial não pode ser uma ligação que todos ou a maioria dos Estados possam mostrar. Afinal, se todos os Estados mostrarem um vínculo estreito com a mesma situação, a problemática acerca da partilha do espaço regulamentar entre os Estados continuará sendo o calcanhar de Aquiles do exercício da jurisdição.

Ademais, essa conexão genuína entre o Estado e os fatos que pretende regular e apreciar deve respeitar os princípios e limitações do direito internacional, a saber 1) o princípio da territorialidade (objetiva e subjetiva); 2) o princípio da nacionalidade (ativa e passiva); 3) o princípio da proteção; 4) o princípio dos efeitos e 5) o princípio da universalidade[38].

[38]LOPES, *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista*. *op. cit*., pág. 209.

À luz da territorialidade objetiva, autoriza-se um Estado a exercer jurisdição se o ato tiver sido iniciado no estrangeiro, mas concluído no seu território. Na hipótese contrária, se um ato foi iniciado no seu território, mas completado no estrangeiro (territorialidade subjetiva), o Estado também está autorizado a exercer jurisdição. Ou seja, um Estado pode exercer a jurisdição fora do seu território nas situações em que algum elemento constitutivo da conduta ocorreu ali.

Ao amparo de critérios pessoais, o princípio da nacionalidade ativa permite a jurisdição de um Estado sobre seus cidadãos e bens nacionais ainda que eles se encontrem fora do território[39]. A essência desse princípio se inspira no conceito de Estado como um grupo de pessoas, onde quer que se encontrem, que estão sujeitas a uma mesma autoridade.

Ao revés, o princípio da nacionalidade passiva "é invocado para fundamentar a aplicação da lei nacional a condutas e atividades ocorridas no estrangeiro, danosas para os nacionais"[40]. Para Ryngaert, o princípio da nacionalidade passiva é, muito provavelmente, a base mais agressiva da jurisdição extraterritorial, o que justificaria as várias opiniões dissidentes a ele direcionadas[41].

No campo do direito penal, por exemplo, as vigorosas críticas ao princípio da nacionalidade passiva são no sentido de que ele não corresponde à forma como o sistema judicial está internamente organizado, não tendo qualquer objetivo social de repressão. Apesar dos argumentos para abandonar o princípio, as recentes práticas estatais parecem considerar razoável o exercício da jurisdição com base nesse princípio para certos crimes ligados ao terrorismo internacional[42].

Em razão do princípio da proteção, diante de ameaças estrangeiras que afetem a soberania e segurança do Estado de foro, está ele autorizado a exercer a jurisdição em relação

[39]O princípio fundamenta, ainda, a jurisdição sobre as atividades e condutas de nacionais, incluindo empresas, aeronaves e barcos.
[40]FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia*. Tese de Doutoramento, Faculdade de Direito da Universidade Nova de Lisboa, 2019, p. 36. Disponível em <http://hdl.handle.net/10362/89180>. Acesso em 10 de dezembro de 2022.
[41] RYNGAERT, *Jurisdiction in International Law*. *op. cit*., p. 110-111.
[42] *Ibid.*

a pessoas, bens e atos perpetrados no estrangeiro. Para alguns doutrinadores[43], esse princípio emana do direito inerente de autodefesa de um Estado.

A doutrina dos efeitos, por sua vez, não abrange apenas os elementos constitutivos da conduta verificados em determinado território, mas também os efeitos produzidos, de modo a "autorizar a jurisdição sobre atos no estrangeiro que têm ou pretendam ter efeitos dentro do território do Estado a exercer a jurisdição*"*[44].

Diferentemente da territorialidade e da doutrina dos efeitos – princípios em que o liame com o Estado a exercer a jurisdição é territorial –, o princípio da universalidade abandonou, ao menos aparentemente, qualquer conexão (territorial ou não) entre o fato e o Estado de foro, permitindo o exercício jurisdicional sobre determinados atos por serem considerados matéria de interesse público internacional[45]. Em outras palavras, segundo o princípio da universalidade, a natureza do ato pode, por si só, conferir jurisdição a qualquer Estado – é o caso, por exemplo, de atos relacionados com crimes de guerra e crimes contra a humanidade.

Acrescenta-se, ainda, um outro limite à jurisdição extraterritorial, imposto a partir do princípio da não ingerência nos assuntos internos, segundo o qual um país possui autonomia para tratar de seus próprios assuntos e interesses, de forma a não sofrer intromissões de outros países. Nada obstante, ante a própria natureza principiológica, esse princípio não é absoluto, não podendo ser invocado "relativamente a matérias que são essencialmente internacionais" à luz *"*das suas inevitáveis repercussões*"*[46].

A compreensão acerca da jurisdição extraterritorial ganha rumo, também, à luz das três diretrizes propostas por Svantesson, segundo o qual a jurisdição só pode ser exercida quando 1) existe uma ligação substancial entre a matéria e o Estado que procura exercer a jurisdição; 2) o Estado que procura exercer jurisdição tem um interesse legítimo na matéria;

---

[43]Autores europeus continentais entendem nesse sentido. Os autores de *Common Law*, contudo, costumam rejeitar essa justificativa, principalmente porque é propensa à politização e ao abuso. RYNGAERT, *Jurisdiction in International Law*, *op. cit*., p. 115.

[44] COLANGELO, *What is Extraterritorial Jurisdiction? Op. cit.*, p. 1314.

[45]BARROS, Tomás Soares da Silva. *Fundamento e alcance do princípio da jurisdição universal*. Dissertação de Mestrado em Ciências Jurídico-Políticas, Faculdade de Direito da Universidade de Coimbra, 2016, p. 65. Tese de Mestrado. Disponível em <https://estudogeral.uc.pt/bitstream/10316/42011/1/Tomás%20Barros.pdf>. Acesso em 10 de dezembro de 2022.

[46]FONSECA, A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia. *op. cit.*

3) o exercício da jurisdição é razoável dada à proporcionalidade entre os interesses legítimos do Estado e outros interesses (estatais) concorrentes[47].

A relevância do princípio da territorialidade no sistema de atribuição de competências está enraizada na própria noção de Estado. Afinal, para além de ser uma consequência da condição de Estado, o controle do território é um atributo essencial dessa condição. Nesse sentido, Kohl explica que:

> "Como a noção de Estado é tão elementar para a nossa compreensão do direito e mesmo da vida em geral, também é difícil de imaginá-lo sem o Estado. Também é contraintuitivo ver o Estado não simplesmente como uma instituição sujeita ao princípio da territorialidade, mas como a sua própria personificação. Mas é isso que é. O quão estreita é a noção de poder regulador, de territorialidade e de Estado."[48]

Nada obstante, o crescente aumento de eventos transnacionais, principalmente as atividades da (na) Internet, minaram o princípio da territorialidade como base da partilha do espaço regulamentar entre os Estados – sem, contudo, abandoná-lo por completo.

1.3 A JURISDIÇÃO (EXTRA)TERRITORIAL NA INTERNET

Atravessar fronteiras facilmente e poder transitar em lugares estrangeiros para fazer pesquisas, conversar, comprar, vender e dentre tantas outras atividades diárias *online* revela que o mundo diminuiu (figurativamente, é claro) e que a distância física já não importa tanto. No entanto, a despeito dessas inúmeras oportunidades, a natureza global da Internet na esfera jurídica é labiríntica.

Isso porque o Direito e suas regras foram desenvolvidos a partir do pressuposto de que as atividades estão geograficamente delimitadas, de maneira que "o direito de regular uma conduta é partilhado entre Estados geograficamente definidos em uma base predominantemente geográfica"[49]. Essa regra de que cada Estado regula o que ocorre no seu

---

[47] SVANTESSON, Dan Jerker B. *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, in* Symposium Article, International Data Privacy Law, 2015, Vol. 5, nº 4, p. 227. Disponível em <https://doi.org/10.1093/idpl/ipv024>. Acesso em 5 de novembro de 2022.

[48] KOHL, *Jurisdiction and the Internet – Regulatory Competence over Online Activity. op. cit.,* p. 7. Tradução livre.

[49] *Ibid.*

território funciona bem quando as condutas estão bem definidas dentro de um único território, o que, certamente, não é o caso das condutas *online.*

Nesse cenário, tratando-se a Internet de um ecossistema digital global e transnacional com múltiplos atores, tornou-se problemático manter unicamente as regras legais baseadas em critérios territoriais para a partilha de atividades entre os Estados, buscando-se, assim, novos critérios para responder às disputas reais e imediatas resultantes das atividades *online.*

Para tanto, a implementação dessas regras legais exige o reconhecimento de certos princípios e garantias fundamentais que cumpram funções semelhantes aos de caráter constitucional (dentro dos Estados), tais como a proteção dos direitos humanos e fundamentais, especialmente a privacidade, a proteção de dados, a proteção da propriedade e o livre acesso. A interpretação aberta e em camadas das constituições democráticas dos Estados funciona como o fundamento e ponto de partida sem, contudo, ignorar a influência e o poder normativo das eventuais ordens resultantes.

Kettemann acrescenta que é preciso que a constituição seja democraticamente legitimada e que retrate a responsabilidade do Estado, por meio de mecanismos que garantam a segurança da infraestrutura *online,* a fim de que a Internet se torne "operational as an instrument for democratic decision-making structures globally"[50].

Além da observância desses princípios e garantias fundamentais, um ambiente *online* estável reivindica uma interoperabilidade legal (jurídica) para a Internet. Como se sabe, uma das bases fundacionais da Internet é a chamada interoperabilidade, que se traduz na capacidade técnica de "operar com o outro", ou seja, de transferir dados através de distintas plataformas, aplicações e sistemas.

Na seara jurídica, a interoperabilidade seria "a capacidade tanto de permitir uma mobilidade ascendente na economia global como de reforçar as estruturas de poder existentes, a depender das escolhas feitas"[51]. Apesar de em algumas situações poder acentuar os riscos de violação de privacidade e segurança, a partilha entre sistemas jurídicos

[50] Operacional como um instrumento para estruturas democráticas de tomada de decisão a nível global. KETTEMANN, Matthias C. *The Normative Order of the Internet: A Theory of Rule and Regulation Online*, online edn. Oxford Academic, 2020, p. 211. Disponível em <https://doi.org/10.1093/oso/9780198865995.003.0006>. Acesso em 15 de fevereiro de 2023.
[51] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit.,* p. 214. Tradução livre.

interoperáveis conduz a um conjunto coerente de leis mundiais supranacionais – ainda que heterogéneas –, estabelecendo regras que criem condições de igualdade e intercâmbio social. Afinal, padrões de situações similares devem ser tratados de forma semelhante.

Ora, a capacidade de "operar com o outro" é inerente ao próprio sistema jurídico, na medida em que uma norma pode ser transponível para além das fronteiras nacionais, alcançando outras jurisdições. É por isso que se afirma que, a despeito de concorrerem umas com as outras por serem constituídas em regimes jurídicos e políticos heterogéneos, as jurisdições também aprendem umas com as outras.

Dessa forma, em um mundo altamente conectado e interligado, a atuação em conjunto dos milhares de sistemas jurídicos propicia, para além da redução de custos monetários (pois leis não-interoperáveis tendem a aumentar os custos), um desenvolvimento ainda mais inovador da Internet e um estímulo para os negócios globais e para o *compliance* por organizações espalhadas pelo mundo.

Isso, contudo, não significa que a interoperabilidade busca extinguir todas as diferenças entre os sistemas jurídicos, homogeneizando-os integralmente. O que se busca é um meio-termo: não fragmentar totalmente as leis, mas também não as harmonizar por completo; sob pena de tratar distintamente situações análogas e de ameaçar a diversidade cultural.

Certamente, o alcance satisfatório da interoperabilidade legal exige um importante e considerável desempenho dos governos. Na prática, os meios de alcance foram definidos por Kettemann nos termos seguintes:

> "Estruturalmente, a interoperabilidade legal pode ser alcançada ou através de processos de desenvolvimento de normas *multistakeholder*[52] com as autoridades governamentais em funções coordenadas ou através de uma abordagem de baixo para cima sem coordenação central. Nem a harmonização total das leis nem a fragmentação completa e a não-interoperabilidade fazem sentido de um ponto de vista jurídico-económico e normativo. Weber, Palfrey, e Gasser concordam: "um nível intermédio de interoperabilidade jurídica pode normalmente ser considerado como uma boa política". Para além das abordagens autorreguladoras à interoperabilidade por parte das companhias, os Estados podem empregar diferentes modelos regulamentares visando à interoperabilidade:

[52] Governança multissetorial ou multipartite.

> harmonização (unificação da lei), padronização, reconhecimento mútuo, reciprocidade e cooperação."[53]

Importa compreender como os sistemas jurídicos operam uns com os outros no que diz respeito às regras sobre conflitos de lei no espaço, uma vez que, dada a natureza transfronteiriça da Internet, tais regras não estão atreladas unicamente a ligações territoriais – embora também não as tenham abandonado por completo. Nesse sentido, as regras materiais (ou substanciais) são de suma relevância na gestão da interoperabilidade legal, sem esquecer, contudo, que as normas processuais (ou instrumentais) também exercem um papel considerável.

É claro que as jurisdições (internas) soberanas continuam a ser um instrumento essencial para especificar os espaços e os Estados continuam a ser responsáveis por certas atividades *online* que emanam do seu território. Porém, esse ambiente tão virtual e "des-territorializado" como a Internet tornou as abordagens jurisdicionais muito mais complexas, pois as atividades *online* podem ser praticadas em qualquer lugar e os usuários podem estar *online* em qualquer lugar, de modo que qualquer Estado poderia reivindicar jurisdição.

Em tais situações, no intuito de promover uma rede jurisdicional mais estreita e clara, o exercício da jurisdição, quando atrelado a uma ligação territorial, essa deve ser substancial, que pode consistir na 1) produção de efeitos dentro do território (à luz da territorialidade objetiva); na 2) localização do computador do infrator dentro do território através de um endereço de IP identificado (à luz da territorialidade subjetiva) e 3) no armazenamento do conteúdo em um servidor local[54].

Nada obstante, não é sempre que se pode definir, com clareza, essas ligações territoriais, de modo que as instituições jurídicas internacionais passaram a ter um desafio significativo na aplicação da jurisdição das atividades *online*, revelando-se, assim, a necessidade de desenvolver estruturas transnacionais de *due process* e princípios jurisdicionais para a Internet[55].

---

[53] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit.,* p. 215. Tradução livre.
[54] RYNGAERT, *Jurisdiction in International Law*. *op. cit*., p. 79-80. Tradução livre.
[55] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit*., p. 216. Tradução livre.

Kettemann justifica a necessidade de desenvolver essa estrutura legal comum em três questões centrais de particular impacto transnacional:

> "(...) Primeiro, as condições e critérios sob os quais as apreensões de nomes de domínio (e a ação a nível do DNS[56]) pelos Estados podem ser justificadas à luz do seu impacto global; segundo, como os intermediários da Internet podem desenvolver normas de restrição e moderação de conteúdos que combinem o respeito pela maioria das normas de mais de 190 sistemas jurídicos e pelos direitos humanos internacionais (e dar prioridade aos últimos em casos de conflitos); e terceiro, o que limita as decisões judiciais nacionais a obrigar as empresas a divulgar dados de utilizadores localizados em um país diferente."[57]

Esses desafios jurisdicionais de extraterritorialidade e soberania motivaram o desenvolvimento de uma nova forma de *soft law* transnacional[58], materializada em quadros (guias) processuais transnacionais que garantissem a integração entre os mais de 190 sistemas jurídicos (*procedural interoperability*) e o devido processo. No contexto da União Europeia, essa discussão na forma de *soft law* e as orientações não vinculativas internacionais tornaram-se uma vantagem jurídica, na medida em que influenciaram o processo de formação de normas juridicamente obrigatórias e suscetíveis a sanções concernentes às variadas atividades *online* e, especialmente, o processo de consolidação do direito à proteção de dados pessoais no cenário internacional[59].

2 DO DIREITO À PRIVACIDADE AO DIREITO À PROTEÇÃO DE DADOS PESSOAIS E AO DIREITO À AUTODETERMINAÇÃO INFORMATIVA

[56] *Domain Name System* (Sistema de Nomes de Domínio). O DNS é um sistema de bancos de dados utilizado na Internet com o objetivo de traduzir endereços de IP (*Internet Protocol*) em nomes de sites.
[57] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit*., p. 216-217.
[58] *Ibid.*
[59] RIBEIRO, Alanna C.B.M; BRITTO, Nara P.R. Ayres de. *Soft law e hard law como caminho para afirmação do direito à proteção de dados*, 2020. Disponível em <https://ayresbritto.adv.br/soft-law-e-hard-law-como-caminho-para-afirmacao-do-direito-a-protecao-de-dados/>. Acesso em 15 de fevereiro de 2023.

2.1 DOS DESDOBRAMENTOS DO DIREITO À PRIVACIDADE

Dotada de uma natureza multifacetada, a privacidade possui características variáveis a depender do contexto social, económico e cultural vigente, de forma a assegurar uma "proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso"[60].

A compreensão histórica do direito à privacidade tem como ponto de partida a publicação do artigo "*The Right to Privacy*" nos Estados Unidos, no final do século XIX, escrito por Samuel Warren e Louis Brandeis, por meio do qual os autores trouxeram a ideia de que a proteção do indivíduo contra a imposição de sofrimento psicológico e pessoal deveria atingir um nível mais profundo, o que intitularam de *right to privacy* (direito à privacidade), destacando esse direito da estrutura da tutela da propriedade.

Nessa conceção tradicional, o direito à privacidade envolvia uma dicotomia entre as esferas pública e privada, na medida em que assegurava ao indivíduo o direito de ocultar certos aspectos de sua vida privada do domínio público. A privacidade pressupunha, assim, uma não intervenção do Estado na esfera privada individual, de modo a garantir o que os referidos autores chamaram de direito de ser deixado em paz *(the right to be left alone*)[61].

A abordagem era, portanto, formalista, pois compreendia a "subsunção do direito à privacidade à função negativa de um direito fundamental personalíssimo, cujo corolário imediato limitava o reconhecimento da proteção constitucional ao sigilo ao conteúdo das comunicações"*[62];* e generalista, a se desdobrar em outros interesses, como a intimidade (identifica a integridade pessoal, o modo de ser da pessoa, que não consente chegar ao conhecimento público) e a vida privada (possui um arco de proteção amplo, abrangendo os aspectos mais secretos da personalidade).

---

[60] BRASIL. Supremo Tribunal Federal (Plenário). *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal.* Relator: Ministra Rosa Weber. 7 de maio de 2020, p. 108.
[61] BRANDEIS, Louis D.; WARREN, Samuel D. *The right to privacy*, i*n*: Harvard Law Review, vol. 4, nº 5, 1890.
[62] STF, *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. op. cit.*, p. 105.

Em contrapartida, na Europa, o direito à privacidade se desenvolveu tempos depois, na segunda metade do século XX, com a invenção do computador e com o avanço das tecnologias da informação. Essa nova realidade europeia clamava por uma reinvenção da privacidade, na medida em que a inaugural abordagem americana mostrava-se obsoleta. A começar pelo fato de que o computador potencializou o processamento de informações pessoais, o que fez nascer uma preocupação com o controlo e partilha de tais informações.

Assim, as primeiras legislações europeias que trataram sobre privacidade se preocuparam, eminentemente, com a proteção de dados pessoais, a saber: a Lei de Proteção de Dados do Estado de Hesse, na Alemanha Ocidental, em 1970; e a lei nacional editada pela Suécia, em 1973, também sobre a proteção de dados.

Ehrhardt e Peixoto acrescentam outras diferenças no desenvolvimento do direito à privacidade nos Estados Unidos e na Europa:

> "A preocupação dos europeus com a privacidade também difere da preocupação dos americanos no sentido de que a proteção dos dados pessoais é uma medida necessária, inicialmente, contra o Estado, numa relação vertical, ao passo que nos Estados Unidos, o direito à privacidade surge como uma garantia contra os abusos cometidos por particulares, ou seja, horizontalmente.
> As raízes da privacidade nos Estados Unidos estão em um direito do indivíduo, de caráter negativo, enquanto que as raízes europeias, estão também na sociedade, apresentando características de direito positivo, no qual se exige do Estado que se tomem medidas para garantir a proteção de dados pessoais, como a instalação de órgãos de controle, além de a proteção visar grupos minoritários que podem sofrer discriminações com a exposição de seus dados pessoais. Na Europa se desenvolve o aspecto social da privacidade"[63].

Nesse sentido, nota-se que as normas europeias incorporaram o direito à proteção de dados pessoais como um direito autônomo, ao passo que as normas americanas não lhe atribuíram essa autonomia, incorporando-o como um novo aspecto decorrente do direito à privacidade. Isso repercutiu, inclusive, na esfera internacional, pois enquanto alguns instrumentos jurídicos internacionais elevam o direito à privacidade ao patamar de direito

[63]EHRHARDT, Marcos; PEIXOTO, Erick Lucena Campos. *Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias*, *in* Revista Jurídica Luso-Brasileira, Ano 6, 2020, nº 2, p. 397. Disponível em <https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf>. Acesso em 28 de fevereiro de 2022.

humano fundamental, os instrumentos europeus estendem esse atributo ao próprio direito à proteção de dados.

Foi então que, a fim de se adequar às novas tecnologias da informação, o direito à privacidade experimentou transformações significativas tanto no seu sentido como no seu alcance, afastando-se do eixo "pessoa-informação-segredo", como cita Doneda, para se amparar no eixo "pessoa-informação-circulação-controle". Consoante as explicações do autor:

> "A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos".[64]

Machado e Guimarães complementam que "em matéria de dados pessoais, a informação extrapola o âmbito da pessoa" e nesse cenário de despersonalização, marcado "pela coisificação do ser humano em um conjunto de algoritmos passíveis de transação no mercado", um direito da personalidade que tutele os dados se consolida em pré-condição de cidadania[65].

A nova abordagem ampliou o alcance da privacidade para compreender o direito de escolher livremente o seu modo de vida e, também, o direito de controlar o acesso dos seus próprios dados, atrelando-os à personalidade e ao seu desenvolvimento, em uma complexa teia de relações com, por exemplo, o direito ao sigilo, o direito à intimidade, o direito à imagem e, *a fortiori*, o direito à proteção de dados pessoais. É por abrigar todos esses interesses ligados à personalidade que Solove chamou a privacidade de palavra guarda-chuva[66].

Esse controle do acesso dos dados pessoais está muito bem explicado pelas palavras de Machado e Guimarães:

---

[64] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* 3ª ed. São Paulo: Thompson Reuters Brasil, 2021, p. 41.
[65] GUIMARAES, *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018 com alterações da MPV 869/2020*. *op. cit.,* prefácio – VIII.
[66] SOLOVE, Daniel J. *Understanding privacy*. Kindle edition. Cambridge, London: Harvard University Press, 2008.

> "Mais do que o simples direito à informação, o controle dos dados pessoais requer uma justificativa sobre tudo que possa nos afetar, desde a fase de coleta até o descarte. Não é suficiente uma fugaz resposta *"The algorithm did it*", sendo necessária uma noção de *answerability*, isto é, uma explicação clara sobre uma determinada conduta, lesiva ou potencialmente lesiva."[67]

A proteção de dados pessoais nasceu, portanto, como "uma continuação por outros meios" da proteção da privacidade. Uma continuação, pois se desenvolveu a partir da própria proteção da privacidade e com ela compartilha pressupostos ontológicos similares. Por outros meios, pois assumiu características próprias ao antepor uma dimensão coletiva e social da privacidade em detrimento da dimensão invidualista que a limitava, dedicando-se a tutelar os interesses da pessoa e as relações da própria personalidade com o mundo exterior[68].

Há, ainda, quem descreva o direito à privacidade sob a ótica de três dimensões que coexistem entre si. Quando o controlo de acesso se referir a um espaço físico e, especialmente, ao domicílio – a casa é um ambiente indispensável para a vida privada –, a privacidade está inserida na dimensão espacial. Quando o controlo de acesso for sobre o estilo de vida, as escolhas, os comportamentos e os gostos do indivíduo, fala-se na dimensão decisional da privacidade.

O modelo (tri)dimensional da privacidade se completa com a dimensão informacional, a qual, graças ao desenvolvimento tecnológico nas últimas décadas, ao intenso fluxo de informações que o acompanhou e ao desenvolvimento de ferramentas tecnológicas complexas para tratar essas informações, está a experimentar desafios sem precedentes.

A privacidade informacional envolve o controlo de acesso aos dados pessoais que são coletados e processados por atividades *online* passíveis de configurar situação de perigo, atividades essas que compreendem, por exemplo, a coleta de informação; o processamento de informação; a disseminação de informação e a invasão.

---

[67] GUIMARAES, *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018 com alterações da MPV 869/2020*. *op. cit.,* prefácio – IX.
[68] DONEDA, *Da privacidade à proteção de dados pessoais. op. cit.,* p. 47.

Cabe reforçar que compreender a privacidade à luz dessas dimensões exige a perceção de que as três convivem conjuntamente, de forma que, em inúmeras situações, elas se encontram e coincidem, tornando difícil dizer qual direito da privacidade foi violado e, até mesmo, em qual dimensão ele se insere. Nesse sentido, Ehrhardt e Peixoto exemplificam que:

> "A proteção da privacidade em sua dimensão decisional tem um ponto de encontro com a dimensão informacional. Muitos dos assuntos que dizem respeito ao modo de viver da pessoa acabam virando dados, os chamados dados sensíveis, cuja proteção é uma das principais preocupações na chamada sociedade da informação."[69]

Com essa roupagem de controlo de acesso a dados pessoais por terceiros, o direito à reserva da vida privada se desdobrou não apenas no direito à proteção de dados, como também no direito à autodeterminação informativa. Tal expressão foi anunciada pela primeira vez, em 1983, pelo Tribunal Constitucional da Alemanha, no julgamento referente à Lei do Censo alemã[70], que previa uma ampla coleta de dados no país, a fim de mensurar estatisticamente a distribuição espacial e geográfica da população. Por representar um risco na utilização desses dados para fins de controle das atividades e dos comportamentos dos cidadãos, o Tribunal alemão, então, foi provocado, ocasião na qual analisou a referida norma à luz da dimensão informacional do direito à privacidade, de modo a reconhecer esse direito não apenas como um direito negativo de não intervenção, mas também como uma projeção do direito da personalidade.

Foi nesse cenário que o julgado se mostrou emblemático, na medida em que, ao adotar uma abordagem mais abrangente da privacidade, reconheceu a autodeterminação informativa como parcela fundamental do direito atribuído a todo indivíduo de desenvolver livremente sua personalidade, o que "abrange meios e escolhas individuais para realização pessoal e, paralelamente, o relacionar-se com a sociedade (poder público e entes privados)"[71]. Em outras palavras, a afirmação de um direito à autodeterminação informativa

---

[69] EHRHARDT, *Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. op. cit.,* p. 403.
[70] ALEMANHA. Tribunal Constitucional federal. BVerfGE 65, 1, "Recenseamento" (*Volkszählung*).
[71] BESSA, Leonardo Roscoe. *A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa.* 26 de outubro de 2020. Disponível em <https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa>. Acesso em 20 de março de 2023.

não concentra a proteção propriamente no conteúdo dos dados (se público ou privado), mas sim, nas finalidades do seu tratamento por terceiros e nos riscos dele decorrentes.

Sob essas razões, concluiu o Tribunal alemão pela "vagueza e amplitude da norma, que possibilitava o cruzamento dos dados coletivos com outros registros públicos, bem como a sua transferência para outros órgãos da administração"[72], declarando, assim, a inconstitucionalidade parcial da Lei do Censo alemã.

Entende-se, portanto, a autodeterminação informativa como a faculdade que o indivíduo possui de exercer algum controle sobre os seus dados pessoais, seja de forma a definir quais e como esses dados podem ser tratados por terceiros, seja de forma a exigir a correção ou cancelamento deles. Em outras palavras, ainda que se compreenda o direito à autodeterminação informativa como um direito-garantia do direito à reserva da intimidade da vida privada, é certo que aquele possui "um âmbito mais amplo do que esse: visa impedir que o indivíduo se torne um objeto de informação, garantindo-lhe o domínio sobre os seus próprios dados"[73].

2.2 A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL: A ERA DIGITAL E O REGULAMENTO (UE) 2016/679

Como já mencionado, foi no âmbito europeu, à luz do desenvolvimento do aspecto social da privacidade, que se enraizou a conotação contemporânea da privacidade, manifestada, sobretudo, através da proteção de dados pessoais. A Lei de Proteção de Dados do Estado de Hesse, na Alemanha Ocidental, editada em 1970, e três anos depois, uma lei nacional editada pela Suécia, foram o seu marco inicial e, em que pese serem de direito interno, esses diplomas jurídicos contribuíram para a consolidação desse direito na seara internacional[74].

[72]STF, *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. op. cit.*, p. 67.
[73] PORTUGAL. Acórdão do Tribunal Constitucional nº 268/2022, de 3 de junho de 2022, Processo nº 828/2019, de Relatoria do Conselheiro Afonso Patrão, pág. 21. Disponível em <https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html>. Acesso em 1º de abril de 2023.
[74] RIBEIRO, *Soft law e hard law como caminho para afirmação do direito à proteção de dados. op. cit.*

Em 1981, o Conselho da Europa editou o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados: a Convenção 108 para a proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais[75], cujo objetivo era alcançar uma maior unidade entre os Estados-membros e salvaguardar o direito à privacidade no que diz respeito ao tratamento automático dos dados pessoais.

Por muitos anos, a Convenção 108 norteou a proteção de dados no contexto europeu, até que, em 1995, o Parlamento Europeu e o Conselho adotaram a Diretiva 95/46/CE[76] relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, a qual já era um prenúncio de uma legislação que, posteriormente, veio a se tornar um modelo global para a proteção de dados pessoais.

É certo que as mencionadas normas foram concebidas na tentativa de atender às necessidades em matéria de proteção de dados pessoais pertinentes a cada período, o que veio a ficar cada vez mais difícil com a crescente automatização desses dados. Afinal, as últimas décadas foram marcadas por acelerados e inimagináveis progressos tecnológicos, a ponto dos dispositivos de tecnologia da informação e comunicação se tornarem onipresentes na vida particular e profissional de muitas pessoas[77]. A dependência por esses dispositivos é tanta que, atualmente, são eles os responsáveis por propiciar a realização de tarefas cotidianas, das mais simples às mais complexas.

Nesse contexto de hiperconectividade, é evidente que foram inúmeras as transformações constatadas em todas as ordens normativas: social, moral, religiosa e jurídica. Uma das transformações que ganhou destaque foi o grande volume de dados estruturados (e não estruturados) gerados a cada segundo no meio digital – os chamados *Big Data* – e, principalmente, a forma como o tratamento (por exemplo, a recolha, a conservação,

---

[75] Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais. Disponível em https://rm.coe.int/1680078b37. Acesso em 24 de fevereiro de 2023.

[76] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial da União Europeia, L 281. Disponível em <https://edps.europa.eu/sites/default/files/publication/dir_1995_46_pt.pdf>. Acesso em 2 de março de 2023.

[77] HASSANI, Nadia. *Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations.* Terminal [En ligne], 124 | 2019, mis en ligne le 30 juin 2019. Disponível em <http://journals.openedition.org/terminal/4040>. Acesso em 20 de novembro de 2022. Tradução livre.

a utilização e a divulgação) desses dados é feito. Afinal, o resultado do tratamento desses dados revelou-se uma matéria-prima de extrema relevância para o direcionamento de publicidades, de campanhas políticas e de políticas públicas.

Em termos práticos, é possível pensar na relevância que os *Big Data* têm na área da saúde, uma vez que o tratamento de dados de saúde de vários indivíduos auxilia na prevenção de epidemias, no aumento da precisão dos diagnósticos clínicos e laboratoriais e amplia a efetividade de pesquisas e análises sobre o comportamento de doenças no organismo. Também no sistema jurídico, pois além de auxiliar na previsibilidade de determinados cenários – como antever o valor de uma condenação ou indicar a possibilidade de reversão de certa decisão em determinado Tribunal –, o tratamento dos dados permite a elaboração de relatórios para monitorar a atuação do Poder Judiciário.

Ademais, a exploração dos megadados assumiu grande importância na publicidade e comercialização de produtos, representando, atualmente, um dos pilares da economia digital globalizada. Hassani acrescenta que "as previsões são que a quantidade de dados armazenados explodirá para 175 Zb ($175x10^{21}$ bytes) até 2025 – 5,3 vezes mais do que hoje –, levando-nos da era dos grandes dados para a era dos enormes dados a uma velocidade muito alta"[78].

Os dados pessoais e a tecnologia são, portanto, o principal ativo do mundo contemporâneo. Inclusive, em face de tamanha relevância, há quem diga que os dados são o novo petróleo – *"data is the new oil"* –, tendo em vista que o papel por eles desempenhados na atual Era Digital seria análogo ao exercido pelo petróleo e demais combustíveis fôsseis na Era Industrial[79]. Tanto é assim que, hoje, as empresas mais valiosas não são as que exploram petróleo ou derivados, mas sim, são as empresas de tecnologia e de dados, como Google, Facebook e Apple.

Nada obstante, os dados pessoais no meio digital mostraram-se altamente vulneráveis e sensíveis (afinal, possuem um caráter particular e privado), tornando-se o epicentro de vários escândalos por conta da sua má utilização. A exemplo, em 2018, a rede social Facebook conseguiu obter dados de perfis de usuários, com o objetivo de influenciar

[78] *Ibid.*
[79] CORDEIRO, A. Barreto Menezes. *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019*. Coimbra: Edições Almedina, 2020, p. 29.

eleitores em campanhas políticas. As informações obtidas foram coletadas por meio de testes de personalidade na própria página da rede social, sendo possível traçar o perfil das pessoas e, assim, direcionar propagandas eleitorais de acordo com esse perfil.

No mesmo ano, o *Quai d'Orsay* (Ministério das Relações Exteriores francês) foi vítima de um *hacker* que roubou os dados pessoais de milhares de franceses contidos em uma base de dados que permitia às pessoas a preparar uma viagem ao estrangeiro e a obter informações relacionadas com a segurança do país de destino. Posteriormente, esses dados foram encontrados à venda na rede clandestina de internet[80].

Esses e muitos outros episódios revelaram a ganância comercial, a cibercriminalidade e a fuga maciça de dados em torno do crescimento exponencial do tratamento automatizado de informações pessoais, de maneira a colocar os titulares dessas informações em uma posição de enorme fragilidade, uma vez que não se sabia, ao certo, quais as informações eram armazenadas pelos mais distintos responsáveis pelo tratamento; quais eram as finalidades desse armazenamento e qual era o destino das informações. Nas palavras de Cordeiro, *"*as informações pessoais armazenadas, pelos mais distintos responsáveis pelo tratamento, públicos e privados, são superiores às informações que nós próprios detemos sobre a nossa vida"[81].

Nestas circunstâncias, a proteção de dados pessoais tornou-se (ainda mais) uma das principais preocupações da comunidade internacional, em especial, da União Europeia, que legitimou o direito à proteção dos dados pessoais ao patamar de direito fundamental, consagrando-o no artigo 8º, nº 1 da Carta dos Direitos Fundamentais da União Europeia e no artigo 16º, nº 1 do Tratado de Funcionamento da União Europeia. Assim, desde a assinatura do Tratado de Lisboa em 2007, a União Europeia "dispõe de uma base jurídica específica para adotar legislação destinada a defender este direito fundamental"[82], a ser reconhecido para todos que entrem em contato com a União.

Por ter sido redigido à imagem dos textos constitucionais nacionais, o catálogo de direitos fundamentais instituído na CDFUE para além de vincular a própria União Europeia,

---

[80]HASSANI, *Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations. op. cit.* Tradução livre.

[81] CORDEIRO, *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019. op. cit.,* p. 29.

[82] Conforme informações extraídas em <https://www.consilium.europa.eu/pt/policies/data-protection/>. Acesso em 28 de fevereiro de 2023.

vincula seus Estados-Membros, "garantindo que a convenção do exercício em comum, em cooperação ou pelas instituições da União, de poderes estaduais não implique uma redução da tutela dos cidadãos"[83]. Destaca-se que a relação é mais interativa do que hierárquica, na medida em que, "quando o Estado atua no domínio de aplicação do direito da União Europeia, o sentido a dar aos direitos fundamentais que parametrizam a validade das normas internas deve privilegiar uma consonância com as normas europeias"[84].

E foi nesse intuito de adequar a proteção já existente a um cenário inédito de intenso fluxo de dados, somado à fundamentabilidade do direito à proteção de dados que materializa o interesse legítimo da União Europeia na matéria, que o bloco europeu editou um regulamento com vocação extraterritorial e com influência nas legislações do mundo todo – o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

Nos termos dos ensinamentos de Lopes, a substituição da Diretiva 95/46/CE pelo regulamento teve a clara e inequívoca finalidade de:

> "(…)estabilizar um enquadramento mais claro e coerente da protecção de dados que, para além de absorver os desenvolvimentos ocorridos em termos normativos e jurisprudenciais resultantes da interpretação e concretização daquela Directiva, pudesse garantir um "nível equivalente de proteção das pessoas singulares e a livre circulação de dados pessoais na União"[85].

3 DAS MANIFESTAÇÕES DA (EXTRA)TERRITORIALIDADE DO REGULAMENTO (UE) 2016/679 E OS SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

3.1 BREVES COMENTÁRIOS SOBRE O REGULAMENTO (UE) 2016/679

[83] Acórdão do Tribunal Constitucional nº 268/2022. *op. cit.,* pág. 21.
[84] *Ibid.*
[85] LOPES, *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista*. *op. cit.,* p. 205.

Adotar medidas para regular o tratamento de dados pessoais por meios não automatizados[86] tem, certamente, uma suma importância, mas regular o tratamento desses dados, principalmente, por meios total ou parcialmente automatizados e a livre circulação deles na era dos megadados, a fim de proteger e defender os direitos e interesses dos seus titulares, mostrou-se uma necessidade urgente e global. Um mundo cada vez mais interconectado e digital e a natureza transfronteiriça dos megadados tornam a temática afeta a todos os países e a seus respetivos cidadãos. Todavia, foi a União Europeia quem assumiu uma posição determinante ao editar o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho – Regulamento Geral sobre a Proteção de Dados (RGPD), em vigor desde maio de 2018.

Com 99 (noventa e nove) artigos e 173 (cento e setenta e três) considerandos, o RGPD criou as bases e diretrizes para assegurar o direito fundamental da proteção de dados pessoais e para garantir a livre circulação desses dados. Apesar de ter sido discutido e adotado pelos países membros da União Europeia, a sua aplicação pode transcender o território desses países de modo a alcançar outras jurisdições, seja direta – nos casos em que os elementos de conexão previstos no artigo 3º amparam a jurisdição extraterritorial – ou indiretamente – como forma de influência global no desenvolvimento de regras protetoras dos dados pessoais por outras jurisdições.

Acerca dos considerandos, cabe destacar que, em que pese não terem valor jurídico obrigatório, já que apenas a letra da lei possui força vinculativa, eles assumem uma função primordial na interpretação do regulamento, na medida em que esclarecem as razões das normas ali previstas. Essa função, contudo, não pode ser invocada para suprimir tais normas, tampouco para interpretá-las em sentido manifestamente contrário à sua letra[87].

Em face dessa propensão extraterritorial, especialmente trazida pelo artigo 3º, surgem discussões e críticas sobre a aplicabilidade prática do Direito da União Europeia para além das fronteiras de seus Estados-Membros, bem como sobre uma possível violação ao princípio da não ingerência por parte do bloco europeu ao impor suas soluções legislativas

[86] Tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados abrange meios não digitais, meios físicos e manuais, desde que os dados pessoais estejam contidos ou sejam destinados a um sistema de ficheiros, na aceção do Considerando 15 do regulamento.

[87]CORDEIRO, *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019. op. cit.,* p. 49.

a outros países. Os críticos temem que a extensão territorial da jurisdição nacional se torne um *realpolitik*[88] da regulamentação da Internet e, nesse sentido, Kettemann exemplifica:

> "Considere o RGPD: enquanto anteriormente o TJUE tinha de estabelecer uma aplicação extraterritorial por meio da sua jurisprudência, o RGPD é agora formalmente dotado de um alcance transnacional. A dimensão orientada para o futuro da resoberanização[89] é a imposição, às empresas estrangeiras, de leis nacionais, que podem estar em conflito com o direito internacional. A "localização de dados" e a orientação geográfica forçada para erigir um semblante de muros fronteiriços nacionais na Internet fazem parte desta tendência".[90]

Entretanto, apesar do artigo 3º(2) não ter uma razão de ser inerentemente territorial, apresentando outros elementos de conexão hábeis a estender o âmbito de aplicação do regulamento para além do território da União, deve-se considerar que não são meras conexões fortuitas e ocasionais que darão azo a essa extensão extraterritorial. Como ensina Lopes:

> "Tendo em consideração estas indicações, julgamos que o âmbito de aplicação do Regulamento Geral sobre a Protecção de Dados cumpre aqueles limites, não só porque houve, de facto, um exercício de ponderação claro na identificação dos critérios de jurisdição previstos no artigo 3º, como estes se alinham com o propósito de protecção de direitos fundamentais numa entidade que, como a União Europeia, se assume, no plano interno e internacional, como uma verdadeira e comprometida Comunidade de Direito."[91]

Ademais, como já dito, a magnitude da proteção desses dados e a sua circulação ilimitada no meio digital têm repercussões globais. Sob esse contexto, o regulamento não exerce ingerência em assuntos internos de um país, pois o assunto importa à comunidade internacional como um todo, revelando-se como uma influência a outros Estados na elaboração de modelos de privacidade.

---

[88] Conforme conceito extraído do Priberam Dicionário, *realpolitik* é a política internacional ou de relações diplomáticas baseada essencialmente em questões práticas e pragmáticas, em detrimento de questões ideológicas ou éticas. Disponível em <https://dicionario.priberam.org/realpolitik>. Acesso em 28 de março de 2023.

[89] Resoberanização foi a tradução mais precisa de *resovereignization*. A despeito do termo não ser reconhecido na Língua Portuguesa, entende-se que resoberanização é o ato de se tornar soberano novamente (prefixo *re* + soberanizar).

[90] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit*., p. 217. Tradução livre.

[91] LOPES, *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista op. cit.,* p. 210.

Assim como, sob o prisma da jurisdição extraterritorial, não se observa uma "jurisdição global não negociada com terceiros Estados"[92]. Decerto, pela ótica da abordagem restritiva (abordada em parágrafo anterior), o exercício da jurisdição implicaria permissões. No entanto, como o direito à proteção de dados se eleva ao nível de um direito fundamental, a jurisdição exige uma análise mais aprofundada, de modo que o seu exercício pode não ser só permissivo, como também obrigatório, criando obrigações especificas para a União proteger tal direito extraterritorialmente.

Isso significa que, para além da capacidade de influenciar a forma como os dados são tratados no estrangeiro, a União Europeia deve aproveitar essa influência para garantir que os dados de um titular de dados da UE sejam respeitados e protegidos. É, para Ryngaert e Taylor, "um dever de abstenção de prestar assistência a violações (extraterritoriais) de terceiros (dever de respeitar) e dever de impedir essas violações de terceiros (dever de proteger)"[93].

Trata-se, portanto, de um regulamento geral global, na medida em que atinge as incontáveis empresas internacionais que exercem algum tipo de atividade em algum Estado-Membro, assim como os países terceiros e as organizações internacionais que queiram fazer parte das transferências de dados pessoais. Nas palavras de Andréa, Arquite e Camargo, "não seria exagero afirmar que o RGPD nasce como "monstro normativo", um Leviatã a induzir condutas de conformidade (*compliance*) por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais"[94].

Nos próximos tópicos, dar-se-á ênfase às interfaces extraterritoriais do regulamento e aos critérios de jurisdição estabelecidos no artigo 3º e, especialmente, à forte ingerência do

[92]ANJOS, Lucas Costa dos; BRANDAO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teofilo Nunes; POLIDO, Fabrício B. Pasquot. *GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa, in* Instituto de Referência em Internet e Sociedade, 2018, p. 17. Disponível em <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-Primeiras-impressões-de-análise-comparativa-PT.pdf>. Acesso em 20 de novembro de 2022.

[93] RYNGAERT, Cedric; TAYLOR, Mistale. *The GDPR as global data protection regulation*?, *in* Symposium on the GDPR and International Law, 2020. Disponível em <https://www.researchgate.net/publication/338406505_The_GDPR_as_Global_Data_Protection_Regulation>. Acesso em 20 de junho de 2023. Tradução livre.

[94] ANDREA, Gianfranco F. M.; ARQUITE, Higor Roberto L.; CAMARGO, Juliana Moreira. *Proteção de dados pessoais como direito fundamental: a evolução da tecnologia da informação e a lei geral de proteção de dados no Brasil, in* Revista de Direito Constitucional e Internacional, Vol. 28, 2020, p. 123.

RGPD no desenvolvimento e na elaboração das normas sobre a proteção de dados pessoais no Brasil.

3.2 OS CRITÉRIOS DE JURISDIÇÃO DO ARTIGO 3º DO RGPD

Por se tratar de um regulamento, as normas inseridas no RGPD são diretamente aplicáveis a todos os 27 (vinte e sete) países membros da União Europeia, valendo como se fossem direito nacional de cada Estado[95] e sem que seja necessário que as autoridades locais adotem medidas de transposição ou de aplicação. Indiretamente, todavia, essas normas não se restringem às relações da comunidade europeia, pois além de servirem como um modelo global para a proteção de dados pessoais, elas anunciam elementos extraterritoriais hábeis a produzir efeitos em outras jurisdições.

À égide de um quadro de proteção de dados sólido e coerente, o RGPD estabeleceu que o tratamento de dados pessoais deve ser feito em prol das pessoas singulares e não em desfavor delas, a fim de permiti-las a ter o controle sobre a utilização dos seus dados. Nesse contexto, no âmbito de aplicação material, o regulamento incide sobre o "tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados", conforme previsto em seu artigo 2º(1).

Por dados pessoais entende-se a informação relativa a uma pessoa singular identificada ou identificável, independentemente da sua nacionalidade ou do seu local de residência, não abrangendo, porém, as informações referentes às pessoas coletivas e às falecidas[96]. A título exemplificativo, integram o conceito de dados pessoais os nomes e apelidos dos usuários; as moradas; os endereços eletrónicos; os dados de localização; endereços IP e os identificadores de testemunhos de conexão *(cookie*).

É a chamada *Personally Identifiable Information* (PII), a qual abrange informações de uma pessoa identificada, que se destaca como indivíduo, bem como de uma pessoa passível de identificação, direta ou indiretamente, por referência a um identificador

[95]Conforme dispõe o artigo 288º do TFUE: O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.
[96]Artigo 4º(1) do RGPD.

específico, seja ele físico, social, cultural, económico, genético, dentre outros. A PII pode, ainda, referir-se a informações sobre um indivíduo não-identificável, que leva apenas um risco remoto de (re)identificação[97], abordadas no regulamento como pseudonimização[98].

Já o tratamento é definido, nos termos do artigo 4º(2), como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados". O rol dessas operações é extenso e engloba: a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o pagamento ou a destruição.

Ademais, muitas vezes, as referidas operações são efetuadas por um responsável (ou subcontratante) estabelecido em mais de um Estado-Membro ou, ainda, afetam os titulares de dados em vários Estados-Membros, dando azo a um tratamento que não se limita a fronteiras geográficas – intitulado de tratamento transfronteiriço. O artigo 4º(23) o conceitua como:

> "a) O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou
> b) O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro."

Excluem-se do âmbito de aplicação material, dentre outras indicadas no artigo 2º(2), as hipóteses em que o tratamento de dados for efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, ou seja, sem qualquer ligação com uma atividade profissional ou comercial. Tais exceções à aplicação material, todavia, não podem inibir o nível elevado de proteção das pessoas singulares relativamente

[97]EHRHARDT, *Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias*. *op. cit.*

[98] Artigo 4º(5): Pseudonimização – o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

ao tratamento dos seus dados, razão pela qual o TJUE já decidiu que elas devem ser objeto de interpretação estrita, à luz de uma aceção menos ampla[99].

No âmbito de aplicação territorial – eixo central do presente trabalho –, o RGPD alcança o tratamento de dados pessoais realizado no contexto das atividades de um estabelecimento do responsável pelo tratamento ou de um subcontratante situado no território da União Europeia, ainda que o tratamento ocorra fora dos limites territoriais da União, conforme estabelece seu artigo 3º(1)[100]. Para fins de incidência das normas do regulamento, não interessa, portanto, o local onde o tratamento dos dados pessoais ocorreu (se dentro ou fora da União Europeia), importando tão somente que o estabelecimento do responsável pelo tratamento ou do operador[101] esteja situado na União Europeia.

A noção de estabelecimento veio a ser delineada pelo TJUE em seus julgamentos, a partir dos quais é possível pontuar três elementos centrais que definem o termo, a saber: a estabilidade da instalação; a efetividade do exercício de uma atividade e o contexto do exercício dessas atividades[102].

A exemplo do caso *Weltimmo vs. Nemzeti*, em que o TJUE afastou a abordagem formalista do conceito de estabelecimento, de modo a reconhecer que a estabilidade da instalação não pressupõe o registo da pessoa jurídica no território da União Europeia, nos seguintes termos:

> "(…) uma concepção flexível do conceito de estabelecimento, que afasta qualquer abordagem formalista segundo a qual uma empresa só se pode considerar estabelecida no lugar em que estiver registada. Assim, para determinar se uma sociedade, responsável por um tratamento de dados, dispõe de um estabelecimento, na aceção da Diretiva 95/46, num Estado-Membro diferente do Estado-Membro ou do país terceiro em que está registada, há que avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades nesse outro Estado-Membro, tendo em conta a natureza específica das atividades económicas e das prestações de serviços em causa. Este entendimento vale especialmente para as empresas que se dedicam a oferecer serviços exclusivamente na Internet."[103]

---

[99] Ver, por analogia, no tocante ao artigo 3º, nº 2, da Diretiva 95/46, o Acórdão de 10 de julho de 2018, *Jehovan Todistajat,* C-25/17, EU:C:2018:551, nº 37.

[100]Artigo 3º(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.

[101]No presente trabalho, o termo "operador" será utilizado como sinônimo de subcontratante.

[102]CORDEIRO, *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019. op. cit*., p. 93.

[103] Acórdão de 1º de outubro de 2015, *Weltimmo v. Nemzeti*, C-230/14, EU:C:2015:639, nº 29.

Assim como, no caso *Google Spain*[104], restou claro que a natureza jurídica – se sucursal ou filial com personalidade jurídica – não é determinante para caracterizar um estabelecimento. Em síntese, o caso tratava de uma reclamação apresentada por um cidadão espanhol à Agência Espanhola de Proteção de Dados (AEPD) em desfavor de um jornal de grande tiragem, da *Google Spain* e da *Google Inc.* A reclamação se baseava no facto de que, quando um internauta inseria o nome do cidadão espanhol no motor de busca da Google, obtinha acesso a duas páginas do jornal, nas quais figurava um anúncio de venda de imóveis em hasta pública decorrente de um arresto determinado em nome do referido cidadão para fins de recuperação de dívida à Segurança Social.

Por meio dessa reclamação, o cidadão espanhol pleiteava que o referido jornal suprimisse ou alterasse essas páginas, a fim de que seus dados fossem protegidos de alguma forma; bem como que a *Google Spain* e a *Google Inc*. suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa. O TJUE, então, foi instado a analisar, dentre várias outras questões, quais as obrigações que incumbem aos operadores de motores de busca para efeitos da proteção dos dados pessoais das pessoas interessadas que não desejem que determinadas informações pessoais, publicadas em sítios *web* de terceiros, sejam postas à disposição dos internautas indefinidamente.

Em resposta, o Tribunal entendeu que a atividade de um motor de busca consistente em encontrar informações que contenham dados pessoais publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e colocá-las à disposição dos internautas deve ser qualificada como "tratamento de dados pessoais", de modo que o operador desse motor de busca deve ser considerado "responsável" pelo referido tratamento, nos termos da Diretiva 95/46/CE.

Considerando que a *Google Inc*., com sede nos Estados Unidos da América, é a sociedade-mãe do grupo Google e a responsável por indexar sítios *web* do mundo todo, bem como que a *Google Spain*, filial do grupo Google localizada em Madrid, foi constituída para desenvolver suas atividades essencialmente para empresas estabelecidas na Espanha, atuando como agente comercial do grupo nesse Estado-Membro, o Tribunal também se incumbiu de delinear o âmbito de aplicação territorial da mencionada Diretiva, examinando,

[104] Acórdão de 13 de maio de 2014, *Google Spain,* C-131/12, EU:C:2014:317.

para tanto, o sentido do termo estabelecimento, na aceção do artigo 4º(1), alínea a). Tal dispositivo estabelecia que:

> "Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando: a) o tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro(...)"

Nesse cenário, a responsável (direta) pelo tratamento dos dados pessoais era a *Google Inc.,* de forma que o cerne da discussão submetida à apreciação do Tribunal consistia em saber 1) o que é ser um estabelecimento desse responsável pelo tratamento e, particularmente, se a *Google Spain* constitui um estabelecimento da *Google Inc*.; e 2) se o tratamento de dados pessoais pelo seu responsável foi efetuado no "contexto das atividades" de um estabelecimento desse responsável no território de um Estado-Membro.

Pois bem. O Tribunal concluiu que, na medida em que possui personalidade jurídica própria e se dedica ao exercício efetivo e real de uma atividade através de uma instalação estável no território espanhol, a *Google Spain* constitui um estabelecimento na aceção do dispositivo acima transcrito. Além disso, o tratamento de dados pessoais pela *Google Inc.* foi efetuado no contexto das atividades da *Google Spain*, pois a primeira, na qualidade de operadora de um motor de busca, constituiu uma filial em um Estado-Membro destinada a promover e vender os espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro.

O Tribunal acrescentou, ainda, que:

> "As atividades do operador do motor de busca e as do seu estabelecimento situado no Estado-Membro em causa estão indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades.
> (...) A própria exibição dos dados pessoais numa página de resultados de uma pesquisa constitui um tratamento desses dados. Ora, sendo a referida exibição de resultados acompanhada, na mesma página da exibição de publicidade relacionada com os termos da pesquisa, há que declarar que o tratamento de dados pessoais em questão é efetuado no contexto da atividade publicitária e comercial do estabelecimento do responsável pelo

> tratamento no território de um Estado-Membro, neste caso, o território espanhol"[105].

Cumpre salientar que, em que pese os casos *Weltimmo vs. Nemzeti* e *Google Spain* terem sido discutido ao abrigo da (atualmente revogada) Diretiva 95/46/CE, o entendimento neles sedimentados acerca do termo "estabelecimento" foi um paradigma para a elaboração das regras do RGPD, tendo sido materializado, inclusive, no Considerando 22 desse regulamento, segundo o qual "o estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto".

Nestas condições, portanto, ainda que a empresa diretamente responsável pelo tratamento dos dados tenha sede em país terceiro, a existência de uma agência ou filial em país do bloco europeu que realize atividades indissociavelmente ligadas às realizadas pelo responsável pelo tratamento configura o termo estabelecimento para fins de aplicação da norma da União.

O que se percebe é uma interpretação expansiva do termo estabelecimento justamente para atender ao objetivo do RGPD, qual seja, garantir uma proteção eficaz e elevada dos direitos fundamentais das pessoas singulares, especialmente, o direito à proteção de dados. E isso acaba por alcançar, por exemplo, as empresas responsáveis pelo tratamento de dados que utilizam computação em nuvem (*cloud computing*) – que "se valem de arranjos pelos quais recursos computacionais são fornecidos de modo flexível e independentemente da localização, que permitem uma rápida e ininterrupta alocação de recursos sob demanda"[106].

Outra regra que demarca o âmbito de aplicação territorial do regulamento é a prevista no item (2) do artigo 3º, a qual, ao contrário da regra do item (1), dispensa o elo territorial entre a União Europeia e o estabelecimento do responsável pelo tratamento ou subcontratante, na medida em que prevê que:

> "O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável

[105]Acórdão *Google Spain. op. cit.,* nº 56 e 57.

[106]ANJOS, *GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. op. cit.,* p. 15.

> 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".

Nada obstante a versão do regulamento traduzida em português mencionar "titulares residentes no território da União", deve-se considerar a expressão titulares de dados que se encontrem na União, uma vez que as características (ou qualidades) desses titulares são irrelevantes, importando tão somente o local onde eles se encontram quando o tratamento ocorre[107]. A finalidade do regulamento é proteger não apenas os residentes – temporários ou permanentes –, mas também os turistas, trabalhadores temporários, apátridas e quaisquer outros sujeitos que se encontrem no território da União Europeia[108].

Para melhor compreender esse dispositivo, faz-se necessário tecer alguns comentários acerca das figuras do responsável pelo tratamento e do subcontratante. O responsável pelo tratamento é, nos termos do artigo 4º, "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais".

O subcontratante é uma interposta entidade – pessoa natural ou jurídica, autoridade pública, agência ou órgão – que trata os dados pessoais por conta do responsável nas situações em que o responsável pelo tratamento delega, contratualmente[109], as operações relativas ao tratamento de dados. Para reconhecer um sujeito (pessoa natural ou jurídica) como subcontratante é preciso que ele seja autônomo juridicamente em relação ao responsável pelo tratamento e que o tratamento dos dados seja efetuado em nome do responsável.

---

[107] Conforme Retificação do Regulamento (UE) 2016/679. Documento disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679R(02)>. Acesso em 19 de junho de 2023.
[108]CORDEIRO, *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019. op. cit.,* p. 96.
[109]Artigo 28º(3): O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante(…).

Desse modo, à luz do amplo âmbito de aplicação territorial traçado no artigo 3º itens (1) e (2), as relações entre subcontratante e responsável pelo tratamento de dados podem ser estabelecidas sob três cenários:

> **Primeiro**: quando ambos os agentes possuem estabelecimento na União Europeia;
> **Segundo**: quando o subcontratante tem estabelecimento fora da União e é contratado por um responsável pelo tratamento com estabelecimento em algum Estado-Membro;
> **Terceiro**: quando o subcontratante possui estabelecimento no território da União e é contratado por um responsável que possui estabelecimento em país que não faz parte do bloco europeu.

No primeiro cenário, não há dúvidas de que o Regulamento (UE) 2016/679 será aplicado tanto ao responsável pelo tratamento dos dados como ao subcontratante, já que o estabelecimento de ambos fica situado em território da União Europeia e é exatamente isso que determina o item (1) do artigo 3º.

No segundo cenário, por sua vez, a aplicação do regulamento ao responsável pelo tratamento de dados que possui estabelecimento em Estado-Membro é certa, também por força do item (1) do artigo 3º, suscitando, contudo, questionamentos quanto ao alcance das normas do RGPD ao subcontratante cujo estabelecimento se localiza fora dos limites territoriais da União Europeia. E é aqui que se revelam as interfaces extraterritoriais do regulamento.

Isso porque, em que pese o RGPD não ser imediatamente aplicado ao subcontratante à luz do critério territorial do estabelecimento – previsto no artigo 3º(1) –, o regulamento será aplicado quando o tratamento de dados pessoais realizado pelo subcontratante em nome do responsável for relativo à oferta de bens ou serviços a titulares de dados que se encontrem na União Europeia ou for relativo ao controlo do comportamento de titulares que se encontrem na União, conforme dispõe o item (2) do artigo 3º[110].

[110] 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes 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.

A oferta de bens e serviços[111] deve ser verificada independentemente de estar associada a um pagamento e a partir da intenção do subcontratante de oferecer os bens e serviços a titulares de dados em um ou mais países do bloco europeu. Apesar de parecer subjetivo analisar uma intenção, há fatores que podem revelar que o operador tem o intuito de oferecer bens e serviços a esses titulares.

Nesse sentido, o considerando 23 explica que "o mero fato de estarem disponíveis na comunidade europeia um sítio web, um endereço eletrônico ou qualquer outro meio de contacto do subcontratante não basta para demonstrar essa intenção". Em contrapartida, a utilização de uma língua ou de uma moeda de uso corrente em um ou mais Estados-Membro, com a possibilidade de encomendar bens ou serviços nessa outra língua, e a referência a utilizadores ou clientes que se encontrem na União constituem indicadores relevantes de que o operador tem o intuito de promover essa oferta[112].

Ademais, para determinar se uma atividade de tratamento se refere ao controlo do comportamento de titulares de dados na União – desde que esse comportamento tenha lugar na União –, é preciso verificar se esses titulares são seguidos com alguma intensidade na Internet e se os dados a serem tratados podem ser, potencialmente, sujeitos a técnicas de definição de perfil, a fim de, especialmente, tomar decisões relativas a esses sujeitos, analisar e prever suas preferências, comportamentos e atitudes[113].

Em outras palavras, essa forma de atividade de tratamento tem a finalidade de monitorar, de alguma maneira, a atividade *online* de seus usuários, especialmente para fins publicitários; além de coletar e processar tanto informações comportamentais sobre hábitos de compra na Internet, histórico de navegação e maneira de uso de dispositivos, como informações sobre interesses políticos e condições socioeconómicas.

Para além dessas hipóteses de aplicação do RGPD ao subcontratante cujo estabelecimento se localiza fora dos limites territoriais da União Europeia, cabe destacar que, indiretamente, as normas desse regulamento também podem alcançar esse subcontratante em razão do contrato (ou outro ato normativo ao abrigo do direito da União

[111]Como exemplo de oferta de serviços, citam-se os serviços de marcação de restaurantes, hotéis ou de viagens; os serviços de *streaming.* CORDEIRO, *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019. op. cit.,* p. 98.
[112]Considerando 23.
[113]Considerando 24.

ou dos Estados-Membros) celebrado para o tratamento em subcontratação. Ou seja, ainda que as atividades do subcontratante não se amoldem às especificidades do artigo 3º(2), ele deverá observar as normas do RGPD por força do contrato firmado com o responsável pelo tratamento[114].

No tocante ao terceiro e último cenário, em que o subcontratante possui estabelecimento no território da União e é contratado por um responsável que possui estabelecimento em país que não faz parte do bloco europeu, a aplicação do regulamento ao subcontratante é inquestionável – em razão do item (1) do artigo 3º. Já em relação ao responsável que possui estabelecimento fora da União Europeia, o regulamento a ele se estenderá no limite das normas direcionadas ao subcontratante do segundo cenário, previstas no artigo 3º(2). Ou seja, desde que as atividades de tratamento realizadas pelo responsável (que possui estabelecimento fora da União Europeia) estejam relacionadas com a oferta de bens e serviços de titulares localizados na União Europeia ou com o controlo do comportamento desses titulares, aplicam-lhe as normas do regulamento.

Desse modo, caso as atividades de tratamento de dados pessoais não estejam compreendidas nessas hipóteses e o responsável pelo tratamento não tenha estabelecimento na União, não se vislumbra o alcance das normas do RGPD a esse responsável, mesmo sendo ele quem determina as finalidades e os meios de tratamento de dados pessoais. Os apontamentos de Anjos, Brandão, Machado, Oliveira e Pólido acerca do assunto são interessantes:

> "(…) e não estendê-la, em sua totalidade, para alcançar inclusive empresas sediadas em países não membros da União Europeia (e. g., EUA e países da América Latina) cuja atividade não se encontra compreendida nos termos do Art. 3(1) e Art. 3(2) do GDPR. Do contrário, haveria a vinculação, à normativa europeia, de qualquer entidade responsável no globo que porventura decida otimizar seus serviços de processamento de dados e de tecnologia da informação com a contratação de um operador com base na Europa" [115].

A exceção, entretanto, está prevista no item (3) do artigo 3º e diz respeito às situações nas quais o responsável pelo tratamento, apesar de não ter estabelecimento na

[114]ANJOS, *GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. op. cit.,* p. 17.
[115] *Ibid.*

União, tem estabelecimento em lugar em que o direito de um Estado-Membro é aplicado por força do direito internacional público. Em tais situações, aplica-se o RGPD ao tratamento de dados pessoais por um responsável não estabelecido na União, mas desde que seja estabelecido em lugar em que o direito de um Estado-Membro é aplicado por força do direito internacional público.

As formas de extraterritorialidade evidentes na legislação europeia em matéria de proteção de dados têm, portanto, bases jurisdicionais identificáveis através da lente do direito internacional público, conforme muito bem definido por Ryngaert e Taylor:

> "Em primeiro lugar, o braço longo da legislação da UE em matéria de proteção de dados, com o seu consequente impacto extraterritorial, baseia-se indiscutivelmente na territorialidade, uma vez que é desencadeado por uma ligação territorial de uma atividade ou pessoa com a UE. Nos termos do RGPD, a territorialidade pode mesmo ser o princípio fundamental, em que a aplicação do regulamento a entidades não sediadas na União é desencadeada pelo facto de estas visarem ou controlarem indivíduos "na União". Em segundo lugar, o amplo alcance geográfico da legislação da UE em matéria de proteção de dados parece estar relacionado com os direitos individuais baseados na filiação demonstrável de alguém na UE, que seria normalmente a cidadania ou a residência. Assim, as reivindicações da UE podem ser justificáveis ao abrigo do princípio da personalidade passiva, que permite à UE proteger os cidadãos ou residentes da UE, por exemplo, no contexto de transferências de dados de sujeitos da UE para jurisdições não conformes. De facto, muitas vezes, as afirmações da UE baseiam-se numa combinação dos princípios da territorialidade e da personalidade passiva, tal como ilustrado pelo facto de uma pessoa em causa ter de demonstrar uma filiação "terri-nacional" na UE ao apresentar um pedido de apagamento dos seus dados a um *website*".[116]

Dito de outra forma, é certo que o título "âmbito de aplicação territorial" dado ao artigo 3º pode sugerir que as normas de jurisdição ali estabelecidas possuem raízes essencialmente territoriais, aplicando-se, portanto, tão somente aos Estados-Membros. De facto, não tem como desvincular por completo essas normas de uma ligação territorial, todavia, a hegemonia dessa ligação se revela com tamanha subtileza, a ponto de evidenciar outros elementos de conexão hábeis a autorizar um alcance extraterritorial do regulamento.

[116] RYNGAERT, Cedric; TAYLOR, Mistale. *The GDPR as global data protection regulation*?, *op. cit.*

3.3 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Restou demonstrado que a aplicação do RGPD não se restringe ao âmbito dos Estados-Membros, de forma que a tutela do direito à proteção de dados pessoais em países alheios ao bloco europeu – como, por exemplo, o Brasil – também pode se sujeitar às disposições desse regulamento por força do seu artigo 3º(2). Além dessa aplicação direta do regulamento europeu, sob o prisma da magnitude da interoperabilidade jurídica destacada em capítulos anteriores, a convergência global das normas – ou seja, a busca por padrões normativos uniformes – que tratam da proteção de dados pessoais era (e é) medida impositiva. A pensar nisso, especialmente em ser interoperável com um dos principais regimes globais referente à privacidade e à proteção de dados pessoais, a Lei nº 13.709, de 14 de agosto de 2018, intitulada como Lei Geral de Proteção de Dados Pessoais (LGPD), foi impulsionada, inspirada e, pode-se dizer, espelhada no RGPD.

3.3.1 Impulsionada

Impulsionada, pois, em países europeus, a afirmação do direito à proteção de dados pessoais foi acelerada e, desde 1995[117], esse direito está resguardado por normas específicas, tendo sido expressamente sublimado ao patamar de direito fundamental desde 2007, na aceção do artigo 8º, nº 1 da CDFUE e no artigo 16º, nº 1 do TFUE. No Brasil, diferentemente, o processo foi mais lento e a cultura da valorização e proteção dos dados pessoais, em voga na Europa há tempos, só veio a ser implementada recentemente.

Nada obstante o Brasil ter se deparado com a Internet em 1990, foi somente em 2014 que os princípios, as garantias, os direitos e os deveres sobre o uso desse instrumento foram materializados em uma legislação, na Lei nº 12.965/2014, também conhecida como Marco Civil da Internet. Nesse cenário, até a entrada em vigor dessa lei, a preocupação do legislador e dos outros operadores do Direito com os dados pessoais era pontual, de modo

[117] Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. É certo que, antes de 1995, o assunto já era discutido no âmbito europeu. Contudo, optou-se por estabelecer o marco temporal a partir dessa Diretiva.

que os dados pessoais estavam protegidos apenas em legislações esparsas e em referência a relações jurídicas especificas, como nas relações consumeristas e nas operações financeiras.

Com o Marco Civil da Internet, os dados pessoais receberam uma proteção mais expressiva; porém, ainda assim, essa legislação não tratou exaustivamente do assunto, o que ocorreu somente em setembro de 2020, com a entrada em vigor da Lei nº 13.709/2018 (LGPD) – uma legislação específica sobre o tratamento de dados pessoais, inclusive nos meios digitais.

Ademais, no Brasil, em que pese os avanços, o direito à proteção de dados não era reconhecido como um direito fundamental, pelo menos não como um direito expressamente positivado na Constituição. Esse cenário, contudo, começou a mudar a partir de uma paradigmática decisão do Supremo Tribunal Federal (STF), cuja questão jurídica central implicava a ponderação entre, de um lado, o compartilhamento de dados pessoais para fins de produção estatística com a finalidade de desenvolver políticas públicas; e do outro lado, o direito à intimidade e à vida privada dos titulares desses dados[118].

O imbróglio era, em suma, o seguinte: durante a pandemia de Covid-19, o Presidente da República à época editou medidas provisórias, que são normas com força de lei editadas em situações de relevância e urgência, a fim de determinar o compartilhamento de dados pessoais de clientes de empresas de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de produção estatística oficial com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

Sob o risco de violar a intimidade e a vida privada dos titulares desses dados compartilhados massivamente, a Suprema Corte brasileira foi, então, instada a analisar a constitucionalidade de tais medidas provisórias, oportunidade na qual revelou o entendimento de que a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, os quais são:

> "(...) extraídos da garantia da inviolabilidade da intimidade e da vida privada, do princípio da dignidade da pessoa humana e da garantia processual do habeas data, previstos na Constituição Federal de 1988, razão pela qual sua manipulação e tratamento hão de observar, sob pena de

[118] STF, *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. op. cit.*

> lesão a esses direitos, os limites delineados pela proteção constitucional"[119].

Diante dessas circunstâncias e ao abrigo de, dentre outros fundamentos, o de que as referidas medidas provisórias não delimitavam o objeto, a amplitude e a finalidade específica da estática a ser produzida com os dados obtidos, tampouco estabeleciam métodos de segurança para protegê-los ou mitigar os riscos de vazamentos, a Corte decidiu que tais normas extrapolaram os limites fixados pelo direito fundamental à privacidade e pelo direito recém elevado à direito fundamental: o direito à proteção de dados.

Com essa decisão, inaugurou-se um panorama peculiar no domínio do direito à proteção de dados: à míngua de uma previsão expressa de tal direito na condição de direito fundamental explicitamente autônomo, no corpo da Constituição da República Federativa do Brasil de 1988, esse direito foi associado a alguns princípios e garantias fundamentais, como é o caso do princípio da dignidade da pessoa humana e da inviolabilidade da intimidade, e foi reconduzido à categoria de direito fundamental (implicitamente positivado) por força da atuação do órgão máximo do Poder Judiciário brasileiro[120].

Os debates que se sucederam foram muitos. Havia quem sustentasse um atentado ao princípio da separação dos poderes, na medida em que o STF teria arrogado as atribuições do Poder Legislativo ao "acrescentar" – ainda que implicitamente – um direito fundamental à Constituição. Assim como, havia quem reivindicasse a necessidade de aprovação e promulgação de uma proposta de emenda à Constituição (PEC), que observa uma tramitação especial e exige o preenchimento de vários requisitos[121], para incorporar um direito fundamental ao catálogo de direitos da Constituição Federal do Brasil.

---

[119] *Ibid.*, p. 2 e 10.

[120] SARLET, Igor Wolfgang. *A EC 115/22 e a proteção de dados pessoais como Direito Fundamental*. 11 de março de 2023. Disponível em <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental>. Acesso em 17 de março de 2023.

[121] O artigo 60º da Constituição Federal do Brasil prevê que a Proposta de Emenda à Constituição (PEC) pode ser apresentada pelo presidente da República, por um terço dos deputados federais ou dos senadores ou por mais da metade das assembleias legislativas, desde que cada uma delas se manifeste pela maioria relativa de seus componentes. Não podem ser apresentadas PECs para suprimir as chamadas cláusulas pétreas da Constituição (forma federativa de Estado; voto direto, secreto, universal e periódico; separação dos poderes e direitos e garantias individuais). A PEC é discutida e votada em dois turnos, em cada Casa do Congresso, e será aprovada se obtiver, na Câmara e no Senado, três quintos dos votos dos deputados (308) e dos senadores (49).

O que importa é que esses debates não perduraram por muito tempo, uma vez que a Emenda Constitucional nº 115, promulgada em fevereiro de 2022, acrescentou o inciso LXXIX ao artigo 5º da Constituição da República Federativa do Brasil de 1988, positivando formalmente a proteção de dados pessoais como um direito fundamental autônomo:

> TÍTULO II
> DOS DIREITOS E GARANTIAS FUNDAMENTAIS
> CAPÍTULO I
> DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS
> Art. 5º 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, nos termos seguintes:
> (...)
> 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)

Graças ao despertar europeu acerca da importância dos dados pessoais e da necessidade de assegurar-lhes um âmbito de proteção próprio e sólido, compelindo o restante do mundo a fazer o mesmo; no Brasil, o direito à proteção de dados pessoais está a ganhar contornos concretos, sendo tratado como parte integrante da Constituição e, portanto, com *status* normativo superior, que conta com uma legislação infraconstitucional própria.

3.3.2 Influenciada

A lei brasileira nº 13.709/2018, a chamada LGPD, inspirou-se no Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, na medida em que se serviu do trabalho e dos ideais desse regulamento como base para suas disposições. Não se pode olvidar, entretanto, que o RGPD foi elaborado sob o contexto social e econômico da União Europeia, a fim de atender às necessidades dos seus 27 (vinte e sete) Estados-Membros, o que, certamente, não se reproduz uniformemente nos países alheios ao bloco.

Logo, em que pese a considerável influência do regulamento na lei brasileira e as semelhanças entre ambos, a LGPD foi elaborada sob a ótica social e econômica do Brasil, de maneira a prescrever disposições ímpares, que se coadunam às particularidades brasileiras no domínio da proteção de dados pessoais.

Com pretensões meramente exemplificativas, uma dessas disposições diz respeito à autodeterminação informativa, trazida expressamente pela lei brasileira como um dos fundamentos da proteção de dados pessoais, nos termos do artigo 2º, inciso II[122]. Conforme mencionado em parágrafo anterior, a autodeterminação informativa foi desvelada pelo Tribunal Constitucional alemão e desenvolvida sob o prisma do sistema jurídico europeu, todavia, não foi expressamente abordada no RGPD como um fundamento – apesar de se manifestar implicitamente em muitas disposições[123].

Ora, obviamente não se quer dizer que o legislador europeu pretendeu não assegurar o direito à autodeterminação informativa. Esse direito é devidamente assegurado no âmbito europeu e sua essência reflete em diversas disposições do RGPD; mas o legislador europeu optou por não delimitar categoricamente o direito à autodeterminação informativa como fundamento da proteção de dados pessoais. Conforme conclusões do Tribunal Constitucional português no Acórdão nº 268/2022:

> "Daqui decorre a conclusão de que as garantias contidas no direito à autodeterminação informativa dependem da estatuição legal de armazenamento dos dados pessoais num Estado-Membro da União Europeia: é nessas jurisdições que vigoram os padrões de proteção constitucionalmente impostos – plasmados quer nas Constituições nacionais, quer na CDFUE, quer nas normas de direito europeu derivado (designadamente, o RGPD) – e se assegura a atuação da autoridade administrativa independente (mesmo transfronteiriça), por atenção à rede de autoridades de controlo prevista no sistema de proteção europeu de dados pessoais(...)"[124]

Diferentemente, na LGPD, o legislador brasileiro pretendeu dar um destaque à autodeterminação informativa, situando-a expressamente nos fundamentos da disciplina da proteção de dados pessoais, ao lado da intimidade e privacidade, por exemplo, "justamente para possibilitar a afirmação do direito à autodeterminação informativa como um

---

[122] Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
(...)

[123] Como, por exemplo, no artigo 5º(1), alínea a e alínea b, que preveem, respectivamente, que "os dados pessoais são objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados" e "são recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades(...)".

[124] Acórdão do Tribunal Constitucional nº 268/2022, *op. cit*., p. 39.

contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo"[125].

Como em um Estado Democrático nenhum direito é absoluto, o direito à autodeterminação informativa está sujeito a restrições (assim como o direito à proteção de dados pessoais), desde que essas restrições sejam orientadas pelo princípio da proporcionalidade, pelo interesse público ou por outros valores constitucionais. Nesses casos, a limitação do direito à autodeterminação informativa exige a justificação exaustiva das finalidades previstas para o tratamento dos dados pessoais e a transparência desse tratamento.

O âmbito de aplicação territorial também é tratado de forma distinta pelo RGPD e pela LGPD, uma vez que, para fins de incidência do regulamento europeu, não interessa o local onde o tratamento dos dados pessoais ocorreu (se dentro ou fora da União Europeia), importando tão somente que o estabelecimento do responsável pelo tratamento ou do operador esteja situado na União Europeia. À legislação brasileira, ao contrário, não importa o país de sede da pessoa natural ou da pessoa jurídica de direito público ou privado que realizará o tratamento, tampouco o país onde estejam localizados esses dados.

Para fins de alcance da LGPD, o que interessa é justamente o critério considerado "desinteressante" pelo regulamento europeu: o local do tratamento dos dados pessoais – ou o local do titular dos dados; ou o local em que são oferecidos os bens e fornecidos os serviços; ou o local da coleta dos dados pessoais –, nos termos do artigo 3º:

> 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; ou (Redação dada pela Lei nº 13.853, de 2019)
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

[125] STF, *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. op. cit*., p. 108.

Observa-se que tais regras estão, contundentemente, conectadas ao território brasileiro, de modo que a aplicação da LGPD é assegurada mesmo nos casos em que os dados pessoais estejam localizados no exterior ou nos casos em que as empresas que realizam a operação de tratamento tenham sede no estrangeiro, desde que i) o tratamento desses dados tenha sido realizado no Brasil; ou ii) os titulares desses dados estejam no Brasil; ou iii) esses dados pessoais tenham sido coletados no Brasil.

Guimarães e Machado ilustram tais disposições com a seguinte situação hipotética:

> "Sendo assim, se um brasileiro, em visita a um museu na Europa, fornece seus dados, e estes são tratados pela entidade de forma contrária à LGPD, esse fato não será objeto de interesse da lei. Porém, se um brasileiro, em sua casa no Brasil, utilizando-se da internet, comprar um bilhete de entrada em um museu europeu, fornecendo seus dados, e este tratar desses de forma contrária à lei brasileira, tal fato é objeto de proteção da LGPD."[126]

Isso revela um alcance extraterritorial da LGPD – ainda que sutilmente em razão dessa forte conexão com elementos do território brasileiro. Portanto, nada obstante as distintas regras de aplicação, tanto o RGPD como a LGPD alcançam atos praticados fora do respetivo território – de uma forma mais tangível, certamente, no regulamento europeu por ter sido o pioneiro no domínio da proteção dos dados pessoais no que diz respeito ao tratamento e à livre circulação desses dados, repercutindo no cenário global e, principalmente, em todos os países do bloco.

Além disso, outra disposição que ambas as normas abordam, mas o fazem de maneira distinta refere-se ao tratamento de categorias especiais de dados pessoais. Em seu artigo 9º, item (1), o RGPD insere nas categorias especiais de dados pessoais os dados que revelam "a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

[126] GUIMARAES, João Alexandre; MACHADO, Lécio. *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018 com alterações da MPV 869/2020*. Rio de Janeiro: Editora Lumen Juris, 2020, p. 18.

A LGPD, por sua vez, dá a essas categorias especiais de dados pessoais o nome de "dado pessoal sensível", fazendo uma distinção expressa, no seu artigo 5º, entre dado pessoal e dado pessoal sensível, conceituando esse último como: "dado pessoal 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".

Vê-se que tanto o RGPD como a LGPD dão uma atenção especial a certas categorias de dados pessoais, definindo-as em termos bastante similares. O que diferencia ambas as normas, portanto, são as situações nas quais dados como esses podem ser objeto de tratamento. O artigo 9º(1) do regulamento europeu proíbe, expressamente, o tratamento das categorias especiais de dados pessoais[127]; mas logo em seguida, no item 2, ameniza o alcance dessa proibição ao estabelecer especificamente os casos em que ela não se aplica.

Nota-se, assim, que o RGPD inaugura o artigo 9º com uma proibição categórica, como regra geral, para depois trazer as exceções – as situações nas quais o tratamento de categorias especiais de dados pessoais pode ser realizado. A força normativa é no sentido de que (em regra) não se pode tratar as categorias especiais de dados pessoais, a não ser que se verifique um dos seguintes casos:

> a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas (...);
> b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social (...);
> c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
> d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais (...);
> e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

[127] Artigo 9º(1): É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

> f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;
> g) Se o tratamento for necessário por motivos de interesse público importante (...);
> h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado (...);
> i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública (...);
> j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos (...)

A abordagem da LGPD, por sua vez, é mais subtil, na medida em que não traz uma proibição taxativa. O artigo 11 da legislação brasileira estabelece que o tratamento de categorias especiais de dados pessoais – os chamados dados pessoais sensíveis – pode ocorrer, mas apenas nas hipóteses previstas no inciso I e no inciso II. Nesse caso, a força normativa é no sentido de que os dados pessoais sensíveis podem ser tratados, desde que ocorra as seguintes hipóteses:

> I – Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II – Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (...);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (...)

Malgrado a correspondência entre algumas das mencionadas hipóteses, a LGPD e o RGPD diferem-se, por exemplo, no que diz respeito ao tratamento de dados pessoais especiais/sensíveis quando o titular dos dados tiver dado o seu consentimento explícito, na medida em que a norma brasileira prevê que esse consentimento pode ser dado tanto pelo titular como pelo seu responsável legal (artigo 11º, inciso I); enquanto a norma europeia limita o consentimento ao titular (artigo 9º(2), alínea a).

No mais, ao abrigo de uma interpretação literal mais ampla que o RGPD, a lei brasileira autoriza o tratamento de dados especiais/sensíveis se esse tratamento for necessário para o exercício regular de direitos em processo judicial, administrativo e arbitral e, inclusive, em contrato (artigo 11º, inciso II, alínea d). O regulamento europeu restringe o tratamento de dados especiais/sensíveis ao exercício ou à defesa de direitos em processo judicial – não prevendo o tratamento de tais dados quando for necessário ao exercício de direitos em processo administrativo, arbitral ou em contrato (artigo 9º(2), alínea f).

Aponta-se, ainda, que ambas as legislações autorizam o tratamento de dados pessoais especiais/sensíveis para fins de investigação científica – a LGPD o faz no artigo 11º, inciso II, alínea c); e o RGPD o faz em seu artigo 9º(2), alínea j). Porém, a abrangência da regra constante no regulamento europeu é maior, na medida em que permite o tratamento de tais dados também para fins de arquivo de interesse público, para fins de investigação histórica e para fins estatísticos.

3.3.3 Espelhada

Por espelhada, quer-se dizer algo que reflete em um espelho, ou seja, é o ato de tornar igual. Nesse sentido, em razão da forte influência do RGPD sobre a LGPD e da consequente simetria entre ambas as normas, pode-se até afirmar que a lei brasileira é espelhada no regulamento europeu, na medida em que prevê várias disposições idênticas à norma europeia – ainda que com termos distintos, o teor e o fim esperado são os mesmos.

A começar pelo fato de que ambas as normas se aplicam somente às pessoas singulares, ou como a lei brasileira prefere chamar, às pessoas naturais. O artigo 1º do RGPD[128] e o seu Considerando 14[129] são taxativos ao dispor que as regras ali previstas são relativas à proteção dos dados pessoais das pessoas singulares, não abrangendo os dados pessoais relativos às pessoas coletivas.

[128] Artigo 1º(1): O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[129] A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.

Assim como, na aceção dos seus artigo 1º e artigo 5º, inciso I, a LGPD dispõe sobre o tratamento de informações relacionadas à pessoa natural identificada ou identificável, inclusive nos meios digitais, com o objetivo de, dentre outros, proteger o livre desenvolvimento da personalidade da pessoa natural. A pessoa nada mais é que o titular das relações jurídicas, podendo ser pessoa natural ou pessoa jurídica. A pessoa natural, também chamada de pessoa física, é o ser humano; ao passo que a pessoa jurídica é uma organização que visa à realização de certos interesses. Portanto, ao especificar que o seu objeto é o tratamento de dados da pessoa natural, a LGPD também delimita seu âmbito de aplicação às pessoas físicas, não estendendo-o às pessoas coletivas.

Outra disposição que ambas as normas abordaram semelhantemente refere-se às bases legais para o tratamento de dados pessoais, ou seja, às hipóteses em que o tratamento é considerado lícito. No RGPD, a licitude do tratamento ficou a cargo do artigo 6º[130], enquanto na LGPD, é o artigo 7º quem dispõe sobre o assunto. Em ambas as normas, é lícito, portanto, o tratamento de dados pessoais realizado quando 1) houver o consentimento do titular; quando 2) for necessário para a execução de um contrato; quando 3) for necessário para o cumprimento de uma obrigação jurídica (obrigação legal ou regulatória, nos termos da lei brasileira) pelo responsável pelo tratamento; quando 4) for necessário para a proteção de interesses vitais do titular dos dados ou de terceiro; quando 5) for necessário ao exercício de funções de interesse público e à execução de políticas públicas e, por fim, quando 6) for necessário para atender aos interesses legítimos do responsável pelo tratamento ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[130]Artigo 6º. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b)O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Além dessas hipóteses, a lei brasileira acrescenta mais três situações em que o tratamento de dados poderá ser realizado, não previstas pelo regulamento europeu, a saber: quando for necessário para a proteção de crédito; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; e para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária[131].

A despeito das denominações distintas, os sujeitos envolvidos no tratamento de dados pessoais são designados de forma correlata por ambas as normas. Em uma "ponta" do tratamento, está o titular dos dados, que é a pessoa natural (singular) identificada ou identificável a quem se referem os dados objeto de tratamento, nos termos do artigo 5º, inciso V da lei brasileira e do artigo 4º(1) do regulamento.

Na outra "ponta" do tratamento, estão a pessoa singular ou coletiva, a autoridade pública ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais – a quem o RGPD intitula de responsável pelo tratamento –; bem como a pessoa singular ou coletiva, a autoridade pública ou outro organismo que trata os dados pessoais por conta do responsável pelo tratamento – nomeado de subcontratante pelo RGPD. Na LGDP, esses papeis são exercidos, respectivamente, pelo controlador e pelo operador, na aceção do artigo 5º, incisos VI e VII, tendo a lei brasileira acrescentado, no inciso IX, que ambos os sujeitos são qualificados de "agentes de tratamento".

---

[131] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Quando o responsável pelo tratamento ou subcontratante não for estabelecido na União, o regulamento europeu previu a participação de um outro sujeito: o representante – uma pessoa singular ou coletiva estabelecida na União que, designada por escrito por um responsável pelo tratamento ou subcontratante (não estabelecido na União), representa-o(s) no que se refere às obrigações respetivas.

Há, por fim, a figura do encarregado, que é tratado pela lei brasileira como sendo o sujeito indicado pelo controlador e operador para atuar como um canal de comunicação entre o controlador, os titulares dos dados e a ANPD[132], recebendo comunicações dessa autoridade nacional e orientando os funcionários e os contratados da entidade acerca das práticas a serem tomadas em relação à proteção de dados. No RGPD, o encarregado é o sujeito designado pelo responsável pelo tratamento ou subcontratante sempre que o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; ou nas demais situações elencadas no artigo 37º(1)[133], a fim de, dentre outras funções, aconselhar o responsável pelo tratamento ou o subcontratante e os trabalhadores que tratem os dados a respeito das suas obrigações; bem como cooperar com a autoridade de controlo[134].

Conhecidas algumas disposições da LGPD, as quais foram aqui destacadas exemplificativamente, com o mero intuito de demonstrar a forte influência exercida pelo regulamento europeu na legislação brasileira, bem como de pontuar alguns dos principais aspectos de convergência e divergência entre ambas as normas, caberá no próximo capítulo compreender as transferências de dados pessoais realizadas para além das fronteiras dos Estados-Membros e o nível de proteção exigido pela União Europeia no âmbito dessas transferências.

---

[132] Artigo 5º, inciso VIII, da LGPD.

[133] Artigo 37º(1): O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:
(...)
b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º.

[134] Artigo 39º do RGPD.

4 O FLUXO TRANSFRONTEIRIÇO DE DADOS PESSOAIS

4.1 O QUE DIZ O RGPD SOBRE AS TRANSFERÊNCIAS DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS?

Para além das inúmeras operações realizadas sobre os dados pessoais, a integração económica e social resultante da acelerada evolução tecnológica e da globalização provocou um aumento significativo dos fluxos transfronteiriços desses dados. E esse intercâmbio dos dados pessoais se intensificou não só entre os Estados-Membros da União, como também entre eles e países terceiros e entre eles e organizações internacionais, o que fez com que o regulamento destinasse um capítulo inteiro – capítulo V – para tratar sobre o assunto.

De extrema importância para o contínuo desenvolvimento tecnológico e informático, a circulação de dados pessoais para além das fronteiras geográficas não pode ser tolhida, sob pena de engessar a inovação por eles orientada. O objetivo é, então, equilibrar o trânsito transfronteiriço de dados com a garantia de que nenhuma transferência de dados pessoais para países terceiros ou para organizações internacionais irá comprometer o nível de proteção das pessoas singulares assegurado pelo RGPD.

É, então, por mais essa razão: para assegurar que, na transferência de dados pessoais para países terceiros, esses dados sejam protegidos a um nível substancialmente equivalente ao garantido pela União Europeia, que se diz que o âmbito de aplicação territorial do RGPD se estende para além das fronteiras geográficas dos Estados-Membros, alcançando – ainda que indiretamente – o ordenamento jurídico de diversos Estados, como por exemplo o do Brasil, com notáveis reflexos na sua legislação sobre a proteção de dados pessoais, conforme visto anteriormente. Dito de outra forma,

Nesse aspecto, a União Europeia atua como uma catalisadora de normas, na medida em que o país terceiro, na busca por fazer jus à decisão de adequação e ter acesso ao mercado interno da União, vê-se pressionado a harmonizar sua legislação com a europeia. Rangel de Mesquita explica essa atuação da União Europeia nos seguintes termos:

> "O posicionamento da UE de induzir pressão nos países terceiros no sentido de aproximar estas legislações com a europeia está de acordo com um princípio que rege a sua atuação externa, qual seja, o princípio da

> responsabilidade, que traduz um objetivo de longa data dos seus órgãos de incrementar a visibilidade e a eficácia da sua atuação internacional no sentido de torná-la uma potência capaz de marcar eticamente a globalização"[135].

Para tanto, o regulamento europeu prevê que as transferências de dados pessoais podem ser feitas com base em uma decisão de adequação e, se não for esse o caso, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou para uma organização internacional se tiverem apresentado garantias adequadas, e na condição dos titulares dos dados gozarem de direitos oponíveis e de medidas judiciais eficazes.

Tratando-se de transferências com base em uma decisão de adequação, o artigo 45º determina que caberá à Comissão, levando em consideração critérios claros, objetivos e os demais elementos indicados nessa disposição, avaliar e decidir se o país terceiro, um território ou um (ou mais) setor específico desse país terceiro, ou a organização internacional em causa assegura um nível de proteção adequado. Essa avaliação e decisão têm em conta, nomeadamente, em que medida o país terceiro, um território ou setor específico desse país terceiro, ou a organização internacional respeita o primado do Estado de direito, o acesso à justiça, as regras internacionais no domínio dos direitos humanos e a sua legislação geral e setorial.

Nos casos em que a Comissão decide que o país terceiro ou a organização internacional oferece um nível adequado de proteção de dados, as transferências de dados pessoais para esse país ou organização internacional poderão ser efetuadas sem que seja necessária mais nenhuma autorização. Assim como, verificando que o país terceiro ou a organização internacional deixou de assegurar um nível adequado de proteção de dados, pode a Comissão alterar, substituir ou revogar a decisão de adequação, desde que envie ao país terceiro ou à organização internacional uma notificação e uma declaração completa acerca dos motivos[136].

Caso não haja uma decisão sobre o nível de proteção adequado (ou quando essa decisão tiver sido revogada pela Comissão por reconhecer que o país terceiro ou organização

[135] RANGEL DE MESQUITA, Maria J. *A Actuação Externa da União Europeia depois do Tratado de Lisboa.* Almedina, 2011, p. 184.
[136] Considerando 103 e Considerando 107.

internacional deixou de assegurar um nível adequado de proteção de dados), as transferências de dados pessoais para um país terceiro ou para uma organização internacional só poderão ser realizadas se os responsáveis pelo tratamento ou subcontratantes apresentarem garantias adequadas aos titulares dos dados, nos termos do artigo 46º.

Tais garantias podem ser previstas em regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Para além dessas garantias, os titulares de dados devem gozar de direitos oponíveis e de medidas jurídicas corretivas eficazes, especialmente o direito a recurso administrativo ou judicial e o direito de exigir indemnização, quer no território da União, quer no país terceiro[137].

Há, entretanto, situações específicas nas quais, mesmo na falta de uma decisão de adequação ou de garantias adequadas, as transferências de dados pessoais para países terceiros ou organizações internacionais poderão ser efetuadas por compreenderem, por exemplo, importantes razões de interesse público, como no caso de intercâmbio internacional de dados entre autoridades de concorrência, de supervisão financeira ou entre serviços em matéria de saúde pública. Nessas situações, as transferências de dados são tão necessárias que justificam as derrogações, as quais só se aplicam caso se verifique uma das condições ilustradas no artigo 49º:

> "a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
> b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
> c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;
> d) A transferência for necessária por importantes razões de interesse público;
> e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
> f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;

[137] Considerando 108.

> g) A transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto".

E quando a transferência não puder se basear em uma decisão de adequação ou em garantias adequadas, e não for possível aplicar nenhuma das derrogações previstas para as situações específicas acima transcritas? Pois bem. Frisa-se, primordialmente, que essa hipótese só deverá ser possível em raros casos em que não se aplique nenhum dos outros motivos de transferência.

Assim sendo, prevê o regulamento que a transferência só poderá ser efetuada se 1) não for repetitiva; 2) apenas disser respeito a um número limitado de titulares dos dados; 3) for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham aos interesses ou aos direitos e liberdades do titular dos dados; e 4) o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais.

Por último, mas não menos importante, quando não se aplicar nenhuma dessas hipóteses autorizadoras da transferência de dados pessoais para um país terceiro ou para uma organização internacional (há quem prefira chamar de motivos de transferência), ou seja, em relação às transferências ou divulgações não autorizadas pelo direito da União, como as exigidas por decisões judiciais e decisões de autoridades administrativas de um país terceiro, essas transferências apenas serão reconhecidas ou executadas se tiverem um acordo internacional como base em vigor entre o país terceiro em causa e a União Europeia ou um dos seus Estados-Membros[138].

O âmbito de aplicação do RGPD nas transferências de dados pessoais para países terceiros foi concretizado pelo TJUE no Acórdão de 16 de julho de 2020*[139],* envolvendo a seguinte situação litigiosa: no território da União, a utilização do Facebook demanda a celebração de um contrato com a *Facebook Ireland* (filial da *Facebook Inc.,* que tem sede

[138] Artigo 48º.
[139] Acórdão de 16 de julho de 2020, *Facebook Ireland e Schrems*, C-311/18, EU:C:2020:559.

nos Estados Unidos). Assim, os dados pessoais dos utilizadores dessa rede social residentes no território da União são, no todo ou em parte, transferidos para os Estados Unidos, onde são objeto de tratamento por servidores pertencentes à *Facebook Inc.* De acordo com a *Facebook Ireland*, a transferência de grande parte dos dados pessoais para a *Facebook Inc*. era feita com base nas cláusulas-tipo de proteção de dados que figuravam na Decisão de Execução (UE) 2016/1250 da Comissão, de 16 de julho de 2016.

Nessas circunstâncias, um cidadão austríaco apresentou uma queixa ao *Data Protection Commissioner* (comissário), pedindo-lhe, em suma, que a *Facebook Ireland* fosse proibida de transferir seus dados pessoais para a *Facebook Inc.*, com sede nos Estados Unidos, sob a justificativa de que o direito americano previa a colocação dos dados pessoais que são transferidos à *Facebook Inc*. à disposição das autoridades americanas, como o FBI, no âmbito de diversos programas de vigilância, o que seria incompatível com os artigos 7º, 8º e 47º da CDFUE.

A discussão, então, foi submetida ao TJUE pelo órgão jurisdicional de reenvio – Tribunal Superior da Irlanda –, a fim de saber, dentre outras questões, se o artigo 2º, nº 1 e o artigo 2º, nº 2, alíneas a), b) e d), do RGPD devem ser interpretados no sentido de que está abrangida pelo âmbito de aplicação daquele regulamento uma transferência de dados pessoais efetuada por um operador económico estabelecido em Estado-Membro para outro operador económico estabelecido em um país terceiro, quando, durante ou na sequência dessa transferência, esses dados são suscetíveis de ser tratados pelas autoridades desse país terceiro para efeitos de segurança pública, de defesa e de segurança do Estado[140].

De início, asseverou-se que a transferência de dados pessoais de um Estado-Membro para um país terceiro configura um tratamento de dados pessoais, nos moldes do artigo 4º(2) do RGPD, razão pela qual a exclusão de tal operação do âmbito de aplicação desse regulamento só se justificaria por força das hipóteses previstas no artigo 2º(2). Assim, ao amparo de uma interpretação estrita do mencionado dispositivo, o Tribunal concluiu que:

> "No caso vertente, uma vez que a transferência de dados pessoais em causa no processo principal é efetuada pela Facebook Ireland para a Facebook Inc., a saber, entre duas pessoas coletivas, essa transferência não está abrangida pelo artigo 2º, nº 2, alínea c), do RGPD, que visa o tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. A referida transferência também

[140] *Ibid*., nº 80.

> não está abrangida pelo âmbito de aplicação das exceções que figuram no artigo 2º, nº 2, alíneas a), b) e d), deste regulamento, uma vez que as atividades aí referidas a título de exemplo são, em qualquer caso, atividades próprias dos Estados ou das autoridades estatais, alheias aos domínios de atividade dos particulares (v., por analogia, no que respeita ao artigo 3º, nº 2, da Diretiva 95/46, Acórdão de 10 de julho de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, nº 38 e jurisprudência referida).
> Ora, a possibilidade de os dados pessoais transferidos entre dois operadores económicos para fins comerciais sofrerem, no decurso ou na sequência da transferência, um tratamento para efeitos de segurança pública, de defesa e de segurança do Estado, pelas autoridades do país terceiro em causa, não pode excluir a referida transferência do âmbito de aplicação do RGPD".[141]

Portanto, ainda que os dados pessoais transferidos para fins comerciais por um operador económico estabelecido em um Estado-Membro para outro operador económico estabelecido em um país terceiro sejam suscetíveis de tratamento pelas autoridades desse país terceiro para efeitos de segurança pública, de defesa e de segurança do Estado, essa transferência de dados está abrangida pelo âmbito de aplicação do regulamento.

No mais, o Tribunal também se pronunciou acerca dos elementos que devem ser considerados para determinar o caráter adequado do nível de proteção exigido pelo artigo 46º(1) e pelo artigo 46º(2), alínea c), do RGPD no contexto de uma transferência de dados pessoais para um país terceiro. O nível de proteção exigido por tais disposições é no sentido de que os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas e na condição dos titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes, sendo possível prever essas garantias adequadas em cláusulas-tipo de proteção de dados adotadas pela Comissão.

A natureza dessas garantias adequadas foi definida pelo Tribunal à guarida do Considerando 104[142] do regulamento, de maneira a assegurar que as pessoas cujos dados

---

[141] *Ibid.,* nº 85 e nº 86.

[142] 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

pessoais são transferidos para um país terceiro com base, por exemplo, em cláusulas-tipo de proteção de dados se beneficiem de um nível de proteção substancialmente equivalente ao garantido na União – como no âmbito de uma transferência baseada em uma decisão de adequação[143]. Para Kettemann:

> "A nível europeu, no caso *Schrems*, o TJUE declarou que o nível de proteção de dados noutros Estados deve ser "razoável" (ou seja, "igual em substância" para a União se fosse permitida uma transferência de dados dos utilizadores europeus). A equivalência é subsequentemente substanciada pelo TJUE com referência à legislação europeia de proteção de dados (salientando ao mesmo tempo que o nível de proteção não precisa de ser idêntico)."[144]

E no que concerne à avaliação do nível de proteção assegurado no contexto dessa transferência, o Tribunal apontou como elementos a serem considerados as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União e o destinatário da transferência estabelecido no país terceiro, bem como, "no que diz respeito a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro"[145].

À luz de tudo o que foi exposto, depreende-se que o fluxo dos dados pessoais no ecossistema digital, por sua própria natureza transfronteiriça, envolve diversos Estados e fomenta a interação entre eles, de modo que sempre que esses dados atravessam fronteiras fora do território da União Europeia, aumenta-se o risco das pessoas singulares não poderem exercer os seus direitos à proteção de dados, seja porque o país terceiro tenha um regime jurídico incoerente, com restrição de medidas preventivas ou com medidas de reparação insuficientes, seja porque as autoridades de controlo não consigam dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras.

---

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.

[143] *Facebook Ireland e Schrems*. *op. cit.*, nº 96.

[144] KETTEMANN, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*. *op. cit.,* p. 166. Tradução livre.

[145] *Facebook Ireland e Schrems*, *op. cit.,* nº 105.

O fluxo legítimo e ponderado dos dados pessoais exige, por conseguinte, uma cooperação estreita e sólida entre os Estados, a fim de proporcionar a assistência mútua internacional no que diz respeito à aplicação da legislação de proteção de dados pessoais. Para efeitos de elaboração das regras de cooperação internacional, o artigo 50º do RGPD[146] determinou que compete à Comissão e às autoridades de controlo, dentre outras medidas, "trocar informações e colaborar com as autoridades competentes de países terceiros em atividades relacionadas com o exercício dos seus poderes, com base na reciprocidade e em conformidade com o regulamento[147]".

4.2 TRANSFERÊNCIAS DE DADOS PESSOAIS ENTRE ESTADOS-MEMBROS E O BRASIL

4.2.1 Com base em uma decisão de adequação

Delineada a conjuntura em que o campo da proteção de dados pessoais no Brasil se desenvolveu e percorridas as principais normas sobre o assunto, resta avaliar se nas transferências de dados realizadas entre Estados-Membros e o Brasil, esse país – na condição de país terceiro – cumpre o nível de proteção exigido pela União Europeia. Como já dito nos parágrafos anteriores, o RGPD previu alguns mecanismos[148] para enquadrar as transferências de dados de um país membro da UE para um país terceiro.

---

[146] Artigo 50º. Em relação a países terceiros e a organizações internacionais, a Comissão e as autoridades de controlo tomam as medidas necessárias para:
a) Estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;
b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;
c) Associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais;
d) Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros.

[147] Considerando 116.

[148] Didaticamente elencados no artigo *"Que regras se aplicam se a minha organização transferir dados para fora da UE?"*. Disponível em <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt>. Acesso em 27 de abril de 2023.

Um deles é a decisão de adequação adotada pela Comissão Europeia, por meio da qual se declara que um país terceiro oferece um nível adequado de proteção, possibilitando, assim, que a transferência dos dados para esse país seja semelhante às transferências de dados no interior da União Europeia: sem entraves burocráticos e sem que seja necessário apresentar garantias complementares.

Além de atender aos elementos (de ordem material) previstos no artigo 45º(2) do RGPD, uma decisão de adequação percorre os seguintes procedimentos (de ordem formal): uma proposta da Comissão Europeia; um parecer do CEPD; uma aprovação de representantes dos países da UE; para então, finalmente, culminar na decisão da Comissão Europeia, através de um ato de execução, que declara que um país terceiro garante um nível adequado de proteção.

Fala-se em RGPD, sem esquecer, contudo, que a Diretiva 95/46/CE já tratava das decisões de adequação como instrumento autorizativo para o fluxo de dados transnacionais. Nesse cenário, desde a vigência da Diretiva, alguns países já foram objeto de uma decisão de adequação[149], a saber: Andorra (em 2010)[150], Argentina (em 2003)[151], Canadá (em 2001)[152], Ilhas Faroé (em 2010)[153], Guernsey (em 2003)[154], Israel (em 2011)[155], Ilha de Man

[149] Conforme informações extraídas do sítio eletrônico <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt?etrans=pt>. Acesso em 27 de abril de 2023.

[150] Decisão 2010/625/UE, Decisão da Comissão, de 19 de outubro de 2010, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Andorra.

[151] Decisão 2003/490/CE, Decisão da Comissão**,** de 30 de junho de 2003, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais na Argentina.

[152] Decisão 2002/2/EC**,** Decisão da Comissão, de 20 de dezembro de 2001, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos**.**

[153] Decisão 2010/146/UE, Decisão da Comissão, de 5 de março de 2010, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativamente à adequação do nível de protecção assegurado pela Lei sobre o tratamento de dados pessoais das Ilhas Faroé.

[154] Decisão 2003/821/EC, Decisão da Comissão, de 21 de novembro de 2003, relativa à adequação do nível de protecção de dados pessoais em Guernsey.

[155] Decisão 2011/61/UE, Decisão da Comissão, de 31 de janeiro de 2011, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pelo Estado de Israel no que se refere ao tratamento automatizado de dados.

(em 2004)[156], Jersey (em 2008)[157], Nova Zelândia (em 2013)[158], Suíça (em 2000)[159] e Uruguai (em 2012)[160].

É claro que isso não impede que tais decisões venham a ser questionadas e, se for o caso, que os referidos países deixem de ser considerados "adequados". Inclusive, foi o que aconteceu com os Estados Unidos da América. Também ao tempo da vigência da Diretiva 95/46/CE, os Estados Unidos foram considerados pela Comissão, por meio da Decisão 2000/520 (intitulada *Safe Harbor*), um país terceiro que oferecia um nível adequado de proteção. Entretanto, em 2015, a partir das revelações feitas por Edward Snowden acerca da vigilância massiva e indiscriminada dos dados de cidadãos europeus, o TJUE declarou inválida a Decisão 2000/520 no julgamento do caso que ficou conhecido como *Schrems I*[161].

Com a invalidação da mencionada decisão e a partir de novas negociações com os EUA, a Comissão adotou outra decisão de adequação, a Decisão de Execução (EU) 2016/1250 (*EU-U.S. Privacy Shield*), que vigorou de 2016 a 2020. Contudo, em 2020, essa decisão também veio a ser invalidada pelo TJUE no julgamento do caso *Schrems II*[162]. Atualmente, portanto, não está em vigor nenhuma decisão de adequação no panorama União Europeia e Estados Unidos[163]– o que significa que a transferência dos dados só poderá ser efetuada mediante a apresentação de garantias adequadas e na condição de as pessoas gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

---

[156] Decisão 2004/411/EC, Decisão da Comissão, de 28 de abril de 2004, relativa à adequação do nível de proteccção de dados pessoais na Ilha de Man.
[157] Decisão 2008/393/EC, Decisão da Comissão, de 8 de maio de 2008, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Jersey.
[158] Decisão 2013/65/UE, Decisão de Execução da Comissão, de 19 de dezembro de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela Nova Zelândia.
[159] Decisão 2000/518/EC, Decisão da Comissão, de 26 de julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça.
[160] Decisão 2012/484/UE, Decisão de Execução da Comissão, de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados.
[161] Acórdão de 6 de outubro de 2015, *Schrems e Data Protection Commissioner*, C-362/14, EU:C:2015:650.
[162] Acórdão de 16 de julho de 2020, *Facebook Ireland e Schrems*, C-311/18, EU:C:2020:559.
[163]Mas a Comissão Europeia iniciou, em dezembro de 2022, o processo formal de adoção de uma decisão de adequação. Disponível em <https://ec.europa.eu/commission/presscorner/detail/pt/ip_22_7631>. Acesso em 27 de abril de 2023.

Para além dos países referidos, a Comissão decidiu recentemente – já ao abrigo do RGPD –, através de atos de execução, que o Japão (em 2019)[164], a República da Coreia (em 2021)[165] e o Reino Unido (em 2021)[166] garantem um nível de proteção adequado. No que diz respeito ao Brasil, uma decisão de adequação (ainda) não foi adotada, o que faz emergir a seguinte questão: o Brasil poderia ser objeto de uma decisão de adequação? Ou seja, poderia a Comissão declará-lo, com efeitos vinculativos para os Estados-Membros, como um país terceiro que assegura um adequado nível de proteção de dados?

Como ponto de partida, é preciso entender o conceito de nível de proteção adequado ao abrigo das disposições do artigo 45º do RGPD em conjunto com a norma desenvolvida pelo TJUE nos processos *Schrems I* e *Schrems II*, no sentido de que um nível de proteção adequado é aquele substancialmente equivalente ao garantido dentro da UE. O intuito não é exigir que as normas às quais o país terceiro recorre para assegurar tal nível de proteção sejam idênticas às implementadas dentro da União, mas sim, estabelecer parâmetros e requisitos essenciais para essas normas.

A decisão de adequação, portanto, nada mais é do que o reconhecimento formal, pela Comissão Europeia, de que o nível de proteção de dados de um país terceiro é substancialmente equivalente ao nível de proteção assegurado pela UE. Para tanto, a Comissão deve levar em consideração os elementos indicados no artigo 45º(2) do RGPD, a saber:

> 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;

[164] Decisão de Execução (UE) 2019/419 da Comissão, de 23 de janeiro de 2019, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Japão no âmbito da Lei relativa à proteção de informações pessoais.
[165] Commission Implementing Decision, of 17.12.2021, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act.
[166] Commission Implementing Decision, of 28.6.2021, pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

> 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
> 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.

Particularmente, no caso do Brasil, a subsunção dos mencionados elementos deve ser feita à luz da Constituição da República Federativa do Brasil de *f*1988, que prima pelo Estado Democrático de Direito, protege a privacidade e o sigilo das comunicações, garante a concessão do *habeas data* e assegura, dentre outros princípios fundamentais, a dignidade da pessoa humana e a prevalência dos direitos humanos; bem como à luz da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), acrescida de outras legislações setoriais pertinentes, como, por exemplo, a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Um dos elementos indicados na acima transcrita alínea a) diz respeito à legislação em vigor no país terceiro sobre o acesso das autoridades públicas a dados pessoais, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal. A importância de tal elemento para avaliar o nível de proteção assegurado pelo país terceiro foi reforçada pelo TJUE no acórdão *Schrems II*, ocasião na qual o TJUE, ao avaliar as limitações da proteção de dados pessoais baseadas em programas de vigilância para fins de segurança nacional, as quais "decorrem da regulamentação interna dos Estados Unidos relativa ao acesso e à utilização, pelas autoridades publicas americanas, desses dados transferidos da União para os Estados Unidos"[167], entendeu que a legislação de tal país não garantia um nível de proteção substancialmente equivalente ao exigido no direito da União, de modo a invalidar a decisão de adequação adotada pela Comissão.

[167] Acórdão de 16 de julho de 2020, *Facebook Ireland e Schrems*, *op. cit.,* parágrafo 185.

Acrescenta-se, a título exemplificativo, que na Decisão de Execução (UE) 2019/419, ao reconhecer formalmente que o Japão assegura um nível adequado de proteção, a Comissão evidenciou as normas japonesas concernentes ao acesso e à utilização de dados pessoais transferidos da UE por autoridades públicas no Japão para fins de aplicação do direito penal e de segurança nacional, avaliando-as categoricamente e "igualmente as limitações e garantias, incluindo a supervisão e os mecanismos individuais de recurso disponíveis na legislação japonesa, no tocante à recolha e utilização subsequente de dados pessoais transferidos por autoridades públicas para operadores comerciais no Japão"[168].

No Brasil, o acesso das autoridades públicas brasileiras a dados pessoais é regulado nas disposições previstas na Lei nº 12.527/2011 (Lei de Acesso à Informação), assim como na LGPD, que prevê em seus artigos 23º a 32º as regras para o tratamento de dados pessoais pelo poder público e a consequente responsabilidade em caso de infração. De acordo com os referidos artigos, o tratamento de dados pessoais pelas autoridades públicas brasileiras deverá atender à finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. No mais, é vedado ao poder público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que exija a transferência; quando a transferência objetivar a prevenção de fraudes e irregularidades, ou proteger a segurança e integridade do titular dos dados; ou quando houver previsão legal, contratos ou convênios que respaldem a transferência.

Entretanto, por força do seu artigo 4º, inciso III, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Nessas hipóteses, o tratamento de dados pessoais deverá ser regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular dos dados[169].

É certo que essa legislação específica, que trata das ingerências ao direito à proteção de dados, de modo a permitir o acesso e a utilização de dados pessoais pelas autoridades

[168] Decisão de Execução (UE) 2019/419 da Comissão, *op. cit.,* parágrafo 113.
[169] Conforme artigo 4º, §1º, da LGPD.

publicas brasileiras para fins de segurança pública, de defesa nacional, de segurança do Estado e de direito penal ainda não está em vigor, o que obstaculiza, por ora, uma decisão de adequação relativa ao Brasil.

Nada obstante, já está em trâmite no Parlamento brasileiro o Projeto de Lei 1515/2022[170], que trata da aplicação da LGPD para fins de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais, o qual, caso se torne lei, adequará "o sistema de justiça criminal brasileira aos ditames de investigação penal preconizados internacionalmente, buscando proteger direitos e garantias dos cidadãos frente ao poder de vigilância do Estado"[171], na medida em que definirá os requisitos para o tratamento de dados pessoais por uma autoridade pública, impedindo um poder indiscriminado de acesso aos dados pessoais. Destaca-se que também está em trâmite no Parlamento brasileiro o Projeto de Lei 2630/2020[172], que trata das *fake news* e visa instituir a lei brasileira de liberdade, responsabilidade e transparência na Internet, de modo a delimitar a capacidade das autoridades de segurança pública e nacional de compelir os controladores de dados pessoais a entregar tais dados.

Ambos os projetos legislativos, portanto, estão a caminhar para a aprovação, o que elevará o ordenamento jurídico brasileiro aos padrões internacionais e assegurará um nível de proteção ainda mais robusto. Além do mais, a LGPD tem forte inspiração no RGPD, conforme já detalhado anteriormente, o que favorece uma possível decisão de adequação. Assim como o regulamento europeu, a lei brasileira reserva um capítulo inteiro – o Capítulo V – para tratar das regras sobre a transferência internacional de dados pessoais, estabelecendo em seu artigo 33º, taxativamente, as hipóteses nas quais essa transferência é permitida e exigindo, para tanto, um grau de proteção de dados pessoais adequado, a ser avaliado por uma autoridade nacional.

Outro elemento a ser considerado pela Comissão na avaliação do nível de proteção é se há, no país terceiro, uma autoridade de controlo em efetivo funcionamento e hábil a assegurar e impor o cumprimento das regras de proteção de dados, bem como a cooperar

---

[170] A íntegra do Projeto está disponível em <https://www.camara.leg.br/propostas-legislativas/2326300>.

[171] PRATES, Fernanda; MEGGIOLARO, Daniella; FERNANDES, Maíra. *Lei de Proteção de Dados para segurança pública e persecução penal.* Revista Consultor Jurídico, 28 de outubro de 2022. Disponível em <https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal>. Acesso em 2 de maio de 2023.

[172] A íntegra do Projeto está disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>.

com as autoridades de controlo dos Estados-Membros. No Brasil, desde 2020, a figura de autoridade de controlo[173] é exercida pela Autoridade Nacional de Proteção de Dados (ANPD), à qual compete, dentre outras inúmeras atribuições, zelar pela proteção de dados pessoais; elaborar as diretrizes que regulamentam o tratamento de dados pessoais; fiscalizar e aplicar as penalidades em caso de descumprimento da LGPD; informar a população acerca das políticas de proteção de dados; estimular o cumprimento das normas pelas empresas que fazem uso dos dados pessoais e promover ações de cooperação com autoridades de proteção de dados pessoais de outros países[174].

A atuação da ANPD é de tamanha importância que ela assumiu o *status* de órgão independente do Poder Executivo brasileiro, com autonomia administrativa e financeira[175], o que traz mais confiabilidade ao sistema brasileiro regulatório e fiscalizatório de proteção de dados. E para endossar uma atuação ainda mais efetiva, a ANPD conta com o auxílio do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)[176], um órgão de natureza consultiva, cujas principais atribuições são elaborar estudos, realizar debates e audiências públicas sobre a proteção de dados e da privacidade e sugerir ações a serem realizadas pela ANPD.

No que diz respeito aos compromissos internacionais – elemento a ser considerado pela Comissão na aceção da alínea c) do artigo 45º(2) do RGPD –, o primeiro e mais relevante instrumento internacional com efeitos vinculativos adotado no domínio da proteção de dados pessoais foi a Convenção 108 do Conselho da Europa, instituída em janeiro de 1981, consubstanciando-se em "um marco internacional que começou a pavimentar potencial estrutura global de proteção de dados"[177].

---

[173] Artigo 5º, inciso XIX, da LGPD – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
[174] A ANPD foi criada pela Lei nº 13.853/2019, que incluiu o artigo 55-J na LGPD, nele estabelecendo todas as atribuições dessa autoridade.
[175] Nos termos da Lei nº 14.460, de 25 de outubro de 2022, a ANPD é uma autarquia de natureza especial.
[176] Criado pela Lei nº 13.853/2019.
[177] CAMARGO, Guilherme; FACHINETTI, Aline F. *Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil.* Revista Consultor Jurídico, 4 de julho de 2021. Disponível em < https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados#:~:text=Além%20do%20Brasil%2C%20que%20se,potencial%20futuro%20framework%20global%20de>. Acesso em 8 de maio de 2023.

A Convenção 108 está disponível para adesão por países europeus e não-europeus e, atualmente, 55 (cinquenta e cinco) países já a ratificaram[178]. Em que pese não ser um desses países signatários, o Brasil é, desde outubro de 2018, membro observador da Convenção[179], o que o possibilita de participar das reuniões do Comité da Convenção e, consequentemente, das discussões envolvendo aspetos da proteção de dados pessoais. Em razão das intensas relações comerciais entre Brasil e países europeus e diante da relevância da proteção de dados nessas relações, o Brasil – representado pela ANPD – tem participado ativamente das discussões relativas à Convenção.

A título exemplificativo, na 43ª Reunião Plenária da Convenção 108, em novembro de 2022, a ANPD se fez presente, ocasião na qual foram discutidas, principalmente, as cláusulas contratuais no contexto das transferências internacionais de dados pessoais. Essa participação ativa do Brasil, além de facilitar as cooperações internacionais envolvendo a proteção dos dados pessoais, evidencia o seu compromisso de buscar as melhores práticas regulamentadoras em nível mundial para a LGPD[180].

Ademais, não se pode olvidar que graças ao ímpeto europeu de elevar o direito à proteção de dados pessoais ao patamar de direito fundamental, na aceção do artigo 8º, nº 1 da CDFUE e do artigo 16º, nº 1 do TFUE, o Brasil também atribuiu a esse direito um *status* normativo superior, positivando-o formalmente, no inciso LXXIX do artigo 5º da Constituição da República Federativa do Brasil de 1988, como um direito fundamental autônomo.

Para melhor elucidar os aspetos que circunscrevem a decisão de adequação, o CEPD elaborou um documento de referência relativo à adequação[181], segundo o qual a

---

[178] Conforme informações disponíveis em <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>. Acesso em 8 de maio de 2023.

[179] Conforme informações disponíveis em <https://www.coe.int/en/web/data-protection/-/brazil-and-the-data-protection-commission-of-gabon-to-join-the-committee-of-convention-108-as-observers->. Acesso em 8 de maio de 2023.

[180] Conforme informações disponíveis em <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-43a-reuniao-plenaria-da-convencao-108-na-franca>. Acesso em 8 de maio de 2023.

[181] WP 254 rev. 01, Documento de referência relativo à adequação, adotado em 28 de novembro de 2017. Disponível em <https://ec.europa.eu/newsroom/article29/items/614108/en>. Acesso em 2 de maio de 2023.
O presente documento visa fornecer orientações à Comissão Europeia e ao GT29, ao abrigo do RGPD, com vista à avaliação do nível de proteção de dados em países terceiros e organizações internacionais, estabelecendo quais os princípios centrais da proteção de dados que devem ser incluídos no quadro normativo de um país terceiro ou organização internacional para assegurar uma equivalência substancial em relação ao quadro normativo europeu. Além disso, pode servir para orientar os países terceiros e as organizações internacionais interessados em alcançar a adequação.

qualificação "adequada" engloba não só o conteúdo das normas aplicáveis, como também, a forma como a sua aplicação efetiva é assegurada:

> "A adequação pode ser alcançada através de uma combinação de direitos conferidos aos titulares dos dados e de deveres impostos a quem trata os dados ou quem exerce o controlo sobre esse tratamento e supervisão por organismos independentes. Contudo, as normas relativas à proteção de dados só são eficazes se tiverem caráter executório e forem aplicadas na prática. Por conseguinte, é necessário ter em conta não apenas o conteúdo das normas aplicáveis aos dados pessoais transferidos para um país terceiro ou organização internacional, mas também o sistema existente para assegurar a eficácia dessas normas. A existência de mecanismos executórios eficientes é extremamente importante para a eficácia das normas de proteção de dados". [182]

De acordo com o aludido documento, para assegurar um nível de proteção substancialmente equivalente ao estabelecido na legislação da União, o sistema jurídico do país terceiro deve conter, no que diz respeito ao conteúdo:

I. Conceitos básicos, como dados pessoais; tratamento de dados pessoais; responsável pelo tratamento; subcontratante, dentre outros;

II. Os fundamentos, de forma clara, para o tratamento de dados lícito, leal e legítimo;

III. O direito do titular dos dados de acesso, retificação e apagamento; e

IV. As restrições relativas a transferências subsequentes.

O sistema jurídico brasileiro, especificamente as normas constantes na LGPD, compreende esses quatro mecanismos, visto que o artigo 5º da LGPD traz dezanove conceitos basilares em matéria de proteção de dados, os quais, a despeito de utilizarem algumas terminologias distintas das usadas no regulamento europeu, são coerentes com o RGPD e refletem os conceitos nele consagrados.

Os fundamentos para o tratamento de dados pessoais – ou requisitos como a LGPD preferiu nomear – foram estabelecidos, de forma clara, no artigo 7º da lei brasileira e,

[182] *Ibid.,* p. 3.

inclusive, tanto o RGPD como a LGPD regulam o tema de modo muito semelhante, conforme as minuciosas comparações feitas no capítulo anterior.

O direito atribuído ao titular dos dados de obter a confirmação de que os dados pessoais que lhe digam respeito são (ou não) objeto de tratamento e, se for o caso, o direito de aceder aos seus dados pessoais estão assegurados pelas normas brasileiras, no artigo 18º, incisos I e II, da LGPD[183]. Já o direito à retificação dos dados pessoais inexatos ou incompletos está previsto no artigo 18º, inciso III, da LGPD[184]. O "direito a ser esquecido" – assim nomeado pelo RGPD para designar o direito de obter o apagamento dos dados pessoais quando, por exemplo, tais dados deixarem de ser necessários para a finalidade que motivou seu tratamento ou quando foram tratados ilicitamente[185] – foi consagrado no artigo 18º, inciso IV, da LGPD como sendo o direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com os preceitos da legislação brasileira.

O último dos quatro mecanismos indicados no documento elaborado pelo CEPD – as restrições relativas a transferências subsequentes – refere-se às "outras transferências dos dados pessoais por parte do destinatário inicial da transferência de dados original, as quais só devem ser permitidas se o destinatário seguinte (ou seja, o destinatário da transferência subsequente) também estiver sujeito a normas (incluindo normas contratuais) que garantam um nível de proteção adequado"[186].

Nesse sentido, verificam-se duas situações na LGPD em que os dados pessoais podem ser transferidos a um destinatário alheio à transferência original: a primeira situação está prevista no artigo 16º, inciso III, o qual determina que os dados pessoais devem ser eliminados após o término de seu tratamento, mas autoriza a conservação desses dados para

---

[183] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados; (...)

[184] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
(...)
III - correção de dados incompletos, inexatos ou desatualizados;

[185] Artigo 17º do RGPD.

[186] WP 254 rev. 01. *op. cit*., p. 6.

fins de transferência a terceiros, exigindo, para tanto, que sejam respeitados os requisitos de tratamento de dados dispostos na lei.

A segunda situação refere-se às transferências internacionais de dados, no caso em que o Brasil, na condição de destinatário inicial da transferência de dados original, transfere tais dados a um destinatário internacional seguinte (ou seja, o destinatário da transferência subsequente). Nesta situação, o artigo 33º da LGPD estabelece que a transferência internacional de dados pessoais só é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei – grau esse que será avaliado pela ANPD com base nos elementos indicados no artigo 34º.

Em ambas as situações, portanto, as normas brasileiras estipulam restrições relativas a transferências subsequentes, seja impondo o respeito aos requisitos de tratamento de dados dispostos na LGPD, seja exigindo um nível adequado de proteção dos dados por parte do destinatário internacional seguinte.

Também ao abrigo do documento do CEPD, as normas do país terceiro devem endossar, em relação ao conteúdo, os princípios básicos em matéria de proteção de dados, tais como o princípio da limitação da finalidade do tratamento; o princípio da qualidade, proporcionalidade e conservação dos dados; o princípio da segurança e da confidencialidade e o princípio da transparência. Todos esses princípios – e outros mais – estão expressamente consagrados no artigo 6º da LGPD[187].

[187] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respetivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Ademais, como apontado no excerto extraído do documento elaborado pelo CEPD, uma decisão de adequação também implica o estabelecimento, no sistema jurídico do país terceiro, de mecanismos processuais hábeis a garantir a aplicação efetiva das normas de proteção de dados. Nesse cenário, um sistema jurídico coerente com o europeu deve ter:

I. Uma autoridade de controlo independente e competente;

II. Um bom nível de responsabilização e de sensibilização;

III. Instrumentos de reparação e

IV. Medidas para auxiliar os titulares de dados no exercício de seus direitos.

No Brasil, o campo da proteção de dados pessoais está a ser fortemente adubado e as normas dele integrantes já são hábeis a extrapolar o plano teórico, estruturando um sistema normativo dotado, cada vez mais, de caráter executório. A começar pela instituição da (já citada) ANPD, em efetivo funcionamento desde 2020, a quem foi atribuída a missão de atuar como órgão central de interpretação da LGPD e de estabelecer diretrizes para a sua implementação, conferindo-lhe, para tanto, autonomia técnica e decisória[188].

Por meio da ANPD, por exemplo, foram celebrados acordos de cooperação técnica com a Secretaria Nacional do Consumidor do Ministério da Justiça e da Segurança Pública, com a Agência Espanhola de Proteção de Dados, com o NIC.br[189], com o Conselho Administrativo de Defesa Econômica (CADE) e com o Tribunal Superior Eleitoral (TSE)[190], a fim de assegurar o cumprimento das atribuições dos órgãos públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental com maior eficiência e promover o adequado funcionamento dos setores regulados[191], bem como para

---

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[188] A autonomia conferida à ANPD se deu a partir da promulgação da Lei nº 14.460/2022, quando ela foi transformada em autarquia de natureza especial.

[189] O Núcleo de Informação e Coordenação do Ponto BR (NIC.br) é uma associação, sem fins lucrativos, criada em 08 de março de 2005, para a execução do registro de Nomes de Domínio, alocação de endereços de IP e administração do domínio nacional de nível superior (ccTLD), atualmente exercendo atividades de regulação, segurança ímpares na sua área de atuação.

[190] Conforme informações extraídas em < https://www.gov.br/anpd/pt-br>. Acesso em 2 de maio de 2023.

[191] Artigo 55-J, inciso XXIII, da LGPD.

auxiliar na comunicação às autoridades competentes das infrações penais das quais tiver conhecimento[192].

Outro mecanismo que assegura a eficácia das normas é o regime de responsabilização conjugado com o dever de prestação de contas adotado pela LGPD, o qual, inclusive, é elencado como princípio a ser observado nas atividades de tratamento de dados pessoais, nos termos do artigo 6º. Tal regime implementa a noção de responsabilidade proativa, segundo a qual os agentes de tratamento devem não só cumprir as normas, como devem também demonstrar o cumprimento, aplicando proactivamente medidas eficazes que previnam a ocorrência do dano. A lei brasileira, portanto, aborda a responsabilização sob a ótica da prevenção de danos, de modo que não basta reparar o dano, é necessário evitá-lo e preveni-lo.

Nestas circunstâncias, conforme prevê o artigo 42 da LGPD, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Para propiciar essa responsabilização, a lei brasileira exige que o controlador – aquele que faz o tratamento dos dados – seja devidamente personificado, determinando, em seu artigo 9º[193], que o titular dos dados tenha acesso facilitado às informações de identificação e de contato desse sujeito.

O sistema jurídico brasileiro dispõe, também, de sanções administrativas aplicáveis de forma gradativa, isolada ou cumulativamente, aos agentes de tratamento de dados em razão das infrações cometidas às normas previstas na LGPD. São elas: advertência; multa simples; multa diária; publicização da infração após devidamente apurada e confirmada sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se

[192] Artigo 55-J, inciso XXI, da LGPD.

[193] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
(...)
III - identificação do controlador;
IV - informações de contato do controlador; (...)

refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados[194]. Na aceção do artigo 55-K, a aplicação de tais sanções compete exclusivamente à ANPD e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outros órgãos estatais.

Por fim, para fazer valer os seus direitos e interesses, os titulares de dados contam com o auxílio da ANPD, na medida em que esse órgão é responsável por promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança e por ouvir a sociedade em matérias de interesse relevante[195]. E, em relação às vias de recurso (administrativas e judiciais), a LGPD garante ao titular de dados, para além do direito de peticionar junto à autoridade de controlo brasileira contra o controlador em relação aos seus dados pessoais[196], a faculdade de exercer a defesa de seus interesses e direitos em juízo, individual ou coletivamente, na forma da legislação pertinente sobre os instrumentos de tutela individual e coletiva[197]; bem como o direito à indemnização no caso de dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais.

Ser formalmente reconhecido como um país terceiro adequado para fins de transferência internacional de dados pessoais – sem que, portanto, seja necessária mais nenhuma autorização – exige um elevado padrão de conformidade com a legislação europeia; ainda mais nos dias atuais, em que a Comissão Europeia está a ser pressionada, tanto do ponto de vista comercial como jurídico, a adotar decisões de adequação mais estáveis, sob pena de invalidação pelo TJUE – como ocorreu com os Estados Unidos. É preciso, a partir de uma exaustiva análise da ordem jurídica do país terceiro, considerar tanto as regras aplicáveis ao tratamento de dados pelos operadores comerciais e importadores de dados como as limitações e garantias relativas ao acesso a dados pessoais pelas autoridades públicas.

No tocante à ordem jurídica brasileira, à luz dos princípios e normas aqui discutidos, o reconhecimento formal, pela Comissão, do adequado nível de proteção encontraria óbice,

[194] Artigo 52º da LGPD.
[195] Artigo 55-J, incisos VI e XIV.
[196] Conforme artigo 18º, §1º, e artigo 55-J, inciso V, ambos da LGPD.
[197] Artigo 22º da LGPD.

ao menos por ora, na ausência de uma legislação em vigor que trate das limitações e garantias relativas ao acesso a dados pessoais pelas autoridades públicas para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. No entanto, com o Brasil a caminhar a passos largos em direção ao nível de proteção de dados pessoais essencialmente equivalente ao garantido e exigido pela União Europeia, é possível que, em um futuro próximo, ele venha a ser objeto de uma decisão de adequação.

4.2.2 Com base na apresentação de garantias adequadas

De toda forma, em que pese o Brasil não ser formalmente reconhecido pela Comissão como um país que oferece um nível de proteção de dados substancialmente equivalente ao nível assegurado pela União Europeia, as transferências de dados de um país membro da UE para o Brasil poderiam se amparar em um outro mecanismo previsto no RGPD: as garantias adequadas.

Conforme determina o artigo 46º(1) do RGPD, nas situações em que não tenha sido tomada qualquer decisão de adequação, a transferência de dados pessoais para um país terceiro ou para uma organização internacional só pode ser efetuada mediante a apresentação de garantias adequadas e na condição das pessoas gozaram de direitos oponíveis e de medidas judiciais corretivas eficazes. O item (2) do artigo 46º elenca os instrumentos que, por si só, podem prever as garantias adequadas, sem que se requeira autorização específica de uma autoridade de controlo. São eles: instrumento juridicamente vinculativo e com força executiva; regras vinculativas aplicáveis às empresas; cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo e aprovadas pela Comissão; código de conduta e procedimento de certificação.

Se as garantias forem previstas, por exemplo, por meio de cláusulas-tipo de proteção de dados adotadas pela Comissão nos termos da alínea c) do item (2), a entidade que irá transferir os dados pessoais – denominada de exportador de dados – e a entidade do país terceiro que receberá tais dados – denominada de importador de dados – devem observar

a Decisão de Execução (UE) 2021/914[198]. Na medida em que tais cláusulas operam como cláusulas contratuais modelo, elas asseguram (sem qualquer autorização específica complementar) que os dados serão transferidos e processados de acordo com o regulamento europeu.

Já o item (3) especifica outros instrumentos que também podem prever as garantias, contudo, sob reserva de autorização da autoridade de controlo competente. Tais instrumentos são as cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; e as disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

O regulamento é silente quanto ao que seriam essas garantias adequadas e à sua natureza, recorrendo-se, então, às Recomendações 02/2020 do CEPD, que figuram como uma bússola para o tema. Ao amparo da jurisprudência (especialmente dos acórdãos *Schrems I e Schrems II*) e dos esclarecimentos prestados pelo TJUE, as Recomendações 02/2020 desenvolveram a concepção das garantias essenciais europeias, as quais constituem uma norma de referência para a avaliação do nível de ingerência nos direitos fundamentais à privacidade e à proteção de dados pessoais pelo país terceiro no contexto de uma transferência internacional de dados[199].

Frisa-se, oportunamente, que as garantias essenciais europeias fazem parte da avaliação para determinar se um país terceiro proporciona um nível de proteção substancialmente equivalente ao garantido na União, mas elas não têm o condão, por si só, de definir todos os elementos que possam ser necessários para avaliar se o regime jurídico de um país terceiro impede o exportador de dados e o importador de dados de assegurarem salvaguardas adequadas, em conformidade com o artigo 46º do RGPD.

---

[198] Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32021D0914.

[199] Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância, adotadas em 10 de novembro de 2020, pelo Comité Europeu de Proteção de Dados, nº 56. Disponível em <https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_pt.pdf>. Acesso em 05 de maio de 2023.

Em outras palavras, as quatro garantias indicadas nas Recomendações 02/2020 devem ser vistas em termos globais na análise conjunta da legislação pertinente em matéria de medidas de vigilância por autoridades públicas do país terceiro, do nível mínimo de salvaguardas para a proteção dos direitos dos titulares dos dados e das vias de recurso previstas na legislação nacional do país terceiro.

Quis-se dar o devido destaque para tal ponto, uma vez que, como já mencionado, ainda não vigora no Brasil uma legislação específica acerca do poder de vigilância do Estado, com acesso a dados pessoais pelas autoridades públicas, para fins exclusivos de segurança pública, de defesa nacional, de segurança estatal ou de investigação e repressão de infrações penais. O que se tem é o Projeto de Lei 1515/2022[200], em trâmite no Parlamento brasileiro, com vista a regular o assunto.

Entretanto, ainda assim, avaliar-se-á o nível de proteção assegurado no Brasil – se substancialmente equivalente ao garantido na União – a partir das garantias essenciais europeias sob a ótica da Lei nº 13.709/2018 (LGPD), que dispõe em seu Capítulo IV sobre o tratamento de dados pessoais pelo poder público, e das salvaguardas para a proteção dos direitos dos titulares dos dados e das vias de recurso previstas nessa legislação.

Dito isso, as Recomendações 02/2020 estabelecem que os requisitos legais aplicáveis para justificar as restrições à proteção de dados e aos direitos à privacidade podem ser resumidos nas seguintes garantias essenciais europeias:

I. O tratamento deve se basear em regras claras, precisas e acessíveis;

II. Deve demonstrar a necessidade e proporcionalidade em relação aos objetivos legítimos prosseguidos;

III. Deve existir um mecanismo de supervisão independente e

IV. Os indivíduos devem dispor de vias de recurso eficazes.

Na qualidade de direitos fundamentais, o exercício do direito à privacidade e do direito à proteção de dados pessoais só pode sofrer restrições previstas em lei, consoante

[200] Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. A íntegra do Projeto está disponível em <https://www.camara.leg.br/propostas-legislativas/2326300>.

artigo 52º(2) da CDFUE. A primeira garantia, então, consagra a necessidade de uma base jurídica clara, precisa e acessível que justifique o tratamento de dados pessoais, por configurar uma ingerência ao exercício do direito à privacidade e do direito à proteção de dados pessoais. Clara e precisa quanto às circunstâncias do tratamento, ao seu âmbito de aplicação, aos seus efeitos para o indivíduo e ao alcance da restrição ao exercício dos direitos em causa. E acessível no sentido de pública, de poder ser invocada pelos indivíduos perante um tribunal, conferindo-lhes direitos oponíveis às autoridades públicas.

As restrições a direitos fundamentais devem, ainda, corresponder efetivamente a objetivos de interesse geral ou à necessidade de proteção dos direitos e liberdades de terceiros, de modo a respeitar o conteúdo essencial desses direitos, nos termos do artigo 52º(1) da Carta. A este respeito, a segunda garantia essencial europeia está relacionada com o princípio da necessidade e da proporcionalidade, no sentido de que as limitações ao direito à proteção de dados pessoais devem ocorrer na estrita medida do necessário e devem ponderar, de um lado, a gravidade da ingerência e, do outro lado, a importância do objetivo de interesse público prosseguido.

O CEPD acrescenta, como terceira garantia essencial europeia, que qualquer ingerência no direito à proteção de dados deve estar sujeita a um sistema de supervisão eficaz, independente e imparcial, que deve ser assegurado quer por um juiz, quer por outro organismo independente[201]. A finalidade dessa supervisão é verificar as justificativas que amparam as ingerências ao direito em causa e se as condições para tais ingerências foram respeitadas.

Diante de restrições a direitos fundamentais, o artigo 47º da Carta assegura um meio de recurso eficaz a todos aqueles cujos direitos e liberdades tenham sido violados. A quarta e última garantia essencial europeia, portanto, consubstancia-se nos direitos de recurso do indivíduo: toda pessoa que considere que seu direito à privacidade e à proteção de dados não foi ou não é respeitado deve dispor de medidas jurídicas corretivas eficazes, a fim de fazer valer seus direitos.

No Brasil, a LGPD é a base jurídica que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais

[201]*Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância. op. cit.,* nº 39.

de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, possuindo, nos termos do seu artigo 1º, parágrafo único[202], caráter vinculativo no direito interno. As suas disposições englobam tanto o tratamento de dados efetuado por pessoa natural e por pessoa jurídica de direito privado, como pelas pessoas jurídicas de direito público[203].

Reservando um capítulo para regular o tratamento de dados pessoais pelas pessoas jurídicas de direito público – Capítulo IV –, a LGPD estabelece de forma clara e precisa que o tratamento de dados pessoais pelo poder público deve atender à uma finalidade pública, na persecução do interesse público, e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Para tanto, exige que sejam informadas as hipóteses nas quais o tratamento de dados pessoais é realizado, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, bem como que seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Ademais, nos moldes como previsto no artigo 25º da LGPD, o tratamento de dados pessoais pelo poder público mostra-se estritamente necessário à execução de políticas públicas, à prestação dos serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Logo, o objetivo prosseguido com tal ingerência, desde que sejam observados os princípios elencados no artigo 6º da Lei, tende a respeitar o conteúdo essencial dos direitos à privacidade e à proteção de dados pessoais.

As vias de recurso nas situações em que haja violação ao direito à proteção de dados pelas autoridades públicas brasileiras estão asseguradas pelo artigo 23º, §3º da LGPD, o qual prevê que o exercício dos direitos do titular tem guarida, em especial, na Lei do *Habeas Data*[204], na Lei do Processo Administrativo[205] e na Lei de Acesso à Informação,

---

[202] Art. 1º (...) Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.
[203] O termo "pessoas jurídicas de direito público" abrange os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.
[204] Lei nº 9.507/1997.
[205] Lei nº 9784/1999.

determinando esta última norma que os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou da utilização indevida de informações sigilosas ou informações pessoais[206]. Além disso, as Recomendações 02/2020 explicam que uma proteção eficaz contra as restrições à proteção de dados pessoais pode ser assegurada não só por um tribunal, mas também por um órgão que ofereça garantias essencialmente equivalentes às exigidas pelo artigo 47º da Carta, o que, no caso do Brasil, fica a cargo da ANPD.

Sem contar os mecanismos de supervisão que a ANPD exerce sobre as autoridades públicas, na medida em que pode solicitar a agentes do poder público a publicação de relatórios de impacto à proteção de dados pessoais, sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais e, quando houver infração à Lei, enviar informe com medidas cabíveis para fazer cessar a violação. Compete, ainda, a tal órgão emitir parecer técnico complementar para garantir o cumprimento da lei e solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado[207].

Pois bem. É chegada a hora de concluir. No bojo das transferências de dados pessoais para países terceiros ou organizações internacionais, a União estará atenta aos interesses legítimos dos países terceiros, na medida em que é obrigada a salvaguardar a proteção dos dados daqueles que se encontrem em seu território, mesmo que em um contexto extraterritorial. Certamente, as formas de extraterritorialidade do Regulamento (UE) 2016/679, com a sua robusta influência no cenário normativo global, culminaram no desenvolvimento de um arcabouço legal brasileiro em matéria de proteção de dados que em muito se assemelha ao regulamento europeu, prospectando legítimos interesses em comum. Contudo, essa semelhança, por si só, não basta para reconhecer (automaticamente, sem qualquer autorização específica) que o nível de proteção de dados pessoais assegurado pelo Brasil é adequado, na aceção do artigo 45º do regulamento europeu.

Um olhar para o passado, para o caminho que já se percorreu até aqui, revela o consistente progresso brasileiro no campo da proteção de dados e como a tutela desse direito

[206] Artigo 34º da Lei nº 12.527/2011.
[207] Conforme artigos 29º, 30º, 31º e 32º da LGPD.

está a ser efetiva. Por sua vez, um olhar para o futuro anuncia a necessidade desse campo continuar a ser fortemente adubado, especialmente com a promulgação de legislações setoriais referentes ao acesso das autoridades públicas a dados pessoais em matéria de segurança pública, defesa, segurança nacional e direito penal, de modo a posicionar o Brasil cada vez mais perto do nível de proteção substancialmente equivalente ao garantido pela União Europeia e, desta forma, atribuir-lhe o *status* de país terceiro "adequado", formalmente reconhecido pela Comissão.

Enquanto não se obtém uma decisão de adequação, resta ao Brasil, quando da participação nas transferências de dados com um Estado-Membro, apresentar as garantias adequadas, nos termos do artigo 46º do regulamento.

CONSIDERAÇÕES FINAIS

Ao longo das últimas décadas, o dinâmico progresso tecnológico que se está a experimentar foi (e é) o responsável por promover um intenso fluxo transfronteiriço de dados pessoais. Arrisco-me, inclusive, a também afirmar o contrário: é o intenso fluxo transfronteiriço de dados o responsável pelo constante progresso tecnológico. Afinal, a circulação de dados pessoais já é intrínseca às relações (econômicas, sociais, culturais etc.) intra e inter-nacionais a ponto de ser determinante para o desenvolvimento dessas próprias relações, bem como para a expansão da cooperação internacional e do comércio internacional; e, certamente, para o fomento do progresso tecnológico.

Seja por isso ou em razão da sua própria natureza (na era digital, a circulação de dados é livre e instantânea), o fato é que o fluxo transfronteiriço de dados se revela irrefreado. O grande desafio concentra-se, então, em evitar que leis domésticas de proteção de dados percam sua eficácia com uma transferência desses dados para um país que não os proteja adequadamente. Já que não se pode (tampouco se deve) frear o fluxo transfronteiriço de dados, resta contrapesá-lo, de modo a assegurar um nível adequado – e, na medida do possível, universal – de proteção aos seus titulares.

É o que Almeida denominou de "busca pela nova ética da globalização*"* ou "pelo mínimo ético universal"[208], que se traduz em "uns quantos princípios fundamentais que impõem aos destinatários respectivos (Estados e indivíduos) obrigações de valor constitucional e que, nessa medida, inoculam gérmenes de mudança no próprio direito público interno"[209], desde que seja respeitado o pluralismo da sociedade internacional e no limite do princípio da igualdade soberana dos Estados.

Nessa busca pela nova ética da globalização, o Regulamento (UE) 2016/679 e a jurisprudência do TJUE assumiram um papel medular no domínio da proteção de dados pessoais e da livre circulação desses dados, na medida em que conceberam regras que viajam com os dados, que os protegem independentemente de onde estejam localizados, estipulando um nível adequado mínimo de proteção: o substancialmente equivalente ao garantido pela União Europeia. Ou seja, caso pretenda ser um importador de dados transferidos por algum

[208] ALMEIDA, *Mutações sistémicas e normativas no direito internacional em face de novos desafios*. *op. cit.,* p. 232.
[209] *Ibid.*

Estado-Membro, o país terceiro deve assegurar (no mínimo) um nível de proteção essencialmente equivalente ao assegurado pela União.

Nesse contexto, o arcabouço legal brasileiro em matéria de proteção de dados pessoais contemplou os objetivos prosseguidos pelo RGPD e reproduziu as suas principais disposições. E, apesar de novel, ele está a se mostrar eficaz na garantia do direito em causa. Não se pode olvidar o reforço significativo da jurisprudência nacional nesse arcabouço legal e a influência que os tribunais internacionais exercem nos tribunais superiores brasileiros, com a tendência desses últimos se orientarem em decisões emanadas pelos primeiros.

Rememora-se a jurisprudência do Supremo Tribunal Federal, aflorada a partir de impulsos legais e jurisprudenciais europeus, que reconduziu, à míngua de uma previsão expressa no corpo da Constituição Federal de 1988, o direito à proteção de dados pessoais à categoria de direito fundamental (implicitamente positivado)[210], embalando, logo depois, a promulgação da Emenda Constitucional nº 115, a fim de positivar formalmente a proteção de dados pessoais como um direito fundamental autônomo.

Para além desses aspectos, a avaliação da adequação do nível de proteção implicaria, conforme reafirmado pelo TJUE nos casos *Schrems I* e *Schrems II*, na vigência de uma legislação pertinente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais. É certo que a ausência de tal norma no ordenamento jurídico brasileiro enreda a adoção de uma decisão de adequação pela Comissão, entretanto, a regulamentação do assunto parece-me ser iminente.

A conversão dos Projetos de Lei nº 2630/2020 e 1515/2022 em leis revela-se fulcral não só em razão das aludidas jurisprudências europeias, que instigam o sistema jurídico brasileiro a adotar as medidas nelas veiculadas, mas também em razão da União Europeia ser um dos principais parceiros comerciais do Brasil. Quer-se dizer que obter formalmente o título de país terceiro adequado permitirá que as transferências de dados pessoais entre o Brasil e os Estados-Membros se realizem sem que sejam exigidas qualquer autorização

[210] STF, *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. op. cit*.

específica ou garantias suplementares (como ocorre atualmente), fomentando, portanto, essas relações comerciais.

Com a concretização de tal cenário, o Brasil estará em vias de inaugurar a "segunda onda" do direito à proteção de dados, o que o permitirá a ser formalmente reconhecido como um país terceiro que assegura aos titulares de dados um nível de proteção substancialmente equivalente ao garantido pela União.

REFERÊNCIAS BIBLIOGÁFICAS

ALMEIDA, Francisco Ferreira de. *Direito internacional público*, 2ª ed. Coimbra: Coimbra Editora, 2003.

ALMEIDA, Francisco António de M. L. Ferreira de. *Mutações sistémicas e normativas no direito internacional em face de novos desafios, in* Scientia Ivridica: Revista de Direito Comparado Português e Brasileiro, Vol. 326, 2011, p. 225-234.

ALONSO, Félix Ruiz. *Pessoa, intimidade e o direito à privacidade*. *In* MARTINS; Ives Gandra da Silva; PEREIRA, Antonio Jorge Jr. (coord.). Direito à Privacidade. São Paulo: Ideias & Letras e Centro de Extensão Universitária, 2005.

ANDRADE, Caio Delgado de. *Soberania, jurisdição e territorialidade: passado, presente e futuro, in* Revista de Direito Constitucional e Internacional, Vol. 117, Ano 28, p. 151-174. São Paulo: Editora RT, 2020.

ANDREA, Gianfranco F. M.; ARQUITE, Higor Roberto L.; CAMARGO, Juliana Moreira. *Proteção de dados pessoais como direito fundamental: a evolução da tecnologia da informação e a lei geral de proteção de dados no Brasil, in* Revista de Direito Constitucional e Internacional, Vol. 28, 2020, p. 115-139.

ANJOS, Lucas Costa dos; BRANDAO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teofilo Nunes; POLIDO, Fabrício B. Pasquot. *GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa, in* Instituto de Referência em Internet e Sociedade, 2018. Disponível em <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-Primeiras-impressões-de-análise-comparativa-PT.pdf>. Acesso em 20 de novembro de 2022.

ANTUNES, Laila D.; BIAZATTI, Bruno de O.; PORTO, Odélio; ROSA, Matheus; VILELA, Pedro. *Jurisdiction and conflicts of law in the digital age: regulatory framework of internet regulation, in* Instituto de Referência em Internet e Sociedade, 2017. Disponível em <https://irisbh.com.br/wp-content/uploads/2017/08/Jurisdiction-and-conflicts-of-law-in-the-digital-age-IRIS.pdf>. Acesso em 14 de abril de 2023.

ARAUJO, Alexandra Maria R. *As transferências transatlânticas de dados pessoais: o nível de proteção adequado depois de Schrems, in* Revista Direitos Humanos e Democracia, Vol. 9, 2017, p. 201-236.

BARROS, Tomás Soares da Silva. *Fundamento e alcance do princípio da jurisdição universal.* Dissertação de Mestrado em Ciências Jurídico-Políticas, Faculdade de Direito da Universidade de Coimbra, 2016. Disponível em <https://estudogeral.uc.pt/bitstream/10316/42011/1/Tomás%20Barros.pdf>. Acesso em 10 de dezembro de 2022.

BASTOS, Fernando Loureiro. *Algumas notas sobre globalização e extraterritorialidade. In* SOUSA, Marcelo Rebelo de; PINTO, Eduardo Vera-Cruz (coord.). Liber Amicorum Fausto de Quadros, Vol. I. Coimbra: Almedina, 2016, p. 437-453.

BESSA, Leonardo Roscoe. *A lei geral de proteção de dados e o direito à autodeterminação informativa.* Revista Consultor Jurídico, 26 de outubro de 2020. Disponível em

<https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa>. Acesso em 20 de março de 2023.

BESSON, Samantha. *Sovereignity.* Oxford Public International Law, Oxford University Press, 2011. Disponível em < https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL>. Acesso em 3 de novembro de 2022.

BRANDEIS, Louis D.; WARREN, Samuel D. *The right to privacy*, i*n* Harvard Law Review, Vol. 4, nº 5, 1890.

BRGRAVE, Lee. A; DOCKSEY, Christopher; KUNER, Cristopher. *The EU general data protection regulation (GDPR): a commentary*. Oxford University Press, 2020.

BU-PASHA, Shakila. *Cross-border issues under EU data protection law with regards to personal data protection, in* Information & Communications Technology Law, Vol. 26, 2017, p. 213-228. Disponível em <https://doi.org/10.1080/13600834.2017.1330740>. Acesso em 15 de novembro de 2022.

CDI. *Report on the Work of its Fifty-Eight Session*, 1 May-9 June and 3 July-11 August 2006, UN Doc. A/61/10, Annex E, nº 2. Disponível em <http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf>. Acesso em 10 de dezembro de 2022.

COLANGELO, Anthony J. *What is Extraterritorial Jurisdiction? In* Cornell Law Review, Vol. 99, Nº 6, 2014. Disponível em <https://ssrn.com/abstract=2363695>. Acesso em 25 de outubro de 2022.

COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS. Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância, adotadas em 10 de novembro de 2020. Disponível em <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_pt>. Acesso em 2 de maio de 2023.

CORDEIRO, A. Barreto Menezes. *Direito da proteção de dados à luz do RGPD e da Lei nº 58/2019.* Coimbra: Edições Almedina, 2020.

DINH, Nguyen; DAILLIER, Patrick; PELLET, Alain. *Direito Internacional Público*, 2ª ed. Lisboa: Fundação Calouste Gulbenkian, 2003.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* 3ª ed. São Paulo: Thompson Reuters Brasil, 2021.

DOUVILLE; Thibault. *Droit des données à la caractere personnel*, 1re édition, Gualino, 2020.

EHRHARDT, Marcos; PEIXOTO, Erick Lucena Campos. *Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias*, *in* Revista Jurídica Luso-Brasileira, Ano 6, nº 2, 2020, p. 389-418. Disponível em https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf. Acesso em 28 de fevereiro de 2022.

FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *A extraterritorialidade do regime geral de proteção de dados pessoais da União Europeia*. Tese de Doutoramento, Faculdade de Direito da Universidade Nova de Lisboa, 2019. Disponível em <http://hdl.handle.net/10362/89180>. Acesso em 10 de dezembro de 2022.

GATT, Lucilla. *European Journal of Privacy Law & Technologies*, G. Giappichelli Editore, 2020.

GRUPO DE TRABALHO DO ARTIGO 29º. *WP 254 rev. 01, Documento de referência relativo à adequação*, adotado em 28 de novembro de 2017. Disponível em <https://ec.europa.eu/newsroom/article29/items/614108/en>. Acesso em 2 de maio de 2023.

GUIMARAES, João Alexandre; MACHADO, Lécio. *Comentários à lei geral de proteção de dados: lei 13.709/2018 com alterações da MPV 869/2020*. Rio de Janeiro: Editora Lumen Juris, 2020.

HASSANI, Nadia. *Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations.* Terminal [En ligne], 124 | 2019, mis en ligne le 30 juin 2019. Disponível em <http://journals.openedition.org/terminal/4040>. Acesso em 20 de novembro de 2022.

IRAMINA, Aline. *RGPD V. LGPD: adoção estratégica da abordagem responsiva na elaboração da lei geral de proteção de dados do Brasil e do regulamento geral de proteção de dados na União Europeia*, *in* Revista de Direito, Estado e Telecomunicações, Vol. 12, nº 2, 2020.

KAMMINGA, Menno T. *Extraterritoriality, i*n R. Wolfrum Ed., The Max Planck Encyclopedia of Public International Law, Oxford University Press, 2020.

KELSEN, Hans. *As relações sistemáticas entre o direito interno e o direito internacional público, in* Revista de Direito Internacional, Vol. 10, n.3, 2013.

KETTEMANN, Matthias C. *The normative order of the internet: a theory of rule and regulation online*, online edn. Oxford Academic, 2020. Disponível em <https://doi.org/10.1093/oso/9780198865995.003.0006>. Acesso em 15 de fevereiro de 2023.

KLUWER, Wolters. *Cómo sobrevivir al GDPR: todo lo que necessitas saber sobre protección de datos,* 1ª edición. Madrid: Bosch, 2018.

KOHL, Uta. *Jurisdiction and the internet – regulatory competence over online activity, in* Cambridge University Press, 2007.

LEENES Ronald; BRAKEL van Rosamunde; GUTWIRTH Serge; DE HERT Paul. *Data protection and privacy: the internet of bodies*, Volume 11. London: Bloomsbury Publishing Plc, 2018. Disponível em ProQuest Ebook Central <https://ebookcentral.proquest.com/lib/pgrbr/detail.action?docID=5633106>. Acesso em 20 de junho de 2023.

LOPES, Dulce Margarida de Jesus. *Eficácia, reconhecimento e execução de actos administrativos estrangeiros.* Tese de Doutoramento, Faculdade de Direito da Universidade

de Coimbra, 2017. Disponível em <http://hdl.handle.net/10316/79669>. Acesso em 30 de outubro de 2022.

LOPES, Dulce. *Regulamento Geral de Protecção de dados: Uma leitura Internacional Privatista, in* Direito Internacional e Comparado: trajetória e perspectivas. Homenagem aos 70 anos do professor catedrático Rui Manoel Moura Ramos, Vol. I. São Paulo: Editora Quartier Latin do Brasil, 2021.

LYNSKEY, Orla. *The foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2016. Disponível em ProQuest Ebook Central <https://ebookcentral.proquest.com/lib/pgrbr/detail.action?docID=4310752>. Acesso em 20 de abril de 2023.

MAGALHAES, Filipa Matias; PEREIRA, Maria Leitão. *Regulamento Geral de Proteção de Dados: Manual Prático*, 3ª ed. Porto: Editora Vida Econômica, 2020.

PEDROSA, Clara Bonaparte. *Direito e Tecnologia: Discussões para o Século XXI.* Editora Deviant, 2020.

PETERS, Anne. *Humanity as the A and Ω of sovereignty*, *in* The European Journal of International Law, Vol. 20, nº 3, 2009, p. 513-544. Disponível em https://academic.oup.com/ejil/article/20/3/513/402328. Acesso em 20 de fevereiro de 2023.

PINHEIRO, Luis de Lima. *Direito internacional privado, Introdução e Direito de Conflitos, Parte Geral*, Vol. I, 2ª ed. Coimbra: Edições Almedina, 2008.

RANGEL, Vicente Marotta. *Jurisdição internacional: considerações preambulares, in* estudos em homenagem à professora Doutora Isabel de Magalhães Collaço, Vol. II. Almedina, p. 643-652, 2002.

RANGEL DE MESQUITA, Maria J. *A actuação externa da União Europeia depois do Tratado de Lisboa*. Almedina, 2011.

REUSING, Luciana; WACHOWICZ, Marcos. *Proteção de Dados Pessoais em Perspectiva: LGPD e RGPD na ótica do direito comparado*. Curitiba: Gedai, 2020.

RIBEIRO, Alanna C.B.M; BRITTO, Nara P.R. Ayres de. *Soft law e hard law como caminho para afirmação do direito à proteção de dados*, 2020. Disponível em <https://ayresbritto.adv.br/soft-law-e-hard-law-como-caminho-para-afirmacao-do-direito-a-protecao-de-dados/>. Acesso em 15 de fevereiro de 2023.

RYNGAERT, Cedric. *Jurisdiction in International Law*, 2ª ed. Oxford: Oxford University Press, 2015.

RYNGAERT, Cedric; TAYLOR, Mistale. *The GDPR as global data protection regulation*?, *in* Symposium on the GDPR and International Law, 2020. Disponível em <https://www.researchgate.net/publication/338406505_The_GDPR_as_Global_Data_Protection_Regulation>. Acesso em 20 de junho de 2023.

SANTOS, Sofia Berberan; GABRIEL, João. *Regulamento Geral sobre a Proteção de Dados.* Lisboa: Edição GPA Academy, 2020.

STAIGER, Dominic; WEBER, Rolf H. *Transatlantic data protection in practice.* Zurich: Springer-Verlag GmbH Germany, 2017.

SVANTESSON, Dan Jerker B. *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, in* Symposium Article, International Data Privacy Law, Vol. 5, Nº 4, 2015. Disponível em <https://doi.org/10.1093/idpl/ipv024>. Acesso em 5 de novembro de 2022.

TIBURCIO, Carmen. *The current practice of international co-operation in civil matters*, t. 393. Leiden: Recueil des cours, Leiden, 2018.

VAN CALSTER, Geert. *Sur de bases fragiles. Le RGPD et les règles de competénce concernant les infractions au droit au respect de la vie privée, in* L'Observateur de Bruxelles, 2018, p. 28-30. Disponível em <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias1995283&context=SearchWebhook&vid=32KUL_KUL:Lirias&lang=en&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,LIRIAS1995283&offset=0>. Acesso em 2 de junho de 2023.

ZALUCKI, K. *Extraterritorial Jurisdiction in International Law*, *in* International Community Law Review, Vol. 17(4-5), 2015, p. 403-412. Disponível em: https://doi.org/10.1163/18719732-12341312. Acesso em 2 de dezembro de 2022.

JURISPRUDÊNCIA

Acórdão do Tribunal de Justiça (Grande Secção) de 13 de maio de 2014, *Google Spain,* Processo C-131/12, EU:C:2014:317. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0131>. Acesso em 15 de fevereiro de 2023.

Acórdão do Tribunal de Justiça (Terceira Secção) de 1º de outubro de 2015, *Weltimmo v. Nemzeti*, Processo C-230/14, EU:C:2015:639. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0230>. Acesso em 15 de fevereiro de 2023.

Acórdão do Tribunal de Justiça (Grande Seção) de 6 de outubro de 2015, *Schrems e Data Protection Commissioner*, C-362/14, EU:C:2015:650. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362>. Acesso em 30 de março de 2023.

Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020, *Facebook Ireland e Schrems*, Processo C-311/18, EU:C:2020:559. Disponível em <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=440820>. Acesso em 30 de março de 2023.

Acórdão do Tribunal Constitucional nº 268/2022, de 3 de junho de 2022, Processo nº 828/2019, de Relatoria do Conselheiro Afonso Patrão. Disponível em

<https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html>. Acesso em 1º de abril de 2023.

Corte Permanente de Justiça Internacional. Acórdão de 7 de setembro de 1927, *The Case of the S.S. LOTUS*, série A, nº 10. Disponível em <https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf>. Acesso em 9 de novembro de 2022.

Supremo Tribunal Federal (Plenário). Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6387/Distrito Federal. Relator: Ministra Rosa Weber. 7 de maio de 2020. Disponível em <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em 2 de março de 2023.

ATOS NORMATIVOS E PROJETOS DE LEI

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 20 de novembro de 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 30 de março de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 10 de janeiro de 2023.

BRASIL, Câmara dos Deputados. Projeto de Lei 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983>. Acesso em 03 de abril de 2023.

BRASIL, Câmara dos Deputados. Projeto de Lei 1515/2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274>. Acesso em 03 de abril de 2023.

COMISSAO EUROPEIA. Decisão de Execução (UE) 2019/419 da Comissão, de 23 de janeiro de 2019, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Japão no âmbito da Lei relativa à proteção de informações pessoais. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32019D0419>. Acesso em 27 de junho de 2023.

COMISSAO EUROPEIA. Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32021D0914>. Acesso em 10 de março de 2023.

CONSELHO DA EUROPA. Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, para a proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais. Disponível em <https://rm.coe.int/1680078b37>. Acesso em 24 de fevereiro de 2023.

PARLAMENTO EUROPEU E CONSELHO. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial da União Europeia, L 281. Disponível em <https://edps.europa.eu/sites/default/files/publication/dir_1995_46_pt.pdf>. Acesso em 2 de março de 2023.

PARLAMENTO EUROPEU E CONSELHO. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga da Diretiva 95/46/CE (Regulamento Geral sobra a Proteção de Dados), Jornal Oficial da União Europeia, L 119. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 30 de outubro de 2022.