AMANDA CUNHA E MELLO SMITH MARTINS

Privacidade, proteção de dados e danos transnacionais: aspectos do Direito Internacional Privado brasileiro

Dissertação de Mestrado

Orientador: Professor Titular Doutor Gustavo Ferraz de Campos Monaco

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo – SP

2020

AMANDA CUNHA E MELLO SMITH MARTINS

Privacidade, proteção de dados e danos transnacionais: aspectos do Direito Internacional Privado brasileiro

Dissertação de Mestrado apresentada à Banca do Programa de Pós-Graduação *stricto sensu* em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de mestre em Direito, na área de concentração de Direito Internacional e Comparado, sob a orientação do Prof. Titular Doutor Gustavo Ferraz de Campos Monaco.

UNIVERSIDADE DE SÃO PAULO

FACULDADE DE DIREITO

São Paulo – SP

2020

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Smith Martins, Amanda Cunha e Mello
Privacidade, proteção de dados e danos transnacionais: aspectos do Direito Internacional Privado brasileiro / Martins, Amanda Cunha e Mello Smith; orientador Prof. Titular Gustavo Ferraz de Campos Monaco -- São Paulo, 2020.
262p.

Dissertação (Mestrado – Programa de Pós-Graduação em Direito Internacional e Comparado) – Faculdade de Direito, Universidade de São Paulo, 2020.

1. Privacidade. 2. Proteção de dados. 3. Dados plurilocalizados. 4. Danos transnacionais. 5. Direito Internacional Privado. I. Monaco, Prof. Dr. Gustavo Ferraz de Campos, orient. II. Título.

A Banca Examinadora, abaixo assinada, aprova a Dissertação

Privacidade, proteção de dados e danos transnacionais: aspectos do Direito Internacional Privado brasileiro

elaborada por

AMANDA CUNHA E MELLO SMITH MARTINS

como requisito parcial para a obtenção do grau de

MESTRE EM DIREITO INTERNACIONAL E COMPARADO

BANCA EXAMINADORA:

_____

Dr. Gustavo Ferraz de Campos Moraco – USP (Orientador)

_____

Dra. Juliana Abrusio – Mackenzie

_____

Dr. Juliano Souza de Albuquerque Maranhão – USP

_____

Dra. Marilda Rosado de Sá Ribeiro – UERJ

À minha família, pelo exemplo e incentivo,
especialmente aos meus avós professores,
Maria Lucia e *Rubens Murillo*.

Ao *Dr. Arnoldo Wald Filho*, pelas oportunidades e
experiências proporcionadas.

Ao *André*, pelo apoio incondicional, e por todos os
cafés compartilhados.

AGRADECIMENTOS

Este estudo não teria sido possível sem a valiosa contribuição do meu orientador, Prof. Dr. Gustavo Ferraz de Campos Monaco, e dos meus colegas acadêmicos. Foi um privilégio – sem exageros – poder contar, ao longo dos últimos nos, com tal exemplo de dedicação e comprometimento com a academia. Assim como foi um prazer acompanhar a trajetória acadêmica do professor Gustavo na última década, e vê-lo chegar, recentemente, à titularidade do Departamento de Direito Internacional da Faculdade.

De fato, o resultado desta dissertação dificilmente teria sido o mesmo sem os diversos comentários e a efetiva orientação do professor Gustavo, cujos conhecimentos e afeição pela área do Direito Internacional Privado foram verdadeira inspiração para o estudo do tema. Agradeço imensamente pelas horas dedicadas à leitura e apontamentos nas versões preliminares do texto.

Igualmente valiosa a contribuição dos meus colegas orientandos, sempre abertos a discussões e dispostos a ler e comentar os textos uns dos outros, resultando em uma produção muito mais rica e interdisciplinar. Agradeço a todos os orientandos do professor Gustavo pela solidariedade e empatia, e por terem se revelado mais do que colegas de academia, mas verdadeiros amigos. E ao nosso orientador, por ter possibilitado a reunião de um grupo tão querido.

Assim, não posso deixar de citar alguns desses colegas que se fizeram especialmente presentes na minha trajetória de mestranda: Marina Rocha, Analluza Bolivar Dallari, André Braga, Nadja Nogueira, Kim Diz e José Luiz Souza. Agradecimento especial a Raquel Santoro, pessoa que tenho como exemplo e referência não apenas na academia, mas também como advogada e profissional brilhante. E, também, alguns dos meus colegas de graduação que se fizeram presentes de diversas formas ao longo do trabalho: Antonio Cury, Carlos Liguori e André Moricochi.

Por fim, e não menos importante, agradeço ao Solano de Camargo, a quem tenho o privilégio de considerar como um irmão acadêmico, muito embora meus conhecimentos ainda estejam aquém dos dele. Precisamente por tal razão, suas ideias e contribuições foram indispensáveis durante todo o percurso deste trabalho, especialmente pelas discussões e debates que levaram à escolha do tema, e pela sinceridade nos comentários e críticas, sempre objetivos e produtivos.

"Todos tienen tres vidas: una vida pública, una vida privada y una vida secreta."

(Gabriel García Márquez,
Gabriel García Márquez: una vida).

SMITH MARTINS, Amanda Cunha e Mello. *Privacidade, proteção de dados e danos transnacionais:* aspectos do Direito Internacional Privado brasileiro. 262 p. Dissertação (Mestrado em Direito) – Departamento de Direito Internacional Comparado da Faculdade de Direito, Universidade de São Paulo – USP. São Paulo, 2020.

RESUMO

Esta dissertação propõe uma análise da privacidade e da proteção de dados, especificamente sob o âmbito do Direito Internacional Privado. Assim, são abordados temas relevantes no contexto da Sociedade da Informação, os quais permitem avaliar a forma como conceitos e critérios de conexão tradicionalmente utilizados podem ser aplicados em conflitos que envolvem a Internet. Diante do caráter deslocalizado do meio digital, há a ressignificação das fronteiras e da soberania, suscitando novos desafios em termos de conflitos de qualificação, jurisdição internacional, lei aplicável e reconhecimento de sentenças estrangeiras. O objetivo principal do estudo é fornecer ferramentas adequadas para a solução de conflitos que envolvem dados plurilocalizados e danos transnacionais.

Palavras-chave: Privacidade. Proteção de dados. Dados plurilocalizados. Danos transnacionais. Direito Internacional Privado.

SMITH MARTINS, Amanda Cunha e Mello. Title: *Privacy, data protection and transnational damages:* aspects of Brazilian Private International Law. 262 p. Dissertation (Master in Law) – Department of Comparative International Law, Faculty of Law, University of São Paulo – USP. São Paulo, 2020.

ABSTRACT

The dissertation aims to analyze privacy and data protection specifically under the scope of Private International Law. Therefore, it addresses relevant subject-matters in the context of an information society, in order to evaluate how traditional definitions and connecting factors can be applied in disputes involving the internet. Given the delocalized character of the digital environment, a redefinition of borders and State sovereignty takes place, raising new challenges regarding conflicts of qualification, international jurisdiction, applicable law and recognition of foreign awards. The main objective is to provide adequate tools for the resolution of disputes involving pluri-localized data and transnational damages.

Key words: Privacy. Data protection. Pluri-localized data. Transnational damages. International Private Law.

LISTA DE SIGLAS

AGU	Advocacia Geral de União
ANPD	Autoridade Nacional de Proteção de Dados Brasileira
BITNET	*Because It's Time to NETwork*
CCPA	*California Consumer Privacy Act*
CCTCI	Comissão de Ciência e Tecnologia, Comunicação e Informática
CDC	Código de Defesa do Consumidor
CIDIP	Convenção Interamericana sobre normas gerais de Direito Internacional
CJF	Conselho da Justiça Federal
CNIL	Comissão Nacional de Informações e Liberdade
COAF	Conselho de Controle de Atividades Financeiras
COAF	Conselho de Controle de Atividades Financeiras
CPC	Código de Processo Civil
DFFT	*Data Free Flow with Trust*"
DL	*Deep Learning*
DL	*Deep Learning*
DPO	*Data Protection Officer*
ECA	Estatuto da Criança e do Adolescente
ECPA	Lei de Privacidade de Comunicação Eletrônica
EEA	European Economic Area
EEE	Espaço Econômico Europeu
ETA	*Electronic Transaction Act*
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
FCA	Financial Conduct Authority
FCA	*Financial Conduct Authority*
FMCNA	Fresenius Medical Care North America
GPDR	Regulamento Geral sobre a Proteção de Dados
HIPAA	*Health Insurance Portability and Accountability Act*
IA	Inteligência Artificial
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
ICO	*Initial Coin Offerings*
IDEC	Instituto Brasileiro de Defesa do Consumidor
IGA	Acordo de Cooperação Intergovernamental
IP	*Internet Protocol*

IRIS	Instituto de Referência em Internet e Sociedade
IUJ	Incidente de Uniformização de Jurisprudência
LGPD	Lei Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
LIL	Lei de Informática e Liberdades
LINDB	Lei de Introdução às Normas do Direito Brasileiro
LINDB	Lei de Introdução às Normas do Direito Brasileiro
LNCC	Laboratório Nacional de Computação Científica
LRD	Lei para uma República Digital
LRD	Lei para uma República Digital
MCI	Marco Civil da Internet
MCI	Marco Civil da Internet
MCT	Ministério da Ciência e Tecnologia
MINICOM	Ministério das Comunicações
ML	*Machine Learning*
ML	*Machine Learning*
MPDFT	Ministério Público do Distrito Federal e Territórios
NSA	Agência de Segurança Nacional Norte-Americana
OCDE	Organização de Cooperação e Desenvolvimento Econômico
ODR	*Online Dispute Resolution* Privado
PROPIA	*Protection of Personal Information Act*
RGPD	Regulamento Geral de Proteção de Dados
RGPD	Regulamento Geral de Proteção de Dados da União Europeia
RISTJ	Regimento Interno do Superior Tribunal de Justiça
SAP	Sistema de Automação Processual
SAPIENS	Sistema de Apoio à Procuradoria Inteligente
SICAU	Sistema Integrado de Controle das Ações da União
TJUE	Tribunal de Justiça da União Europeia
TJUE	Tribunal de Justiça da União Europeia
UIF	Unidade de Inteligência Financeira
UIF	Unidade de Inteligência Financeira
UNICAMP	Universidade de Campinas
USP	Universidade de São Paulo

SUMÁRIO

INTRODUÇÃO

Muita coisa mudou desde setembro de 1988 quando a Internet chegou no Brasil. Se hoje as pessoas podem se conectar em tempo real, utilizar a Inteligência Artificial para otimizar processos e contar com a tecnologia no cotidiano de suas residências e empresas, isto só foi possível a partir da utilização acadêmica do recurso[1].

A recente aprovação de legislações específicas sobre a proteção de dados, tais como a Lei Geral de Proteção de Dados (LGPD)[2], traduz a importância e a valorização crescentes dos dados. As relações sociais sofreram mudanças significativas nas últimas décadas, de modo que a informação passou a condicioná-las, transformando-as não apenas em bens de consumo, mas, também, em fator de produção e instrumento de poder[3].

Atualmente, a rede mundial de computadores permite a comunicação entre todas as partes do mundo. Em 1988, contudo, quando a Internet começou a ser utilizada no Brasil, o seu alcance era limitado a algumas universidades, e as primeiras conexões foram feitas exclusivamente em ambiente acadêmico.

A primeira conexão no país foi realizada pelo Laboratório Nacional de Computação Científica (LNCC), localizado no Rio de Janeiro. O Laboratório conectou-se à Universidade de Maryland por meio do acesso à Bitnet. A expressão é um acrônimo de

---

[1] OLIVEIRA, Elsa Dias. *A protecção dos consumidores nos contratos celebrados através da internet*. Coimbra: Almedina, 2002, pp. 13-14. "A Internet, definida frequentemente como 'a rede das redes' (*network of networks*), e que encontra sua tímida gênese ainda nos anos sessenta, conheceu, na última década, um período de franca expansão. As primeiras experiências neste campo começaram a ser feitas a partir de uma agência militar norte-americana de tecnologia informática – ARPA (*Advanced Research Project Agency*), que adotou um protocolo, denominado de TCP/IP (*Transmission Control Protocol/Internet Protocol*), que permitia a qualquer tipo de computador interligar-se à rede. Este protocolo assegurava uma equivalência entre todos os pontos, sem um comando central, e ainda hoje é esse mesmo protocolo que permite que as diversas redes existentes se comuniquem entre si. Posteriormente, a tecnologia ARPANET foi usada para conectar universidades e laboratórios, e foi apenas em 1987 que o uso comercial, da já então Internet, foi liberado. Mas só nos princípios da década de noventa se verificou uma divulgação e expansão maciças do fenômeno Internet."

[2] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 abr. 2020.

[3] COSTA, José Augusto Fontoura; SOLA, Fernanda. Desenvolvimento e direito de autor na sociedade da informação. *Revista de Direito Econômico e Socioambiental*. Curitiba, jul./dez. 2010, v. 1, n. 2, pp. 285-301, p. 297. "[...] importa ressaltar que, na chamada economia de informação, há tanto uma redefinição dos bens econômicos centrais como dos processos produtivos. Os produtos de maior valor agregado deixaram de ser os bens móveis industrializados, como automóveis e eletrodomésticos, para ser bens incorpóreos, como programas de computador, filmes e gravações musicais. Os processos de produção, por seu turno, deixam de ser aqueles desenvolvidos nas linhas de montagem das fábricas, que concentram em um único local as máquinas necessárias, pois na medida em que os bens se desmaterializam o foco passa a ser no projeto e, portanto, em estruturas menos hierarquizadas e rígidas de processo produtivo, com a consequente deslocalização do ambiente, já que as estações de trabalho já não precisam ser dispostas em linha ou concentradas no mesmo endereço."

"*Because It's Time to NETwork"* ou "*Because It's There NETwork"*, rede remota criada em 1981, numa conexão entre as Universidades da Cidade de Nova York e a de Yale[4].

Em pouco tempo outras instituições brasileiras passaram a ter acesso à Bitnet, como a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), a Universidade de São Paulo (USP) e a Universidade de Campinas (Unicamp). Até 1994, as conexões se mantinham limitadas à academia e, depois disso, a empresa Embratel iniciou seus serviços de acesso à Internet em caráter experimental[5]. No ano seguinte, o acesso à Internet começou a funcionar de modo definitivo no Brasil e, desde então, vem se expandindo[6].

Em 2017, a Internet já era utilizada em 74,9% dos domicílios brasileiros, embora dentre aqueles localizados em área rural o percentual de indisponibilidade do serviço ainda fosse de 21,3%, segundo dados do IBGE[7]. Isto representa uma infinidade de dados coletados diariamente, além de troca de mensagens, realização de transações bancárias, compras no cartão de crédito ou acesso a quaisquer páginas[8].

---

[4] CARVALHO, Marcelo Sávio Revoredo Menezes de. *A trajetória da Internet no Brasil:* do surgimento das redes de computadores à instituição dos mecanismos de governança. 239 p. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro. Rio de Janeiro: COPPE, 2006, p. 84. "O acesso à BITNET em setembro de 1988 foi uma vitória para o LNCC e para a comunidade acadêmica como um todo, ainda que não fosse possível a implementação do tão esperado *gateway* internacional no Brasil. A mesma reunião que liberou o acesso à BITNET também concluiu que a Embratel e o LARC envidariam esforços no sentido de uma solução que atendesse à necessidade de comunicação da comunidade acadêmica com as redes no exterior de forma otimizada. O fato é que esta decisão acabou reforçando os interesses de outras instituições que buscavam suas próprias conexões internacionais. A FAPESP iniciou, no segundo semestre de 1988, um projeto para atender a demanda por acesso à BITNET manifestada entre os pesquisadores de algumas instituições de ensino desde o início do ano anterior."

[5] Id., ibid., p. 123. "Em alguns países, especialmente nos Estados Unidos, surgiam indicadores da extensão do uso da Internet pela comunidade não acadêmica, assim como as primeiras ofertas comerciais dos serviços de provimento de acesso. [...] foi apenas uma questão de tempo (e oportunidade) para que acontecesse a abertura comercial da Internet e o Alternex deixasse de ser o único provedor de acesso no Brasil (como vinha sendo até 1995)."

[6] O Governo Federal brasileiro editou em maio de 1995, Nota Conjunta do Ministério das Comunicações (Minicom) e Ministério da Ciência e Tecnologia (MCT), a qual definiu pela primeira vez o conceito de internet no país: "[...] A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a bases de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da Sociedade."

[7] IBGE. Instituto Brasileiro de Geografia e Estatística. Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento. *Pesquisa Nacional por Amostra de Domicílios Contínua* (PNAD Contínua), 2017.

[8] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. *Governança global da internet, conflito de leis e jurisdição*. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), 2018, pp. 54-55. "Em 2016, mais de 3 bilhões de pessoas, isto é, quase metade da população mundial, já possuem acesso à internet, que se tornou um mecanismo indispensável na vida cotidiana. Com o rápido desenvolvimento em poucas décadas, as conexões *online* continuam a aumentar conforme mais pessoas são integradas às tecnologias 2G/3G/4G[/5G] e banda larga, que integram suas vidas pessoais e profissionais. A tecnologia transpõe-se também para as relações jurídicas em escala transnacional. Observa-se um aumento de litígios transfronteiriços envolvendo a Internet e de novos desafios ao Direito, em especial ao Direito Internacional Privado, área dedicada a questões relativas à determinação da lei aplicável, jurisdição e reconhecimento e execução de sentenças estrangeiras. Em uma realidade interconectada, esses desafios não podem ser ignorados. [...] A Internet se revela como plataforma de transações não delimitadas

Conforme crescia o acesso à Internet, também aumentava exponencialmente o volume de dados coletados, permitindo a criação de extensos bancos de dados e metadados, que eram utilizados nas mais diversas finalidades[9]. Metadados são, de forma objetiva, dados sobre outros dados, como localização, data e hora de envio de mensagens e ligações ou informações sobre o aparelho utilizado (como uma câmera fotográfica)[10].

Cada acesso a *websites* gera uma quantidade de dados e de informações e, a partir do momento em que tais dados são enviados, torna-se difícil prever com precisão para onde são enviados ou armazenados, ou qual tratamento lhes é conferido. Trata-se de um ambiente demasiado fluido, no qual as fronteiras assumem caráter virtual.

Assim, a Internet revelou-se um poderoso instrumento de coleta de informações sobre seus usuários, possibilitando a criação de ferramentas que utilizam essas informações para, por exemplo, identificar preferências de compra para publicidade direcionada, reconhecer expressões faciais e criar novos produtos.

É inquestionável a quantidade de benefícios trazida pela democratização do acesso à Internet, ou seja: rápida e barata troca de mensagens e documentos; acesso a informações e notícias em tempo real; e disponibilização dos mais diversos tipos de produtos e serviços. Em outras palavras, a Internet tem permitido a democratização da informação e do conhecimento, bem como ampliado o acesso da população a bens e serviços.

Acervos de museus, teses e dissertações, documentos históricos, discografias completas e inúmeros tipos de arquivos e informações passaram a ser acessíveis *on-line*, muitas vezes gratuitamente. Por outro lado, é preciso mencionar que o advento da Internet também representa novos riscos, como, por exemplo, a utilização irresponsável de dados; a

---

pelas fronteiras estatais. A junção desses temas está ainda em franco desenvolvimento e encontra escasso suporte na literatura, mas é notável que os estudos sobre o "devido processo transnacional" são essenciais ao avanço dos estudos jurídicos sobre a internet."

[9] LYON, David. Surveillance in Cyberspace: the Internet, Personal Data and Social Control. *Queen's Quarterly*, 2002, n.º 109, pp. 345-357, p. 345. "Cada vez que você faz login na Internet, você se envolve em uma troca de informações muito mais ampla do que a maior parte das pessoas imagina. Utilizando as últimas tecnologias de vigilância, alguém pode rastrear cada clique do seu mouse, websites de pesquisa online que você visitou, e até ler as suas mensagens de e-mail e vasculhar seus registros financeiros e correspondência legal. E o novo século irá assistir ao desenvolvimento de ainda mais tecnologias oniscientes. Para a Internet, você é um livro aberto". (Tradução livre). "*Each time you log on to the Internet you are involved in a much broader information exchange than most people realize. Using the latest surveillance technology, someone else can track each click of your mouse, survey each web site you have visited, even read your e-mail messages and rifle through your financial records and legal correspondence. And the new century will see even more omniscient technology developed. As far as the Internet is concerned, you are an open book*."

[10] Outros exemplos de coleta de informações e metadados por serviços *online* são: localização, número de I.P., nome, páginas visitadas, buscas realizadas, resultados de buscas, duração, horário e números de telefone de ligações, assinaturas de serviços, número e tamanho de arquivos anexos a mensagens. Assim, por exemplo, a partir de um único dado, como uma imagem, é possível obter acesso aos metadados relacionados: informações sobre o aparelho ou câmera que tirou a foto, data e hora do registro, local onde a foto foi tirada, dentre outros (Id., ibid.).

difusão de conteúdos ilegais, como pornografia infantil; a facilidade de acesso a produtos ilícitos por meio da *Deep Web* e a aplicativos e serviços maliciosos[11].

Como consequência, houve o surgimento de novos problemas e questionamentos, especialmente quanto à publicidade digital e à proteção de dados, tanto no setor público como na área da saúde, investigações criminais, privacidade e direito do consumidor[12]. A rede mundial de computadores é caracteristicamente descentralizada, representando um desafio aos conceitos tradicionais de fronteira e de soberania estatal[13]. O cometimento de delitos ou ilícitos e a ocorrência de danos não estão mais restritos a um território específico, passando a ter caráter transnacional[14].

No contexto atual da Sociedade da Informação[15], a Internet é uma ferramenta não apenas de acesso à informação, mas, também, de controle e de coleta de dados[16]. No

---

[11] MONACO, Gustavo Ferraz de Campos. Uso indevido de imagem de crianças e o papel da escola básica. *JOTA*. Publicado em 09 fev. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-indevido-de-imagem-de-criancas-e-o-papel-da-escola-basica-09022018. Acesso em: 17 abr. 2020. "O uso de imagens de pessoas é, em si mesmo, um problema do nosso *tempo líquido*, para falar com Zygmunt Bauman. Obriga-nos a adotar uma série de comportamentos que visam resguardar a pouca privacidade que ainda nos resta a nós, pobres mortais. Há, é óbvio, os que não se importarão com essa perda de privacidade (vide *reality shows* tão em voga no mundo do entretenimento televisivo). A esses, sempre sobrará a porta da autorização expressa para o uso de suas próprias imagens ou de seus filhos menores."

[12] MARQUES, Cláudia Lima. A insuficiente proteção do consumidor nas normas de direito internacional privado – da necessidade de uma convenção interamericana (CIDIP) sobre a lei aplicável a contratos e relações de consumo. *Revista dos Tribunais*, 2001, v. 788, pp. 11-56. Transações comerciais são realizadas diariamente, nas quais, por exemplo, comprador, vendedor, fabricante e fornecedor encontram-se cada um em território de um Estado distinto. Da mesma forma, websites específicos promovem contato entre pessoas residentes em países diferentes, as quais podem posteriormente desejar contrair matrimônio ou praticar outros atos jurídicos em relação aos quais deverão ser determinadas a jurisdição e a lei aplicável.

[13] JAYME, Erik. O direito internacional privado do novo milênio: a proteção da pessoa humana face à globalização. *Cadernos do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul – PPGDir/UFRGS*. Porto Alegre, mar. 2003, v. 1, n. 1, pp. 136-146, p. 134. Nas palavras do autor, "qualquer um pode facilmente se libertar das amarras de sua existência limitada: velocidade, ubiquidade, liberdade; o espaço, para a comunicação, não existe mais."

[14] LESSIG, Lawrence. Internet: the architecture of privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1999, v. 1, pp. 56-101, (s.p.): "Nós estamos entrando em uma era na qual a privacidade em qualquer dos seus aspectos será fundamentalmente alterada – uma era na qual a extensão do monitorável, e o alcance do buscável, são muito maiores do que qualquer coisa que conhecemos até o momento." (Tradução livre). "*We are entering an age when privacy in any sense of that term will be fundamentally altered – an age when the extent of the monitored, and the reach of the searchable, is far greater than anything we have known thus far*."

[15] COSTA, José Augusto Fontoura; SOLA, Fernanda. Op. cit., jul./dez. 2010, p. 296. Cumpre destacar a seguinte distinção, com a qual concordamos: "O que se denomina sociedade de informação também recebe, com algumas alterações, o nome de sociedade informacional, economia do conhecimento, sociedade pós-industrial, sociedade pós-moderna e sociedade em rede, entre outros nomes. Preferiu-se manter a expressão 'sociedade de informação' por ser esta a mais comumente utilizada."

[16] BASILIEN-GAINCHE, Marie-Laure. Les frontières européennes – Quand le migrant incarne la limite. *Revue de l'Union Européene,* jun./2017, n.º 609, p. 5. "A tecnologização do controle das fronteiras e da gestão dos estrangeiros parece adaptada às exigências da identificação, da vigilância e do afastamento em um contexto complexificado pelos fenômenos de globalização dos fluxos e dos riscos." (Tradução livre). "*La technologisation du contrôle des frontières et de la gestion des étrangers a paru adaptée aux exigences de l'identification, de la surveillance, et de l'éloignement dans un contexte complexifié par les phénomènes de globalisation des flux et des risques*."

momento em que se destacam iniciativas legislativas que visam garantir a tutela de princípios e direitos básicos no ambiente *online*, a questão da privacidade dos dados pessoais tornou-se incontornável, inexistindo espaço para a circulação de dados e informações sem precauções ou restrições.

De fato, episódios recentes colocaram em evidência a necessidade de adaptação: a partir das revelações feitas por Edward Snowden acerca do tratamento de dados ilícitos por parte do serviço secreto dos Estados Unidos, outros casos nos quais dados foram mal utilizados, ou utilizados de forma maliciosa, passaram a ser descortinados[17].

Restou claro, portanto, desde a eleição de Donald Trump para a presidência dos Estados Unidos, sob acusação de manipular eleitores por meio de dados e postagens da rede Facebook[18], até os casos de vazamento de dados de clientes, como da empresa Netshoes, a necessidade de estabelecer regras para o ambiente *online*.

---

[17] LAFER, Celso. Vazamentos, sigilo, diplomacia: a propósito do significado do WikiLeaks. *Revista Política Externa*, mar./abr./maio 2011, v. 19, n.º 4, p. 12. Conforme aponta Celso Lafer, ao analisar o vazamento de informações e documentos pelo *Wikileaks*, a revolução digital ampliou de forma inédita a escala do armazenamento de informações e documentos, bem como a ubiquidade do potencial de sua divulgação pela Internet, de modo que uma das consequências de tal fenômeno seria a "crescente dificuldade de opor resistência ao devassamento da vida privada, de preservar o sigilo de dados bancários e fiscais, da correspondência proveniente de e-mails, de manter o segredo profissional e o sigilo das comunicações diplomáticas."

[18] ISAAK, Jim; HANNA, Mina J. User Data Privacy: Facebook, Cambridge Analytica and Privacy Protection. *Computer*, 2018, v. 51, n. 8, pp. 56-59, p. 57. Sobre a cessão de dados pessoais a terceiros e as possíveis implicações da utilização de tais dados, cumpre mencionar o episódio envolvendo o Facebook e a empresa *Cambridge Analytica*, o qual resultou em investigações e depoimentos tanto no âmbito do Congresso dos E.U.A. quanto do Parlamento da U.E.: "Em 2013, pesquisadores do Centro de Psicometria da Universidade de Cambridge analizou o resultado de voluntários que se submeteram a um teste de personalidade no Facebook para avaliar o seu perfil psicológico 'OCEAN' – abertura [*openness*], consciência [*conscientiousness*], extroversão [*extraversion*], concordabilidade [*agreeableness*] e neuroticismo [*neuroticism*]) e correlacionar com suas atividades no Facebook (curtidas e compartilhamentos). […] O quiz requeria a permissão do usuário para acesso do GSR ao seu perfil do Facebook, o qual garantia o acesso aos 'amigos' do usuário por meio do Facebook Open API até maio de 2015. […] Cambridge Analytica percebeu que poderia integrar estas informações com uma série de dados de plataformas digitais, navegadores, compras *online*, resultados de votações, e outros, para construir 'mais de 5000 pontos de dados sobre 230 milhões de adultos norte-americanos'. Acrescentando a análise OCEAN aos demais dados públicos e privados adquiridos, a Cambridge Analytica desenvolveu a habilidade de determinar 'micro-alvos' de consumidores ou eleitores para o envio de mensagens pelo 'Projeto Alamo', o qual foi utilizado na campanha eleitoral de Donald Trump. Algumas dessas mensagens eram criadas para a campanha de Trump, enquanto outras simplesmente destacavam 'notícias' disponíveis na Internet (as quais poderiam incluir conteúdo patrocinado pelo governo russo para interferer nas eleições norte-americanas). […] Estes fatores sugerem que mudanças nas políticas tanto no nível corporativo quanto no nível legislativo são necessárias para garantir que os dados dos consumidores e eleitores norte-americanos sejam protegidos, que eles sejam notificados sobre a afiliação daqueles que buscam influenciá-los, e que eles tenham a oportunidade de participar, na condição de consumidores e cidadãos informados." (Tradução livre). "*In 2013, researchers at the University of Cambridge's Psychometrics Centre analyzed the results of volunteers who took a personality test on Facebook to evaluate their "OCEAN" psychological profile (openness, conscientiousness, extraversion, agreeableness, and neuroticism) and correlated it with their Facebook activity (likes and shares). [...]. The quiz required users to grant GSR access to their Facebook profile, which granted access to users' friends' data through the Facebook Open API until May 2015. [...]. Cambridge Analytica realized they could integrate this information with a range of data from social media platforms, browsers, online purchases, voting results, and more to build "5,000+ data points on 230 million US adults." By adding OCEAN*

Tais regras se referem não apenas a princípios, direitos e garantias fundamentais, mas, também, à responsabilidade no tratamento de dados, seja pelo setor público ou privado, reconhecendo o caráter muitas vezes transnacional das relações estabelecidas[19].

Conforme percebido por Dário Moura Vicente, "graças às redes de comunicações electrônicas, a exploração de muitos bens intelectuais passou a fazer-se à escala universal; e tornou-se bastante frequente a ocorrência de violações de direitos sobre esses bens simultaneamente em mais do que um país"[20] – e é nesse ponto que reside o elemento estrangeiro ou de estraneidade que traz relevância ao Direito Internacional Privado[21].

Havendo um ou mais elementos estrangeiros envolvidos em determinado conflito, surgem discussões sobre o tribunal competente para julgar casos transnacionais, assim como sobre a lei a ser aplicada e seu respectivo país de origem. Se a vítima de um dano ou violação de direitos deseja demandar o responsável, deverá saber em qual tribunal nacional ajuizar a respectiva ação, enquanto a parte demandada deverá conhecer a lei que lhe é aplicável a fim de se defender.

---

analysis to the other private and public data acquired, Cambridge Analytica developed the ability to "micro-target" individual consumers or voters with messages most likely to influence their behavior. The OCEAN analysis was paired with a large number of targeted messages in "Project Alamo," which was employed for the election campaign of President Trump. Some of these messages were created for the Trump campaign, and some simply leveraged "news" available on the Internet (which might have included content funded through the Russian campaign to disrupt the US elections). [...] These factors suggest that changes in policies at both corporate and legislative levels are needed to ensure that consumers and voters' personal data is protected, that they are notified of the affiliation of those seeking to influence them, and that they have the best opportunity to participate as informed citizens and consumers."

[19] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 56. "Um provedor de aplicação, como uma rede de relacionamento social, pode ter sua sede ou estabelecimento comercial na Califórnia, armazenar arquivos em *data centers* na Finlândia e contar com uma base de usuários em todo o mundo. Todavia, caso um usuário brasileiro, por exemplo, sinta-se prejudicado por atos praticados ou ocorridos dentro dessa rede social, poderá ele recorrer aos tribunais de seu país para ajuizar uma ação de reparação de danos? Terá que recorrer ao poder judiciário do país onde está sediada a empresa provedora/ofertante da aplicação da rede social? Ou, ainda, aos tribunais do país em que estão os *data centers*? Definir a jurisdição competente para resolver litígios na Internet representa um dos principais desafios para estudiosos de uma área de interface entre o Direito Internacional Privado e o Direito de Internet. A tradição jurídica para delimitação de regras de jurisdição – como componente do Direito Processual Internacional – tem marcado conexão geográfica. A jurisdição continua sendo, afinal, um aspecto central da soberania do Estado, pois ela consiste no exercício do poder de modificar, criar ou extinguir relações e obrigações jurídicas entre as pessoas que de alguma forma se encontram sujeitas a esse Estado. Com o advento da Internet, dúvidas surgiram se essas características clássicas da jurisdição estatal podem ser conciliadas com as peculiaridades do espaço digital. Para decidir em qual país e em qual tribunal julgar determinado caso, atenta-se para fatores determinados pela localização física do autor, do réu, dos bens, da prestação do serviço etc."

[20] MOURA VICENTE, Dário Manuel Lentz de. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, p. 19.

[21] Quanto a tal aspecto, cumpre destacar observação feita pelo orientador professor doutor Gustavo Ferraz de Campos Monaco em sede de revisão deste estudo, no sentido de que a *lex loci delicti commissi* parece anacrônica em tais casos. Isto porque, enquanto por um lado garante uma unicidade do tratamento normativo (o ilícito foi cometido em um local determinado), por outro ignora a deslocalização dos danos potenciais, desnaturando a responsabilidade civil ao conferir papel secundário ao nexo de causalidade. Isto posto, abre-se espaço para o fracionamento, ou *dépeçage*.

Os critérios de conexão tradicionalmente utilizados, ou seja, os quesitos que geralmente determinam a relação existente entre o caso, o tribunal competente e a lei aplicável, são caracterizados pela sua localização – em contraposição ao caráter descentralizado e deslocalizado da Internet no contexto da Sociedade da Informação[22].

Se, por um lado, a rede mundial de computadores permite o acesso fácil e rápido a uma quantidade imensurável de informações circulando livremente[23], por outro, ela é caracteristicamente descentralizada[24], e representa um desafio aos conceitos tradicionais de fronteira e de soberania estatal, oferecendo novas questões em termos de lei aplicável e tribunal competente para a análise da questão plurilocalizada:

> As relações jurídicas respeitantes à produção, utilização e transmissão de informação através de redes electrônicas de comunicação não se eximem, pois, à regulação estadual. O ideal de liberdade que se acha associado à Internet carece, por isso, de ser compatibilizado com o exercício das soberanias estaduais[25].

---

[22] ROBERTO, Wilson Furtado. *Dano transnacional e internet:* direito aplicável e competência internacional. Curitiba: Juruá, 2010, p. 26. "As normas de Direito internacional privado têm por objetivo regular o conflito de leis e determinar a jurisdição internacional competente para processar um litígio que apresente elementos que envolvam dois ou mais ordenamentos jurídicos. Nos casos que envolvem danos transnacionais por violação de direitos da personalidade e da propriedade intelectual, por decorrência do caráter não fronteiriço da internet, torna-se muito difícil a delimitação territorial entre os Estados, portanto, as regras de conflitos de leis e de competência internacional, enquanto baseadas em regras clássicas e/ou vigentes de conexão, podem mostrar-se, de certa maneira, inadequadas e desencorajantes. Entretanto, esse fato não pressupõe sua absoluta inaplicabilidade [...]. Os princípios tradicionais do Direito internacional privado se relacionam com atividades que tenham uma localização física, e não virtual [...]."

[23] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 83-84. "Em oposição à tendência de livre fluxo de dados transfronteiriços, estão os regramentos sobre a localização de dados, que podem ser entendidos como "esforços a nível nacional ou regional para regular o fluxo de dados transfronteiriços ou criar incentivos para localizar o processamento e o armazenamento de dados [...]. Restrições quanto à localização de dados já foram propostas por diversos países, dentre os quais se destacam Alemanha, Rússia e Brasil, particularmente motivados por pressões públicas de combate à vigilância cibernética transfronteiriça e à espionagem de dados praticada por governos estrangeiros e empresas transnacionais. Essas restrições ocorrem no âmbito territorial e podem ser caracterizadas em cinco grandes modalidades: i) restrição do processamento de dados por entidades dentro de determinada jurisdição; ii) requerimento de que dados sejam armazenados *localmente* (dentro de determinado território); iii) mudanças na arquitetura da rede e uso de roteamento de dados para mantê-los dentro de um espaço territorial, como espécie de 'confinamento informacional'; iv) políticas discriminatórias que permitem a implementação dessas restrições apenas por certas organizações, com o critério de origem/nacionalidade; e v) restrições ao movimento transfronteiriço de algumas categorias de dados. [...] A Neutralidade da Rede prescreve que o tráfego de dados na Internet deve ser tratado de maneira não discriminatória para que os usuários da mesma possam escolher livremente o conteúdo, os aplicativos, os serviços e os dispositivos utilizados, sem ser influenciados por uma disponibilização discriminatória do tráfico de dados na Rede. Segundo os defensores da neutralidade da rede, esse princípio é responsável por fazer com que a internet continue sendo uma rede com arquitetura aberta, em que usuários podem consumir, produzir e compartilhar todo tipo de conteúdo entre eles. A neutralidade da rede preserva, desse modo, a integridade da internet. Há pelo menos três formas de discriminar um conteúdo ou aplicação na internet: bloqueando, reduzindo sua velocidade ou cobrando preços diferentes de acesso."

[24] COSTA, José Augusto Fontoura; SOLA, Fernanda. Op. cit., jul./dez. 2010, p. 297.

[25] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 101.

Impõe-se uma análise cuidadosa por se tratar de tema que possui especificidades que afastam a aplicação impensada e automática dos critérios de conexão tradicionais, a fim de que não incida uma lei que manifestamente não guarda qualquer relação com o conflito ou, ainda, que não seja ajuizada ação perante tribunal incompetente. A escolha do critério aplicável possui ampla repercussão em termos políticos, sociais e econômicos, de modo que é preciso justificá-la[26].

Esta pesquisa resultou da análise dos novos problemas e desafios suscitados no contexto da Sociedade da Informação, e parte da ideia de privacidade e sua relação com a proteção de dados para realizar uma análise essencialmente em termos de Direito Internacional Privado, expondo questões controversas e levando em consideração que os conflitos surgidos são eminentemente plurilocalizados.

Como resultado, o estudo está dividido em três partes: inicialmente, são abordados os conceitos, a evolução e o enquadramento normativo da privacidade e da proteção de dados em diferentes ordenamentos jurídicos. O objetivo da primeira parte, portanto, é situar o leitor no tema abordado, oferecendo as ferramentas necessárias à análise posterior.

A segunda parte do estudo, por sua vez, parte da qualificação dos objetos de estudo e da exposição das principais questões controversas, selecionadas a partir da relação que guardam com a proteção de dados, e da relevância no âmbito judicial. Constam, ainda, perspectivas e expectativas ligadas ao ambiente digital e suas implicações sobre o Direito, tanto de forma positiva quanto negativa, apontando novos desafios que podem surgir.

É possível, a partir da qualificação, na terceira parte da dissertação, abordar as questões do Direito Internacional Privado relacionadas à jurisdição competente e à determinação da lei aplicável, avaliando a forma como o enquadramento normativo dado anteriormente influencia tais aspectos. A proposta é, ao final, oferecer questões relevantes para reflexão, bem como ferramentas úteis à solução de eventuais conflitos envolvendo dados plurilocalizados e danos transnacionais.

[26] Id., ibid., pp. 22-23. "É que a aplicação da lei do país de origem da informação disponibilizada em rede, assim como a atribuição de competência internacional aos tribunais desse país, sendo a solução mais conforme com a eficiência econômica e mais favorável à liberdade de expressão, depara com objeções fundadas na proteção dos consumidores e na salvaguarda da soberania estadual; mas a aplicação sem restrições da lei do país de destino da informação sujeitaria os fornecedores desta a ônus e encargos desmesurados, que os desincentivariam de oferecê-la em rede, e permitiria a qualquer Estado censurar a informação disponibilizada na Internet."

CAPÍTULO 1 – PRIVACIDADE E PROTEÇÃO DE DADOS: CONCEITO, EVOLUÇÃO E ENQUADRAMENTO NORMATIVO

A privacidade surge, frequentemente, como conceito atrelado às discussões acerca da proteção de dados. Trata-se, de certo modo, do ponto de partida para justificar a tutela dos dados e informações pessoais no contexto da Sociedade da Informação. Cumpre, assim, tratar não apenas do conceito de privacidade e das transformações que esta foi sofrendo ao longo do tempo, como, também, da forma como os legisladores passaram a enxergar um tema relativamente novo e que sofre mudanças constantes.

1.1 INTRODUÇÃO AO CONCEITO DE PRIVACIDADE

A ideia de privacidade é anterior ao advento ou à popularização da Internet. Cumpre, neste primeiro tópico, introduzir o tema e esclarecer o conceito atual de privacidade e a forma como tal concepção foi sendo alterada no decorrer dos anos.

Enquanto conceitos como privacidade (ou "intimidade", conforme respectiva expressão francesa[27], adotada igualmente pelo texto da Constituição da República Federativa do Brasil de 1988) surgiram há longo tempo, havendo registros de estudos específicos sobre o assunto datados do século XVIII[28], é forçoso reconhecer que a atual dinâmica social e econômica, com acentuadas características internacionais, agrega grande pertinência temática ao assunto.

Há consenso em apontar como marco inicial do direito à privacidade moderna o artigo publicado por Samuel Warren e Louis Brandeis, no ano de 1890[29]. Suas ideias repercutiram, por exemplo, sobre a Carta Magna Inglesa, de 1215, e sobre a 4ª Emenda da Constituição estadunidense[30], de maneira que foram inicialmente adotadas tanto por países europeus quanto pelos Estados Unidos, estando ligadas principalmente ao "direito de ser

---

[27] LAÉ, Jean-François. L'intimité: une histoire longue de la propriété de soi. *Sociologie et sociétés*, 2003, v. 35, n° 2, pp. 139-147. Disponível em: http://id.erudit.org/iderudit/008527ar. Acesso em: 18 jun. 2016.
[28] Id., ibid.
[29] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, 1890, n.º 193.
[30] CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. *Direito, Estado e Sociedade*, jul/dez. 2013, n.º 43, pp. 135-161, pp. 137-138. "O direito à privacidade, cuja génese remonta ao ano de 1890 e ao artigo de Samuel Warren e Louis Brandeis, publicado na Harvard Law Review, teve as suas primeiras manifestações na Magna Carta Inglesa de 1215 e na difusão do princípio *man's house is his castle* na Common Law, na 4.ª Emenda da Constituição dos Estados Unidos da América, aprovada em 1787, e na Constituição Francesa de 1791, estando intimamente relacionado ao surgimento da burguesia e ao crescimento dos centros urbanos."

deixado só", ou "*right to be let alone*", revelando uma perspectiva focada no indivíduo[31]. Há maior relação, por conseguinte, com o direito à intimidade do que com a privacidade em si[32].

Antes disso, a privacidade já havia sido tangenciada por filósofos como Thomas Hobbes, John Locke e Robert Price[33]. Não se tratava, contudo, da concepção atual de privacidade, relacionada à intimidade ou à esfera da vida privada[34] que, a partir do artigo

---

[31] BRANDÃO, André Martins. Interpretação Jurídica e Direito à Privacidade na Era da Informação: uma abordagem da hermenêutica filosófica. *Revista Paradigma*. Ribeirão Preto, SP, ano XVIII, jan./dez. 2013, n.º 22, pp. 232-257, p. 241. "Essa tese foi defendida em um voto de dissenso por Brandeis trinta e oito anos depois, quando se tornou Justice da Suprema Corte Americana, no caso *Olmstead v. United States*. Nessa ação, a Corte decidiu que a interceptação telefônica não se tratava de uma violação ao direito à privacidade, pois não se tratava de uma invasão física do domicílio do indivíduo. O voto de dissenso de Brandeis, de modo contrário, afirmava que o direito à privacidade "[…] *conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men*" (Olmstead v. United States, 1928). A tese do voto de dissenso de Brandeis influenciou a revisão do precedente acima no caso *Katz v. United States*, julgado em 1967 pela Suprema Corte Americana, no qual foi afirmada a existência do direito à privacidade desde que verificada uma razoável expectativa de privacidade (*reasonable expectation of privacy*). No caso foi defendido como direito "[…] *to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law*" (Katz v. United States, 1967)."

[32] GUERRA, Sidney. Direito fundamental à intimidade, vida privada, honra e imagem. *In*: Anais do XV Encontro Preparatório para o Congresso Nacional do Conpedi. Florianópolis: Fundação Boiteux, 2006. *Anais...* Florianópolis, Conpedi, 2006. Disponível em: http://conpedi.org.br/manaus/arquivos/anais/recife/direitos_fundam_sidney_guerra.p. Acesso em: 05 mar. 2020. "Percebe-se que existe uma grande dificuldade de se estabelecer o que é direito à intimidade e direito à vida privada, razão pela qual Luis Alberto David Araújo optou por utilizar as expressões *vida privada* e *intimidade* como sinônimas. [...] Na verdade, o direito à intimidade tem recebido várias denominações desde o "*right of privacy*" (no direito anglo-americano), "*droit à la vie privée*" (no direito francês), o "*diritto alla riservatezza*" (no direito italiano), o "*derecho a la esfera secreta*" (no direito espanhol), o direito à privacidade e o direito de estar só (no direito brasileiro), por exemplo. [...] Assim, para melhor esclarecimento, verifica-se que a intimidade é algo a mais do que a vida privada, ou seja, a intimidade caracteriza-se por aquele espaço, considerado pela pessoa, como impenetrável, intransponível, indevassável e que, portanto, diz respeito única e exclusivamente à pessoa [...]."

[33] NOJIRI, Sérgio. O direito à privacidade na era da informática: algumas considerações. *Revista Jur – UNIJUS*. Uberaba, MG, maio/2005, v. 8, n.º 8, pp. 99-106, p. 99. "Locke, em *Ensaio sobre o Governo Civil*, desenvolve sua ideia de liberdade como "autonomia para dispor, como bem lhe pareça, de sua pessoa, de seus atos, de seus bens e de tudo quanto lhe pertença, submetendo-se ao que ordenam as leis sobas quais vive" e, ao fim, teria afirmado "a exclusão de toda submissão a vontade arbitrário de outro, para poder seguir livremente a sua." Mill, em sua obra *On Liberty*, de 1859, sustentava a tese de que os únicos aspectos da conduta humana que produziam deveres e responsabilidades sociais seriam aqueles que afetassem os demais. Segundo ele, os aspectos que só dizem respeito ao indivíduo são absolutamente independentes, resultando ser o indivíduo soberano sobre si, seu corpo e sua mente ("*Over himself, over his own body and mind the individual is sovereign*")."

[34] CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. Op. cit., jul./dez. 2013, p. 138. "Em 1846, já o autor alemão Karl Röder abordava a questão da privacidade, definindo como actos violadores do direito natural à vida privada as perguntas indiscretas e a entrada num aposento sem se fazer anunciar. Na jurisprudência, o conhecido caso da actriz francesa fotografada morta a pedido da irmã, cujas fotografias foram posteriormente difundidas sem consentimento, conhecido como o caso Rachel (o nome da actriz em apreço era Elisa Rachel Félix), pode ser referido como o primeiro aresto sobre privacidade. O Tribunal Civil do Sena, por sentença que remonta ao ano de 1858, decidiu que era proibido reproduzir e dar publicidade a fotografias sem o consentimento da pessoa visada ou da sua família, pelo que, no caso concreto, houve uma violação da privacidade." Merece ser referida, ainda, a Lei de Imprensa Francesa, de 1868, que consagrou uma norma percussora, embora sectorial, de protecção da privacidade, a saber: "a publicação, num escrito

de Warren e Brandeis, foi reconhecida como um direito autônomo, com características próprias. A preocupação, à época, se devia ao surgimento de novas tecnologias, como máquinas de fotografia e popularização de jornais impressos de grande circulação[35].

Isto significa que, já em 1890, vislumbrava-se a forma como novas tecnologias podem interferir no direito à vida privada. Com a evolução tecnológica, passou a haver maior preocupação com o tema da privacidade e com a possível violação de direitos de personalidade, inclusive por parte dos legisladores nacionais. Como resultado da evolução, o direito à privacidade passou da noção inicialmente negativa, ligada a intromissões externas não consentidas, a uma concepção positiva, de desenvolvimento de um aspecto da personalidade[36].

Em 1948, o direito à privacidade foi consagrado no texto da Declaração Universal dos Direitos Humanos[37] e, em seguida, pela Convenção Europeia dos Direitos do Homem (Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais) de 1950[38] e, também, pelo Pacto Internacional Relativo aos Direitos Civis e Políticos de 1966[39]. Em todos esses casos, contudo, a proteção conferida está mais ligada à tutela da

---

periódico, de facto relativo à vida privada constitui uma contravenção punida com a pena de quinhentos francos."

[35] BRANDÃO, André Martins. Op. cit., jan./dez. 2013, p. 233. "Quando Warren e Brandeis (1890) escreveram seu artigo seminal *The Right to Privacy*, a preocupação deles era com as novas tecnologias à época, como máquinas de fotografar e grandes jornais, que supostamente haviam invadido o sagrado lugar da vida privada doméstica. Ocorre que na atual era da informação esse problema tem se exacerbado. A tecnologia está cada vez mais acessível e disponível para todos, já são mais de 2.4 bilhões de usuários da internet no mundo, certamente um conjunto muito maior do que Brandeis e Warren (1980) imaginavam quando falavam de proteção à privacidade."

[36] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, SC, jul./dez. 2011, v. 12, n. 2, pp. 91-108.

[37] DHDH. Declaração Universal dos Direitos Humanos. Genebra, Suíça, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 09 jan. 2020. "Art. 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à protecção da lei."

[38] CEDH. Convenção Europeia dos Direitos do Homem. Roma, 4 nov. 1950. Disponível em: https://www.echr.coe. int/Documents/Convention_POR.pdf. Acesso em: 09 jan. 2020. "Art. 8°. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

[39] PACTO INTERNACIONAL DOS DIREITOS CIVIS E POLÍTICOS. 16 dez. 1966. Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf. Acesso em: 09 jan. 2020. "Art. 17, § 1º. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. § 2º. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas."

vida privada do que a uma preocupação com dados pessoais, abordagem que foi se alterando com o decorrer do tempo.

A privacidade e a proteção de dados são conceitos próximos, porém direitos autônomos. Enquanto o direito à privacidade é mais abrangente e pode se referir aos mais diversos aspectos da vida privada, o direito à proteção de dados se mostra apenas como uma das faces do primeiro, tendo se desenvolvido a partir dele, especialmente a partir da década de 1970[40].

O direito à privacidade, diferente do direito à intimidade, parte da ideia de distinção entre as esferas pública e privada, a qual se torna cada vez menos perceptível. Nos tópicos que seguem é abordada a evolução legislativa da privacidade e da proteção de dados no Brasil e em outros países ao redor do mundo. Ao final, restará claro que, tendo um ponto de partida em comum (o artigo de Warren e Brandeis), os conceitos e direitos ligados à privacidade, assim como aqueles relacionados aos dados pessoais, recebem tratamentos distintos, a depender da cultura local[41].

Neste momento já é possível delinear uma primeira questão de Direito Internacional Privado essencial à discussão: havendo diferentes concepções do direito à privacidade e do direito à proteção de dados, e considerando que a qualificação no DIP implica conceituação e classificação, há de se cogitar a possibilidade de ocorrência de conflitos de qualificação.

De fato, conforme a ideia de privacidade foi se transformando nos seios das diferentes sociedades, passou-se a questionar se se trata de um direito fundamental, o que implica na sua indisponibilidade, ou se, por outro lado, é uma questão de natureza contratual (ou mesmo relativa a bens) que poderiam, por conseguinte, ser cedidos ou vendidos livremente. Há, ainda, uma terceira possibilidade: a de que os dados considerados

---

[40] DONEDA, Danilo. Op. cit., jul./dez. 2011, pp. 201-202. "A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da 'diáspora' dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*, além da já mencionada *Bundesdatenschutzgesetz*. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da Lei Francesa)."

[41] JAYME, Erik. Sociedade multicultural e novos desenvolvimentos no Direito Internacional Privado. *Cadernos do Programa de Pós-Graduação em Direito da UFRGS*, mar. 2003, v. 1, n.º 1, pp. 102-103. Concorda-se com o posicionamento de Erik Jayme quanto à possibilidade de solução de conflitos entre culturas, conforme raciocínio exposto no seguinte trecho: "Estes avanços tendentes à elaboração de métodos complexos para resolver os conflitos entre culturas diversas não excluem, portanto, de dar relevância, com a finalidade de proteger a identidade da pessoa, as técnicas clássicas do direito internacional privado. [...] Além disso, precisa-se desenvolver, para resolver os problemas interculturais, novas técnicas que considerem, sobre o plano da aplicação da lei material indicada pelas normas de conflito, os preceitos e costumes culturais."

públicos ou de interesse nacional justifiquem a sua coleta por um interesse legítimo (geralmente de caráter coletivo e/ou social), sem a necessidade de consentimento prévio do titular.

A forma como a privacidade e os dados pessoais são tutelados depende, por conseguinte, de uma conceituação inicial. Esta, por não ser unânime, pode provocar conflitos de qualificação, tema que será tratado com maior profundidade no terceiro capítulo deste estudo. Esta análise conceitual inicial, portanto, mostra-se essencial para que seja possível subsumir os fatos de uma eventual lide ou conflito às normas adequadas e efetivamente aplicáveis.

Exemplo interessante pode ser extraído da oposição entre direito à privacidade e direito à informação ou expressão, especialmente em relação ao direito do esquecimento, ou direito a ser esquecido[42], o qual pode ser assim definido:

> Pelo Enunciado 531do CJF: 'a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento'. Com isso, a pessoa pode ter a pretensão de que certa informação sobre seu passado por estar ligada à sua privacidade, à sua honra, etc., não seja mais divulgada, impedindo ou dificultando seu acesso a terceiros, para que caia no esquecimento, uma vez que não envolve interesse público. Assim, por ex., permite-se ao ex-detento, que se reabilitou, o direito de ressociabilização, de reescrever sua história de viver em paz, tendo uma nova chance. O direito a ser esquecido, tido como um direito da personalidade, por estar ínsito no art. 21 do Código Civil, é o de não ser lembrado, por fatos vexatórios depreciativos ou constrangedores ocorridos no passado que não mais correspondem ao presente, uma vez que o envolvido passou a ter vida exemplar, desde que não seja ocupante de cargo público, pois sua vida pretérita interessa à população[43].

Para fins de referência, há três correntes distintas quanto ao direito ao esquecimento: posição pró-informação, posição pró-esquecimento e posição intermediária[44]. Como os próprios nomes indicam, os posicionamentos se diferenciam pelo

---

[42] ABRUSIO, Juliana. O direito ao esquecimento na Internet e a (im)possibilidade de recomeçar. *CESA - Anuário*, 2013, v. 1, pp. 17-26, p. 22. "Diante dos diversos provedores de busca na Internet, tais como Google, Bing e Yahoo!, tornou-se praticamente impossível deixar o passado para trás. Uma informação pode ser resgatada em segundos. Uma pessoa pode ter vários detalhes de sua vida profissional, e também pessoal, exposta em uma lista de indexação de um buscador qualquer da Internet, acessível a qualquer pessoa com conexão à rede mundial de computadores. Fato é que a tecnologia está transformando o passado em um eterno presente."

[43] DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido. *Revista Brasileira de Direito.* Passo Fundo, RS, maio/ago. 2017, v. 13, n.º 2, pp. 7-25. ISSN 2238-0604. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/1670/1205. Acesso em: 8 mar. 2020.

[44] SCHREIBER, Anderson. As três correntes do direito ao esquecimento. *Jota*, 18 jun. 2017. Disponível em: https://bit.ly/2QErVqY. Acesso em: 09 jan. 2020. "Independentemente da posição que se adote sobre esse tema tão candente, a audiência pública evidenciou duas grandes dificuldades que terão de ser enfrentadas pelo STF. Primeiro, o termo 'direito ao esquecimento' não é o melhor: sugere um controle dos fatos, um apagar da História que, além de ser impossível e indesejável, não se coaduna com o significado técnico por

sopesamento entre o direito ao esquecimento (como um reflexo do direito à privacidade) e o direito à informação[45]. Parece mais acertada, contudo, a posição intermediária, que concilia o direito à informação e à privacidade de forma equilibrada, mediante o sopesamento e ponderação em cada caso concreto[46].

Até a vigência do Marco Civil da Internet, o direito ao esquecimento não constava expressamente na legislação brasileira, sendo considerado um desdobramento do direito constitucionalmente previsto. A lei, contudo, dispõe de norma específica acerca da obrigação de exclusão definitiva de dados pessoais, mediante requerimento do titular dos dados – hipótese que está em harmonia com o art. 8º da LGPD que, embora ainda não esteja em vigor, dispõe sobre dever no mesmo sentido.

De todo modo, o direito ao esquecimento constitui expressão do direito da pessoa humana à intimidade, à privacidade e à reserva – direitos que possuem expressa tutela legal, conforme consta em detalhes ao final deste primeiro capítulo.

Se o direito à privacidade é tido como um direito de ordem fundamental, e considerado constitucionalmente protegido, o sopesamento em relação ao direito à informação certamente será diferente do que se for considerado um bem disponível, por

---

trás da expressão, consubstanciado na tutela da identidade pessoal e do direito de toda pessoa humana de ser corretamente retratada em suas projeções públicas. Segundo, o tema, bem ou mal posto, tangencia diversas outras questões polêmicas, como a indexação de resultados por motores de busca da internet, a tutela *post mortem* do direito à imagem, e assim por diante."

[45] TERWANGE, Cécile de. Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *IDP. Revista de Internet. Derecho y Política*, 2012, v. 13. Disponível em: https://www.redalyc.org/pdf/788/78824460006.pdf. Acesso em: 09 jan. 2020. "O direito ao esquecimento, também chamado direito de ser esquecido, é o direito das pessoas físicas de fazerem com que seja apagada a informação a seu respeito após determinado período de tempo. A Internet trouxe consigo a necessidade de um novo equilíbrio entre a livre difusão da informação e a autodeterminação individual. Este equilíbrio é precisamente o que está em jogo com o direito ao esquecimento. Este direito possui três faces: o direito ao esquecimento do passado judicial, o direito ao esquecimento estabelecido pela legislação de proteção de dados, e um novo direito digital ao esquecimento, ainda polêmico, o qual equivaleria à atribuição de uma data de caducidade aos dados pessoais, o que deveria ser aplicável no contexto específico das redes sociais." (Tradução livre). "*El derecho al olvido, también llamado derecho a ser olvidado, es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado. Internet ha traído consigo la necesidad de un nuevo equilibrio entre la libre difusión de la información y la autodeterminación individual. Este equilibrio es precisamente lo que está en juego con el derecho al olvido. Este derecho presenta tres facetas: el derecho al olvido del pasado judicial, el derecho al olvido establecido por la legislación de protección de datos y un nuevo derecho digital y aún polémico al olvido, que equivaldría a la atribución de una fecha de caducidad a los datos personales o que debería ser aplicable en el contexto específico de las redes sociales.*"

[46] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Caso C-131/12.* Google Spain SL e Google Inc vs. Agencia Española de Proteção de Dados, 13 maio 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT Acesso em: 17 abr. 2020. "Dados pessoais – Proteção das pessoas singulares no que diz respeito ao tratamento desses dados – Diretiva 95/46/CE – Arts. 2.°, 4.°, 12 e 14 – Âmbito de aplicação material e territorial – Motores de busca na Internet – Tratamento de dados contidos em sítios web – Pesquisa, indexação e armazenamento desses dados – Responsabilidade do operador do motor de busca – Estabelecimento no território de um Estado-Membro – Alcance das obrigações desse operador e dos direitos da pessoa em causa – Carta dos Direitos Fundamentais da União Europeia – arts. 7° e 8°."

exemplo. De fato: alguns autores entendem que enquanto os direitos fundamentais pertencem ao âmbito constitucional, os direitos da personalidade relacionam-se ao âmbito cível, mesmo que contemplados por norma constitucional[47]. Percebe-se, contudo, que há dificuldades em adotar tal classificação, dispondo os direitos fundamentais e os direitos da personalidade em categorias estanques[48].

Tais questões estão longe de exaurir os temas e questionamentos suscitados pela privacidade e sua evolução como um direito autônomo. São importantes, no entanto, para agregar relevância ao estudo proposto, e demonstrar a forma como, em situações práticas, o método de Direito Internacional Privado, qualificação inclusive, poderá influenciar diretamente sobre o resultado de uma eventual demanda.

---

[47] DINIZ, Maria Helena. Op. cit., maio/ago. 2017. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/1670/1205. Acesso em: 8 mar. 2020. "Os direitos fundamentais pertencem ao direito constitucional, pressupondo relações entre pessoa e poder estatal, tendo incidência publicística imediata, mesmo quando produzirem efeitos no âmbito das relações privadas. Já os direitos da personalidade pertencem à seara cível, apesar de contemplados em norma constitucional, visto que incidem nas relações entre particulares. Há uma dupla dimensão dos direitos da personalidade: a axiológica, em que os valores fundamentais da pessoa se materializam, e a objetiva, consistente nos direitos previstos em lei e na Constituição Federal. [...] Como se pode ver, há uma interdependência entre direitos fundamentais e direitos da personalidade, visto que muitos destes são direitos fundamentais e vice-versa. [...] Tal ocorre porque a CF/88, ao consagrar os direitos da personalidade, fez com que adquirissem o *status* de direitos fundamentais, tendo proteção própria e, com isso, passaram a constituir a concretização da dignidade da pessoa humana. O respeito à dignidade da pessoa humana é o fundamento jurídico-normativo dos direitos fundamentais e dos direitos da personalidade, que concretizam aquele princípio. Daí a intima conexão existente entre eles e, consequentemente, entre o direito a ser esquecido, que neles encontra uma justificativa."

[48] NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. *RIL.* Brasília, jan./mar. 2017, ano 54, n.º 213, pp. 265-288, pp. 269-270. A respeito, cumpre concordar com a seguinte análise: "Mesmo com o aperfeiçoamento de algumas dimensões da personalidade por meio do direito privado entre o século XIX e início do XX, o marco mais característico na continuidade desse processo foi a Constituição de Weimar, de 1919. Ela repercute ainda hoje em diversos países, porque aprimorou a relação entre o direito público e o direito privado, englobando em âmbito constitucional institutos-chave do direito civil, como a família, a propriedade e o contrato [...]. Depois disso, a relação entre direito civil e Constituição passou a ser reavaliada. Ocorreu a conscientização da unidade do ordenamento jurídico e a reestruturação em torno de sua pedra angular que despontou como valor fundamental, baseado agora na dignidade humana. O instituto da personalidade, estudado no direito civil, foi o que apresentou a mais forte vocação para tornar-se o centro de irradiação no direito privado dessa nova dogmática, voltada à proteção da pessoa. [...]. Assim, ocorreu que os direitos em torno da personalidade, bem como seus vários aspectos – como o nome, a honra, a imagem e outros –, acabaram sendo compreendidos pelo direito civil como direitos subjetivos da pessoa, que mereceriam indenização se violados. Vale observar que, na sua estrutura clássica, o direito subjetivo pressupõe a existência de um objeto externo ao sujeito. Entretanto, ao emergir a tutela dos direitos da personalidade, ocorreu a constatação de duas categorias – o "ter" e o "ser" – como um conjunto de interesses humanos. Com essas ponderações, é possível constatar que o debate doutrinário se utilizou da categoria do direito subjetivo na tutela da personalidade como uma reação plausível em determinada época; porém, continuar a usá-la hoje seria fechar os olhos a uma série de mudanças estruturais do ordenamento."

1.2 TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

Conforme apontado, esta primeira parte do estudo visa apresentar um panorama conceitual e legislativo da proteção de dados, demonstrando a forma como a visão sobre o tema se modificou com o passar do tempo, especialmente diante do desenvolvimento de novas tecnologias no seio da Sociedade da Informação.

Destaca-se, desde já, certa oposição entre o tratamento normativo conferido à proteção de dados pelos Estados Unidos, de um lado, e pela União Europeia, de outro. Tal diferenciação passa a ser abordada com maiores detalhes a partir deste tópico, o que permite compreender a sua evolução e, principalmente, as suas implicações sobre o Direito Internacional Privado.

Assim, muito embora se proponha a analisar o posicionamento da União Europeia como um todo, cabe, preliminarmente, expor a forma como alguns ordenamentos jurídicos nacionais já vinham, anteriormente, tratando a temática, inclusive para fins de contextualização das diretivas e regulamentos europeus a serem abordados na sequência. Isto posto, foram selecionados alguns países, como Alemanha, França, Espanha e Portugal, os quais compõem a União Europeia, cujas normas sobre a temática estudada se destacam pelos motivos desenvolvidos a seguir[49].

O conceito de privacidade e a forma como os dados pessoais e as informações são tutelados diferem conforme o contexto analisado[50], de modo que existe uma relação entre a evolução legislativa de tais temas e a cultura jurídica de cada local[51]. Antes mesmo da

---

[49] Id., ibid., p. 272. Exceto o caso da França, os ordenamentos aqui selecionados coincidem com os abordados por Valéria Ribas do Nascimento: "No caso da Alemanha, o texto da Lei Fundamental, de 1949, refere-se a um direito ao livre desenvolvimento da personalidade, com base no qual foi desenvolvido pela doutrina e jurisprudência um direito geral de personalidade. Na Constituição da Espanha, por sua vez, é assegurado o direito ao livre desenvolvimento da personalidade; e, na Constituição de Portugal, é mencionado o direito ao desenvolvimento da personalidade, com o intuito de assegurar proteção isenta de lacunas [...]. Em síntese, é possível afirmar que em diversos ordenamentos existe a busca por um direito geral de personalidade."

[50] DREXL, Josef. Le commerce éléctronique et la protection des consommateurs. *Revue Internationale de Droit Économique*, 2002/2 (t. XVI), doi 10.3917/ride.162.0405. Disponível em: https://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm. Acesso em: 17 abr. 2020. Conforme a visão apresentada por Josef Drexl, é possível apontar duas abordagens fundamentalmente distintas para o tema, as quais refletem cada uma sua cultura particular. Assim, de forma simplificada, o autor constata que os Estados Unidos e as empresas ligadas à informação privilegiam a abordagem da autorregulação, enquanto na União Europeia a abordagem adotada seria a de reguladora mormente tradicional.

[51] OLIVEIRA, Elsa Dias. Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em direito internacional privado. *Cuadernos de Derecho Transnacional*, mar./2013, v. 5, n.º 1, pp. 139-162, (s.p.): "Nos vários ordenamentos jurídicos nacionais o elenco, o conteúdo e as formas de tutela dos direitos de personalidade apresentam variações muito significativas. Estas divergências não são de estranhar se se tiver presente que os direitos de personalidade, intrinsecamente ligados à pessoa, e à sua tutela, refletem de forma muito expressiva os valores ético-jurídicos que estão

União Europeia, a **Alemanha** já era apontada como exemplo de país que valoriza a proteção de dados pessoais, e que entende a privacidade de forma ampla.

A sociedade alemã, marcada pelas atrocidades cometidas durante a Segunda Guerra Mundial, demonstra preocupação especial quanto à proteção de dados pessoais como maneira de proteger seus cidadãos de futuros abusos. Sabidamente, o regime nazista utilizou registros dos indivíduos para monitorar e vigiar a população, identificar grupos e obter informações.

Desde 1983, quando foi proferida decisão no julgamento da "Lei de Recenseamento da População, Profissão, Moradia e Trabalho", ou "Decisão do Censo" pelo Tribunal Constitucional Federal alemão, tais temas assumiram posição de destaque[52]. Como consequência de tal precedente, o entendimento alemão passou a ser o de que seus cidadãos detêm o direito básico à autodeterminação quanto aos seus dados pessoais[53].

Assim, as informações cedidas ao censo passaram a ser segregadas, a fim de permitir o completo anonimato dos cidadãos entrevistados. E, até que tal anonimato fosse

---

subjacentes a cada ordenamento jurídico. Varia, ainda o peso que é atribuído a interesses que podem conflituar com a tutela dos direitos de personalidade, como é o caso, *v.g.*, da liberdade de expressão, da liberdade de imprensa."

[52] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, v. 1, pp. 233-234. "Por meio da Lei do Censo (*Volkszählungsgesetz*) de 1983, promulgada em 25 de março de 1982 (BGBl. I, p. 369), ordenou-se o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho, para fins estatísticos. O objetivo declarado da lei era reunir, por meio de levantamentos feitos por pesquisadores credenciados, dados sobre o estágio do crescimento populacional, a distribuição espacial da população no território federal, sua composição, segundo características demográficas e sociais, assim como também sobre sua atividade econômica. Tais dados sempre foram considerados indispensáveis para quaisquer decisões político-econômicas da União, Estados e municípios. O último censo havia acontecido em 1970. A Lei do Censo de 1983 listava os dados que deveriam ser levantados pelos pesquisadores e determinava quem estava obrigado a fornecer as informações. O § 9º da Lei previa, entre outras, a possibilidade de uma comparação dos dados levantados com os registros públicos e, também, a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa. [...]. O TCF considerou presentes as condições processuais das Reclamações Constitucionais (julgadas conjuntamente), pois os reclamantes teriam sido atingidos, em grande parte, de modo próprio, direto e atual. O pressuposto "ser diretamente atingido" foi, no entanto, relativizado: embora o ato executório fosse o levantamento do dado em si, quando este ocorresse, a potencial violação, nesse caso, transformar-se-ia em uma lesão irreversível por excelência, como costuma ocorrer em contextos de levantamento e administração de dados pessoais como o ocorrido no presente caso. No mérito, o TCF julgou as Reclamações Constitucionais só parcialmente procedentes, confirmando a constitucionalidade da lei em geral. Declarou, porém, nulos principalmente os dispositivos sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa."

[53] CAMARGO, Solano de. As sanções da LGPD e o Inferno de Dante. *Revista do Advogado,* nov. 2019, v. 1, n.º 144, pp. 220-232, (s.p.): "Os alemães dão extrema importância à privacidade e à proteção de dados, havendo um temor generalizado ante a coleta e o tratamento de dados pessoais, principalmente pelo setor público. A proteção aos dados pessoais se tornou uma obsessão jurídica na Alemanha desde que o Tribunal Constitucional Federal proferiu a 'Decisão do Censo', em 1983. Por esse precedente, a Suprema Corte alemã decidiu que seus cidadãos detêm o direito básico à autodeterminação de seus dados pessoais, de forma que o censo nacional deveria segregar tais dados nos questionários, garantindo o completo anonimato para os participantes da pesquisa. Até que o governo alemão pudesse demonstrar a segurança dessa segregação, o país não pôde realizar o censo até 1987."

garantido, em 1987, não foi possível a realização do censo nacional na Alemanha. A mencionada decisão representou o início do reconhecimento do direito à autodeterminação informativa no país, com base na projeção da personalidade do indivíduo, nos termos do art. 2º, inc. I, da Lei Fundamental Alemã[54].

A vigilância estatal repercutiu, também, sobre outros países europeus, como Áustria, Holanda e França, tendo impacto sobre a União Europeia como um todo. Na década de 1980 passou a ficar mais clara a divergência entre os posicionamentos defendidos por Estados Unidos e União Europeia no que tange à proteção de dados, de modo que a Organização de Cooperação e Desenvolvimento Econômico (OCDE) realizou uma série de recomendações sobre o tema, traduzidos em sete princípios básicos[55].

O Parlamento alemão cumpriu com as obrigações decorrentes das diretivas da União Europeia ao internalizá-las em dezembro de 2007, com a promulgação da Lei de Vigilância das Telecomunicações e outras Medidas de Investigações Secretas[56], emenda à Lei de Telecomunicações Alemã[57] e também ao Código de Processo Criminal[58] (*Strafprozessordnung* – StPO). O grande número de reclamações constitucionais submetidas pelos cidadãos alemães ao Tribunal Constitucional demonstra o quanto a privacidade e a proteção de dados são valorizadas como fundamentais[59].

Diferentemente da Alemanha, país no qual houve positivação precoce da proteção da privacidade e direitos da personalidade, a **França**[60] passou a regular tais direitos a partir

---

[54] Id., ibid., (s.p.): "Além da interpretação constitucional de que o abuso no tratamento dos dados pessoais viola os direitos civis, normas específicas como a Lei Federal de Proteção de Dados, o Código Penal, o Código Civil, a Lei de Telecomunicações e a Lei de Telemídia, especificam cuidadosamente a forma como os dados pessoais podem ser tratados. [...] A partir desse cenário histórico, a vigilância estatal dos cidadãos evoca uma profunda inquietação entre os alemães até os dias de hoje. O mesmo temor quanto ao abuso na utilização dos dados ressoou em diversos Estados da União Europeia, como a Áustria, a Holanda, a França e os países que compunham o lado leste da antiga Cortina de Ferro, de forma que nesse contexto se editou a *General Data Protection Regulation* (GDPR), em vigor desde 25 de agosto de 2018. Essa abordagem é materialmente distinta da forma como os dados pessoais são protegidos em outros países."

[55] OCDE. Organização para a Cooperação e Desenvolvimento Econômicos. *Síntese das Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*, 1980. Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 17 abr. 2020.

[56] ALEMANHA. *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie*, 2006/24/EG.

[57] ALEMANHA. Telekommunikationsgesetz – TKG.

[58] ALEMANHA. Strafprozessordnung– StPO.

[59] ALEMANHA. *Tribunal Constitucional Federal Alemão*. BvR 256/08, julgado em 02 mar. 2010. Disponível em: http://www.bverfg.de/e/rs20100302_1bvr025608en.html. Acesso em: 05 mar. 2020. O Tribunal Constitucional alemão considerou inconstitucionais os dispositivos de retenção de dados da Lei de Telecomunicações da forma como se encontravam, tendo sido declarados nulos desde o momento de sua promulgação, em 2008, com a eliminação desses metadados pelas empresas provedoras de serviços de telecomunicações privados.

[60] BIOY, Xavier. Le libre développement de la personnalité en droit constitutionnel, essai de comparaison (Allemagne, Espagne, France, Italie, Suisse). *Revue Internationale de Droit Comparé*, 2003, v. 55, n.º 1, pp. 123-147.

da promulgação da Lei n. 70.643, de 17/07/1970[61], quando introduziu no ordenamento a ideia de direito à intimidade e à vida privada (art. 9º do Código Civil francês), reforçando a tutela da personalidade[62].

A tutela desses direitos se desenvolveu na França, sobretudo no nível infraconstitucional[63]: o principal marco foi a aprovação da Lei para uma República Digital (LRD)[64], cujo art. 54 prevê, assim como o art. 1º da Lei de Informática e Liberdades (LIL)[65]: "Toda pessoa possui o direito de decidir e controlar os usos feitos de seus dados pessoais que lhe concernem, conforme as condições estabelecidas por esta lei"[66].

Os valores constitucionais considerados como superiores dentro do contexto europeu são nomeadamente aqueles ligados à liberdade, à igualdade e ao pluralismo. Díaz Revorio, ao tratar da Constituição **da Espanha** e dos valores constitucionais por ela encerrados, ensina a respeito da "progressiva realização dos valores superiores, sem prejuízo de seu caráter de norma jurídica plenamente eficaz"[67]. Por essa mesma razão

---

[61] FRANÇA. *Loi n. 70-643, 17 juillet 1970*. Tendant à renforcer la garantie des droits individuels des citoyens. Disponible en:https://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006529714&cidTexte=LEGITEXT000006068385&dateTexte=29990101. Accès à: 17 abr. 2020.

[62] MARTIAL-BRAZ, Nathalie. O direito das pessoas interessadas no tratamento de dados pessoais: anotações da situação na França e na Europa. *Revista de Direito, Estado e Telecomunicações.* Brasília, maio 2018, v. 10, n.º 1, pp. 85-108, p. 92. "Em termos gerais, essas normas jurídicas francesas preveem a necessidade de realizar tratamentos de dados de forma lícita e leal para fins estritamente determinados. Estes tratamentos também devem ser proporcionais ao objetivo definido e não ser excessivos. Além disso, é necessário, antes do tratamento, o consentimento da pessoa interessada ou o preenchimento das outras cinco condições expressas de legalidade, em especial 'o interesse legítimo do responsável pelo tratamento ou pelo destinatário, sob pena de desconhecer o interesse ou os direitos e liberdades fundamentais da pessoa interessada', como já indicado acima. Por outro lado, o RGPD prevê atualmente um regime especial e derrogatório para o consentimento de menores quando este é condição da legalidade do tratamento realizado durante a utilização dos serviços da empresa da informação."

[63] FRANÇA. *Loi n. 2004-801, 6 Août 2004*. Relative à la protection des personnes physiques à l'égard des traitments de données à caractère personnel (Lei n. 2004-801, de 6 ago. 2004, relativa à proteção das pessoas físicas em caso de tratamento de dados pessoais). Paris: Journal Official de la République Française (Jornal Oficial da República Francesa), 2004. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676. Acesso em: 17 abr. 2020.

[64] FRANÇA. *Loi n. 2016-1.321, 7 Octobre 2016*. Loi pour une république numérique (Lei para uma República digital, LRD). Paris: Journal Officiel de la République Française (Jornal Oficial da República Francesa), 8 out. 2016. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id. Acesso em: 17 abr. 2020.

[65] FRANÇA. *Loi n. 1978-17, 6 Janvier 1978*. Relative à l'informatique, aux fichiers et aux libertés modifiée – Loi Informatique et Libertés (Lei n. 1978-17, relativa à informática, aos arquivos e às liberdades – Lei para Informática e Liberdades, LIL). Paris: Journal Officiel de la République Française (Jornal Oficial da República Francesa), 7 jan. 1978, p. 227-231. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acesso em: 17. abr. 2020.

[66] "Todas as pessoas dispõem do direito de decidir e de controlar a utilização que será feita a partir dos dados pessoais que lhe concernem, sob as condições fixadas pela presente lei." (Tradução livre). *"Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi."*

[67] DÍAZ REVORIO, Francisco Javier. *Valores superiores e interpretación constitucional*. Madrid: Centro de Estudios Políticos y Constitucionales, 1997, p. 89. *"[...] progresiva realización de los valores superiores, sin prejuicio de su carácter de norma jurídica plenamente eficaz*."

considera especialmente importante a vinculação dos poderes públicos a tais valores, os quais necessitam, para sua realização, de impulso e apoio do poder político.

A Espanha considera o direito à intimidade um direito fundamental, tutelado pela Constituição Federal, em seu art. 18.1: "Garante-se o direito à honra, à intimidade pessoal e familiar e à própria imagem"[68]. Garante, também, pelo mesmo artigo, o direito ao sigilo das comunicações, em especial postais, telegráficas e telefônicas, salvo sob ordem judicial, e prevê expressa limitação ao uso da informática para garantir a honra e a intimidade pessoal e familiar. Trata-se, claramente, de direito de natureza constitucional, irrenunciável e indisponível[69].

Finalmente, quanto ao ordenamento jurídico **português**, o direito à autodeterminação informativa visa evitar que o indivíduo se torne objeto da informação[70]. Assim, o art. 35 da Constituição da República Portuguesa prevê que: "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a

---

[68] ESPANHA. *Constituição Federal. 27 de dezembro de 1978*. Disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf. Acesso em: 09 jan. 2020. "Art. 18. 1. Garante-se o direito à honra, à intimidade pessoal e familiar e à própria imagem. 2. O domicílio é inviolável. Nenhuma entrada ou registro poderão ser feitos sem o consentimento do titular ou determinação judicial, salvo caso de flagrante delito. 3. Garante-se o sigilo das comunicações, especialmente as postais, telegráficas e telefônicas, salvo mediante decisão judicial. 4. A lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos, e o pleno exercício de seus direitos." (Tradução livre). "*Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*." (Tradução livre).

[69] FERNÁNDEZ, Dora García. El derecho a la intimidad. *Dereito*. México, 2010, v. 19, n.º 2, pp. 269-284, pp. 278-279. ISSN 1132-9947. "Ainda assim, o Tribunal Constitucional Espanhol estabeleceu que este direito à intimidade deriva da dignidade da pessoa, reconhecida no artigo 10, fração 1 da Constituição espanhola, e estende-se não apenas à vida pessoal do próprio indivíduo, mas também aos aspectos da vida pessoal daqueles indivíduos com os quais possui uma estreita relação familiar, como cônjuges, pais, filhos, irmãos, etc. Assim, na doutrina espanhola, o direito à intimidade, tanto pessoal quanto familiar, possui as seguintes características: 1. É originário e inerente à pessoa. 2. É absoluto. 3. É extrapatrimonial. 4. É irrenunciável. 5. É imprescritível." (Tradução livre). "*Asimismo, el Tribunal Constitucional Español estableció que este derecho a la intimidad deriva de la dignidad de la persona, reconocida en el artículo 10, fracción 1 de la Constitución Española, y se extiende no sólo a la vida propia personal del individuo sino a los aspectos de la vida personal de aquellos individuos con los que tiene una estrecha relación familiar como pueden ser cónyuges, padres, hijos, hermanos etc. Es así que en la doctrina española el derecho a la intimidad, tanto personal como familiar, tiene las siguientes características: 1. Es originario e inherente a la persona. 2. Es absoluto. 3. Es extrapatrimonial. 4. Es irrenunciable. 5. Es imprescriptible*."

[70] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 143. "Como é sabido, a Constituição portuguesa consagra, no art. 26, n.º 1, o direito à reserva da intimidade da vida privada e familiar. Por seu turno, o art. 80, n.º 1, do Código Civil dispõe que todos devem guardar reserva quanto à intimidade da vida privada de outrem. Tanto a Constituição como o Código tutelam, pois, entre outros valores ligados à personalidade humana, a *privacidade – hoc sensu*, a vida íntima ou privada de cada um –, a qual dele ser preservada contra intromissões alheias, que se traduzam, v.g., na divulgação não autorizada de fatos a ela respeitantes."

sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei".

Quanto aos dados sensíveis,

> a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis[71].

Observa-se que a legislação portuguesa possui natureza negativa nesse aspecto, especialmente no sentido de se abster do tratamento de dados de terceiros[72].

Importante destacar a existência de diferenças culturais no interior da própria União Europeia. Sob tal ótica, é possível citar, a título exemplificativo, o caso da França, cuja Lei para uma República Digital trata os direitos relacionados à pessoa interessada ou titular do direito, bem como aqueles relacionados ao conteúdo de tais direitos, de forma distinta do tratamento conferido pelo recente Regulamento Geral de Proteção de Dados da União Europeia[73].

Por fim, conclui-se que as normas francesas, alemãs, espanholas e portuguesas, citadas anteriormente, são apenas alguns exemplos da forma como o direito à privacidade repercutiu sobre a produção normativa de países europeus, denotando preocupação geral com a proteção dos dados pessoais dos cidadãos, apesar de alguns Estados conservarem certas peculiaridades.

Ainda que países membros da União Europeia compartilhem a origem da ideia de privacidade em comum com os Estados Unidos, baseada no artigo *The Right to Privacy*,

---

[71] PORTUGAL. *Constituição da República Portuguesa*. Art. 35, n.º 3. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 17 abr. 2020.

[72] AMORIM, Ana. O direito à privacidade e a evolução tecnológica: a propósito da publicidade com recurso ao reconhecimento facial. *In*: ANJOS, M. R.; AZEVEDO, P. A.; GONÇALVES, R. M.; VEIGA, F. S. (Eds.). *Atualidades na Ciência Jurídica:* Intercâmbio Ibero-Americano. Maia, Portugal: Ed. Ismai, 2018, pp. 269-276. Disponível em: http://hdl.handle.net/11328/2836. Acesso em: 05 mar. 2020. "Este direito à autodeterminação informativa tem, sobretudo, uma natureza negativa, que permite impedir o acesso aos dados pessoais por terceiros, traduzindo ainda uma garantia do direito à privacidade consagrado genericamente no art. 26 da Constituição da República Portuguesa e no artigo 5.º, inc. X da Constituição Federal do Brasil."

[73] MARTIAL-BRAZ, Nathalie. Op. cit., maio 2018, p. 86. No texto são analisados ambos os aspectos citados, em maiores detalhes, demonstrando a existência de diferenças culturais dentro da União Europeia e o papel das Diretivas em orientar a produção normativa em direção a uma maior harmonia: "Embora haja uma certa movimentação legislativa para a proteção de dados pessoais na Europa e na França, todos os textos adotados não são necessariamente unânimes, principalmente no que concerne aos direitos das pessoas interessadas. Assim, a adoção do Regulamento Geral de Proteção de Dados (RGPD), no dia 27 de abril de 2016 [...] reconheceu e consagrou certos direitos a favor das pessoas interessadas, em termos diferentes daqueles permitidos pela Lei para uma República Digital (LRD), de 7 de outubro de 2016 (*Loi pour une République Numérique*)."

publicado em 1890 por Warren e Brandeis[74], abordando o "*right to be let alone*"[75], as perspectivas se desenvolveram de formas distintas. Inicialmente, a privacidade teria sido marcada por um individualismo exacerbado, consubstanciado na ideia do direito de ser deixado só, com a ausência de comunicação entre um sujeito e os demais[76].

Partindo dessa ideia, a concepção de privacidade passou a ser crescentemente pensada como um aspecto fundamental da realização da pessoa e do desenvolvimento de sua personalidade, até seu atual entendimento na condição de direito fundamental. Durante esse processo, a inserção de um direito à privacidade em ordenamentos de cunho eminentemente patrimonialista fizeram dela uma prerrogativa reservada a estratos sociais determinados[77].

Enquanto a legislação dos Estados-membros da União Europeia apresenta um caráter eminentemente abrangente (com a ressalva já feita sobre a existência de divergências entre os ordenamentos jurídicos nacionais), a estadunidense pode ser considerada setorial. Conforme apontado, os países da União Europeia foram marcados pela Segunda Guerra Mundial, o que justifica a preocupação com a proteção dos dados

---

[74] WARREN, Samuel D.; BRANDEIS, Louis D. Op. cit., 1890, p. 193.

[75] LAFER, Celso. A reconstrução dos direitos humanos: a contribuição de Hannah Arendt. *Estudos Avançados*. São Paulo, ago. 1997, v. 11, n.º 30, pp. 55-65, p. 63. "Para Hannah Arendt, coerente com o seu entendimento do público como o comum e o visível, o privado, na dimensão da intimidade, é aquilo que é exclusivo do ser humano na sua individualidade e, não sendo de interesse público, não deve ser divulgado. A intimidade, como um direito autônomo da personalidade, foi articulada conceitualmente por Rousseau como resposta do indivíduo ao conformismo nivelador da sociedade, aquilo que Hannah Arendt qualifica como 'o surgir do social'. Na fundamentação de sua tutela, entendo que Hannah Arendt oferece como critério para limitar o direito à informação o princípio de exclusividade. Esse critério, articulado nos seus textos *Reflections on Little Rock* e *Public rights and private interests*, é compatível com os preceitos kantianos de publicidade, por ela esposados, à medida que a intimidade enquanto *the right to be let alone* não envolve direitos de terceiros."

[76] SHILS, Edward. Privacy. Its constitution and vicissitudes. *In*: *Law and Contemporary Problems*. Durham, Carolina do Norte, EUA: Duke Law University, LCP, 1966, v. 31, n.° 2, pp. 281-306, p. 281. "A privacidade é uma "*zero-relationship*" entre duas pessoas ou entre um grupo e uma pessoa. É uma "*zero-relationship*" no sentido em que é constituída pela ausência de interação ou comunicação ou percepção dentro de contextos nos quais tais interações, comunicações ou percepções são praticáveis – como, por exemplo, em uma situação ecológica comum, como aquela que surge da continuidade especial ou pertencimento em uma única coletividade acolhedora, como a família, um grupo de trabalho, e, em última instância, toda uma sociedade. A privacidade pode ser aquela de um único indivíduo, mas pode ser também de dois indivíduos, três ou mais. Mas é sempre a privacidade dessas pessoais, singulares ou plurais, via-a-vis outras pessoas." (Tradução livre). "*Privacy is a "zero-relationship" between two persons or two groups or between a group and a person. It is a "zero-relationship" in the sense that it is constituted by the absence of interaction or communication or perception within contexts in which such interaction, communication, or perception is practicable-i.e., within a common ecological situation, such as that arising from spatial contiguity or membership in a single embracing collectivity such as a family, a working group, and ultimately a whole society. Privacy may be the privacy of a single individual, it may be the privacy of two individuals, or it may be the privacy of three or numerous individuals. But it is always the privacy of those persons, single or plural, vis-a-vis other persons."*

[77] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 5. Neste ponto, o autor faz referência a alguns casos de grande relevância e que dispõem de certo distanciamento temporal, dos quais são exemplos: *Pope v. Curl*, 26 Eng. Rep. 608 (1741); *Prince Albert v. Stange* 64 ER 293 (1848); *Tribunal Civil de la Seine*, 16 jun. 1858, D.P. 1853.3.62.

pessoais dos cidadãos e eventuais abusos[78]. Os direitos relacionados à privacidade são tidos como indisponíveis, inadmitindo-se sua cessão a terceiros. Nesse contexto, a atuação dos processadores de dados depende estritamente de autorização legal, com presunção de proibicionismo.

O resultado é uma abordagem abrangente da privacidade, inserida em um sistema cuja autoridade deriva inicialmente dos valores e direitos fundamentais, da forma como são articulados em instrumentos internacionais de direitos humanos e em documentos constitutivos. À lei superior é dada eficácia por meio de legislações nacionais ou supranacionais, bem como de regulamentações administrativas, e a sua aplicação ocorre em todos esses níveis.

É nesse contexto que se insere a Diretiva de 1995[79] da União Europeia, a qual visava eliminar os obstáculos para a circulação de dados de caráter pessoal no âmbito da União, harmonizando o nível de proteção dos direitos e liberdades fundamentais[80]. Considerou-se, então, o fato de que cada país oferecia um nível de proteção aos distintos dados pessoais, de menor ou de maior grau, vetando a transferência de dados àqueles países que não tinham essa mesma proteção considerada adequada[81].

---

[78] PELTZ-STEELE, Richard J. The pond betwixt: differences in the US-EU data protection/safe harbor negotiation. *Journal of Internet law* [1094-2904], 2015, v. 19, pp. 14-30, pp. 20-25. "A atração romântica da Europa à proteção de direitos fundamentais a coloca em um paradigma de direitos. A dignidade pessoal e a autonomia são ditadas pela forma como a informação apresenta a identidade de um indivíduo ao mundo. Assim, o interesse legal de uma pessoa persiste em relação à informação, enquanto esta é repassada. O indivíduo mantém o direito de direcionar e controlar o uso daquela informação, e mesmo de retirá-la do mercado. […] a ética dominante de responsabilidade social na tradição cultural da lei e política na Europa pós-Segunda Guerra tende a colocar a privacidade em um paradigma de direitos humanos. Neste paradigma, os indivíduos possuem, passivamente, proteção dos seus interesses pelo Estado e pelos demais cidadãos." (Tradução livre). "*Europe's romantic attraction to fundamental rights frames data protection in a rights paradigm. Personal dignity and autonomy are dictated by how information presents one's identity to the world. Accordingly, a person's legal interests persist in information as it flows downstream from one pair of hands to the next. The individual retains rights to direct and control the use of that information, and even to recall it from the marketplace. […] the dominating ethic of social responsibility in the cultural tradition of law and policy in post-World War II Europe tends to frame privacy in a paradigm of human rights. In this paradigm, individuals are entitled passively to some protection of their interests by the state and by their fellow citizens.*"

[79] UNIÃO EUROPEIA. *Directive 95/46/EC.* European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.

[80] SOULIER, Jean-Luc; SLEE, Sandra. La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques. Perspective française. *Revue Internationale de Droit Comparé,* abr./jun. 2002, v. 54, n.° 2, pp. 663-676, p. 665. Disponível em: http://www.persee.fr/doc/ridc_0035-3337_2002_num_54_2_18761 Acesso em: 17 abr. 2020. Os autores explicam que a Diretiva de 1995 utiliza o termo "*donnée à caractere personnel*" para designar todo tipo de informação concernente a uma pessoa física identificada ou identificável, denominada "*personne concernée*". Como exemplo de dados pessoais protegidos pela Diretiva, são citadas as informações coletadas por empresas, relativas principalmente a clientes, fornecedores, correspondentes e assalariados.

[81] BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. The Datasphere and the Law: New Space, New Territories. *Revista Brasileira de Políticas Públicas* (Brazilian Journal of Public Policy). Direito e o Mundo Digital, dez. 2017, v. 7, n.º 8. "Diferentemente de qualquer outra esfera, a tecnosfera é implementada em todo

A Diretiva de 1995 revelou-se incisiva, afetando especialmente a atividade de empresas com atuação fora do território da União Europeia, e impedindo o envio de dados e informações a países terceiros, caso não houvesse proteção minimamente adequada a tais dados. Cumpre esclarecer que as diretivas, no âmbito da União, desempenham o papel de direcionamento das produções normativas nacionais, servindo como orientação para o processo legislativo de cada Estado-membro[82].

Nesse caso, cada Estado-membro conserva o poder de livre apreciação para avaliar o nível de proteção oferecida. Da mesma forma, a Diretiva de 1997[83] regrou os contratos celebrados à distância, com implicações sobre o direito de ser informado e sobre o direito de retratação do consumidor[84].

---

o planeta. Por mais surpreendente que possa parecer de início, também está se tornando cada vez mais independente da decisão humana, assim como as demais esferas. A sua autonomia é alavancada pela dependência das nossas sociedades em relação à operação da tecnosfera, sem a qual nossas vidas na Terra seriam consideravelmente mais restritas, conjuntamente com a complexidade de sua organização. […] A datasfera coloca muitos desafios às diferentes construções legislativas (tanto pública quanto privada, em níveis local, nacional, europeu internacional, e transnacional). […] O desenvolvimento de tecnologias de comunicação e informação, como smartphones, e os numerosos sensores espalhados pelos espaços público e privado, promoveram a digitalização de uma quantidade considerável de dados sobe a atividade humana, e sobre o mundo ao nosso redor de uma forma geral." (Tradução livre). "*Like the other spheres, the technosphere is deployed across the entire planet. As surprising as might seem at first, it is also becoming increasingly independent of human decision in much the same way as the other spheres. Its autonomy is advanced further by the dependence our societies place on the technosphere's operation, without which our lives on Earth would be considerably more restricted, together with the complexity of its organization. [...] The datasphere poses many challenges to the various constructions of the law (both public and private, at local, national, European, international and transnational level). [...] The development of information and communication technologies, such as smartphones and the numerous sensors spread across the public and private space, has promoted the digitalization of a considerable quantity of data on human activity and on the world around us in general. [...].*"

[82] JAYME, Erik. Direito Internacional Privado e Cultura pós-moderna. *Cadernos da Pós-Graduação em Direito da UFRGS*. 2. ed. Porto Alegre: PPGDir, 2004, pp. 105-114, p. 112. "Mister algumas palavras sobre a diretiva: afinal, o que é uma diretiva no direito europeu? Bem, a Diretiva é um ato legislativo da comunidade que vincula os Estados ao que concerne à finalidade da diretiva, obrigando os Estados-Membros a transpô-la nos sistemas nacionais. Os Estados, porém, ficam livres para determinar que medidas serão tomadas para atender essa diretiva. É uma legislação – podemos afirmar pós-moderna – porque há três textos que assumem simultaneamente importância para resolver os casos: em primeiro, há a lei nacional, que transpõe a diretiva; em segundo, a diretiva em si e suas normas, porque o juiz é livre para interpretar a lei nacional à luz do direito europeu (logo, da Diretiva); em terceiro, existem os considerandos das diretivas (preâmbulos semelhantes aos dos Tratados Internacionais), os quais fixam sua finalidade e são importantes porque motivam a norma internacional. Os considerandos são muito importantes porque no direito comunitário europeu, as diretivas sem motivação são nulas. Então, são três textos a consultar para resolver um só caso."

[83] UNIÃO EUROPEIA. *Directive 97/66/EC*. European Parliament and the Council concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 15 Dec. 1997.

[84] DREXL, Josef. Le commerce électronique et la protection des consommateurs. *Revue Internationale de Droit Économique*, 2002/2 (t. XVI), doiI 10.3917/ride.162.0405. Disponível em: http://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm Acesso em: 17 abr. 2020. A respeito da Diretiva de 1997, o autor explica que: "Ampliando a concepção tradicional da Internet, o legislador comunitário harmonizou o direito dos Estados-membros com as regras específicas que atribuem direitos individuais aos consumidores. A diretiva sobre os contratos à distância de 1997 [...], que, em matéria de proteção contratual do consumidor, prevê, sobretudo o direito de informação e o direito de retratação do consumidor, é central na política comunitária de proteção do consumidor na Internet." (Tradução livre).

No ano de 2000, o direito à privacidade foi incluído na redação do art. 7º da Carta de Direitos Fundamentais da União Europeia[85], com a posterior celebração do Tratado de Lisboa[86], em 2007[87]. Ainda, com a vigência da Carta de Direitos Fundamentais da União Europeia e de suas disposições específicas, a abordagem defendida por tais regras[88] adquiriu caráter de direito constitucional fundamental[89].

O art. 8º da mesma Carta[90] reconheceu o direito à proteção de dados pessoais como um novo direito fundamental, diferente daquele previsto no art. 7º. Dessa forma, o artigo em questão prevê, além do direito à proteção de dados pessoais, o requisito de que dados sejam processados a partir de finalidades específicas, e a partir do consentimento do indivíduo envolvido, ou com outra base legal. Finalmente, prevê, ainda, o direito de acesso aos dados, assim como de retificar erros a partir do controle de uma autoridade independente.

"*Élargissant sa conception traditionnelle à Internet, le législateur communautaire a harmonisé le droit des États membres par des règles strictes attribuant des droits individuels aux consommateurs. La directive sur les contrats à distance de 1997 [...], qui, en matière de protection contractuelle du consommateur, prévoit surtout le droit d'être informé et un droit de rétractation du consommateur, est centrale en politique communautaire de protection du consommateur sur Internet.*"

[85] UNIÃO EUROPEIA. *Charte des droits fondamentaux de l'Union européenne* (Carta dos Direitos Fundamentais da União Europeia), 2000, C 364/01. Journal Officiel des Communautés Europénnes. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_fr.pdf. Acesso em: 17 abr. 2020. "*Article 7. Respect de la vie privée et familial. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.*"

[86] UNIÃO EUROPEIA. Conference of the Representatives of the Governments of the Member States. *Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community.* 2007/C 306/01, art. 16B, Dec. 13, 2007. Disponível em: https://www.refworld.org/docid/476258d32.html. Acesso em: 17 abr. 2020.

[87] Sobre a evolução do direito comunitário europeu e sua interação com o Direito Internacional Privado: MOURA RAMOS, Rui Manuel Gens de. Introdução ao Direito Internacional Privado da União Europeia: da interação originária do direito internacional privado e do direito comunitário à criação de um direito internacional privado da União Europeia. *In*: MOURA RAMOS, Rui Manuel Gens de; MONACO, Gustavo Ferraz de Campos (Coords.). *Aspectos da unificação europeia do Direito Internacional Privado.* São Paulo: Intelecto, 2016.

[88] Os conceitos específicos relativos à proteção de dados encerrados pela Carta de Direitos de 2000 (processamento de dados limitado e consensual, acesso e retificação de dados, e independência supervisória) são os mesmos princípios defendidos pelo regime europeu de proteção de dados estabelecido pela Diretiva de 1995.

[89] ROTENBERG, Marc. Updating the law of information privacy: the new framework of the European Union. *Harvard Journal of Law and Public Policy* [0193-4872], 2013, v. 36 iss: 2, p. 608.

[90] UNIÃO EUROPEIA. Op. cit., 2000/C 364/01. "Artigo 8. Proteção dos dados pessoais. 1. Toda pessoa possui o direito à proteção dos dados pessoais que lhe concernem. 2. Tais dados devem ser tratados fielmente, observando-se os fins determinados como base para o consentimento do indivíduo, ou em virtude de outro fundamento legítimo previsto em lei. Toda pessoa possui o direito de acesso aos dados coletados que lhe dizem respeito, bem como de obter sua retificação. 3. O respeito às presentes regras submete-se ao controle de uma autoridade independente." (Tradução livre) "*Article 8. Protection des données à caractère personnel. 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante*."

As ideias de consentimento e de legítimo interesse são centrais nas legislações protetivas de dados, e são consideradas pressupostos para que o tratamento seja considerado lícito, com bases que o justifiquem. O **consentimento** relaciona-se à informação do usuário e à autorização para coleta, processamento e compartilhamento de dados pessoais, sendo entendido como instrumento de autodeterminação informacional[91]. Uma autorização automática e genérica não basta para demonstrar que o titular dos dados consentiu livremente com o seu tratamento, tampouco para garantir que o consentimento se deu com finalidade específica e determinada.

A autorização que expressa o consentimento do titular dos dados deve, portanto, ser livre (afastar consentimentos automáticos ou obrigatórios), informada (restar claro quais dados serão coletados e qual a finalidade do seu tratamento) e inequívoca (com verdadeira compreensão e aceitação dos termos).

O conceito de **finalidade**, por conseguinte, também é central para as legislações protetivas de dados, pois delimita o tratamento dos dados coletados e transferidos àquele fim com o qual o titular dos dados consentiu inicialmente[92], limitando-se igualmente à transferência de dados a terceiros. Desse modo, ainda que o consentimento seja válido, se a finalidade extrapolar a inicialmente acordada, o tratamento não será considerado legítimo.

O objetivo é garantir ao indivíduo protagonismo no controle de seus dados, contudo, é questionável a suficiência do consentimento no contexto da Sociedade da Informação. Muitas vezes, para que o usuário possa ter acesso a determinado serviço é imprescindível a coleta de alguns de seus dados pessoais. Nesse aspecto, torna-se difícil afirmar que o consentimento foi livremente manifestado pelo titular dos dados.

É possível, também, propor reflexões acerca de questões ligadas aos direitos de personalidade, e os limites existentes para a sua cessão. A partir do momento em que tais

---

[91] GOMES, Rodrigo Dias de Pinho. *Desafios à privacidade:* Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf. Acesso em: 04 jan. 2020. "Com razão se afirmou que 'o consentimento é o pilar regulatório adotado para a proteção de dados pessoais', funcionando, desde a década de 1990 na Europa, como ponto de partida a legitimar e justificar a licitude da coleta, tratamento e análise de dados pessoais do titular. O regulamento 2016/679 do Parlamento Europeu e do Conselho faz reacender essa chama em diversas passagens, trazendo o instituto do consentimento como a chave mestra do cofre que dá acesso aos dados pessoais, porém contemplando novas formas, além dele, que conferem licitude ao tratamento de dados."

[92] Em caso de alteração na finalidade do tratamento, suas condições, ou no seu compartilhamento, é imprescindível que o titular dos dados seja informado para que o consentimento se conserve como legítimo, reservando-se ao indivíduo o direito de revogação do consentimento dado anteriormente. Ainda, esta revogação independe de alterações, e deverá poder ser feita a qualquer momento, mediante manifestação expressa do titular.

direitos são tidos como fundamentais e indisponíveis, passam a existir limites para o tratamento de dados pessoais.

O **legítimo interesse** está igualmente relacionado ao princípio da finalidade, podendo ser utilizado como uma das bases para o tratamento de dados. Trata-se, ao final, do reconhecimento de que outras partes podem ter interesse no tratamento dos dados coletados. O tratamento pode se basear no consentimento, citado anteriormente, no legítimo interesse (sem necessidade de consentimento ou autorização expresso pelo titular), ou em bases de controle. O desafio, no entanto, reside na delimitação do que se configura como interesse efetivamente legítimo[93].

A avaliação da legitimidade no tratamento dos dados é subjetiva, devendo ser feita caso a caso pelas autoridades de controle e proteção de dados. Com as Diretivas de proteção de dados, cada Estado-membro da União Europeia passou a ser encarregado do estabelecimento de uma autoridade pública responsável pelo monitoramento e aplicação, dentro do seu território, das provisões adotadas no âmbito da União Europeia[94]. Tais autoridades deveriam ser dotadas de poderes investigativos e efetivos de intervenção, e do poder de ajuizar ações judiciais quando observadas violações.

Também era seu dever responder a demandas realizadas por qualquer cidadão, e gerar relatórios periódicos regulares de suas atividades. O mecanismo criado pelas Diretivas europeias foi aprimorado e, em maio de 2018, passou a vigorar o novo Regulamento Geral de Proteção de Dados (RGPD) da União Europeia[95], substituindo a Diretiva e a Lei de Proteção de Dados anteriormente vigentes[96].

Cumpre destacar que o Regulamento prevê expressamente, em seus considerandos, níveis de proteção homogêneos e coerentes entre todos os Estados-membros da União

---

[93] BIONI, Bruno Ricardo. *Proteção de dados pessoais.* A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[94] ROTENBERG, Marc. Op. cit., 2013, pp. 622-623.

[95] UNIÃO EUROPEIA. *Regulamento 2016/679.* Regulamento Geral sobre a Proteção de Dados. Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/45/CE. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020.

[96] RESINA, Fernando *et al.* Cloud – A lei e a prática: guia e perguntas frequentes. Coimbra: Almedina, 2016, p. 69. "O objetivo do Regulamento, [...], é o de adotar um regime de proteção dos dados pessoais que *(i)* sejam mais coerentes em todos os Estados-membros, dado que, embora pese a Diretiva 95/46/CE, os Estados-membros da União Europeia continuam a ter diferenças significativas em termos de dados pessoais (por exemplo, desde logo, em matéria de requisitos de segurança que devem ser cumpridos), o que conduziu à fragmentação do mercado interno, e *(ii)* responda melhor aos desafios colocados pelas tecnologias digitais (desde logo, pela inexistência de fronteiras que resulta da Internet e serviços *cloud*)."

Europeia[97]. Não obstante o nível de proteção equivalente ali previsto, há exceções quanto à aplicação de multas (coimas) com base no texto do Regulamento, já que "os sistemas jurídicos da Dinamarca e Estônia não conhecem as coimas tal como são previstas"[98] no RGPD, restando, portanto, a obrigação de aplicação de multas efetivas, proporcionais e dissuasivas.

São adotados diferentes tipos de atos legislativos pela União, alguns de caráter vinculante e outros não, assim como podem ser aplicáveis a todos os Estados-membros ou não[99]. A proteção de dados foi tratada inicialmente no âmbito das Diretivas anteriormente mencionadas; conforme o próprio nome sugere, Diretivas são atos legislativos que visam

---

[97] UNIÃO EUROPEIA. *Regulamento 2016/679*. Op. cit. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020. Conforme consta expressamente nos considerandos do Regulamento (RGPD), a proteção ali prevista deve ser homogênea e coerente em ***todos*** os Estados-membros da União: "Considerando o seguinte: [...] (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogênea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. [...] (13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores econômicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controle coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros. [...] (22) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado na União. [...]."

[98] Id., ibid. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020. "Considerando o seguinte: [...] (151) Os sistemas jurídicos da Dinamarca e da Estónia não conhecem as coimas tal como são previstas no presente regulamento. As regras relativas às coimas podem ser aplicadas de modo que a coima seja imposta, na Dinamarca, pelos tribunais nacionais competentes como sanção penal e, na Estónia, pela autoridade de controle no âmbito de um processo por infração menor, na condição de tal aplicação das regras nestes Estados-Membros ter um efeito equivalente às coimas impostas pelas autoridades de controlo. Por esse motivo, os tribunais nacionais competentes deverão ter em conta a recomendação da autoridade de controle que propõe a coima. Em todo o caso, as coimas impostas deverão ser efetivas, proporcionadas e dissuasivas. (152). Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro."

[99] UNIÃO EUROPEIA. *Tratado sobre o Funcionamento da União Europeia*. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-1aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 08 mar. 2020. "Art. 288. Para exerceram as competências da União, as instituições adotam regulamentos, diretivas, decisões, recomendações e pareceres."

fixar um objetivo geral a ser alcançado por todos os Estados-membros[100]. Os Regulamentos, como o RGPD, por outro lado, são atos legislativos vinculantes, cujos elementos são aplicáveis a todos os Estados-membros da União[101].

Cabe, ainda, neste momento, destacar o conteúdo do art. 6º do Regulamento que, ao tratar sobre a licitude do tratamento de dados, dispõe claramente que os

> Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados [...], determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, [...][102].

Apesar de permitir expressamente iniciativas legislativas nacionais, visando adaptar as regras do RGPD, o texto do art. 6º não afasta o caráter do Regulamento de norma geral, vinculante e diretamente aplicável: há, tão somente, a permissão de que os legisladores nacionais complementem o texto do Regulamento ou o especifiquem, sem confundi-lo com as Diretivas, que indicam o caminho a ser seguido pelos Estados-membros.

A abordagem adotada nas Diretivas da União, antes mesmo do RGPD, caminhava em uma direção oposta àquela defendida pelos Estados Unidos[103]: enquanto a

---

[100] Id., ibid. As Diretivas vinculam os Estados-membros destinatários quanto a um objetivo em particular, deixando espaço para que as instâncias nacionais determinem a forma e os meios para alcançar o resultado estipulado pela diretiva em questão: "Art. 288. [...] A diretiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios." Deste modo, há, necessariamente, a prévia transposição da Diretiva para o direito interno, a partir de iniciativa do legislador nacional, e somente após tal transposição os cidadãos daquele Estado-membro em particular adquirem direitos e obrigações decorrentes da diretiva. Há, contudo, prazos para transposição das diretivas, os quais devem ser respeitados pelos Estados-membros aos quais são aplicáveis. Excepcionalmente, o TJUE admite que determinadas disposições podem produzir efeitos diretos em um Estado-membro quando a transposição não tenha sido efetuada, ou o tenha sido feito de forma incorreta, e quando as disposições da Diretiva forem imperativas e suficientemente claras e precisas, permitindo a sua invocação por particulares (TJUE, Andrea Francovich e o. contra República Italiana, C-6/90 e C-9/90).

[101] Id., ibid. Os Regulamentos, no âmbito da União, têm caráter geral e obrigatório, sendo obrigatórios e aplicáveis diretamente em todos os seus elementos, desde a sua entrada em vigor, não havendo a necessidade de transposição por meio de ato nacional, como ocorre no caso das Diretivas. Consequentemente, disposições nacionais incompatíveis com regulamentos são automaticamente inaplicáveis a partir da entrada em vigor desses atos normativos. O objetivo dos regulamentos é garantir a uniformidade na aplicação do direito da União, em todos os Estados-membros: "Art. 288. [...] O Regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros."

[102] UNIÃO EUROPEIA. *Regulamento 2016/679*. Op. cit. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020. "Art. 6º. [...] 2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.º 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX."

[103] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 92. "Diferenças estas que se acentuam quando se toma como termo de comparação o Direito vigente nos Estados Unidos. Isto, nomeadamente, porque neste último país em lugar de um elenco exaustivo das limitações aos exclusivos jusautorais de

argumentação europeia era no sentido da proteção das informações pessoais dos seus cidadãos, os Estados Unidos advogavam pela maior liberdade na troca de informações, dispondo de uma legislação específica menos restritiva no que tange à privacidade[104]. A partir da Diretiva de 1995, portanto, tal distinção, que já vinha se delineando há algumas décadas, passou a ser explícita – assim como as suas consequências.

O resultado, na prática, foi que as Diretivas europeias passaram a obstar a transferência de dados de seus cidadãos a países cuja legislação de privacidade fosse por eles considerada insuficiente, ou seja, menos restritiva, como era o caso dos Estados Unidos, como se verá a seguir.

1.3 TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NOS ESTADOS UNIDOS

Os Estados Unidos partem de um modelo libertário de governo, em que os direitos fundamentais derivam de uma Constituição relativamente estática[105]. Assim, os direitos tutelados podem ser adaptados por meio da interpretação jurisprudencial, ou por meio de emendas, enquanto o papel exercido pelo governo deve ser correspondente ao ideal de Estado mínimo, culminando em uma legislação de caráter eminentemente negativo, que visa garantir a proteção das liberdades econômicas e sociais em relação a possíveis interferências. A ideia prevalecente é a de que os indivíduos são pessoalmente

---

utilização e exploração de obras e prestações em rede, como o que a Directiva 2001/29/CE estabelece, vigora uma genérica excepção a esses exclusivos, fundada no *fair use* dos bens em causa; e porque a responsabilidade dos prestadores intermediários de serviços em rede é aí limitada pelo sistema dito de 'notificação e retirada' (*notice and take down*), de um modo geral mais propício à preservação em rede de conteúdos alegadamente ofensivos do que o regime comunitário de imputação de danos a esses agentes económicos sempre que estes tenham ou devam ter conhecimento do carácter ilícito da informação que armazenam."

[104] DREXL, Josef. Op. cit., 2002/2. A abordagem norte-americana daria um maior peso à autonomia do indivíduo, à sua capacidade de fazer valer seus interesses, e às possibilidades de autorregulação, em oposição à abordagem europeia, designada como tradicional.

[105] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 63. "Nos Estados Unidos da América observa-se não existir iniciativa central a respeito dos conflitos *online*, estando a matéria dispersa em decisões judiciais no conjunto dos precedentes. [...]. Com maior nível de independência do que o verificado no Brasil, os Estados Federados nos Estados Unidos têm competência para ditar suas próprias leis de organização interna. Cada Estado, portanto, conta com suas regras de foro e estabelece regras gerais de jurisdição, abarcando também regras especiais de jurisdição sobre não residentes (denominados "*long-arm statutes*"). Porém, algumas regras gerais permanecem no âmbito federal e devem ser respeitadas pelos Estados. Notadamente, a Constituição dos Estados Unidos da América institui alguns mandamentos, entre eles a 14ª Emenda, que estabelece o princípio do devido processo legal e a proteção da lei àqueles sob a jurisdição dos Estados Unidos, também entendido como direito de não ser julgado por autoridades ilegítimas."

responsáveis pelas suas escolhas, como forma de manifestação de sua autonomia individual[106].

Cumpre observar duas características presentes no contexto norte-americano e que influenciam a abordagem da privacidade naquele país: o federalismo e a existência de direitos civis negativos. Nas situações em que houve ação do Estado a privacidade se manifestou como valor constitucional sob três dimensões: o direito à autonomia pessoal[107], o "*right to be let alone*"[108] e o direito à privacidade da informação[109]. Ainda que a

[106] PELTZ-STEELE, Richard J. Op. cit., 2015, v. 19, p. 20. "O melhor governo é aquele que governa menos, de modo que a operação da lei é amplamente negativa, a fim de assegurar que as liberdades econômica e social sejam protegidas de interferências. As funções da lei consistem principalmente de sua capacidade corretiva, reagindo a injustiças, e nivelando novamente as condições. A autonomia individual prospera na liberdade, deixando as pessoas responsáveis por suas próprias escolhas, obtenham elas sucesso ou não." (Tradução livre). "*Government is best that governs least, so the operation of law is largely negative, to ensure that social and economic liberties are protected from interference. Law functions primarily in a corrective capacity, reacting to wrongs by re-leveling the playingfield. Individual autonomy flourishes on liberty, rendering persons responsible for their own choices, whether successful or unsuccessful*."

[107] Nos casos em que o valor constitucional da privacidade foi entendido sob o prisma da autonomia pessoal, houve uma aproximação da visão europeia, que a coloca como um interesse básico de dignidade. É essa abordagem da privacidade como autonomia que é levada em consideração nas discussões relativas ao aborto, a casos relativos a decisões médicas, à recusa de tratamento e ao suicídio assistido.

[108] ESTADOS UNIDOS. Amendment IV. Disponível em: https://constitution.congress.gov/constitution/amendment-4/. Acesso em: 17 abr. 2020. "Não será infringido o direito do povo à inviolabilidade de sua pessoa, casas, papéis e haveres, contra buscas e apreensões irrazoáveis e não se expedirá mandado a não ser mediante indícios de culpabilidade, confirmados por juramento ou declaração, e nele se descreverão particularmente o lugar da busca e as pessoas ou coisas que tiverem de ser apreendidas." (Tradução livre). "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*." A abordagem da privacidade como o "direito de ficar só" ("*right to be let alone*"), ou direito ao isolamento, possui ligação com a Carta de Direitos, de 1791, cuja Quarta Emenda prevê uma "expectativa razoável de privacidade" ("*reasonable expectation of privacy*"). As críticas a tal abordagem, contudo, são no sentido de que meramente uma expectativa razoável seria incompatível com um direito fundamental, e que ela restaria especialmente reduzida no ambiente *online*, em especial quando se considera a "*third-party doctrine*" em contextos nos quais as informações pessoais são voluntariamente cedidas a terceiros.

[109] FLAHERTY, David H. On the utility of constitutional rights to privacy and data protection. *Case Western Reserve Law Review*, 1990-1991, v. 41, pp. 831-855, pp. 837-838. "A qualificação relevante, no entanto, é que a Suprema Corte jamais realizou uma ampla descoberta geral sobre um direito constitucional à privacidade, como alguns comentaristas esperavam que ocorresse na década de 1960, tampouco foi a Constituição explicitamente alterada para esse efeito, ou consta tal alteração na agenda de alguém. Assim, os americanos não têm um direito constitucional federal explícito à privacidade, em contraste com a situação em alguns Estados. A Constituição da Califórnia, alterada em 1972, estabelece que os residentes do Estado têm direito à privacidade: 'Todas as pessoas são por natureza livres e independentes e têm certos direitos inalienáveis, entre os quais os de desfrutar e defender a vida e a liberdade; adquirir , possuir e proteger a propriedade e buscar e obter segurança, felicidade e privacidade'." (Tradução livre). "*The important qualification, however, is that the Supreme Court has never made a broad general finding of a constitutional right to privacy, as some commentators had expected it to do in the 1960s, nor has the Constitution been explicitly amended to this effect, nor is it on anyone's agenda, nor has it even been contemplated. Thus, Americans do not have an explicit federal constitutional right to privacy, in contrast to the situation in some states. The California Constitution, as amended in 1972, provides that residents of the state have a right to privacy: 'All people are by nature free and independent, and have certain inalienable rights, among which are those of enjoying and defending life and liberty; acquiring, possessing, and protecting property; and pursuing and obtaining safety, happiness, and privacy'."*

Constituição não faça menção explícita à privacidade, isto não obstou o seu desenvolvimento como conceito constitucional.

Dário Moura Vicente aponta que Estados Unidos e União Europeia divergem não apenas

> no tocante à disciplina substantiva da produção, utilização e transmissão de informação por meios electrônicos, [mas] que se registram hoje relevantes diferenças entre as ordens jurídicas nacionais: elas se estendem à própria relevância conferida neste domínio à produção normativa estadual, a qual é claramente diferenciada na Europa e nos Estados Unidos da América, em virtude do papel preponderante atribuído neste último país à chamada autorregulação[110].

Especificamente quanto às informações pessoais que constam em registros ou documentos públicos, a Suprema Corte dos Estados Unidos[111] teria proclamado que a "zona de privacidade" constitucionalmente protegida se estende especificamente a duas espécies de interesse[112]: (1) privacidade decisória, definida pela Corte como "independência para tomar certas decisões importantes" ("*independence in making certain kinds of important decisions*"); e (2) privacidade de informação, definida pela Corte como "o interesse individual em evitar a divulgação de assuntos pessoais" ("*the individual interest in avoiding disclosure of personal matters*").

Tal análise ocorreu no julgamento do caso *Whalen v. Roe*[113], marco inicial do reconhecimento da existência de um direito constitucional à privacidade de informação nos Estados Unidos[114]. A partir de então se iniciou o desenvolvimento da privacidade de informação como conceito constitucional[115].

---

[110] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 92.

[111] FLAHERTY, David H. Op. cit., 1990-1991, pp. 831-855. "A história do reconhecimento judicial do direito à privacidade na Constituição dos Estados Unidos é importante porque indica o contexto em que os tribunais têm maior probabilidade de reconhecer demandas de privacidade. As demandas de direitos à privacidade são reconhecidas em litígios federais ao menos desde o final do século XIX, mas apenas em Griswold v. Connecticut que o juiz Douglas, escrevendo o parecer para o tribunal, afirmou a existência de um direito de privacidade contra o Estado anterior à *Bill of Rights*. Douglas argumentou que várias emendas à Constituição incorporavam explícita e implicitamente uma série de proteções aos interesses da privacidade." (Tradução livre). "*The history of the judicial recognition of the right to privacy under the United States Constitution is important because it indicates the context in which courts are more likely to acknowledge privacy claims. Claims to privacy rights have been recognized in federal litigation at least since the late nineteenth century, but it was only in Griswold v. Connecticut that Justice Douglas, writing the opinion for the court, asserted the existence of a right of privacy against the state predating the Bill of Rights. Douglas argued that several amendments to the Constitution explicitly and implicitly embodied a series of protections for privacy interests*."

[112] SOLOVE, Daniel J. Access and aggregation: public records, privacy and the Constitution. (Modern Studies in Privacy Law). *Minnesota Law Review* [0026-5535], 2002, v. 86, iss: 6, p. 25.

[113] WHALEN v. ROE, 429 U.S. 589 (1977); Nixon v. Administrator of Gen. Servs., 433 U.S. 425 (1977); NASA v. Nelson, 562 U.S. 134 (2011).

[114] 429 U.S. 589. Whalen v. Roe (n. 75-839). Argued: October 13, 1976. Decided: February 22, 1977. Nesse caso, a Suprema Corte concluiu que: "Não desconhecemos a ameaça à privacidade implícita no acúmulo de

Sob o ponto de vista norte-americano, as relações estabelecidas entre pessoas e atores comerciais nos Estados Unidos são questões contratuais e de propriedade[116]. Tal raciocínio leva ao entendimento de que informações pessoais podem ser vistas como propriedade, permitindo que cessem os direitos do indivíduo sobre elas se vendidas ou

---

grandes quantidades de informações pessoais em bancos de dados computadorizados ou em outros arquivos governamentais massificados [...]. O direito de coletar e usar esses dados para fins públicos é acompanhado por um dever estatutário ou regulamentar concomitante de evitar divulgações injustificadas [...]. Em algumas circunstâncias, esse dever possivelmente tem suas raízes na Constituição [...].” (Tradução livre). “*We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files [...]. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures [...]. In some circumstances that duty arguably has its roots in the Constitution [...].*”

[115] CITTADINO, Gisele. *Pluralismo, Direito e Justiça Distributiva:* elementos da filosofia constitucional contemporânea. 4. ed. Rio de Janeiro: Lumen Juris, 2009, pp. 22-25. De fato, há um debate relevante nos Estados Unidos acerca da forma como a Constituição deve ser concretizada, e sobre como os conceitos constitucionais devem ser desenvolvidos. Uma de suas facetas é elucidada na obra de Gisele Cittadino, que explica em seu texto as principais visões no que se refere à forma de tornar juridicamente eficazes as normas constitucionais – e, por conseguinte, o que se refere ao desenvolvimento e evolução dos conceitos constitucionais. Sob esse aspecto, opõem-se a corrente interpretativista – mais liberal, e que parte do pressuposto de que uma sociedade democrática e liberal se caracteriza pelo pluralismo, resultando na submissão da *law of judges* ao *rule of law* – e a corrente não interpretativista – que autoriza o Judiciário na tarefa de interpretar a Constituição, a recorrer aos valores substantivos da comunidade, bem como a princípios jurídicos, no intuito de julgar conforme o “projeto de constituição” .

[116] FLAHERTY, David H. Op. cit., 1990-1991, pp. 831-855, pp. 834-835. Quanto ao direito à privacidade da informação, trata-se de abordagem aceita pela Suprema Corte norte-americana em três ocasiões, nas quais se decidiu que o acesso público a informações pessoais restava suficientemente justificado. “A distinção essencial entre proteção de privacidade e proteção de dados ou privacidade de informações não é frequentemente compreendida, especialmente na América do Norte. A proteção de dados preocupa-se especialmente com o controle da coleta, uso e disseminação de informações pessoais. Desde 1970, as legislaturas na Europa e na América do Norte têm respondido a temores generalizados sobre o impacto dos computadores na coleta, vinculação e uso de dados ao aprovar leis de proteção. Essas leis buscam principalmente controlar a coleta, o uso e a disseminação de informações pessoais pelo governo por meio de códigos de práticas justas de informações. A Lei de Privacidade dos Estados Unidos [*Privacy Act*] de 1974 é um exemplo importante e influente de uma lei de proteção de dados. A Lei de Proteção de Dados da Inglaterra [*Data Protection Act*] de 1984 tem a vantagem, no mundo de língua inglesa, de ser devidamente intitulada. Embora o objetivo do ato seja proteger a privacidade, a palavra nunca aparece nela. Isso é uma melhoria no uso da palavra privacidade em uma lei sem qualquer tentativa de definição. Além dessas leis gerais, a maioria dos países, e especialmente os Estados Unidos, elaborou legislação setorial específica que aplica práticas gerais de informações justas a questões precisas de proteção de dados. Tais estatutos gerais e específicos estão dando, atualmente, a contribuição mais significativa para a proteção de todas as formas de privacidade individual nas sociedades industriais avançadas.” (Tradução livre). “*The essential distinction between privacy protection and data protection, or informational privacy, is not commonly understood, especially in North America. Data protection is especially concerned with controlling the collection, use, and dissemination of personal information. Since 1970 legislatures in Europe and North America have responded to widespread fears about the impact of computers on data collection, linkage, and use by enacting protective laws. These laws primarily seek to control the government's collection, use, and dissemination of personal information by means of codes of fair information practices. The United States' Privacy Act of 1974 is a leading and influential example of a data protection law. England's Data Protection Act of 1984 has the advantage, in the English-speaking world, of being properly titled. Although the goal of the act is to protect privacy, the word never appears in it. This is an improvement on using the word privacy in a law without any attempt at definition. In addition to such general laws, most countries, and especially the United States, have fashioned specific sectoral legislation that applies general fair information practices to precise data protection issues. Such general and specific statutes are making the most significant contribution to the protection of all forms of individual privacy in advanced industrial societies today*.”

cedidas, enquanto as limitações oferecidas aos processadores de dados são restritas e sujeitas a uma presunção de permissibilidade[117].

A abordagem contratualista do direito à privacidade da informação norte-americana fez com que a Suprema Corte, por vezes, tenha se deparado com o chamado "*secrecy paradigm"*, ou paradigma do sigilo[118]. O Judiciário refutou o reconhecimento da existência de um direito constitucional à privacidade de informação em relação a dados que tenham sido anteriormente divulgados ou que constem em registros públicos[119].

Quanto à lei aplicável a determinado litígio, são duas as principais vertentes defendidas nos Estados Unidos: a livre escolha, por um lado e, por outro, a ausência de escolha de lei aplicável, limitando a aplicabilidade do princípio da autonomia da vontade às obrigações contratuais, que seriam as únicas a permitir a escolha da lei aplicável[120].

Resta evidente, portanto, a importância da qualificação dos dados, seja na condição de bens imateriais ou na de direitos, contratuais ou não, já que a lei que rege o bem e a que

---

[117] PELTZ-STEELE, Richard J. Op. cit., 2015, p. 25. "Conforme explicado acima, a ética dominante da responsabilidade pessoal na tradição cultural das leis e políticas dos EUA tende a enquadrar a privacidade em um paradigma de contrato e propriedade. Nesse paradigma, os indivíduos agem afirmativamente, para barganhar e proteger seus próprios interesses. O papel do governo é ficar fora do caminho, e o papel da lei é garantir que isso aconteça. Se existe um lugar para a lei, é no sentido de realizar uma correção ou remediação, quando os acordos são violados. Consequentemente, as informações pessoais são uma mercadoria e os dados pessoais podem ser vendidos, licenciados ou doados." (Tradução livre). "*As explained above, the dominating ethic of personal responsibility in the cultural tradition of US law and policy tends to frame privacy in a paradigm of contract and property. In this paradigm, individuals act affirmatively, to bargain for and protect their own interests. The role of government is to stay out of the way, and the role of law is to make sure that it does. If there is a place for law, it is as a corrective, or remediation, when agreements are broken. Accordingly, personal information is a commodity, and personal data may be sold, licensed, or given away*."

[118] SOLOVE, Daniel J. Op. cit., 2002, p. 17.

[119] Walls v. City of Petersburg (1990); Scheetz v. Morning Call, Inc., (1991); Cline v. Rogers (1996).

[120] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 65-66. "Diferentemente do Regulamento Roma I, da União Europeia, que conta com regra expressa sobre a escolha de lei aplicável, nos Estados Unidos o tema é mais disperso. Para os estadunidenses não existe codificação uniforme para reger a matéria em todo o país, a qual é relegada aos precedentes dos distintos tribunais dos Estados Federados e ao *Restatement Second of Conflict of Laws*, documento sem força vinculante, ou que é aplicado com força de lei em apenas alguns Estados Federados. O *Restatement Second of Conflict of Laws* estabelece que a lei escolhida pelas partes é a lei que disciplina o contrato. Contudo, a liberdade de escolha pode ser limitada se ela não guardar uma relação de vínculos mais estreitos com a relação jurídica ou contrariar uma norma fundamental do Estado. Vê-se, dessa forma, que existe um elemento condicionante de relação do contrato com a lei aplicável. Dispositivo similar é também encontrado no *Uniform Commercial Code* (UCC), uma sistematização de normas comerciais adotada pelos Estados Federados, e que prevê o poder das partes para escolha da lei aplicável ao contrato – de maneira geral, vez que não há regra específica para as transações eletrônicas. Verifica-se, igualmente, que existem regras especiais para transações na internet, como contratos de compra e venda e de licença de *software*, contidas no *Uniform Information Transaction Act* (UCITA). Ainda que adotado por apenas dois estados norte-americanos, o UCITA prevê a eleição de lei aplicável a essas modalidades de contratos, contempladas as ressalvas da matéria de proteção ao consumidor. No silêncio das partes, alguns dispositivos normativos suprem a ausência de escolha da lei aplicável. No caso do UCC, escolhe-se a relação mais significativa ao contrato. O *Restatement Second of Conflict of Laws*, por sua vez, instrui que, na ausência de determinação, será aplicada a lei local do Estado, quando o local de celebração e o do cumprimento do contrato encontram-se no mesmo Estado."

rege a obrigação poderão ou não coincidir. Assim, conceituar e classificar os dados é passo imprescindível para a definição da lei aplicável, de maneira que a lei adequada poderá variar a depender do ordenamento em questão e da classificação de dados, especialmente quanto ao meio digital. Mais adiante serão analisadas em maiores detalhes as implicações da qualificação dos dados tratados como bens ou como direitos.

Em 28 de junho de 2018 foi aprovado o *California Consumer Privacy Act* (CCPA)[121], estatuto estadual[122] que visa aumentar a proteção da privacidade dos consumidores no Estado da Califórnia (Estados Unidos), em vigor desde 01 de janeiro de 2020[123]. As normas tratam do princípio da transparência, já que impõem a necessidade de o indivíduo saber que seus dados estão sendo coletados, bem como se são vendidos ou repassados a terceiros.

Consta, ainda, expressamente, o direito de acesso aos dados coletados, bem como o direito de negar a sua venda. O princípio da não discriminação pelo exercício dos direitos relativos à privacidade também é abordado, sendo reservado ao titular o direito de solicitar a exclusão dos seus dados. A iniciativa californiana tem sido bem recebida, já que garante aos indivíduos maior controle sobre suas informações pessoais, e por representar um maior alinhamento com a proteção conferida no âmbito da União Europeia[124].

---

[121] ESTADOS UNIDOS. *The California Consumer Privacy Act (CCPA).* AB375. 2018. Disponível em: https://www.isipp.com/resources/full-text-of-the-california-consumer-privacy-act-of-2018-ccpa/ Acesso em: 07 jan. 2020.

[122] ESTADOS UNIDOS. *Illinois – Biometric Information Privacy Act (BIPA).* (740 ILCS 14/). Disponível em: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 Acesso em: 18 abr. 2020. Neste ponto, cumpre destacar, também, a existência da Biometric Information Privacy Act, BIPA, no Estado de Illinois, considerada uma das normas mais rigorosas no que se refere à privacidade de crianças on-line no país, demonstrando preocupação dos legisladores estadunidenses em regulamentar o ambiente digital, destacando-se a autonomia que os Estados possuem para tanto. Contudo, por tratar-se de norma restrita a questões de biometria, optou-se por priorizar a análise do CCPA.

[123] O CCPA se aplica a quaisquer empresas que realizam a coleta de dados e cujos negócios são realizados na Califórnia, desde que: (i) o lucro anual da empresa exceda US$ 25 milhões; (ii) vendam ou comprem dados pessoais de 50 mil ou mais lares (*households*) ou consumidores; ou (iii) devam mais de metade dos lucros anual à venda de informações pessoais dos consumidores.

[124] LAPOWSKY, Issie. Bill Could Give Californians Unprecedented Control Over Data. *Wired*, 22 jun. 2018. Disponível em: www.wired.com/story/new-privacy-bill-could-give-californians-unprecedented-control-over-data. Acesso em: 17 abr. 2020: "Os legisladores da Califórnia apresentaram uma lei de privacidade abrangente ao legislador estadual que daria aos californianos controle sem precedentes sobre seus dados e controlaria o poder de seus vizinhos do Vale do Silício. Apresentado pelo membro da Assembleia Estadual Ed Chau e pelo senador estadual Robert Hertzberg, o projeto permitiria que os residentes da Califórnia descobrissem o que as empresas de informações e os corretores de dados coletam sobre eles, de onde essas informações vêm e como são compartilhadas. Isso daria às pessoas o poder de solicitar a exclusão de seus dados e ordenar que as empresas parassem de vender suas informações pessoais. Ele [*o CCPA*] impõe limites à venda de dados de usuários com menos de 16 anos de idade e proíbe as empresas de negar serviço aos usuários por exercerem seus direitos sob a fatura. [...] O projeto de lei da Califórnia se une a uma onda de interesse internacional na legislação de privacidade, principalmente diante da aprovação do Regulamento Geral de Proteção de Dados na União Europeia, que exige que as empresas articulem claramente quais dados estão coletando, obtenham o consentimento do usuário e ofereçam aos usuários uma portabilidade cópia de seu registro se solicitado, entre outras coisas. Com essa legislação, Chau e Hertzberg esperam dar aos

O CCPA não cria novas obrigações administrativas, mas visa reduzir os riscos específicos de privacidade criados pelo comércio de dados no Estado da Califórnia. Assim, enquanto o RGPD, no âmbito da União Europeia, protege qualquer informação relacionada a um indivíduo identificável, o CCPA leva em consideração também os lares ou famílias.

Enquanto na Califórnia o CCPA é restrito aos dados de indivíduos ali residentes, relevando um âmbito de incidência material circunscrito ao território daquela unidade da Federação americana, na União Europeia são protegidos todos e quaisquer dados que por lá circulem[125].

Cumpre ressaltar, contudo, certas críticas, especialmente no âmbito da incidência material da norma californiana[126]: apesar de prever direitos aos consumidores e aos

---

californianos alguns dos mesmos direitos e proteções que os europeus desfrutam agora." (Tradução livre). "*Lawmakers in California have introduced a sweeping privacy bill to the state legislature that would give Californians unprecedented control over their data and rein in the power of their Silicon Valley neighbors. Introduced by State Assembly member Ed Chau and state senator Robert Hertzberg, the bill would allow California residents to find out what information businesses and data brokers collect about them, where that information comes from, and how it's shared. It would give people the power to ask for their data to be deleted and to order businesses to stop selling their personal information. It places limits on selling data on users younger than 16 years of age, and prohibits businesses from denying service to users for exercising their rights under the bill. [...]. The California bill joins a wave of international interest in privacy legislation, most notably the passage of the General Data Protection Regulation in the European Union, which requires companies to clearly articulate what data they're collecting, obtain user consent, and give users a portable copy of their record if requested, among other things. With this legislation, Chau and Hertzberg are hoping to give Californians some of the same rights and protections that Europeans now enjoy."*

[125] BAHL, Aman; BHARSAKLE, Sarthak. The Privacy Jungle – Comparative Study of the Indian Personal Data Protection Act, 2018, with EU GDPR and California Privacy Law. *Indian Journal of Law and Public Policy (IJLPP),* dez. 2019. Disponível em: https://ijlpp.com/the-privacy-jungle-comparative-study-of-the-indian-personal-data-protection-act-2018-with-eu-gdpr-and-california-privacy-law/. Acesso em: 06 jan. 2020. "As repercussões do GDPR foram vistas na forma de vários blogueiros, organizações sem fins lucrativos e empresas menores que ficaram *offline* porque não conseguiram atender aos vários novos requisitos. No entanto, uma diferença notável é que o CCPA protege os dados pertencentes apenas a seus residentes, enquanto o GDPR administra [...] qualquer processamento de dados pessoais nos territórios locais, como, por exemplo, dentro da UE, ou no território indiano, que inclui o processamento de dados pessoais, pertencentes a pessoas que residem em países que não sejam os referidos países, conforme o caso. Assim, esta lei se aplica a empresas estrangeiras que não apenas coletam informações sobre os residentes, mas também se elas processam dados pessoais estrangeiros em território europeu ou indiano." (Tradução livre). "*The repercussions of the GDPR were seen in the form of multiple bloggers, non-profit organizations and smaller businesses turning offline, because they could not meet with the several new requirements. However, a noteworthy difference is that CCPA protects the data belonging to only of its residents whereas the GDPR [...] administer any processing of personal data on the local territories, i.e. within the EU or Indian territory, which includes processing of personal data pertaining to persons residing in countries other than that of the said countries as the case maybe. Thus, this law applies to foreign companies which not only collect information about residents, but also if they merely process foreign personal data on European or Indian territory*."

[126] CHRISTENSEN, Katie. The California Consumer Privacy Act of 2018: are your interests at stake? *Golden Gate University School of Law – GGU Law Review Blog*. 10 jan 2018. Disponível em: https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1055&context=ggu_law_review_blog.
Acesso em: 06 jan. 2020. "É consensual entre os defensores dos consumidores e os analistas de negócios que a CCPA em seu estado atual é insatisfatória. Por exemplo, Justin Brookman, diretor de política de privacidade e tecnologia da União do Consumidor, considera a CCPA 'modesta' em relação aos direitos do consumidor [...] e deve ser ampliada. Brookman prevê que empresas em todo o país [...] adotem os padrões

titulares dos dados de uma forma geral, os termos são considerados vagos, deixando ampla margem para interpretação[127]. É preciso reconhecer a importância da flexibilidade das normas, especialmente em um contexto tão fluido, e ressaltar os problemas que podem advir de regras demasiadamente vagas. De todo modo, nos Estados Unidos em geral, comparativamente à União Europeia, verifica-se uma tutela menos restritiva (e não necessariamente débil ou fraca) dos direitos da personalidade e da privacidade[128].

---

da CCPA por questões práticas. Por outro lado, Robert Callahan, vice-presidente de assuntos governamentais da Associação da Internet, critica a CCPA e alega que ela foi escrita por um defensor da privacidade do consumidor sem veiculação pública adequada. Callahan argumenta que a CCPA e sua imposição de multas por violação são uma grande ameaça [...] para aqueles que desejam fazer negócios na Califórnia." (Tradução livre). "*It is mutually agreed, from both consumer advocates and business analysts, that the CCPA in its current state is unsatisfactory. For example, Justin Brookman, director of privacy and technology policy for the Consumer's Union, considers the CCPA to be "modest" in regard to consumers rights [...] and should be expanded. Brookman predicts that companies throughout the nation [...] will adopt the standards of the CCPA for practical concerns. Contrastingly, Robert Callahan, Vice President of State Government Affairs for the Internet Association, criticizes the CCPA and claims it was writen by a consumer privacy advocate without proper public veing [...]. Callahan argues that the CCPA and its imposition of fines for violation is a major threat [...] to those who wish to do business in California*."

[127] MANN, Drake. The California Consumer Privacy Act of 2018: why it matters to clients in Arkansas. *The Arkansas Lawyer*, 2019, v. 54, n.° 1. Disponível em: https://www.gill-law.com/wp-content/uploads/2019/03/Mann-proof-edited-locked.pdf. Acesso em: 06 jan. 2020. "Além disso, a definição de 'informações pessoais' da CCPA é notavelmente ampla e inclui informações capazes de serem associadas a, ou [que] poderiam ser razoavelmente vinculadas, mesmo que indiretamente, a um consumidor ou família em particular. [...] Se uma empresa do Arkansas hospeda um site que executa funções básicas de rastreamento (registra um endereço IP e identificadores de publicidade *online* para 50.000 ou mais californianos (ou domicílios da Califórnia), deve examinar atentamente o CCPA. […]. As pessoas, de um modo geral, não gostam de ser forçadas a fazer coisas – a história do atrito comercial com qualquer regulamentação governamental. As empresas do Arkansas podem esperar até que estejam sob a jurisdição da CCPA, do GDPR ou de alguma legislação federal futura, ou eles podem realizar apenas as mudanças que são obrigadas a fazer, ou, ainda, as empresas de Arkansas podem adotar uma atitude diferente, expressa por um escritor como a Regra de Ouro da Privacidade: 'que as empresas devem colocar os interesses das pessoas sobre as quais os dados se referem. à frente dos seus'." (Tradução livre). "*In addition, the CCPA's definition of "personal information" is notably broad and includes information "capable of being associated with, or [which] could reasonably be linked, even indirectly," with a particular consumer or household. [...] This, if an Arkansas company hosts a website that performs basic tracking functions (logs na IP address and online advertising identifiers for 50,000 or more Californians (or California households), it should look closely at the CCPA. [...] People, generally speaking, do not like being forced to do things, and the story of business chafing at any government regulation itself. Arkansas businesses can wait until they come under the jurisdiction of the CCPA, the GDPR, or some future federal legislation, and they can make only those changes they are forced to make. Or Arkansas businesses can adopt a different atitude – an atitude expressed by one writer as the Golden Rule of Privacy: 'that companies should put the interests of the people whom data is about ahead of their own'."*

[128] VAAS, Lisa. Two schoolkids sue Google for collecting biometrics. *Naked Security*. 07 abr. 2020. Disponível em: https://nakedsecurity.sophos.com/2020/04/07/two-schoolkids-sue-google-for-collecting-biometrics/. Acesso em: 18 abr. 2020. "Dois alunos processaram o Google, alegando que este está coletando ilegalmente impressões de voz, impressões faciais e outras informações de identificação pessoal (PII). Os estudantes foram identificados apenas como HK e JC na denúncia, que foi apresentada na quinta-feira em San Jose, CA, no Tribunal Distrital dos EUA do norte da Califórnia. [...] De acordo com o processo, mais da metade das crianças em idade escolar do país usa os produtos educacionais do Google, incluindo os de Illinois, a maioria com menos de 13 anos. Illinois entra em ação porque possui a mais rígida lei de privacidade biométrica do país: a Lei de Privacidade da Informação Biométrica (BIPA). O BIPA exige que entidades privadas – como o Google – obtenham consentimento informado antes de coletar nossa biometria, incluindo impressões faciais e de voz. A denúncia alega que o Google está violando o BIPA, e a mais rigorosa lei federal de privacidade de crianças *online* do país, a Lei de Proteção de Privacidade Online de

Em 26 de novembro de 2019, representantes do partido Democrata americano, sob liderança da senadora Maria Cantwell, apresentaram no Senado um abrangente projeto de lei federal sobre privacidade e proteção de dados. O projeto, à semelhança do CCPA[129], visa regulamentar as práticas comerciais das empresas de tecnologia em nível federal.

Submetido à discussão no Comitê de Comércio do Senado, em 04 de dezembro de 2019, o projeto prevê direitos aos consumidores, como o direito à informação (quais dados são coletados, com quem as informações são compartilhadas, e por qual motivo)[130]. Garante, também, o direito de exclusão ou correção dos dados, de modo que, se aprovado, o projeto aproximaria a legislação estadunidense de proteção de dados das normas europeias[131].

Crianças (COPPA). A COPPA exige que sites e serviços *online* divulguem total e claramente suas práticas de coleta, uso e divulgação de dados e que obtenham consentimento verificável dos pais antes de coletar, usar ou divulgar os dados que coletam de crianças menores de 13 anos." (Tradução livre). *"Two schoolchildren have sued Google, alleging that it's illegally collecting their voiceprints, faceprints and other personally identifiable information (PII). The students were identified only as HK and JC in the complaint, which was filed on Thursday in San Jose, CA, in the US District Court of Northern California. [...] According to the lawsuit, over half of the nation's school children use Google's education products, including those in Illinois, most of whom are under the age of 13. Illinois comes into play because it's got the strictest biometrics privacy law in the land: the Biometric Information Privacy Act (BIPA). BIPA requires private entities – like Google – to first get our informed consent before collecting our biometrics, including faceprints and voiceprints. The complaint alleges that Google's violating both BIPA and the nation's strictest federal online children's privacy law, the Children's Online Privacy Protection Act (COPPA). COPPA requires websites and online services to fully and clearly disclose their data collection, use, and disclosure practices and that they obtain verifiable parental consent before collecting, using, or disclosing the data they collect from children younger than 13."*

[129] ESTADOS UNIDOS. *Consumer Online Privacy Rights Act (Copra) of 2019*. Disponível em: https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf. Acesso em: 06 jan. 2020. "Todos os dias, dados pessoais são transmitidos de empresa para empresa, acumulados em perfis digitais e, em seguida, usados sem o conhecimento, entendimento ou consentimento do consumidor. Sem direitos e proteções significativos, os consumidores continuarão impotentes e vulneráveis ao abuso. À medida que nossos dispositivos se tornarem mais inteligentes e nossos perfis digitais se tornam mais precisos e poderosos, tais riscos irão aumentar." (Tradução livre). "*Every day, personal data is passed from company-to-company, amassed into digital profiles, and then used without consumer knowledge, understanding, or consent. Without meaningful rights and protections, consumers will continue to be powerless and vulnerable to abuse. As our devices become smarter, and our digital profiles become more precise and powerful, these risks will grow*."

[130] SAUNDERS, David; GLOVER, Allison. Insight: a Federal Privacy Bill May be Closer than Once Thought. *Bloomberg Law*, 14 fev. 2020. Disponível em: https://news.bloomberglaw.com/privacy-and-data-security/insight-a-federal-privacy-bill-may-be-closer-than-once-thought. Acesso em: 05 mar. 2020. Além do projeto apresentado pela senadora Maria Cantwell conjuntamente ao Partido Democrata, há dois outros projetos federais sobre o tema nos Estados Unidos: foi apresentado, além do *Copra*, o *Staff Discussion Draft do United States Consumer Data Privacy Act of 2019* (CDPA) pelo senador Roger Wicker, bem como um terceiro projeto, de iniciativa da *House Energy and Commerce Committee*. No texto em questão é realizada comparação entre as disposições dos três projetos que permanecem em tramitação.

[131] WARZEL, Charlie. Will Congress Actually Pass a Privacy Bill? *The New York Times*. 10 dez. 2019. Disponível em: https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html Acesso em: 06 jan. 2020. "Pouco antes do Dia de Ação de Graças, a senadora Maria Cantwell introduziu a Lei de Direitos de Privacidade Online do Consumidor. [...] A Electronic Frontier Foundation era geralmente a favor, mas tinha apreensões em torno de um ponto: 'A COPRA satisfaz duas das três principais prioridades da EFF para a legislação federal de privacidade de dados do consumidor: aplicação privada pelos próprios consumidores; e nenhuma preempção de leis estaduais mais fortes. A COPRA dá um passo parcial em direção à terceira

1.4 *SAFE HARBOR AGREEMENT* E *PRIVACY SHIELD*

Os conceitos de privacidade e proteção de dados pessoais foram incorporados a partir do final da Segunda Guerra Mundial: a palavra "privacidade" surgiu, em termos legislativos, em 1948, com a Declaração Universal dos Direitos Humanos, elaborada no seio das Nações Unidas[132]. A partir da Convenção Europeia de Direitos Humanos, de 1950[133], porém, o Conselho da Europa delimitou abordagem diferente da estadunidense.

O art. 8º da Convenção Europeia de Direitos Humanos resguarda o direito à privacidade, e autoriza a limitação pública quando "necessário em uma sociedade democrática". Nesse ponto, a legislação europeia apresenta caráter ativo, impondo deveres e obrigações ao Estado para garantir proteção aos seus cidadãos[134].

A partir da década de 1960 houve uma mudança na concepção individualista de privacidade relacionada ao direito de ser deixado só, possivelmente em decorrência do surgimento de novas dinâmicas associadas à informação[135]. Em consequência, a

---

prioridade da EFF: não há esquemas de *pagamento pela privacidade*. [...].' Realidades legislativas à parte, há algumas razões para otimismo. Os projetos de Cantwell e Wicker não são tão distantes. Embora eu não tenha visto todos os detalhes da lei de Wicker, os dois parlamentares estão olhando muito para a proteção de dados. Ambos parecem achar que a FTC deveria ter mais poder executório. Tudo isso é um passo adiante das discussões anteriores sobre Hill, que se concentraram principalmente em questões teóricas, como se o projeto de lei deveria ser modelado segundo o RGPD da União Européia. Diante de tais desentendimentos, há certa sensação de progresso." (Tradução livre). "*Just before Thanksgiving, Senator Maria Cantwell introduced the Consumer Online Privacy Rights Act. [...] The Electronic Frontier Foundation was generally in favor but had misgivings around one point: "COPRA satisfies two of EFF's three key priorities for federal consumer data privacy legislation: private enforcement by consumers themselves; and no preemption of stronger state laws. COPRA makes a partial step towards EFF's third priority: no "pay for privacy" schemes." [...]. Legislative realities aside, there's some reason for optimism. The Cantwell and Wicker bills are not really that far apart. While I haven't seen the full details of the Wicker bill, both lawmakers are looking at data protections much more granularly. Both seem to think the F.T.C. ought to have more power to enforce. This is all a step forward from previous discussions on the Hill, which focused largely on theoretical issues like whether the bill should be modeled after the European Union's G.D.P.R. Seeing these disagreements feels a bit like progress."*

[132] ONU. Organização das Nações Unidas. *Declaração Universal dos Direitos Humanos*. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 05 mar. 2020.

[133] UNIÃO EUROPEIA. Conselho da Europa. *Convenção Europeia de Direitos Humanos.* 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 05 mar. 2020.

[134] Sobre a evolução do direito comunitário europeu e sua interação com o Direito Internacional Privado, ver: MOURA RAMOS, Rui Manuel Gens de. Op. cit., 2016.

[135] EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. O direito à privacidade na sociedade da informação. *In*: LIMA, Alberto Jorge de Barros; NETTO, Antonio Alves Pereira; SOTTO-MAYOR, Lorena Carla Santos Vasconcelos; LIMA NETO, Manoel Cavalcante de (Orgs.). *I Encontro de Pesquisas Judiciárias da Escola Superior da Magistratura do Estado de Alagoas – ENPEJUD:* Poder Judiciário: estrutura, desafios e concretização dos direitos. Maceió: Fundesmal, 2016. Disponível em: http://enpejud.tjal.jus.br/index.php/exmpteste01/article/view/63/44. Acesso em: 04 jan. 2020. "A privacidade apresenta vários perfis que não se excluem entre si, mesmo o clássico "direito de ser deixado em paz" não perdeu sua utilidade totalmente, mas o perfil que mais se adequa à sociedade da informação é aquele apresentado por Rodotà, a privacidade como o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir a sua própria esfera particular. Sob o manto da privacidade abrigam-se a intimidade (intimidade em sentido estrito e vida privada), o sigilo, a imagem e a proteção de dados pessoais. A

informação pessoal adquiriu maior importância[136], e foi relacionada com dois fatores que figuram quase sempre entre as justificativas para a utilização de informações pessoais: o controle e a eficiência[137].

Os dados pessoais foram pioneiramente utilizados pelo Estado: com a finalidade de garantir uma administração pública eficiente, seria necessário conhecer a população a ele submetida a partir da coleta de dados e informações, por vezes de forma compulsória[138].

Até então a utilização de dados e informações fora da esfera estatal era limitada, principalmente por razões estruturais, considerando a desproporção de meios dos organismos privados em relação ao Estado[139]. O desenvolvimento de novas tecnologias capazes de coletar, transferir e armazenar informações resultou na redução de custos, o que, por sua vez, viabilizou a criação de bancos de dados por organismos particulares, não apenas públicos, trazendo novas possibilidades de utilização pelo Estado[140].

---

extimidade integra a intimidade, sendo mais um complemento desta e não um direito autônomo, sendo que o exercício da limitação da própria intimidade não figura como renúncia a este direito."

[136] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. Danilo Doneda aponta que o direito à privacidade não mais se estrutura em torno do eixo "pessoa-informação-segredo", inserido no paradigma da "*zero-relationship*", mas sim no eixo "pessoa-informação-circulação-controle". No caso, o que se observa é a modificação da estrutura do eixo do paradigma exposto, de modo que o segredo em torno das informações do indivíduo é convertido na sua circulação, e em seu respectivo controle.

[137] CEYHAN, Ayse. Technologization of Security: management of uncertainty and risk in the age of biometrics. *Surveillance & Society*, 2008, v. 2, n.º 5, p. 109. "Defino tecnologias de identificação como sistemas atrelados, trabalhando juntos para coletar, processar, armazenar e disseminar informações para permitir que os agentes da lei realizem, em sua tomada de decisões, a coordenação, controle, análise e visualização de tais informações. Eles reúnem, processam e disseminam todos os identificadores capazes de identificar indivíduos." (Tradução livre). "*I define technologies of identification as in terrelated systems working together to collect, process, store and disseminate information to support law enforcement agents in their decision-making coordination, control, analysis and visualization. They gather, process and disseminate all identifiers capable of identifying individuals*."

[138] DONEDA, Danilo. Op. cit., 2006, p. 8.

[139] CEYHAN, Ayse. Op. cit., 2008, pp. 102-123, p. 103. "Tecnologias de identificação, vigilância e avaliação de riscos se tornaram a peça central das políticas de segurança desde o 11 de setembro. As tecnologias de segurança que eram utilizadas anteriormente em programas-piloto como controles de fronteira ou atribuições de benefícios sociais e em populações marginais específicas (principalmente imigrantes) ampliaram seu escopo para abranger toda a população, o que significa que todos os indivíduos estão sujeitos à identificação e vigilância tecnológicas. [...] Seguindo esta tendência, em 2004 a UE adotou o passaporte biométrico para os cidadãos da União e o visto biométrico para nacionais de países terceiros. Além disso, a imposição do passaporte biométrico pelo governo dos EUA a estrangeiros que buscam entrada no país contribuiu para a transformação da biometria em uma norma global de segurança (Salter 2006)." (Tradução livre). "*Identification technologies, surveillance and risk assessment have become the centerpiece of security policies since 9/11. Security technologies which were previously used in pilot programs such as border controls or welfare benefit attributions and on specific, marginal populations (mainly immigrants) have now broadened their scope to embrace the whole population, meaning that all individuals are subject to technological identification and surveillance. [...]. Following this trend, in 2004 the EU adopted the biometric passport for the citizens of the Union and the biometric visa for third country nationals. In addition to these, the US administration's imposition of the biometric passport to foreigners who seek entry into the country contributed to the transformation of biometrics into a global norm of security* (Salter 2006)."

[140] Id., ibid., p. 109.

Na década de 1970, a Convenção Europeia de Direitos Humanos mostrava indícios de que se tornaria ultrapassada e, na década seguinte, o Conselho da Europa adotou a *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, também conhecida como "Convenção 108"[141], que reconhecia a necessidade de reconciliar os valores fundamentais do direito ao respeito da privacidade e ao livre fluxo de informações entre os povos.

Na década de 1990 esboçava-se a discussão entre Estados Unidos e União Europeia, especialmente quando países europeus passaram a desenvolver regras específicas concernentes à coleta[142], transferência e proteção de informações pessoais sob a supervisão de agências regulatórias especificamente designadas para tal finalidade, denominadas "*data protection authorities*"[143], definidas mediante diretivas específicas a partir de 1995.

O fato de Estados Unidos e União Europeia assumirem posições distintas quanto à privacidade e à proteção de dados não implica em total impossibilidade de coexistência: a troca de dados e informações é possível mesmo quando a sua percepção é distinta[144] e ocorrer a partir de instrumentos específicos.

Exemplos disto são o *Safe Harbor Agreement*[145] (ou "Porto Seguro", em tradução para o português), decisão proferida no seio da Comissão das Comunidades Europeias no

---

[141] UNIÃO EUROPEIA. Conselho da Europa. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Jan. 28, 1981, Eur. T.S. n. 108 [Convention 108].

[142] Anteriormente foi exposta a evolução legislativa sobre o tema tanto no âmbito nacional de Estados-membros da atual União Europeia, quanto da própria União, especialmente a partir das diretivas de 1995 e de 1998, e do Regulamento Europeu de Proteção de Dados, em vigor desde 2018.

[143] UNIÃO EUROPEIA. *Directive 95/46/EC*. Op. cit., 1995.

[144] DOLINGER, Jacob; TIBURCIO, Carmen. *Direito Internacional Privado*. 15. ed. Rio de Janeiro: Forense, 2020, pp. 38 e ss. As atividades de caráter internacional que são objeto de convenções internacionais uniformizadoras das regras jurídicas que disciplinam determinada matéria, como é o caso do *Safe Harbor agreement*, constituem o chamado Direito Internacional Uniformizado, conforme concepção de Jacob Dolinger e Carmen Tiburcio.

[145] UNIÃO EUROPEIA. Comissão das Comunidades Europeias. Documento de trabalho dos serviços da Comissão sobre a aplicação da Decisão 520/2000/CE, de 26 de julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativo ao nível de proteção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce dos Estados Unidos da América*. Disponível em: https://ec.europa.eu/transparency/regdoc/ rep/2/2002/PT/2-2002-196-PT-1-1.Pdf. Acesso em: 05 mar. 2020. "[…] No exercício das competências que lhe são atribuídas pelo nº 6 do art. 25 da Directiva 95/46/CE, a Comissão adotou, em 26 de julho de 2000, a Decisão 2000/520/CE1 onde reconhece que os princípios internacionais de 'porto seguro', emitidos pelo *Department of Commerce dos Estados Unidos da América*, asseguram nível adequado de proteção dos dados pessoais transferidos a partir da Comunidade Europeia. A referida decisão foi previamente apresentada à apreciação do Parlamento Europeu, nos termos da Decisão 1999/468/CE do Conselho. A resolução do Parlamento, adotada em 5 de julho de 2000, solicitava a Comissão a garantir o acompanhamento do acordo de 'porto seguro' através da apresentação de relatórios periódicos sobre a sua aplicação ao Grupo de Trabalho criado nos termos do art. 29 e ao Comitê instituído pelo art. 31 da Directiva 95/46/CE, bem como à Comissão das Liberdades e dos Direitos dos Cidadãos, do Parlamento. Com o presente documento, a Comissão submete agora o relatório de final de 2001, prometido pelo Comissário Frits Bolkestein à referida Comissão. […] As recentes decisões da Comissão que aprovam cláusulas contratuais-tipo para a transferência de dados para países terceiros em nada prejudicam a validade do acordo de 'porto seguro', que deverá permanecer uma

ano de 2000[146], e declarada inválida em 2015, bem como seu substituto, o *E.U.-US Privacy Shield*[147], aqui considerados como marcos na oposição entre as duas concepções que, conforme tratado anteriormente, vinha se delineando já há alguns anos.

As implicações práticas das divergências entre Estados Unidos e Europa podem ser traduzidas em termos comerciais devido ao considerável benefício econômico ocasionado pela transferência de dados. Ao se impor a necessidade de uma solução, passou a ser negociado o *Safe Harbor Agreement* a partir de questões frequentemente elaboradas pelo Departamento de Comércio dos EUA sobre o tema da transferência de dados.

Dessa forma, entre 1998 e 2000, foram desenvolvidos os *Safe Harbor Privacy Principles*, elaborados com o objetivo de evitar que organizações particulares na União Europeia ou nos Estados Unidos que atuassem com a coleta e armazenamento de dados perdessem ou divulgassem acidentalmente tais informações[148], a partir do que seria considerado um "nível adequado" de proteção[149].

Como parte do *Safe Harbor*, empresas dos Estados Unidos se comprometeram a cumprir uma série de princípios básicos de privacidade, supervisionados e executados pela

---

opção atraente para as organizações elegíveis regularmente envolvidas em transferências de dados. […] Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho [...]. O nível adequado de proteção da transferência de dados a partir da Comunidade Europeia para os Estados Unidos da América (EUA), nos termos da presente decisão, pode conseguir-se se as organizações derem cumprimento aos princípios da 'privacidade em porto seguro' relativos à proteção de dados pessoais transferidos de um Estado-Membro para os EUA (a seguir denominados "os princípios") e as diretrizes das questões mais frequentes (a seguir designadas "FAQ") que servem de guia no que respeita à aplicação dos princípios estabelecidos pelo Governo dos Estados Unidos em 21 de julho de 2000. […] Os pareceres emitidos pelo grupo de trabalho "Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais", criado pelo art. 29 da Directiva 95/46/CE, sobre o nível de proteção facultado pelos princípios de 'porto Seguro' nos EUA, foram tidos em conta na preparação da presente decisão."

[146] UNIÃO EUROPEIA. *Comissão das Comunidades Europeias, 2000/520/EC*: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX: 32000D0520 & from=EM. Acesso em: 05 mar. 2020.

[147] KISS, Jemima. Privacy Shield deal lets US tech firms transfer European customers' data again. *The Guardian*, 08/07/2016. Disponível em: https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union. Acesso em: 17 abr. 2020.

[148] MOURA VICENTE, Dário Manuel Lentz de. *Direito Internacional Privado*. Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, pp. 148-149. "A aplicação destes preceitos suscita especiais dificuldades no tocante às transferências de dados para os Estados Unidos da América, onde, na falta de legislação de âmbito geral, a regulamentação da matéria é em larga medida deixada aos próprios interessados. Eis o que levou o Departamento de Comércio dos Estados Unidos a definir, em 21 de julho de 2000, na base de consultas com os respectivos destinatários, um conjunto de princípios, ditos de "porto seguro", sobre proteção da privacidade (*Safe Harbor Privacy Principles*), destinados a serem utilizados exclusivamente por organizações estabelecidas nos Estados Unidos que recebam dados pessoais oriundos da Comunidade Europeia."

[149] Id., ibid., p. 149. "A Comissão Europeia reconheceu esses princípios, pela Decisão 2000/520/CE, de 26 de julho de 2000, como susceptíveis de assegurar um 'nível adequado' de proteção dos dados pessoais transferidos para os Estados Unidos".

U.S. Federal Trade Comission. A partir de então, milhares de empresas passaram a utilizar as disposições do acordo como base para a realização de comércio transatlântico, assim como para a transferência de dados entre as diferentes jurisdições a partir da obtenção de autocertificações. Para isso, em 29 de setembro de 2000, o *Department of Commerce dos EUA* publicou informação sobre todas as diligências administrativas que as empresas deveriam realizar para garantir o registro como aderentes ao *Safe Harbor* ("Porto Seguro").

Em 01 de novembro do mesmo ano, o *Safe Harbor* passou a ser operacional, permitindo a autocertificação e a adesão por empresas norte-americanas que desejassem transferir e tratar dados da União Europeia. As medidas ali constantes foram de ação obrigatória aos Estados-membros da União, sendo necessária a implementação de todas as medidas necessárias à transferência de dados constantes no *Safe Harbor*[150], de modo a possibilitar a adesão (neste caso, voluntária) de empresas estadunidenses.

Assim, em julho de 2000, a Comissão das Comunidades Europeias divulgou a decisão que consagrou tais princípios[151], disposta na forma de seis artigos, somados a sete

[150] UNIÃO EUROPEIA. Comissão das Comunidades Europeias. Documento de trabalho dos serviços da Comissão sobre a aplicação da Decisão 520/2000/CE da Comissão, de 26 de julho de 2000. Op. cit. Disponível em: https://ec.europa.eu/transparency/regdoc/rep/2/ 2002/PT/2-2002-196-PT-1-1.Pdf. Acesso em: 05 mar. 2020. "[…] Os Estados-Membros foram obrigados a implementar todas as medidas necessárias às transferências de dados para as organizações norte-americanas registadas na lista do 'porto seguro' até 25 de outubro de 2000, ou seja, noventa dias após a data de notificação da decisão. Na maioria dos Estados-Membros não foi necessário alterar as regras em vigor. Na Suécia, a decisão foi transposta em 1 de janeiro de 2001 mediante alteração da lei sobre dados pessoais (1998:1191), na sua secção 12/13. Em 24 de novembro de 2000, a lei finlandesa sobre proteção de dados pessoais 986/2000 foi alterada para possibilitar a entrada em vigor das decisões da Comissão com base no nº 6 do art. 25 da diretiva. Na Bélgica, espera-se que nos próximos meses seja adotado um decreto real sobre transferência de dados transfronteiras. Até lá, a Decisão 2000/520/CE da Comissão tem efeito directo naquele país. Na Irlanda, enquanto se espera a publicação da lei que transpõe a Directiva 95/46/CEE, os arts. 25 e 26 da directiva serão transpostos por regulamentos que se encontram atualmente em fase de acabamento. Noutros casos, a implementação da decisão da Comissão que reconhece o nível adequado de protecção facultado pelo 'porto seguro' é efetuada pelas entidades nacionais responsáveis pela proteção de dados, conforme acontece em Itália. […] Embora o acordo de 'porto seguro' seja voluntário, não é exclusivamente baseado na autorregulamentação: tem por base a própria legislação norte-americana, sendo através da vigilância e de medidas de execução das autoridades públicas correspondentes nos EUA. Tais medidas, particularmente no que diz respeito às deficiências persistentes identificadas no presente relatório, garantirão a credibilidade do acordo e servirão os seus intentos, enquanto garantia de uma protecção adequada dos dados pessoais transferidos da UE para os EUA."

[151] PELTZ-STEELE, Richard J. The pond betwixt: differences in the US-EU data protection/safe harbor negotiation. *Journal of Internet Law* [1094-2904], 2015, v. 19, p. 21. "A proteção de dados garantida legalmente nos Estados Unidos está longe de ser 'adequada' para garantir a proteção de dados. Segundo os padrões da Diretiva da UE. Por conseguinte, a União Europeia e os Estados Unidos negociaram uma correção no Safe Harbor Agreement de 2000. Para garantir a integridade dos dados, e permitir sua transferência dos Estados da Diretiva para os Estados Unidos, as entidades receptoras de dados passaram a contar com a possibilidade de aderir a uma série de princípios acordados [...]." (Tradução livre). "*The patchwork of data protection law in the United States is far from "adequate" to ensure data protection to the standards of the EU Directive. Accordingly, the European Union and United States negotiated a fix in the 2000 Safe Harbor Agreement. To ensure the integrity of data transferred from Directive nations onward to the United States, receiving entities could pledge their allegiance to an agreed on series of principles […].*"

anexos[152]. Trata-se de texto relevante ao Espaço Econômico Europeu (EEE) ou *European Economic Area* (EEA), assim como o era a mencionada Diretiva de 1995 (revogada pelo RGPD), cuja relevância e aplicabilidade implicaram naqueles países[153].

O primeiro dos *Safe Harbor Principles* é o princípio da notificação ou comunicação (*notice*), segundo o qual os indivíduos devem ser informados sobre a coleta de seus dados e sobre como serão utilizados. Em seguida, há o princípio da escolha (*choice*), que implica na opção dos indivíduos de que seus dados não sejam mais coletados ou utilizados.

Em terceiro lugar há o princípio da transferência progressiva (*onward transfer*), o qual limita a transferência de dados a terceiros, caso esses não respeitem diretrizes básicas de proteção de dados. O princípio da segurança (*security*), por sua vez, prevê esforços para prevenir perda ou vazamento de dados coletados, e o princípio da integridade dos dados (*data integrity*) atrela a coleta de dados ao princípio da necessidade, conforme o uso ao qual é destinada.

Há, ainda, o princípio do acesso (*access*), segundo o qual indivíduos devem ter garantido o acesso a informações armazenadas a seu respeito, bem como solicitar a sua remoção ou correção, e o princípio do cumprimento ou aplicação (*enforcement*), que prevê meios eficazes para o cumprimento dos demais princípios.

A partir da decisão, em 2000 (conhecida por *Safe Harbour Decision*[154]), a transferência de dados de cidadãos da União Europeia a empresas norte-americanas passou a ser possível desde que preenchidos certos requisitos: as empresas norte-americanas que respeitassem os princípios elaborados e registrassem certificado atestando a sua

---

[152] UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *2000/520/EC*. Op. cit. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=EN. Acesso em: 05 mar. 2020.

[153] EEA-Lex. Disponível em: https://www.efta.int/eea-lex. Acesso em: 05 mar. 2020. Para tanto, é necessária a inclusão formal do texto no Acordo do EEE (ou seja, seus anexos ou protocolo), por uma decisão apartada. Todas as emendas podem ser encontradas no endereço ora indicado, bem como o texto completo do Acordo, datado de 1992.

[154] UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *2000/520/EC*. Op. cit. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=EN. Acesso em: 05 mar. 2020. Especificamente acerca da possibilidade de sobreposição de jurisdições e acerca da competência, destacam-se os seguintes trechos dos anexos à decisão: "Por último, coloca-se a questão da interligação da jurisdição da FTC (*Federal Trade Commission*) com a de outros serviços federais que garantem a aplicação da lei, particularmente nos casos em que essas jurisdições se sobrepõem. Temos vindo a desenvolver sólidas relações de trabalho com numerosos outros organismos desta natureza, incluindo os serviços bancários federais e os procuradores-gerais estaduais. É frequente coordenarmos investigações para maximizar os nossos recursos em instâncias cujas jurisdições se sobrepõem. É, também, frequente remetermos assuntos para o serviço federal ou estadual de investigação. […] Nos termos da alínea b) do n.º 2 do art. 1º, os entes públicos administrativos nos EUA com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulars, independentemente do seu país de residência ou da sua nacionalidade, sempre que exista incumprimento dos princípios em conformidade com as FAQ, são as seguintes: 1. A Federal Trade Commission; 2. O Department of Transportation. […]."

conformidade com os parâmetros europeus, poderiam transferir dados para os Estados Unidos.

Quanto à sua natureza jurídica, cumpre destacar que se trata de decisão proferida no âmbito da Comissão das Comunidades Europeias – diferenciando-se, portanto, das Diretivas e Regulamento abordados anteriormente. Tais decisões são vinculantes em relação aos seus destinatários específicos, sendo diretamente aplicáveis. No caso da "*Safe Harbour Decision*", trata-se de decisão expressamente relevante em todo o âmbito do Espaço Econômico Europeu[155], sendo obrigatória a sua observação por todos os Estados-membros da União, conforme já exposto anteriormente.

Em 2005, Dário Moura Vicente apontava, de forma lúcida, falhas no sistema criado pelos princípios do *Safe Harbor*:

> Pese embora a garantia pública assim dada ao método de autorregulação praticado nesta matéria nos Estados Unidos, bem como o seu reconhecimento pela Comissão Europeia, não é pacífica na doutrina nem a suficiência nem a fiabilidade do esquema descrito a fim de satisfazer as exigências da Directiva 95/46/CE em matéria de transferência internacional de dados[156].

Como resultado, no final de 2015, foi proferida decisão pelo Tribunal de Justiça da União Europeia (TJUE)[157], invalidando o *Safe Harbor*[158], que durante 15 anos estabeleceu as condições sob as quais poderia ser feita a transferência transatlântica de dados, especificamente entre Estados Unidos e União Europeia.

---

[155] UNIÃO EUROPEIA. Tratado sobre o Funcionamento da União Europeia. Op. cit. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-1aa75ed71a1.0019.01/DOC_3&format= PDF. Acesso em: 08 mar. 2020. "Art. 288. [...] A decisão é obrigatória em todos os seus elementos. Quando designa destinatários, só é obrigatória para estes."

[156] MOURA VICENTE, Dário Manuel Lentz de. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, pp. 149-150.

[157] Corte de Justiça da União Europeia, Luxemburgo, 6 de outubro de 2015, Julgamento no Caso C-362/14, Maximillian Schrems *v.* Data Protection Commissioner.

[158] CORREIA, Emanuella Chagas Jaguar. O efeito vinculante do reenvio prejudicial na União Europeia: um caminho para desenvolver o direito comunitário. *Revista de la Secretaría del Tribunal Permanente de Revisión*, 2014, año 2, n.° 4, pp. 65-82, p. 68. Considerando que os *Safe Harbour Principles* estão dispostos em decisão por parte da Comissão das Comunidades Europeias, como já exposto anteriormente, a decisão proferida pelo TJUE no sentido de sua revogação foi possível pois, conforme explanado pela autora, "De acordo com o artigo 23, § 2º do Estatuto do Tribunal de Justiça da União Europeia, as partes, os Estados-membros europeus, a Comissão das Comunidades Europeias e, se for o caso, a instituição, órgão ou organismo da União que tiver adotado o ato cuja validade ou interpretação esteja sendo questionada, terão o direito de apresentar alegações ou observações escritas ao Tribunal. O art. 24, § 1º do Estatuto vai além, ao estipular que o Tribunal de Justiça é competente para pedir às partes do processo que apresentem todos os documentos que o TJUE considere oportunos para a deliberação sobre as perguntas formuladas. O parágrafo seguinte do mesmo artigo permite que o Tribunal de Justiça peça às partes, aos Estados-membros e às instituições, órgãos e agências europeias que não sejam partes diretas no processo qualquer tipo de informação que o Tribunal considere necessária para o processo decisório."

A decisão que pôs fim à aplicação dos chamados *Safe Harbor Privacy Principles* foi tomada após as revelações feitas por Edward Snowden, em 2013[159], que dirigiu ofensas sistemáticas aos princípios inerentes à privacidade e à proteção de dados, intensificando as discussões sobre o assunto e polarizando a contenda entre os Estados Unidos e a União Europeia[160].

Em um contexto que dependia essencialmente das possibilidades garantidas pelo *Safe Harbor*, Edward Snowden[161] trouxe as tensões novamente à tona, ao fazer revelações a respeito do governo dos Estados Unidos, com implicações diretas sobre o tema da privacidade e da proteção de informações pessoais[162].

Em 2013, o estudante austríaco de Direito, Max Schrems, deu início a uma ação junto ao Poder Judiciário irlandês em face do *Safe Harbor Agreement*, com fulcro, principalmente, nas informações disponibilizadas por Snowden[163]. Suas alegações estavam baseadas no fato de que o vazamento daquelas informações pessoais comprovaria que o regime de proteção de dados norte-americano seria ineficaz e que, portanto, o acordo seria incapaz de proteger os cidadãos europeus da vigilância ou do vazamento de dados.

---

[159] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. *Comunicado de Imprensa nº 117/15*. Luxemburgo, 6 out. 2015. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150 117en.pdf. Acesso em: 17 abr. 2020.

[160] GIBBS, Samuel. What is 'safe harbour' and why did the EUCJ just declare it invalid? *The Guardian*, 06 out. 2016. Disponível em: https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection. Acesso em: 17 abr. 2020.

[161] FARELL, Henry; NEWMAN, Abraham. The Transatlantic Data War. *Foreign Affairs*, jan./fev. 2016. Disponível em: https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war. Acesso em: 17 abr. 2020. Os autores argumentam a respeito que: "Graças às revelações do ativista da privacidade e ex-contratado da NSA Edward Snowden, o ressentimento em relação ao estado de segurança dos EUA tornou-se uma oposição ativa. Os arquivos de Snowden mostraram que os Estados Unidos, conjuntamente com aliados-chave, haviam explorado sistematicamente vulnerabilidades técnicas para espionar o mundo, reunindo grandes quantidades de dados nas comunicações pessoais de centenas de milhões de pessoas e vasculhando-as em busca de informações de segurança relevantes." (Tradução livre). "*Thanks to the revelations of the American privacy activist and former NSA contractor Edward Snowden, resentment toward the U.S. security state has grown into active opposition. Snowden's files showed that the United States, together with key allies, had systematically exploited technical vulnerabilities to spy on the world, gathering vast amounts of data on the personal communications of hundreds of millions of people and combing them for relevant security information*."

[162] PELTZ-STEELE, Richard J. Op. cit., 2015, p. 21. O autor explica que após a negociação do *Safe Harbor Agreement*, o tema restou inquietamente pacificado durante mais de uma década, até esforços europeus para a atualização da legislação referente à proteção de dados iniciados em 2011. Em 2013, as negociações sofreram o impacto das revelações de Edward Snowden, as quais levaram o Parlamento europeu e líderes políticos nacionais a interferir nas negociações e levantar objeções, principalmente no que se refere ao seu foco no setor privado.

[163] IRLANDA. High Court. *Maximillian Schrems v. Data Protection Commissioner*. IEHC 310, 18 June 2014. "[...] as revelações de Snowden demonstram uma enorme extrapolação por parte das autoridades de segurança, com uma indiferença quase que estudada quanto aos interesses de privacidade dos cidadãos comuns. Seus direitos de proteção de dados foram seriamente comprometidos por programas de vigilância em massa e amplamente não supervisionados." (Tradução livre). "[…] *the Snowden revelations demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens. Their data protection rights have been seriously compromised by mass and largely unsupervised surveillance programmes.*"

A decisão proferida pela Suprema Corte da Irlanda corroborou as alegações de Schrems[164], entendendo que

> as revelações feitas por Snowden demonstram um enorme abuso por parte das autoridades de segurança, com uma indiferença quase estudada quanto à privacidade e interesse dos cidadãos comuns. A proteção de dados foi seriamente comprometida por vigilância de massa em larga escala, em programas não supervisionados[165].

O caso recebeu tratamento semelhante quando foi levado ao Tribunal de Justiça da União Europeia (TJUE), que considerou em sua decisão que haveria uma relação direta entre o *Safe Harbor* e a obscuridade existente na coleta de dados pelos setores público e privado dos Estados Unidos[166], de maneira que foi declarada inválida a Decisão 2000/250 da Comissão.

---

[164] BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. The Datasphere and the Law: New Space, New Territories. *Revista Brasileira de Políticas Públicas (Brazilian Journal of Public Policy).* Direito e o Mundo Digital, dez. 2017, v. 7, n.º 8, p. XVI. "*The issue at stake in the Schrems case is therefore not so much the flows of data as the territory in which a lawyer examines the conditions of any use of personal data. The study subject is indeed the global flows of data but it can be examined in different ways from either side of the Atlantic. In its decision, the Commission considered that the American legal system could guarantee an adequate level of protection. The Court of Justice revoked this view and to a certain extent repatriated this assessment to within the European legal territory*."

[165] IRLANDA. High Court. Op. cit., IEHC 310, 18 June 2014.

[166] CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. *Julgamento do Caso C-362/14*. Maximillian Schrems *v.* Data Protection Commissioner. Luxemburgo, 6 out. 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=920501. Acesso em: 08 mar. 2020. "[...] 134. Com efeito, as decisões adotadas pela Comissão com fundamento no art. 25, n° 6, da Diretiva 95/46, apresentam características específicas. Destinam-se a avaliar se o nível de proteção dos dados pessoais oferecido por um país terceiro apresenta ou não um caráter adequado. Trata-se aí de uma avaliação que está destinada a evoluir em função do contexto factual e jurídico que prevalece no país terceiro. 135. Tendo em conta o fato de que a decisão de adequação constitui um tipo específico de decisão, a regra segundo a qual a apreciação da sua validade só pode ser feita em função dos elementos que existem na data da sua adoção deve ser flexível neste caso. Uma tal regra levaria a que vários anos depois da adoção de uma decisão de adequação, a apreciação de validade que o Tribunal de Justiça fizesse só pudesse ter em conta eventos que ocorreram ulteriormente, e isto mesmo que um tal reenvio prejudicial para apreciação da validade não tenha limite no tempo e que o seu lançamento possa ser precisamente a consequência de fatos posteriores que revelam as insuficiências do ato em causa. 136. No caso em apreço, a manutenção em vigor da Decisão 2000/520 durante cerca de 15 anos testemunha a confirmação implícita da avaliação feita em 2000 pela Comissão. Quando, no âmbito de um pedido de decisão prejudicial, o Tribunal de Justiça é levado a analisar a validade de uma avaliação mantida no tempo pela Comissão, é, portanto, não só possível, mas também adequado que possa confrontar esta avaliação com circunstâncias novas que ocorreram depois da adoção da decisão de adequação. [...] 215. Por conseguinte, ao adotar e manter em vigor a Decisão 2000/520, a Comissão excedeu os limites que o respeito do princípio da proporcionalidade impõe à luz dos arts. 7°, 8° e 52, n° 1 da Carta. A isto acresce a constatação de uma ingerência não justificada no direito dos cidadãos da União a um recurso jurisdicional efetivo, protegido pelo art. 47 da Carta. 216. Consequentemente, esta decisão deve ser declarada inválida na medida em que, em virtude das violações dos direitos fundamentais precedentemente descritas, não se pode considerar que o sistema "porto seguro" que esta instaura, assegura um nível de proteção adequado aos dados pessoais que são transferidos da União no âmbito desse sistema. 217. Perante esta constatação de violação dos direitos fundamentais dos cidadãos da União, considero que a Comissão devia ter suspendido a aplicação da Decisão 2000/520. [...] 237. [...] A Decisão 2000/520 da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios

A decisão proferida pelo TJUE acentuou as tensões entre a União Europeia e os Estados Unidos, que passaram a enveredar esforços no sentido de negociar uma nova forma de regulamentar a coleta, transferência e armazenamento de dados, que fosse capaz de preservar a privacidade dos cidadãos.

Incontornável reconhecer a sua relevância em um contexto social que se apresenta fundamentalmente baseada na troca de informação[167]. Ademais, as revelações feitas por Edward Snowden por meio dos jornais "*The Guardian*"[168] e "*The Washington Post*"[169] atribuíram grande importância à discussão acerca da privacidade e da proteção de dados[170].

Como reflexo dos requerimentos feitos pelo TJUE em sua decisão, invalidando a estrutura do *Safe Harbor*, foram feitas longas negociações em torno do chamado *EU-U.S. Privacy Shield*[171], impondo obrigações mais rígidas às companhias norte-americanas a

---

de "porto seguro" e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, é inválida."

[167] SOLOVE, Daniel J. Op. cit., 2002, p. 3. O autor explica em sua obra a forma como empresas pertencentes ao setor privado têm utilizado tais informações para a elaboração de dossiês completos acerca da vida pessoal dos indivíduos: "Um número crescente de empresas de grande porte está montando dossiês sobre praticamente cada indivíduo, combinando informações de registros públicos com informações coletadas pelo setor privado, como compras, hábitos de consumo, assinaturas de revistas, atividade de navegação na web e histórico de crédito. Cada vez mais, esses dossiês de informações fortificadas de registros públicos são vendidos de volta às agências governamentais para uso na investigação de pessoas". (Tradução livre). "*A growing number of large corporations are assembling dossiers on practically every individual by combining information in public records with information collected in the private sector such as one's purchases, spending habits, magazine subscriptions, web surfing activity, and credit history. Increasingly, these dossiers of fortified public record information are sold back to government agencies for use in investigating people*".

[168] GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, 06 jun. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Acesso em: 05 jul. 2016. GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, 07 jun. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 17 abr. 2020. Em 05 de junho de 2013 o jornal britânico "*The Guardian*" publicou a primeira reportagem sobre os programas de espionagem estadunidenses, demonstrando que a Agência Nacional de Segurança (NSA) coleta dados sobre ligações telefônicas, fotos, e-mails e videoconferências de usuários de serviços oferecidos por empresas como o *Google* ou o *Skype*. A reportagem foi assinada pelo jornalista Glenn Greenwald, o qual posteriormente lançou um *website*, "*The Intercept*", para divulgação de mais informações sobre o caso. Disponível em: https://theintercept.com/. Acesso em: 17 abr. 2020.

[169] Logo em seguida à publicação no jornal "*The Guardian*" o jornal estadunidense "*The Washington Post*" também publicou informações fornecidas por Edward Snowden, detalhando um programa de vigilância secreta que envolvia equipes de inteligência da Microsoft, Facebook, Google e outras empresas do Vale do Silício (NAKASHIMA, Ellen. Verizon providing all call records to U.S. under court order. *The Washington Post*, 06/06/2013. Disponível em: https://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html. Acesso em: 17 abr. 2020).

[170] MARKON, Jerry; NAKASHIMA, Ellen; O'KEEFE, Ed. Lawmakers defend and criticize NSA program to collect phone logs. *The Washington Post*, 06 jun. 2013. Disponível em: https://www.washingtonpost.com/world/national-security/administration-lawmakers-defend-nsa-program-to-collect-phone-records/2013/06/06/2a56d966-ceb9-11e2-8f6b-67f40e176f03_story.html?tid=a_inl. Acesso em: 17 abr. 2020.

[171] EU-US. *Privacy Shield Framework*. Principles Issued by the U.S. Department of Commerce. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg Acesso em: 08 mar. 2020. "O EU-U.S. e o Swiss-U.S. Privacy Shield Frameworks foram projetados pelo Departamento de Comércio dos EUA e pela Comissão Europeia e Administração Suíça, respectivamente, para fornecer às

partir de 2016[172], a fim de resguardar o direito dos cidadãos de preservar as suas informações e dados pessoais[173].

Dessa forma, os Estados Unidos foram obrigados a monitorar e a executar de maneira mais rigorosa as disposições relativas à proteção de dados, bem como a cooperar com as autoridades europeias de proteção de dados para que as suas empresas pudessem, mais uma vez, transferir e armazenar dados dos seus cidadãos. Fica claro, portanto, o caráter transnacional das relações estabelecidas via internet, o qual deve ser levado em conta ao tratar da matéria.

---

empresas de ambos os lados do Atlântico um mecanismo para atender aos requisitos de proteção de dados ao transferir dados pessoais da União Europeia e da Suíça aos Estados Unidos em prol do comércio transatlântico. Em 12 de julho de 2016, a Comissão Europeia considerou EU-U.S. Privacy Shield adequado para permitir a transferência de dados de acordo com a legislação da UE. Em 12 de janeiro de 2017, o governo suíço anunciou a aprovação do Swiss-U.S. Privacy Shield Frameword como um mecanismo legal válido para cumprir os requisitos suíços para transferência de dados pessoais da Suíça para os Estados Unidos. Veja-se as declarações do Conselho Federal Suíço e do Comissário Federal Suíço de Proteção de Dados e Informações. O Privacy Shield, administrado pela International Trade Administration (ITA) no Departamento de Comércio dos EUA, permite que as organizações sediadas nos EUA ingressem em uma ou em ambas as estruturas do Privacy Shield, para se beneficiarem das determinações de adequação. Para ingressar no Privacy Shield, uma organização sediada nos EUA deverá se autocertificar para o Departamento de Comércio (por meio do site) e se comprometer publicamente a cumprir os requisitos ali constantes. Embora a adesão ao Privacy Shield seja voluntária, uma vez que uma organização qualificada assume o compromisso público de cumprir os seus requisitos, tal compromisso se torna obrigatório (ou exequível) de acordo com a lei dos EUA. [...].” (Tradução livre). “*The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law [...]. On January 12, 2017, the Swiss Government announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States. See the statements from the Swiss Federal Council and Swiss Federal Data Protection and Information Commissioner. The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S.-based organizations to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy determinations. To join either Privacy Shield Framework, a U.S.-based organization will be required to self-certify to the Department of Commerce (via this website) and publicly commit to comply with the Framework’s requirements. While joining the Privacy Shield is voluntary, once an eligible organization makes the public commitment to comply with the Framework’s requirements, the commitment will become enforceable under U.S. law. [...].”*

[172] Id., ibid. Sobre os países aos quais o *Privacy Shield* se aplica, veja-se: “Considerando que a Decisão da Comissão sobre a adequação da proteção fornecida pelo EU-U.S. Privacy Shield se aplica à Islândia, Liechtenstein e Noruega, o Privacy Shield será aplicável tanto à União Europeia quanto a esses três países. Consequentemente, as referências à UE e aos seus Estados-Membros serão entendidas como incluindo a Islândia, o Liechtenstein e a Noruega.” (Tradução livre). “*Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to Iceland, Liechtenstein and Norway, the Privacy Shield Package will cover both the European Union, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein and Norway*.”

[173] EU-US. European Data Protection Supervisor (EDPS). Press Release EDPS/2016/11. *Privacy Shield:* more robust and sustainable solution needed. Brussels, 30 May 2016. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShi eld_EN.pdf. Acesso em: 08 mar. 2020.

> Na maior parte das vezes, será parte os territórios institucionais tradicionais, nos quais cada Estado, cada região mundial, é convidado a definir seu âmbito de ação, seja sozinho ou em cooperação com outros. Contudo, novos atores, localizados em novos territórios, poderão também desempenhar seus papéis. Esta é a direção na qual o novo acordo conhecido como *EU-US Privacy Shield*, atualmente em processo de adoção, está se esforçando para mudar de modo a conferir às empresas que lidam com fluxos de dados transatlânticos um mecanismo de autocertificação. [...] da mesma forma como seu antecessor, este acordo não será capaz de impedir completamente o fluxo de dados além do controle. Também não irá dissipar a discussão sobre se a troca de dados deve ser controlada a nível europeu ou se pode ser delegada de forma válida a atores localizados em novos territórios. A "datasfera" é um fenômeno existente na tecnosfera, o qual a lei poderia compreender como novo espaço. Ela é marcada por dois tipos de território: antigo e novo. Este espaço oferece uma estrutura para análise jurídica necessária para compreender as novas relações se desenvolvendo com tais territórios. Uma noção abrangente, a datasfera permite que este novo espaço seja definido holisticamente. Não desagua nem compete com outros espaços. Ela abre o campo jurídico de investigação para uma nova realidade atualmente presente em todas as áreas da atividade humana[174] (Tradução livre.).

1.5 REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD) DA UNIÃO EUROPEIA

O mecanismo de proteção de dados criado pelas Diretivas europeias foi modificado e atualizado, desde que, em 25 de maio de 2018, passou a vigorar o Regulamento Geral de

[174] BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. Op. cit., dez. 2017, p. XVII. "Na maior parte das vezes, será nos territórios institucionais tradicionais onde cada Estado, cada região do mundo, é convidado a definir seu escopo de ação, sozinho ou em cooperação com outros. No entanto, novos participantes, localizados em novos territórios, também podem ter seu próprio papel a desempenhar. Essa é a direção na qual o novo acordo conhecido como EU-U.S. *Privacy Shield*, atualmente [em 2017] em processo de adoção, tem como propósito oferecer às empresas que lidam com fluxos de dados transatlânticos um mecanismo de autocertificação. No entanto, da mesma maneira que seu antecessor, esse arranjo não será capaz de impedir a totalidade do fluxo e o controle de dados pessoais. Tampouco dispensará a discussão sobre se o intercâmbio de dados deve ser controlado a nível europeu ou se pode ser validamente delegado a *players* estabelecidos nos novos territórios. A 'esfera de dados' [*datasphere*] é um fenômeno existente no âmbito da tecnosfera, o qual poderia ser compreendido, legalmente, como um novo espaço. É marcado por dois tipos de território: antigo e novo. Esse espaço oferece uma estrutura para a análise jurídica necessária para entender as novas relações que se desenvolvem com esses territórios. Uma noção abrangente, a esfera de dados permite que esse novo espaço seja definido holisticamente. Não desafia nem compete contra os outros espaços. Abre o campo jurídico da investigação para uma nova realidade hoje presente em todas as áreas da atividade humana." (Tradução livre). "*Most often, it will be for the traditional institutional territories where each State, each world region, is invited to define its scope of action, either alone or in cooperation with others. However, new players, located on new territories, may also have their own role to play. This is the direction in which the new arrangement known as the EU-US Privacy Shield, currently in the process of adoption, is striving to move by giving companies handling transatlantic data flows a mechanism of self-certification. However, in the same way as its predecessor, this arrangement will not be capable of preventing the full movement beyond control of personal data. Neither will it dispel discussion on whether data exchange should be controlled at European level or whether it can be validly delegated to players established in the new territories. The "datasphere" is a phenomenon existing in the technosphere, which the law could seek to understand as a new space. It is marked by two types of territory: old and new. This space offers a framework for legal analysis necessary for understanding the new relationships developing with these territories. An overarching notion, the datasphere allows this new space to be defined holistically. It does not challenge, or even compete against the other spaces. It opens up the legal field of investigation to a new reality nowadays present in all areas of human activity."*

Proteção de Dados (RGPD) da União Europeia[175]. Enquanto pelo sistema anterior eram mantidas e informadas 28 autoridades distintas de proteção de dados, com a aprovação do novo RGPD passou a haver um único diploma normativo, resultando em benefício econômico substancial[176].

Além de centralizar as autoridades de proteção de dados, o RGPD estabelece, seja por uma pessoa, empresa ou organização, regras relativas ao tratamento dos dados pessoais relativos a pessoas na UE[177]. "Tratamento de dados" é entendido aqui como qualquer atividade que envolva a coleta, guarda, transferência ou destruição de dados.

Há, também, previsão de sanções severas em caso de violação ao Regulamento: conforme a gravidade da infração, a multa aplicada poderá ter valor de até 20 milhões de euros, ou de 4% do faturamento global da empresa[178]. Desde o início da vigência do

---

[175] UNIÃO EUROPEIA. *Regulamento 2016/679*. Op. cit. Disponível em: http://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=uri serv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020.

[176] RESINA, Fernando *et al. Cloud – A lei e a prática:* guia e perguntas frequentes. Coimbra: Almedina, 2016, p. 68. "O novo Regulamento Europeu de Proteção de Dados, [...] vem instituir uma novidade: um sistema *one stop shop* (uma espécie de "balcão único") para as autoridades de Proteção de Dados dos Estados-membros. Tal significa, em termos sucintos, que os clientes apenas terão, em princípio, que interagir com a autoridade do país onde têm estabelecimento principal, embora os cidadãos possam sempre interagir e apresentar queixas junto da autoridade do seu país."

[177] O RGPD não se aplica ao tratamento de dados pessoais de pessoas falecidas ou de pessoas coletivas. Tampouco se aplica ao tratamento de dados por motivos exclusivamente pessoais, ou no exercício de atividades domésticas, desde que inexista relação com uma atividade profissional ou comercial.

[178] WORLOCK, Charlotte. European Union: GDPR – The First Complaints. *Mondaq*, 07 jun. 2018. Disponível em: http://www.mondaq.com/uk/x/708562/data+protection/GDPR+The+First+Complaints. Acesso em: 17 abr. 2020. "Já no próprio dia 25 de maio de 2018 foram apresentadas quatro queixas por violação do RGPD contra o Google (na França), Instagram (na Bélgica), WhatsApp (na Alemanha) e Facebook (na Áustria), por *None of Your Business* (NOYB) , uma ONG de privacidade criada pelo ativista e advogado da privacidade Max Schrems, agindo em nome de um único titular de dados para cada reclamação, e solicitando que multas máximas de 4% do respectivo lucro mundial anual sejam impostas a cada empresa. Em 28 de maio de 2018, queixas semelhantes foram registradas contra o Facebook, Google, Apple, Amazon e LinkedIn na França por um grupo francês de direitos digitais, Quadrature du Net (*La Quad*). Cada uma das reclamações da La Quad é apresentada em nome de cerca de 9.000 a 10.000 titulares de dados, e a La Quad também indicou que pretende apresentar reclamações semelhantes contra Android, WhatsApp, Instagram, Skype e Outlook. [...] Todas as queixas apresentadas pela NOYB e La Quad alegam que as empresas em questão adotaram uma abordagem de *pegar ou largar* para consentir e, portanto, estão explorando seu domínio de mercado, forçando os titulares de dados a consentir no processamento de seus dados pessoais para uma finalidade além da necessária (nesse caso, compartilhar ou usar dados para publicidade direcionada) porque, a menos que as pessoas concordem em dar seu consentimento, não poderão usar o serviço." (Tradução livre). "*On 25 May 2018 itself, four complaints alleging breaches of GDPR were lodged against Google (in France), Instagram (in Belgium), WhatsApp (in Germany) and Facebook (in Austria), by "None of Your Business" (NOYB), a privacy NGO created by privacy activist and lawyer, Max Schrems, acting on behalf of a single data subject for each complaint, and requesting that maximum fines of 4% of worldwide annual turnover be imposed upon each company. On 28 May 2018, similar complaints were filed against Facebook, Google, Apple, Amazon and LinkedIn in France by a French digital rights group, Quadrature du Net ("La Quad"). Each of La Quad's complaints are brought on behalf of around 9,000 to 10,000 data subjects, and La Quad also indicated that they intend to bring similar complaints against Android, WhatsApp, Instagram, Skype and Outlook. [...] All of the complaints lodged by NOYB and La Quad allege that the targeted companies have adopted a "take it or leave it" approach to consent, and therefore are exploiting their market dominance by forcing data subjects to consent to the processing of their personal*

Regulamento, já foram aplicadas sanções a grandes empresas, como o Facebook e o Google, conforme será exposto mais detalhadamente a seguir.

O novo RGPD representa, portanto, uma garantia ainda maior à proteção dos dados dos cidadãos da União Europeia, principalmente no que se refere aos princípios da transparência, do livre acesso, da finalidade e da adequação, já que prevê meios de controle do indivíduo sobre os seus dados pessoais mesmo quando cedidos[179]. O principal objetivo é impedir a utilização indevida de dados coletados em redes sociais, cadastros digitais e bancos de dados.

O RGPD está centrado na ideia de consentimento do titular de dados, de modo que a utilização e o armazenamento de seus dados devem ser claros e consentidos. Importante ressaltar que se o consentimento foi anterior à vigência do Regulamento, este será válido desde que esteja em conformidade com as condições que ali constam. Caso os requisitos não tenham sido cumpridos, é necessário novo consentimento do titular, devidamente informado.

A aprovação do RGPD suscitou novas dúvidas e questões, inclusive quanto às situações que não estavam plenamente reguladas. Exemplo disso é a tecnologia "*blockchain*", a qual se encontra em fase inicial de desenvolvimento, sendo possível que futuramente necessite de normas específicas[180].

---

data for a purpose beyond that which is necessary (in this case sharing or using data for targeted advertising) because, unless individuals agree to give their consent, they are unable to use the service."

[179] BASILIEN-GAINCHE, Marie-Laure. Op. cit., jun. 2017, p. 6. A autora critica a proteção de dados no âmbito da União Europeia no atual contexto migratório, apontando as distinções entre os cidadãos europeus e indivíduos refugiados: "A tecnologização, portanto, não marca apenas seu império no espaço, de modo que as fronteiras virtuais da sociedade europeia vão além e dentro dos limites territoriais dos Estados da região. Ela exerce, igualmente, controle sobre indivíduos, cujos dados pessoais são objeto de uma vigilância contínua". (Tradução livre). "*La technologisation ne marque donc pas seulement son empire dans l'espace, de telle sorte que les frontières virtuelles de la société européenne vont au-delà et en deçà des limites territoriales des États de la zone. Elle exerce également une emprise sur les individus, dont les données personnelles font l'objet d'une surveillance continue*."

[180] GONÇALVES, Pedro Vilela Resende; CAMARGOS, Rafael Coutinho. Blockchain, Smart Contracts e "Judge as a Service" no Direito Brasileiro. II Seminário Governança das Redes e o Marco Civil da Internet: globalização, tecnologias e conectividade. *Anais...* Belo Horizonte: Instituto de Referência em Internet e Sociedade-IRIS, 2017, pp. 207-212. "*Blockchain*" pode ser definido como um protocolo que conjuga a criptografia, o arquivamento de atos, em número indeterminado de computadores, havendo exigência de vínculo entre o ato posterior e o anterior. Assim, é criada uma espécie de "corrente" indissociável de arquivos, ou seja, um procedimento que resulta em um bloco encadeado de atos. A generalização da formalização eletrônica para a atividade administrativa permite, deste modo, a aplicação do protocolo de *blockchain*. De tal maneira, a sucessão encadeada de atos, típica do instituto do procedimento, será institucionalizada na dimensão digital, permitindo identificar a data e a autoria de cada ato, inviabilizando por completo o acréscimo superveniente de informações essenciais, bem como a tentativa de correção *a posteriori* de eventuais defeitos ou insuficiências. Além de agregar maior confiabilidade aos procedimentos, o *blockchain* permite o cumprimento das garantias relativas à proteção de dados, em especial quanto à eficiência.

A distinção entre dados pessoais e não pessoais é de importância central, já que estes últimos não estão sujeitos ao RGPD ou outras legislações protetivas de dados. A tecnologia "*blockchain*" é utilizada, por exemplo, para converter dados pessoais em não pessoais[181], utilizando técnicas de anonimização que impedem a identificação do titular[182].

As novas empresas, independentemente do porte, estão adotando o modelo de "*privacy by design*", ou seja, vêm considerando a privacidade desde o momento de sua concepção, a fim de garantir a proteção adequada de dados. A privacidade pode ser protegida com o uso da rede "*blockchain*", por canais privados, ou a partir de uma combinação entre ambos[183]. Tal princípio está incluso no RGPD e implica, desde o início (ou desde a sua concepção), na necessidade de compatibilização de projetos com as suas normas.

Há, também, questionamentos sobre a forma como ocorre o consentimento e se o titular dos dados está ciente do modo de sua utilização. O TJUE entende ser insuficiente um mero "*click*" indicando que os termos e condições gerais foram aceitos, sendo necessário que o usuário tenha efetivamente conhecimento daquilo que está aceitando[184].

---

[181] Id., ibid. A anonimização de dados por meio da rede "*blockchain*" passa essencialmente por quatro etapas: (i) legitimidade do tratamento, com direito de revogação e esquecimento: eliminação dos dados para os quais não houve consentimento; (ii) princípio da exatidão e direito de retificação: permitir que dados equivocados sejam retificados ou excluídos; (iii) limitação do prazo de conservação dos dados: os dados devem ser mantidos somente durante o tempo necessário à finalidade da sua coleta; e (iv) integridade e confidencialidade: por fim, os dados são anonimizados, permitindo seu acesso por todos os participantes da rede "*blockchain*".

[182] SILVA, Matheus Passos. A segurança da democracia e a *blockchain*. *Projeção, Direito e Sociedade*, 2018, v. 9, n. 1, pp. 119-138. A função "*hash*" é uma técnica criptográfica que permite gerar, para qualquer tipo de documento, informação ou dado, um código alfanumérico correspondente, tratando-se de um identificador único. O identificador permanece o mesmo enquanto o dado não for alterado e, conforme houver qualquer modificação, é gerado um identificador diferente. Assim, a solução "*hash*" em "*blockchain*" consiste na geração de identificadores únicos ("*hashs*") para dados pessoais, com o seu armazenamento na rede. Os dados, por sua vez, são mantidos armazenados em uma base de dados externa, cuja gestão é feita pelo responsável pelo tratamento daqueles dados. Existe, ainda, a utilização de "*salt*", que consiste em um conjunto de valores aleatórios acrescidos ao "*hash*", com o objetivo de dificultar a identificação do titular, e reforçar a anonimização.

[183] Id., ibid. Canais privados são vias de transmissão de dados e informação criados a partir de dois ou mais locais, e que desejam compartilhar tais informações entre si, de forma privada e dentro da rede "*blockchain*", sem que os demais membros da rede tenham acesso àquilo que foi compartilhado, e limitando o acesso daqueles fora do canal privado. As mensagens compartilhadas desta forma estão sempre criptografadas a fim de garantir a confidencialidade. A partir de uma chave é possível ter acesso ao conteúdo da informação. Ressalte-se que as informações armazenadas em "*blockchain*" não são jamais eliminadas nem modificadas – contudo, sem a chave, não é possível o seu acesso. A eliminação da chave corresponde, na prática, à eliminação do dado, por eliminar o meio de acesso a ele, muito embora o dado continue existindo, armazenado na rede "*blockchain*".

[184] UNIÃO EUROPEIA. TJUE. *Bundesverband der Verbraucherzentralen und Verbraucherverbände* – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH. Processo C-673/17, 01 out. 2019. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=D5DC4CA415C605B28E70747FD3C5158C?text&docid=218462&pageIndex=0&doclang=PT&mode=req&dir&occ=first&part=1&cid=1458627. Acesso em: 08 mar. 2020.

Ainda não foi estabelecida a forma ideal para garantir que o consentimento do titular seja válido[185].

Os impactos do RGPD não estão restritos ao comércio e direitos do consumidor: especificamente no campo médico e de pesquisa, há dúvidas sobre como serão afetadas a coleta e a utilização de dados de pacientes. Na área da investigação científica há certa flexibilidade quanto à especificação da finalidade do tratamento de dados – desde que mantidos os elementos essenciais (consentimento de livre vontade, informado, claro, e tão específico quanto possível)[186].

O RGPD possui mérito por uniformizar a proteção de dados no território da União, oferecendo maiores garantias à privacidade dos cidadãos[187]. O fato é que, desde que

[185] CAMARGO, Solano de. Op. cit., 2019, (s.p.). "Cookies, por sua vez, são pequenos arquivos criados pelos sites visitados e que são salvos no computador ou no *smartphone* do usuário, por meio do navegador. Esses arquivos contêm informações que servem para identificar o visitante, tanto para personalizar a página de acordo com o perfil do usuário como para facilitar o transporte de dados entre as páginas de um mesmo site. Ocorre que, em 1º de outubro de 2019, o Tribunal de Justiça da União Europeia (TJUE) decidiu, no caso C-673/2017, que o mero click autorizando a instalação de cookies demonstrou ser um mecanismo insuficiente para provar o consentimento do usuário à coleta de seus dados pessoais. Os juízes do TJUE não propuseram alternativas às caixas de texto, tais como a necessidade de rolagem completa da página da web ou outro meio qualquer, de forma que a questão permanece em aberto. [...] A limitação europeia à instalação de cookies – que certamente será, em algum momento, direcionada à Autoridade Nacional de Proteção de Dados ou às cortes brasileiras, mostra um longo e espinhoso caminho a uma nova realidade, em que muitas empresas não se encontram nem perto de estarem preparadas."

[186] UNIÃO EUROPEIA. Comissão Europeia (CE). Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/how-consent-processing-scientific-research-obtained_pt#resposta. Acesso em: 17 abr. 2020. "É permitida alguma flexibilidade em relação ao grau de especificação e pormenorização na prestação do consentimento no contexto da investigação científica. Quando da recolha de dados pessoais, os investigadores podem não conseguir identificar plenamente as finalidades do seu tratamento. Nestes casos, podem pedir às pessoas que deem o seu consentimento para determinadas áreas da investigação científica ou partes de projetos de investigação. No entanto, o consentimento deve manter os seus principais elementos, ou seja, ser dado de livre vontade, informado, obtido de modo claro e afirmativo e tão específico quanto a investigação em questão o permita. Os investigadores devem garantir que cumprem as normas éticas e metodológicas exigidas na sua área."

[187] REYNOLDS, Matt. What is article 13? The EU's divisive new copyright plan explained. *Wired*. Publicado em: 24 maio 2019. Disponível em: https://www.wired.co.uk/article/what-is-article-13-article-11-european-directive-on-copyright-explained-meme-ban. Acesso em: 17 abr. 2020. Sobre as críticas ao RGPD e ao art. 17: "A diretiva sobre direitos autorais recebeu críticas pelos dois lados do debate, mas é possível separar defensores e detratores em duas categorias. A favor da diretiva existem organismos da indústria que representam produtores de conteúdo. Isso inclui a *Society of Authors e a Alliance for Intellectual Property e Proponents*, com sede no Reino Unido. Em junho de 2018, 84 organizações europeias de música e mídia, incluindo o *Universal Music Group* e o *Waner Music Group* declararam publicamente seu apoio à diretiva. No Parlamento Europeu, o principal deputado que defende a directive junto ao Parlamento é Axel Voss, um deputado alemão e membro do Partido Popular Europeu. [...] O outro lado do debate, críticos da diretiva, inclui o influente grupo de *lobby* do Vale do Silício, o CCIA, cujos membros incluem Google, Facebook, eBay, Amazon e Netflix. Em 12 de junho, um grande grupo de grandes nomes da internet, incluindo o fundador da Wikipedia Jimmy Wales e Tim Berners-Lee, assinou uma carta aberta argumentando contra a diretiva. Vale ressaltar que, apesar da diretiva possuir exceção excluindo explicitamente a Wikipedia e o GitHub dessas regras, as duas empresas mantiveram sua oposição à diretiva. O YouTube é de longe o crítico mais importante do artigo 13, com a empresa fazendo um grande esforço para promover a oposição à diretiva entre seus criadores e usuários." (Tradução livre). "*The Directive on Copyright has gained vocal critics on both sides of the debate, but you can broadly chunk up defenders and detractors into two categories. In*

vigente, o RGPD tem exercido influência sobre todos os países com os quais os Estados-membros da UE trocam dados. Assim, trata-se de diploma normativo extremamente relevante que repercutiu sobre outros ordenamentos jurídicos ao redor do mundo, suscitando iniciativas de harmonização.

Finalmente, cumpre analisar a relação existente entre o RGPD e o *Privacy Shield*, abordados no tópico anterior, a fim de avaliar se, em tese, poderiam ou não ser colocados em pé de igualdade. Sob tal aspecto, vale retomar as observações feitas anteriormente sobre a natureza jurídica dos regulamentos e o seu papel no âmbito da União Europeia.

O RGPD, portanto, propõe-se a modernizar, padronizar e unificar as práticas de proteção de dados em toda a União Europeia, podendo levar à imposição de multas ou coimas, e impedir a transferência de dados para países cuja proteção é considerada insuficiente, como ocorre nos Estados Unidos. Por tal razão, o *Privacy Shield* mantém sua relevância mesmo após a vigência do Regulamento, já que nos termos deste último, a transferência e o tratamento de dados por empresas estadunidenses não seria possível.

O *Privacy Shield*, portanto, continua sendo utilizado como base e como solução para permitir a transferência de dados entre União Europeia e Estados Unidos – muito embora seja insuficiente para garantir a proteção desejada[188]. Destarte, empresas submetidas ao regime do RGPD não podem se valer do *Privacy Shield* para alegar conformidade com os padrões mínimos estabelecidos por aquele Regulamento[189].

---

favour of the Directive are industry bodies representing content producers. These include the Society of Authors, and the UK-based Alliance for Intellectual Property and Proponents. In June 2018 84 European music and media organisations, including Universal Music Group and Waner Music Group publicly declared their support for the Directive. In the European Parliament the lead MEP presenting the directive to Parliament is Axel Voss, a German MEP and member of the European People's Party. [...] The other side of the debate, critics of the Directive, include the influential Silicon Valley lobbying group the CCIA, whose members include Google, Facebook, eBay, Amazon and Netflix. On June 12 a large group of internet grandees including Wikipedia founder Jimmy Wales and Tim Berners-Lee signed an open letter arguing against the Directive. It's worth noting that despite the Directive including an exception that explicitly excludes Wikipedia and GitHub from these rules, both companies have maintained their opposition to the Directive. YouTube is by far the most vocal critic of Article 13, with the firm making a big effort to promote opposition to the directive among its creators and users."

[188] G29. *Déclaration du G29 relative à la décision de la Commission européenne concernant le Privacy Shield* (bouclier de protection des données UE-États-Unis). 29 juillet 2016. Disponível em: https://www.cnil.fr/fr/ declaration-du-g29-relative-la-decision-de-la-commission-europeenne-concernant-le-privacy-shield. Acesso em: 08 mar. 2020.

[189] PAUCHET, Maria. RGPD vs Privacy Shield? *In*: *Digital We Trust* – Faire le lien entre confiance et simplicité. Disponível em: https://www.indigitalwetrust.fr/2017/11/rgpd-privacy-shield/. Acesso em: 08 mar. 2020. "O *Privacy Shield* é um acordo entre a UE e os Estados Unidos para permitir a transferência de dados pessoais da UE para os Estados Unidos. O *Privacy Shield*, portanto, funciona como uma solução alternativa para oferecer uma base legal à transferência de dados pessoais da União Europeia (UE) para os Estados Unidos. As empresas cujas atividades estão sujeitas ao RGPD não poderão, portanto, se utilizar do *Privacy Shield* para comprovar sua conformidade com os regulamentos europeus. Ainda, o *Privacy Shield* é um dispositivo interessante, mas insuficiente; o G29 (Comitê das várias CNILs europeias) manifestou preocupação e solicitou vários esclarecimentos em comunicado de imprensa datado de 13 de abril de 2016.

1.6 INFLUÊNCIA DO RGPD SOBRE OUTROS ORDENAMENTOS

O Regulamento Geral de Proteção de Dados em vigor na União Europeia influenciou outras nações mundiais a aprovarem leis específicas sobre o tema, inclusive o Brasil[190]. Alguns países já contavam com dispositivos sobre privacidade e proteção de dados, mas a necessidade de adequação ao modelo europeu para permitir a troca de informações desencadeou novas ações nesse sentido, reproduzindo, por vezes, as disposições do RGPD.

Na América Latina destaca-se, primeiramente, o **Chile**, país que desde 1999 possui regras específicas quanto à proteção de dados pessoais, quando entrou em vigor a Lei n. 19.628 sobre proteção de dados de caráter pessoal[191]. Apesar de a lei regular a utilização de dados por terceiros, não havia previsão de mecanismos de fiscalização, tampouco previsões específicas relacionadas à Internet.

A legislação chilena de proteção de dados está em fase de adaptação, encontrando-se em trâmite legislativo a reforma que propõe a criação de uma agência de proteção de

---

Com o recurso a outros meios, como cláusulas contratuais, regras comerciais vinculantes permanecem possíveis." (Tradução livre). "*Le Privacy Shield est un accord entre l'UE et les États-Unis permettant le transfert des données personnelles de l'UE vers les États-Unis. Le Privacy Shield fonctionne donc comme une solution de contournement pour fournir une base légale au transfert des données personnelles de l'Union Européenne (UE) vers les États-Unis. Les entreprises dont l'activité sera soumise au RGPD ne pourront donc pas se prévaloir de leurs adhésions au Privacy Shield pour démontrer leur conformité au règlement européen. De la même manière, le Privacy Shield est un dispositif intéressant mais insuffisant; le G29 (Comité des différentes CNIL européennes) a ainsi exprimé des inquiétudes et a demandé diverses clarifications, dans son communiqué du 13 avril 2016. Le recours aux autres moyens tels que des clauses contractuelles, des règles d'entreprise contraignantes reste toujours possible*."

[190] CÔRREA, Adriana Espíndola; LOUREIRO, Maria Fernanda Battaglin. Novo regulamento europeu é reforço na proteção dos dados pessoais? (Parte 1). *CONJUR*, 2018. Disponível em: https://www.conjur.com.br/2018-jul-09/direito-civil-atual-regulamento-europeu-ereforco-protecao-dados-pessoais. Acesso em: 17 abr. 2020. "O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, conhecido como Regulamento Geral sobre a Proteção de Dados (GPDR), que entrou em vigor em maio, registra, expressamente, a importância fundamental da circulação de dados nas sociedades atuais, para as empresas, associações e entes públicos. Alerta, também, para o aumento exponencial do tratamento de dados pessoais, associado ao desenvolvimento das tecnologias de informação. E aponta para a necessidade de harmonizar a crescente utilidade e conveniência de tratamento desses dados com as liberdades e direitos fundamentais."

[191] VALENTE, Jonas. Legislação da proteção de dados já é uma realidade em outros países. *Agência Brasil*, 2018. Disponível em: http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 17 abr. 2020. "Os Estados Unidos também são referência mundial. Não pela existência de uma lei geral, mas pela legislação fragmentada. A Lei de Privacidade de Comunicação Eletrônica (ECPA, na sigla em inglês), de 1986, proíbe a interceptação de mensagens telefônicas ou eletrônicas (como e-mails) e garante a segurança de informações tanto durante a transmissão quanto no armazenamento, inclusive em computadores. [...] Diversos países têm legislações de proteção de dados na América Latina, como Chile, Argentina, Uruguai e Colômbia. A lei chilena, de 1999, limita o uso dos dados ao propósito informado no ato da coleta, com a exceção de registros tornados públicos. Ela garante aos titulares o direito de acessar as informações de posse de alguma empresa, corrigi-la ou eliminá-la se o armazenamento não respeitar as exigências da Lei ou o tratamento for concluído. A lei prevê a responsabilização de empresas controladoras de dados em caso de prejuízos aos titulares, com sanções definidas pela Justiça. O texto estabelece algumas diferenças para o Poder Público, limitando o tratamento de dados ao previsto na lei e impedindo divulgação de informações sobre condenações depois de prescreverem."

dados pessoais[192]. O projeto tem forte influência do RGPD, de modo que se espera uma harmonia entre ambos.

Na **Argentina**, no ano de 2000, houve a aprovação da Lei de Proteção de Dados Pessoais com vistas a regular as bases públicas e privadas de dados, a partir do seu uso limitado e para a finalidade para a qual foram obtidos[193]. O tratamento foi condicionado ao consentimento do titular dos dados, com as ressalvas de que essa autorização não seria exigida nos casos de bases públicas, no cumprimento de obrigações legais, no exercício de funções próprias do Estado, e quando as informações se limitassem a nome, identidade, profissão, data de nascimento e endereço[194].

---

[192] VALENZUELA, Daniel Álvarez. Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridade de control em matéria de protección de datos? *RDUCN – Revista de Derecho*. Coquimbo, jun. 2016, v. 23, n.º 1. Disponível em: https://scielo.conicyt.cl/scielo.php?pid=S0718-97532016000100003&script=sci_arttext&tlng=em. Acesso em: 06 jan. 2020. "Em termos de proteção de dados pessoais, a especificação legal do bloco constitucional consta da mencionada Lei n.º 19.628, que sem prejuízo de ser denominada 'sobre proteção da privacidade', trata antes da regulamentação legal do mercado de processamento de dados pessoais. Embora a lei reconheça uma série de direitos às pessoas físicas que detêm os dados, elas devem ser exercidas perante os tribunais civis, em um procedimento longo e oneroso, que constitui uma barreira para o cidadão comum. Até a presente data, após quinze anos de validade de seus regulamentos, não há jurisprudência civil relevante que sancione o tratamento inadequado de dados pessoais. Dada a situação de falta de proteção dos direitos dos titulares de dados pessoais, alguns tiveram que recorrer a outras medidas judiciais, como a ação de proteção por violação de garantias constitucionais, com resultados incertos e mal padronizados, o que tampouco fornece um nível adequado de proteção dos direitos das pessoas. Por outro lado, desde a aprovação da lei em 1999, a preocupação com a proteção de dados pessoais em particular, e com a proteção da vida privada das pessoas em geral, aumentou significativamente, talvez motivada pelo desenvolvimento de tecnologias que facilitam o processamento de grandes volumes de dados pessoais, a baixo custo." (Tradução livre). "*En materia de protección de datos personales, la concreción legal del bloque constitucional está contenida en la ya mencionada Ley n.° 19.628, que sin perjuicio de nominarse «sobre protección de la vida privada», más bien trata sobre la regulación legal del mercado de tratamiento de datos personales. Si bien la ley reconoce una serie de derechos a las personas naturales titulares de los datos, estos deben ser ejercidos ante tribunales civiles, en procedimiento de larga y costosa tramitación, lo que constituye una barrera para el ciudadano común. A la fecha, luego de quince años de vigencia de sus normas, no existe jurisprudencia civil relevante que haya sancionado el tratamiento indebido de datos personales. Ante la situación de desprotección de los derechos de los titulares de datos personales, algunos han debido recurrir a otras medidas judiciales, como la acción de protección por afectación de garantías constitucionales, con resultados inciertos y poco estandarizados, lo que tampoco otorga un adecuado nivel de protección de los derechos de las personas. Por otra parte, desde la aprobación de la ley en 1999, la preocupación por la protección de los datos personales en particular y por la protección de la vida privada de las personas en general, ha aumentado de manera importante, motivada quizás por el desarrollo de tecnologías que facilitan el procesamiento de grandes volúmenes de datos personales, a bajo costo."*

[193] ARGENTINA. *Ley Nacional de Protección de Datos Personales nº 25.326, de 30 de outubro de 2000*. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em: 06 jan. 2020.

[194] CEJAS, Eileen Berenice; GONZÁLEZ, Carlos César. Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales. *SID 2015 – 15º Simposio Argentino de Informática y Derecho*. Disponível em: http://sedici.unlp.edu.ar/bitstream/handle/10915/55549/Documento_completo.pdf?sequence=1. Acesso em: 06 jan. 2020. Além da mencionada lei argentina de proteção de dados, há dois outros diplomas normativos que se destacam a respeito do tema, relacionando-se à videovigilância e às condições para sua licitude. "A Resolução n.º 283/2012 do Ministério da Segurança da Presidência da Nação regula o sistema de videovigilância – no âmbito da Polícia Federal da Argentina, da Gendarmaria Nacional, da Prefeitura Naval da Argentina e/ou da Polícia de Segurança Aeroportuária, cujo objetivo é a prevenção de delitos, permitindo que as imagens sejam utilizadas como evidência documental no âmbito de um processo judicial. Os princípios aos quais esta regra se refere são os de legalidade, respeito pela

Assim, as empresas argentinas possuem o dever de atualizar dados incompletos e errados, sendo vetado manter registros após o término da atividade para a qual os dados foram coletados. Os entes responsáveis pelo tratamento também devem garantir o acesso dos titulares às suas informações, sendo permitido, contudo, o repasse de dados a terceiros desde que cumpram um "interesse legítimo" do ente que os estão cedendo. No caso de órgãos públicos há regras específicas, como o direito de negar o acesso, a correção e a supressão das informações[195].

No **México**, por sua vez, destaca-se a Lei Federal de Proteção de Dados Pessoais em Posse dos Particulares, vigente desde 2010, e o respectivo regulamento, em vigor desde 2011[196]. Conjuntamente, a lei e o regulamento estabelecem parâmetros para o tratamento legítimo, controlado e informado de dados[197]. Até o momento não houve nova iniciativa

---

privacidade das pessoas e transparência; por fim, e em referência à Lei 25.326 – é preciso preencher os requisitos estabelecidos em relação ao tratamento de dados, dever de confidencialidade e confidencialidade, proteção e salvaguarda de informações, cumprimento exclusivo do objetivo específico de sua criação, operação e registro de informações. banco de dados exigido pela Lei Nacional de Proteção de Dados Pessoais n.º 25.326. De maior relevância [...], é a disposição 10/2015 do DNPDP, que contém uma série de princípios que se aplicam aos sistemas de videovigilância no território argentino, princípios (denominados condições de licitude no texto legal) que são os seguintes: (i) consentimento, (ii) respeito à finalidade, (iii) qualidade dos dados, (iv) segurança e confidencialidade, (v) exercício dos direitos do titular dos dados, (vi) registro e (vii) manual de processamento de dados. [...] Pelo exposto, recomenda-se: [...] que a Lei nº 25.326, relativa à proteção de dados pessoais, seja emendada ou promulgada uma lei que crie um órgão autônomo e autônomo capaz de avaliar o uso de dados dos diferentes órgãos do Estado." (Tradução livre). "*La Resolución n.º 283/2012 del Ministerio de Seguridad de la Presidencia de la Nación regula el sistema de video vigilancia — en el ámbito de Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval Argentina y/o Policía de Seguridad Aeroportuaria cuya finalidad es la prevención del delito, y brinda la posibilidad de que esas imágenes funcionen como prueba documental en el marco de un proceso judicial. Los principios a los que hace referencia esta norma son los de legalidad, respeto de la privacidad de las personas y transparencia; por último y en referencia a la ley 25.326 — debe cumplimentar las exigencias previstas en materia de procedimiento, tratamiento de datos, deber de reserva y confidencialidad, protección y resguardo de información, cumplimiento exclusivo de la finalidad específica de su creación, funcionamiento e inscripción de banco de datos exigidos por la Ley Nacional de Protección de Datos Personales nº 25.326. De mayor importância [...], es la disposición 10/2015 de la DNPDP que contiene una serie de principios que se aplican a los sistemas de video vigilancia en el território argentino, dichos principios (denominados condiciones de licitud en el texto de la norma) son: (i) consentimiento, (ii) respeto de la finalidad, (iii) calidad del dato, (iv) seguridad y confidencialidad, (v) ejercicio de los derechos del titular del dato,(vi) inscripción y (vii) manual de tratamiento de datos. [...] Por lo expuesto se recomienda: [...] Que se modifique la Ley nº 25.326 de Protección de Datos Personales o se sancione una ley a partir de la cual se cree, un organismo autónomo y autárquico capaz de auditar el uso de datos de los distintos organismos de Estado."*

[195] VALENTE, Jonas. Legislação da proteção de dados já é uma realidade em outros países. *Agência Brasil*, 2018. Disponível em: http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 17 abr. 2020.

[196] MÉXICO. *Nueva Ley DOF, de 05 de julho de 2010*. Ley Federal de Protección de Datos Personales em Posesión de los Particulares. Disponível em: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf Acesso em: 17 abr. 2020.

[197] MENDONÇA, Fernanda Graebin. Proteção de dados pessoais na Internet: análises comparativas da situação do direito à autodeterminação informativa no Brasil e em países latino-americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA*, 2016, v. 11, n. 1, p. 305.

legislativa para adequar o ordenamento mexicano ao RGPD, muito embora o volume de investimentos realizados pela Espanha no país seja expressivo[198].

O **Peru** também conta com legislação específica sobre proteção de dados: em 2011 foi aprovada a Lei n. 29.733[199], com foco na proteção e garantia de um adequado exercício dos direitos do titular de dados pessoais e no cumprimento de obrigações pelas entidades que realizam tratamento de dados. Alguns anos depois, em 2017, foi aprovada reforma que incluiu nova classificação de descumprimentos e infrações na matéria – contudo, o cumprimento da legislação ainda é incipiente, indicando que, futuramente, haverá adaptações ao RGPD[200].

---

[198] GARCÍA, María de los Angeles Guzmán. *El Derecho Fundamental a la Protección de Datos Personales en México:* análisis desde la influencia del orenamiento jurídico espanhol. Tese (Doutorado) – Universidad Complutense de Madrid – Facultad de Derecho, sob orientação do Prof. Dr. Ildefonso Soriano López, 2013, pp. 277-278. "Até alguns anos atrás, a regulamentação sobre o assunto era insuficiente, para não dizer nula, uma vez que não era regulamentada no nível federal, por meio de uma lei. Isso porque as iniciativas propostas pelos diferentes partidos políticos não prosperaram. [...]. Desde que a LAI foi promulgada em 2002, o direito à proteção de dados pessoais foi timidamente previsto, porque foi regulamentado em breves sete artigos do capítulo IV da referida lei, que se aplica apenas ao setor público. Mais tarde, em 2007 e 2009, com as reformas feitas na Constituição mexicana, essas mudanças na Magna Carta abririam caminho para o Congresso Federal promulgar a atual Lei Federal de Proteção de Dados Pessoais de Indivíduos, publicada no DOF em 2010." (Tradução livre). "*Hasta hace un par de años, la regulación en la materia era insuficiente, por no decir nula, al no encontrarse regulada en el ámbito federal, mediante una Ley. Esto se debía a que las iniciativas propuestas por los diferentes partidos políticos no habían prosperado. [...]. Desde que se emitió la LAI en 2002, el derecho a la protección de datos personales se encontraba tímidamente previsto porque se encontraba regulado en escuetos siete artículos del Capítulo IV de dicha Ley, que aplica solo al sector público. Posteriormente en 2007 y 2009 con las reformas hechas a la Constitución mexicana, estos cambios en la Carta Magna abrirían paso para que el Congreso Federal emitiera la actual Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicada en el DOF en 2010*."

[199] PERU. *Ley n.º 29733*. Ley de Protección de Datos Personales.

[200] VILLALTA, Luis Fernando García. *It compliance, privacidad y protección de datos para empresas públicas en el Perú*. Tese (Trabalho de Conclusão de Curso) – Universidad Nacional del Altiplano, Facultad de Ciencias Jurídicas y Políticas, Escuela Professional de Derecho, sob orientação do Prof. Dr. Javier Sócrates Pineda Ancco. Puno, Peru, 2019, pp. 61-62. "Em resposta aos problemas sociais por parte das instituições em relação ao tratamento, transferência e controle de dados pessoais, e sendo necessário estabelecer garantias que protejam a vida privada das pessoas contra a agressão informática, o Congresso da República aprovou, em 7 de junho de 2010, o Projeto de Lei nº 4079/2009-PE, que propunha a implementação da 'Lei de Proteção de Dados Pessoais', a fim de cumprir os compromissos assumidos pelo Estado de padronizar a legislação interna sobre a proteção de dados pessoais fornecidos nos Tratados internacionais dos quais o Peru faz parte. Assim, em 03 de julho de 2011, a Lei 29733, 'Lei de Proteção de Dados Pessoais' [...] foi promulgada e alterada pelo Decreto Legislativo 1.353, de 06 de janeiro de 2017, sendo regulamentado a partir de 22 de Março de 2013, por meio do DS 003-2013-JUS [...]; e em 11 de outubro de 2013, a Autoridade Nacional para a Proteção de Dados Pessoais, através da Resolução Diretiva n.º 060-2014-JUS / DGPDP, publicou a Diretiva sobre Proteção de Dados Pessoais e Programas Sociais [...], com o objetivo de orientar as medidas técnicas, organizacionais e legais de tratamento de proteção de dados, cuja conformidade é voluntária. Realizando uma análise do LPDP e de seus Regulamentos, pode-se deduzir que se destinam a garantir o direito fundamental à proteção de dados previsto na Constituição, mediante tratamento adequado, aplicável aos dados pessoais contidos nos bancos de dados pessoais da administração pública e privada. Igualmente, essas regras estabeleceram obrigações para os titulares e responsáveis pelo processamento de dados pessoais, cujas ações devem cumprir o disposto nos regulamentos já descritos e os princípios orientadores que orientam todo o tratamento de informações pessoais." (Tradução livre). "*En respuesta a la problemática social por parte de las instituciones sobre el manejo, transferencias y control de los datos personales, y siendo necesaria establecer garantías que tutelen la vida privada de las personas frente a la agresión informática, el Congreso de la República aprobó, el 07 de junio de 2010, el Proyecto de*

Ainda na América do Sul, a **Colômbia** conta com três normas específicas sobre a matéria: a Lei n. 1.266, de 2008[201], que versa sobre a proteção de dados relacionados à informação creditícia e financeira; a Lei n. 1.581, de 2012 e o Decreto n. 1.377, de 2013[202], que tratam sobre a proteção dos direitos dos titulares de dados e as obrigações das entidades que coletam e administram as informações.

Há iniciativas legislativas colombianas que defendem um ordenamento nacional harmonizado com o RGPD[203] – já que, atualmente, a legislação interna do país não dispõe

---

Ley n° 4079/2009-PE que propuso la implementación de la 'Ley de Protección de Datos Personales', con la finalidad de dar cumplimiento a los compromisos adquiridos por el Estado para homologar la legislación interna sobre la protección de datos personales dispuesta en los Tratados internacionales en los cuales Perú es parte. Es así que, el 03 de julio de 2011 se promulgó la Ley 29733 del 'Ley de Protección de Datos Personales' [...] y modificada por el Decreto Legislativo 1353" del 06 de enero de 2017, siendo reglamentada desde el 22 de marzo de 2013, mediante el DS 003-2013-JUS, [...]; y 11 de octubre de 2013 la Autoridad Nacional de Protección de Datos Personales mediante la Resolución Directoral n° 060-2014-JUS/DGPDP, publicó la 'Directiva sobre Protección de Datos Personales y Programas Sociales' [...], con la finalidad de orientar las medidas técnicas, organizativas y legales del tratamiento de protección de datos, cuyo cumplimiento es voluntario. Realizando un análisis a La LPDP y su Reglamento, se puede deducir que tienen como objeto garantizar el derecho fundamental a la protección de datos previstos en la Constitución, ello a través de un adecuado tratamiento, estos son de aplicación a los datos personales contenidos en los bancos de datos personales ya sea de administración pública y de administración privada. Asimismo, estas normas han establecido obligaciones para los titulares y encargados del tratamiento de datos personales, cuya actuación debe ajustarse al contenido de la normativa ya descrita y a los principios rectores que guían todo tratamento de la información personal."

[201] COLOMBIA. *Ley Estatutaria n. 1.266, de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.*

[202] COLOMBIA. *Ley Estatutaria n. 1.581, de 2012*. Reglamentada parcialmente por el Decreto Nacional n. 1.377, de 2013. *Por la cual se dictan disposiciones generales para la protección de datos personales.*

[203] REMOLINA-ANGARITA, Nelson. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *Rev. Colomb. Derecho Int. ildi.* Bogotá, Colômbia, jan./jun. 2010, n° 16, pp. 489-524, p. 493. "A Colômbia, assim como os demais países da América Latina, ainda não foi considerada pela Comissão Europeia como um Estado que garante um nível adequado de proteção. Para um país é importante ter esse nível por três razões: em primeiro lugar, aumenta o grau de proteção legal das informações dos cidadãos, porque o modelo tradicional europeu se caracteriza por ser garantido, rigoroso e eficaz nessa área. Em segundo lugar, gera um cenário mais competitivo para o país ser um local onde podem ser realizadas empresas que envolvem a transferência de informações pessoais da Europa, como é o caso, por exemplo, de centrais de atendimento internacionais. Por último, mas não menos importante, a proteção efetiva dos dados pessoais é considerada um elemento essencial das sociedades democráticas. [...] a Colômbia não possui um nível adequado de proteção de dados pessoais, porque a Lei n.º 1.266, de 2008, apresenta sérias limitações e deficiências em relação às demandas do modelo europeu." (Tradução livre). "*Colombia, al igual que todos los países latinoamericanos, aún no ha sido considerada por la Comisión Europea como um Estado que garantice un nivel adecuado de protección. Para un país es importante contar con ese nivel por tres puntos: en primer lugar, aumenta el grado de protección jurídica de la información ciudadana, porque el modelo europeo tradicional se ha caracterizado por ser garantista, riguroso y efectivo en esa materia. En segundo lugar, genera un escenario más competitivo para que el país sea un lugar en el que puedan realizarse negocios que implican transferencia de información personal desde Europa, tal como sucede, por ejemplo, como los call centers internacionales. Finalmente, y no menos importante, la efectiva protección de datos personales es considerada como un elemento consustancial de las sociedades democráticas. [...] Colombia no tiene um nível adecuado de protección de datos personales, porque la Ley n. 1.266, de 2008 presenta serias limitaciones y falências frente a las exigencias del modelo europeo."*

sobre o direito ao esquecimento, ou sobre a elaboração de perfis a partir dos dados coletados, tampouco sobre a designação de autoridades protetoras de dados[204].

A tendência de regulamentação da transferência de dados também atingiu países da **África**[205] e da **Ásia**. Dentre os países africanos, cumpre destacar, inicialmente, o **Zimbabué**[206], que conta com legislação protetiva de dados desde outubro de 2003, quando entrou em vigor o *Access to Information and Protection of Privacy Act*, publicado originalmente em 15 de março de 2002, com emendas em 2003, 2005 e 2008[207].

---

[204] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 70-71. "A Colômbia não possui normas específicas de determinação de jurisdição para casos com elementos internacionais, havendo certa resistência de parte da doutrina e dos tribunais quanto à sua atualização. Quanto às regras de conexão, o país possui normas que tratam do tema, contudo encontrou-se fortes críticas feitas pela doutrina em relação à sua desatualização. Sobre a jurisprudência conclui-se que ainda não há casos paradigmáticos envolvendo direito internacional privado e internet, sendo escassos os casos correlatos ao tema. [...] As regras de jurisdição colombianas estão presentes em sua Constituição e em legislações específicas, como o Código General del Proceso (GCP). A primeira estabelece, em seu art. 29, o princípio do devido processo legal como direito fundamental. Já o Código General del Processo não possui normas específicas sobre jurisdição internacional, possuindo somente normas sobre competência territorial nacional, artigo 28, que são aplicadas na determinação da competência internacional. As regras de conexão determinadoras da lei aplicável se encontram no Código Civil (CC) de 1873 e no Código de Comércio, de 1973. No geral, essas regras se caracterizam por uma técnica legislativa que privilegia a lei colombiana. No Código Civil as regras de conexão se concentram nos arts. 18 ao 21. O artigo 18 afirma o princípio de territorialidade da lei colombiana, enunciando que "a lei é obrigatória tanto aos nacionais e estrangeiros residentes na Colômbia". Assim, a princípio, prevalece a aplicação da lei colombiana por suas autoridades estatais nas relações privadas internacionais, a não ser que tratados ou convenções internacionais suprimam as normas internas. Por fim, os arts. 19, 20 e 21 estabelecem a extraterritorialidade da lei colombiana para determinados casos, como os direitos e obrigações civis de colombianos domiciliados ou residentes no estrangeiro (estatuto pessoal), direito real e regulação da forma de instrumentos públicos."

[205] COMISSÃO DA UNIÃO AFRICANA (UA); INTERNET SOCIETY (ISOC). Directrizes relativas à Protecção de Dados Pessoais para África. 09 de maio de 2018. "A pesquisa realizada pela CIPESA relativamente a essas directrizes identificou os quadros africanos seguintes que refletem os princípios de privacidade e protecção dos dados similares aos indicados supramencionados: Lei Modelo da SADC sobre a Protecção dos Dados (2010); Lei Suplementar da CEDEAO A/SA.1/01/10 sobre a Protecção de Dados Pessoais (2010); Quadro da CAO para Ciberleis (2008). De acordo com a mesma pesquisa, os países seguintes têm legislação vigente ou proposta (no momento em que estas Directrizes são escritas) que integra princípios similares relativamente aos direitos dos titulares dos dados sujeitos e ao estabelecimento de autoridades de protecção de dados: Angola (2016), Guiné Equatorial (2016), Mauritânia (2017), África do Sul (2013), Burkina Faso (2004), Mali (2013), Gabão (2011), Benim (2009), Gana (2012), Cote d´Ivoire (2013), Lesoto (2012), Madagáscar (2014), Marrocos (2009), Senegal (2008), Tunísia (2004), Zimbabué (2003). As propostas de lei da privacidade e protecção dos dados no Quénia, Níger, Nigéria, Tanzânia e Uganda também têm disposições similares."

[206] NCUBE, Caroline. A comparative analysis of Zimbabwean and South African data protection systems. *Journal of Information, Law & Technology*, 2004, v. 2, p. 18.

[207] ZIMBABUÉ. *Access to Information and Protection of Privacy Act*, 2003. Disponível em: https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Zimbabwe_Access%20to%20Information%20Law_2008_en.pdf. Acesso em: 08 mar. 2020. "Para proporcionar aos membros do público o direito de acesso a registros e informações mantidos por órgãos públicos; responsabilizar os órgãos públicos, concedendo ao público o direito de solicitar a correção de informações pessoais deturpadas; impedir a coleta, uso ou divulgação não autorizada de informações pessoais por órgãos públicos; proteger a privacidade pessoal; prever a regulamentação dos meios de comunicação de massa; estabelecer uma Comissão de Mídia e Informação e providenciar assuntos relacionados a ela ou incidentais aos itens anteriores." (Tradução livre). "*To provide members of the public with a right of access to records and information held by public bodies; to make public bodies accountable by giving the public a right to request correction of misrepresented personal information; to prevent the unauthorised collection, use or disclosure of personal information by public bodies; to protect personal privacy; to provide for the*

Já no caso de **Gana**[208], há discussão atualmente em curso sobre uma possível nova norma protetiva de dados[209], destacando-se, entre aquelas já existentes, o *Electronic Transaction Act* (ETA), de 2009[210], e o *Data Protection Act*, datado de 2012[211].

No ano seguinte (2013) foi aprovada a lei protetiva nacional da **África do Sul**, *Protection of Personal Information Act (PROPIA)*[212]. Trata-se do primeiro instrumento normativo sobre o tema no país, o qual dispõe que o direito à privacidade informacional é derivado do direito constitucional à privacidade[213], regulamentando o tratamento de

---

regulation of the mass media; to establish a Media and Information Commission and to provide for matters connected therewith or incidental to the foregoing."

[208] MAKULILO, Alex Boniface. Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2012, v. 2, n. 3, pp. 163-178.

[209] BUSINESS GHANA. *We are working on a cyber security law* – Ursula meets the press [online]. 14 dez. 2018. Disponível em: https://www.businessghana.com/site/news/General/178337/We-are-working-on-a-cyber-security-law-Ursula-meets-the-press (full-address). Acesso em: 06 jan. 2020. "A Lei de Proteção de Dados de 2012 exige que a Comissão de Proteção de Dados proteja a privacidade dos dados pessoais e pessoais, regulando o processamento de informações pessoais, estabelecendo o processo para obter, manter, usar ou divulgar informações pessoais e assuntos relacionados. O DPC criou, portanto, uma estrutura regulatória que garantirá que o direito e a privacidade dos indivíduos sejam respeitados como um direito humano [...]. Em 2018, o DPC registrou 1.264 controladores de dados e embarcou em vários programas de conscientização e treinamento. Um treinamento para profissionais de proteção de dados com um manual completo de conformidade com o GDPR da UE foi testado com sucesso." (Tradução livre). "*The Data Protection Act, 2012 mandates the Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters. The DPC has therefore created a regulatory framework that will ensure that the right and privacy of individuals are respected as a human right [...]. In 2018, the DPC registered 1,264 data controllers and embarked on several awareness creation and training programs. A Data Protection Practitioner training with a full EU-GDPR compliance manual has been successfully piloted*."

[210] GANA. *Electronic Transactions Act*, 2008. Disponível em: https://www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf. Acesso em: 08 mar. 2020.

[211] GANA. *Data Protection Act*, 2012. Disponível em: http://media.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf Acesso em: 08 mar. 2020. "Um ato para estabelecer uma Comissão de Proteção de Dados, para proteger a privacidade dos dados individuais e pessoais, regulando o processamento de informações pessoais, para fornecer o processo para obter, manter, usar ou divulgar informações pessoais e assuntos relacionados." "*An act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters*."

[212] ÁFRICA DO SUL. *Protection of Personal Information Act (PROPIA*), 2013. Disponível em: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersona linforcorrect.pdf. Acesso em: 08 mar. 2020. "Para promover a proteção das informações pessoais processadas por órgãos públicos e privados; introduzir certas condições para estabelecer requisitos mínimos para o processamento de informações pessoais; prever a criação de um regulador da informação para exercer certos poderes [...]; prever a emissão de códigos de conduta; garantir os direitos das pessoas em relação às comunicações eletrônicas não solicitadas e à tomada de decisão automatizada; regular o fluxo de informações pessoais através das fronteiras da República; e providenciar assuntos relacionados a ela." (Tradução livre). "*To promote the protection of personal information processed by public and private bodies; to introduce certain conditions as to establish minimum requireents for the processing of personal information; to provide for the establishment of na Information Regulator to exercise certain powers [...]; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith*."

[213] NCUBE, Caroline. Op. cit., 2004, v. 2, p. 18. "A *common law* do Zimbábue e da África do Sul são a mesma. A lei romano-holandesa influenciou fortemente os dois países. [...] Claramente, o direito do Zimbábue deriva do direito da África do Sul. E, de acordo com a *common law*, toda pessoa tem direitos de

informações pessoais na África do Sul a partir de sua entrada em vigor, prevista para 01 de abril de 2020.

Dentre os países africanos cumpre mencionar, por fim, **Angola**[214], cuja legislação protetiva de dados é mais recente, tendo a Lei de Proteção das Redes e Sistemas Informáticos entrado em vigor em fevereiro de 2017. A Lei em questão objetiva oferecer maior segurança e garantias no tratamento e transferência de dados, bem como fomentar a inclusão digital e o acesso à informação[215].

Na Ásia, o **Japão**[216] conta com a Lei de Proteção de Dados pessoais que estabelece responsabilidades para as empresas que realizam o tratamento e regula a transferência transnacional dos dados, contudo, ela não oferece tantas garantias quanto o RGPD[217].

---

personalidade, como direitos à integridade física, liberdade, reputação, dignidade e privacidade (SALC IP24 em 3.1.16, Neethling 1998 em 64, 103, 137, 157, 233, 265)." (Tradução livre). "*Zimbabwean and South African common law is the same. Roman-Dutch Law has heavily influenced both countries. [...] Clearly, the common law of Zimbabwe derives from the common law of South Africa. And under the common law every person has personality rights such as the rights to physical integrity, freedom, reputation, dignity, and privacy (SALC IP24 at 3.1.16, Neethling 1998 at 64, 103, 137, 157, 233, 265)*."

[214] ANGOLA. *Lei n. 7, de 16 de fevereiro de 2017*. Lei de Proteção das Redes e Sistemas Informáticos. Disponível em: https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf. Acesso em: 08 mar. 2020. "A presente Lei visa responder, de forma eficaz e eficiente, aos novos desafios da sociedade da informação, à proteção da utilização do espaço cibernético angolano contra os riscos a eles associados e promover a inclusão digital. Pretende, ainda, [...], melhorar a oferta da prestação de serviços digitais, o acesso dos cidadãos à informação e ao conhecimento."

[215] TRAÇA, João Luís; EMBRY, Bernardo. The Angolan Data Protection Act: first impressions. *International Data Privacy Law*, 2012, v. 2, n. 1, p. 40. "Embora a Lei de Protecção de Dados tenha sido promulgada pela Assembleia Nacional como um instrumento através do qual os direitos humanos inalienáveis poderiam ser consagrados neste contexto particular, o legislador angolano demorou muito tempo para elaborar o estatuto, de modo a incorporar um respeito saudável das necessidades pelas empresas, de forma a conduzir suas operações da maneira mais rápida e tranquila possível. Esta lei é um reflexo da Angola contemporânea, na sequência de várias outras reformas legislativas em um momento no qual os negócios em Angola crescem em um ritmo cada vez maior, sem sinais de desaceleração tão cedo. Reforçada por disposições que impõem graves consequências pelo não cumprimento de seus termos, incluindo multas consideráveis de até meio milhão de dólares, a nova Lei de Proteção de Dados busca atuar como baluarte do direito à privacidade pessoal ao mesmo tempo em que reduz ao mínimo os obstáculos possíveis às operações comerciais éticas. Embora adote muito do quadro de proteção de dados da UE e da prática reguladora portuguesa, o resultado final é uma lei que é muito um produto de uma Angola em rápido desenvolvimento." (Tradução livre). "*While the Data Protection Act may have been enacted by the National Assembly as an instrument through which inalienable human rights could be enshrined in this particular context, the Angolan legislator took time and care in framing the statute so as to incorporate a healthy respect for the needs of businesses to conduct their operations as swiftly and as smoothly as possible. This Act is very much a reflection of contemporary Angola, following on from several other legislative reforms at a time when business in Angola is growing at an increasingly fast pace, with no sign of slowing down anytime soon. Bolstered by provisions imposing severe consequences for a failure to comply with its terms, including sizeable fines of up to nearly half a million US dollars (US$), the new Data Protection Act aspires to act as a bulwark for the right to personal privacy at the same time as it keeps to a minimum possible hindrances to ethical business operations. Though it borrows much from both the EU data protection framework and Portuguese regulatory practice, the end result is a law that is very much a product of a rapidly-developing Angola*."

[216] JAPÃO. *Lei n. 57, de 2003*. Lei de Proteção de Informações Pessoais (APPI). Disponível em: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf. Acesso em: 17 abr. 2020.

[217] SIMÃO, Rui Jorge Costa. Alinhamento da União Europeia e Japão sobre Proteção de Dados – e "Step in Japan". *República do Direito:* Associação Jurídica de Coimbra, dez. 2018. "O Japão não é um Estado-

No âmbito do G20, o Japão também se manifestou favorável à governança mundial de dados, lançando no ano de 2019 a "*Osaka Track*", estrutura para a promoção do fluxo seguro de dados entre diferentes países. O primeiro-ministro japonês manifestou-se quanto à importância da "*Data Free Flow with Trust*" (DFFT) em reunião em que diversos países, dentre eles o Brasil, assinaram declaração sobre a economia digital[218].

China[219], **Rússia**[220] e **Índia**[221] são alguns países cujas regulamentações são mais restritivas quanto à transferência de dados. De forma geral, contudo, observa-se a crescente

---

Membro da UE e, portanto, não implementou o GDPR ou a Diretiva de Proteção de Dados. No entanto, a Lei de Proteção de Informações Pessoais (Lei n. 57, de 2003) (a APPI) contém disposições similares. O ACT para alterar a APPI (a Emenda APPI) entrou em vigor integralmente em 30 de maio de 2017. As referências neste resumo à Emenda API indicam as alterações feitas pela emenda. A Emenda APPI permite a divulgação dos chamados *big data* sem obter o consentimento dos titulares de dados e restringe as transferências de dados para um terceiro país sem obter consentimento dos sujeitos de dados onde o nível de proteção de dados é insuficiente. Em outubro de 2015, a Lei sobre o Uso, de Números para Identificar Indivíduos Específicos em Procedimentos Administrativos (Lei n.º 27 de 2013) (a chamada Lei de "Meu Número" – "*My Number"* seu nome original) entrou em vigor, sob a qual um número de ID é alocado a cada indivíduo para que o governo possa administrar os sistemas de segurança social e de impostos de forma eficaz. Por favor, note que este memorando não cobre o *My Number Act*, que é uma lei especial do APPI. [...] O APPI entrou integralmente em vigor em 1º de abril de 2005, seguido pela Emenda APPI, que entrou em vigor em 30 de maio de 2017."

[218] LUCA, Cristina de. G20: Japão propõe que governança mundial de dados seja prioridade. *Blog Porta 23* (Uol). Disponível em: https://porta23.blogosfera.uol.com.br/2019/06/29/g20-japao-propoe-que-governanca-mundial-de-dados-seja-prioridade/. Acesso em: 17 abr. 2020. "Índia, Indonésia e África do Sul não estiveram presentes à reunião. E a índia se recusou formalmente a assinar a declaração. O governo indiano está preocupado com o fato de as empresas chinesas abusarem dos dados indianos, apesar [de] haver algumas semelhanças em como ambos os países protegem os dados de seus cidadãos. [...] A ideia é que a confiança deve ser melhorada para promover fluxos de dados gratuitos. Importantes dados industriais, por exemplo, poderiam se mover mais livremente entre os países com a garantia de fortes medidas de segurança cibernética e salvaguardas de propriedade intelectual. [...]. A maior preocupação é com o surgimento de uma *splinternet* – uma internet fragmentada como resultado de diferentes regulamentações nacionais. [...]. O perigo é que abordagens fragmentadas à privacidade de dados possam impactar negativamente o comércio internacional. Afinal, o fluxo livre de dados através das fronteiras é vital para o crescimento econômico na era digital. Reduz as restrições de distância, reduz os custos de transação, acelera a disseminação de novas ideias e modelos de negócios e reduz as barreiras à entrada no mercado, permitindo que empresas de todos os portes atendam a um vasto público global."

[219] ZHANG, Gil; YIN; Kate. More updates on the Chinese data protection regime in 2019. *International Association of Privacy Professionals.* Disponível em: https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/. Acesso em: 08 mar. 2020. Na China, cumpre destacar a Diretriz Reguladora de Proteção de Dados, de junho de 2019, bem como a lei chinesa de cibersegurança, em vigor desde junho de 2017. Na Diretriz de 2019 são estabelecidas regras específicas sobre a coleta e o uso de dados de clientes, referência importante para uma futura lei nacional sobre proteção de dados. "Em 1º de fevereiro, o Comitê Técnico Nacional de Padronização da Segurança da Informação da China submeteu propostas de revisões da Especificação de Segurança da Informação Pessoal padrão nacional (ref. GB / T 35273-2017) à consulta pública. Em 2 de fevereiro, o Centro de Tecnologia e Certificação da China Cyber Security Review anunciou [...] o programa de conformidade de proteção de dados pessoais de algumas empresas, [...]. A partir de 1º de maio de 2018, o Padrão Nacional foi aplaudido por fornecer clareza sobre o que é esperado dos programas de conformidade de proteção de dados na China. Embora o Padrão Nacional seja um padrão recomendado e não seja de adoção obrigatória para as empresas, as autoridades chinesas têm usado o Padrão Nacional em diversas ações policiais para avaliar se uma empresa cumpriu o requisito de 'implementar medidas técnicas e outras necessárias para proteger dados pessoais', conforme exigido pela Lei de Segurança Cibernética. O Padrão Nacional vem funcionando como *soft law* na China há algum tempo, tornando crítico para as empresas avaliar o *benchmarking* do programa de proteção de dados pessoais em relação a ele. As revisões do Padrão Nacional indicam a expectativa dos reguladores sobre o cumprimento das empresas com a CSL." (Tradução livre). "*On Feb. 1, China's National Information Security Standardization Technical*

Committee introduced proposed revisions to the national standard Personal Information Security Specification (ref. GB/T 35273–2017) for public consultation. On Feb. 2, the China Cyber Security Review Technology and Certification Center announced […] the personal data protection compliance program of some companies, [...]. Effective May 1, 2018, the National Standard was applauded for providing clarity on what is expected for data protection compliance programs in China. Although the National Standard is a recommended standard and is not mandatory for companies to adopt, Chinese authorities have been using the National Standard in various law enforcement actions to assess whether a company has met the requirement of "implementing technical and other necessary measures to protect personal data" as required under the Cybersecurity Law. The National Standard has been functioning as China's de facto "soft law" for some time, making it critical for companies to evaluate personal data protection program benchmarking against the National Standard. The revisions to the National Standard indicate the regulators' expectation on companies' compliance with the CSL."

[220] DLA PIPER. *Data Protection Laws of the World.* Russia, March 2020. Disponível em: www.dlapiperdata protection.com. Acesso em: 08 mar. 2020. "As disposições fundamentais da legislação de proteção de dados na Rússia podem ser encontradas na Constituição russa, em tratados internacionais e em leis específicas. A Rússia é membro da Convenção de Estrasburgo para a proteção de indivíduos em relação ao processamento automático de dados pessoais (Convenção) (ratificada pela Rússia em 2006) e a Constituição da Rússia estabelece o direito à privacidade de cada indivíduo (artigos 23 e 24). A maioria das regras encontra-se em legislação específica, particularmente a Lei de Proteção de Dados n.º 152 FZ, de 27 de julho de 2006 (DPA) e vários atos regulamentares adotados para implementar a DPA, bem como outras leis, incluindo a Lei de Informações, Tecnologias da Informação e Proteção de Informações 149 FZ, de 27 de julho de 2006, que estabelece regras básicas para as informações em geral e sua proteção. Além disso, o Código do Trabalho da Rússia contém disposições sobre a proteção dos dados pessoais dos funcionários (Parte XIV). [...] Em 22 de julho de 2014, foram adotadas emendas importantes à DPA, que entraram em vigor em 1 de setembro de 2015. As alterações exigem que todos os operadores de dados pessoais armazenem e processem quaisquer dados pessoais de indivíduos russos em bancos de dados localizados na Rússia (sujeito a poucas exceções). A penalidade pela violação deste requisito é, em última análise, o bloqueio de sites que envolvem tratamento ilegal de dados pessoais russos. [...] Como as emendas foram aprovadas recentemente e um histórico de execução e interpretação legal não foi estabelecido, ainda não está claro como esse registro e o bloqueio do site funcionariam na prática. De acordo com os esclarecimentos dos reguladores russos, o armazenamento e o processamento de dados pessoais de indivíduos russos fora da Rússia ainda podem estar em conformidade com a lei, desde que o armazenamento e o processamento primário (geralmente interpretado como inicial) sejam realizados na Rússia. Ainda é uma questão em aberto se a manutenção de bancos de dados 'espelhados' na Rússia e em outros lugares seria considerada compatível." (Tradução livre). "*Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). […] On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. [...] As the amendments are newly passed and a track record of enforcement and legal interpretation has not been established, it is still unclear as to how this register and the website blocking would work in practice. According to clarifications of Russian regulators, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as primary (often interpreted as initial) storage and processing of data is done in Russia. It is still an open question whether keeping 'mirror' databases in Russia and elsewhere would be deemed as compliant*."

[221] BAHL, Aman; BHARSAKLE, Sarthak. Op. cit., dez. 2019. Disponível em: https://ijlpp.com/the-privacy-jungle-comparative-study-of-the-indianpersonal-data-protection-act-2018-with-eu-gdpr-and-california-privacy-law/. Acesso em: 06 jan. 2020. "Em 2018, um comitê especialista de Estrutura de Proteção de Dados para a Índia, presidido pela Justiça BN Srikrishna, apresentou seu tão aguardado relatório intitulado 'Uma economia digital livre e justa – Protegendo a privacidade, capacitando os indianos', apresentando uma silhueta sobre o projeto de Lei de Proteção de Dados Pessoais (PDP) de 2018. [...] Na esteira da

importância das discussões atreladas à privacidade e à proteção de dados por todo o mundo, fugindo do escopo do presente estudo, que é realizar uma análise comparativa exaustiva das normas existentes[222].

Conclui-se, a partir dos exemplos selecionados e apontados neste tópico, que o RGPD tem sido utilizado por diversos países como referência no estabelecimento de direitos e garantias mínimas, atingindo, inclusive, a produção normativa brasileira.

1.7 TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL

A preocupação com as mudanças trazidas pela internet não ficou restrita aos países europeus. O Brasil é exemplo de país sobre o qual o Regulamento Europeu exerceu forte influência, levando à aprovação da Lei Geral de Proteção de Dados (LGPD)[223].

---

conscientização promovida pela UE e pelos primeiros países de primeiro mundo, os esforços feitos por parte da Índia não podem ser prejudicados. A Índia sempre foi o ponto de partida para investimentos empresariais e inovou métodos de engenharia; portanto, os passos dados nessa direção não devem ser vistos simplesmente como imitando o mundo ocidental." (Tradução livre). "*In 2018, an expert Committee on Data Protection Framework for India chaired by Justice B. N. Srikrishna, submitted its much-awaited report titled "A Free and Fair Digital Economy – Protecting Privacy, Empowering Indians" giving a silhouette on the Personal Data Protection (PDP) Bill, 2018. [...] In the wake on such awareness brought forward by the EEU and the first world countries, efforts made on the part of India cannot be undermined. India has always been the hot-spot for business investments and innovate engineering methods, therefore the steps taken forward in this direction should not be simply viewed as mimicking the West World*."

[222] GREENLEAF, Graham. Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, 2012, n. 115. O artigo, originalmente publicado em 2012, foi revisado em 2017, resultando em um total de 120 leis nacionais distintas sobre privacidade e proteção de dados, em detrimento das 89 leis tratadas originalmente. Importante ressaltar que se trata de assunto extremamente atual e dinâmico, de forma que as mudanças ocorrem de forma constante, sendo este um dos principais desafios encontrados em termos de direito material ao longo da elaboração da presente dissertação. A partir da revisão realizada pelo autor, foi constatado que: "Nos últimos dois anos, o número de países que promulgaram leis de privacidade de dados aumentou de 109 para 120, um aumento de 10%, com pelo menos mais 30 países contando com projetos de lei em vários estágios de progresso. Essas 120 jurisdições têm leis abrangentes de privacidade de dados para o setor privado, o setor público, ou (na maioria dos casos) ambos, e as leis atendem pelo menos aos padrões formais mínimos baseados em acordos internacionais. [...] o aumento de 10% nos países com leis de privacidade de dados para 120, os 30 ou mais países que planejam promulgar tais leis e os projetos de lei para fortalecer as leis existentes, todos enfatizam a contínua expansão global de dados de leis de privacidade. A expansão da Convenção 108 para além da Europa está lentamente tornando evidente que é o único tratado global viável de privacidade de dados, reforçado pelos desenvolvimentos na UE e na União Africana. São desenvolvimentos muito positivos, mas o ambiente internacional incerto não oferece garantias de que eles continuarão." (Tradução livre). "*In the past two years, the number of countries that have enacted data privacy laws has risen from 109 to 120, a 10% increase, with at least 30 more countries having official Bills for such laws in various stages of progress. These 120 jurisdictions have comprehensive data privacy laws for the private sector, public sector, or (in most cases) both, and the laws meet at least minimum formal standards based on international agreements. [...] the 10% increase in countries with data privacy laws to 120, the 30 or more additional countries planning to enact such laws, and the bills to strengthen existing laws, all underline the continuing global expansion of data privacy laws. The expansion of Convention 108 beyond Europe is slowly making it apparent that it is the only viable global data privacy treaty, reinforced by developments in the EU and the African Union. These are very positive developments, but the uncertain international environment provides no guarantees that they will continue.*"

[223] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 44-45. Sobre a responsabilidade no Projeto de Lei convertido na LGPD: "O artigo 35 do PL no

Anteriormente, a privacidade já era um direito tutelado tanto pela Constituição Federal quanto pela legislação infraconstitucional.

A proteção oferecida, porém, era limitada, pois não trazia sequer uma definição explícita do conceito de dados pessoais. O Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados (LGPD) são essenciais para a regulação do espaço virtual[224], principalmente se for considerada a ampliação do acesso à rede pelos brasileiros[225].

5.276/2016, em consonância ao que dispõe no seu artigo 42, faz opção pelo *regime de responsabilidade civil objetiva*, significando isso que a imputação de danos ao agente de tratamento de dados pessoais não é determinada pela falta de diligência, ou desconformidade a um *standard* de conduta, ao realizar operação com informação pessoal. [...] Sendo, porém, confirmada no Brasil a opção pelo regime de responsabilidade objetiva no terreno da atividade de tratamento de dados pessoais, como atualmente se apresenta no PL n. 5.276/2016, a responsabilização por danos decorrentes de ilícita transferência internacional de informações pessoais haverá de ser, em grande medida, uma discussão sobre causalidade, [...]. Se o debate for travado judicialmente, será possível exigir do agente de tratamento de dados pessoais a inequívoca comprovação de excludente de responsabilidade: só assim se afastará o reconhecimento da obrigação de indenizar, porquanto admissível é a distribuição dinâmica do ônus da prova a fim de evitar que o titular de dados tenha que se desincumbir de prova diabólica, ou seja, impossível (Código de Processo Civil, art. 373, § 1º; PL n. 5.276/2016, art. 42, parágrafo único). [...]. Nesse sentido, se a transmissão de informações de natureza pessoal para país estrangeiro tiver ensejo com ato de sujeito integrante do quadro organizacional de determinado ente, fato de terceiro não existe, ainda que o ato praticado não seja da atribuição ou competência do autor da ilícita transferência. Por sua vez, caso fortuito ou de força maior como hipótese interruptiva do nexo de causalidade têm as marcas da imprevisibilidade e da inevitabilidade. Se o fato não tiver essas características, a excludente de responsabilidade não se configura. Se, porém, houver dano ressarcível imputado ao emissor e/ou ao receptor de dados pessoais em fluxo transnacional, o adimplemento da obrigação de indenizar que surge pode ser exigida de um e/ou outros agente de tratamento de dados pessoais, em razão responsabilidade solidária. Nesses casos, aplica-se o regime das obrigações solidárias positivado nos arts. 275 a 285 do Código Civil brasileiro. A dicção do art. 44 do projeto de lei é expressa neste sentido."

[224] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, jul./dez. 2011, n. 12, n. 2, pp. 91-108, p. 92. "A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação. Os dados pessoais chegam a fazer as vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável. O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental."

[225] FEBRABAN. Federação Brasileira de Bancos. *Pesquisa FEBRABAN de Tecnologia Bancária*, 2019. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 13 out. 2019. "Nas edições anteriores de nosso estudo, observamos um movimento consistente de fortalecimento do *mobile banking*, que, ano a ano, ampliou o seu alcance e a sua relevância nas operações bancárias realizadas pelos consumidores. Desta vez, identificamos que o *mobile banking* rompeu mais uma importante fronteira: a da realização de transações com movimentação financeira como pagamentos de contas e transferências (incluindo DOC e TED). O fato de que os consumidores estão priorizando o celular para efetuar essas operações é um indicador da confiança que depositam nos bancos e de que as instituições financeiras estão no caminho certo em relação à oferta de soluções que reúnem praticidade e segurança."

1.7.1 Constituição Federal

No âmbito constitucional, a Magna Carta prevê expressamente a inviolabilidade da intimidade e da vida privada, elevando-as ao *status* de garantias e direitos fundamentais[226], cujo tema é ressaltado em seu art. 5º, inc. X[227].

Há previsão, ainda, de vedação da violação do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas[228], assim como a garantia do "acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional"[229] e do "direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado"[230].

Além dos dispositivos supramencionados, os quais tratam especificamente da privacidade, a Constituição Federal de 1988 também prevê o remédio constitucional descrito no seu art. 5º, inc. LXXII[231], denominado *habeas data*, destinado especificamente ao acesso e retificação de dados constantes em bancos de dados públicos. De fato, anterior à Constituição Federal de 1988 não havia a tutela específica do direito à privacidade, a qual passou a ser entendida como um direito fundamental subjetivo[232].

---

[226] BRASIL (Constituição, 1988). Constituição da República Federativa do Brasil de 1988, art. 5º, inc. X. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 17 abr. 2020.

[227] INTERNETLAB. Pesquisa em Direito e Tecnologia. *Semanário*, 10 dez. 2019. Disponível em: http://www.internetlab.org.br/pt/itens-semanario/dados-pessoais-apresentado-parecer-pela-aprovacao-de-pec-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-fundamentais/. Acesso em: 04 jan. 2020. "Legislativo. [Dados Pessoais]. Apresentado parecer pela aprovação de PEC que inclui a proteção de dados pessoais no rol de direitos fundamentais. No dia 4.12.2019, o deputado Orlando Silva (PCdoB-SP) apresentou à Comissão Especial o parecer pela aprovação, nos termos do substitutivo, da Proposta de Emenda à Constituição nº 17/2019, que inclui o direito à proteção de dados pessoais, inclusive nos meios digitais, no art. 5º da Constituição Federal, estabelecendo-o como direito fundamental. [...] o substitutivo apresentado por Orlando Silva propõe que o direito à proteção de dados pessoais seja incluído em um inciso autônomo, e não como parte do inciso XII, que estabelece o direito ao sigilo das comunicações. A redação do substitutivo inclui, ainda, um inciso no art. 21 da Constituição, determinando ser de competência da União organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei, inclusive com a criação de uma agência reguladora, que deverá ser independente e integrar a administração pública federal indireta. O parecer vai ser apreciado pela Comissão Especial e, depois, o projeto deve seguir para votação no plenário da Câmara."

[228] BRASIL. Constituição Federal de 1988, art. 5º, inc. XII. Op. cit., 1988.

[229] Id., ibid., art. 5º, inc. XIV.

[230] Id., ibid., art. 5º, inc. XXXIII.

[231] Id., ibid., art. 5º, inc. LXXII.

[232] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da USP*, 1993, p. 440 *et seq.*: "O sigilo de dados é uma hipótese nova, trazida pela Constituição Federal de 1988. [...]. Trata-se de um direito subjetivo fundamental. Como direito subjetivo, manifesta uma estrutura básica, cujos elementos são o *sujeito*, o *conteúdo* e o *objeto*. [...] A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros

Embora existam acordos internacionais com o intuito de uniformizar a matéria relativa à privacidade e à proteção de dados, esses são de caráter tributário, referindo-se aqui especificamente ao FATCA[233] (Lei de Conformidade Tributária de Contas Estrangeiras)[234], ou de cooperação jurídica internacional em matéria penal[235].

No âmbito penal, apesar de não fazer parte deste estudo, há de se ressaltar duas discussões relevantes ligadas ao tema e a disposições da Constituição Federal: as demandas judiciais envolvendo sigilo telefônico, e as questões relacionadas à competência da Unidade de Inteligência Financeira (UIF), órgão administrativo denominado, em 1998, quando foi criado, de Conselho de Controle de Atividades Financeiras (COAF).

Neste último caso, houve, recentemente, julgamento de Recurso Extraordinário pelo colegiado do Supremo Tribunal Federal[236], definindo teses sobre o compartilhamento de dados entre o Ministério Público e os órgãos de inteligência fiscal em processos penais. Ainda há, contudo, aspectos que deverão ser esclarecidos, como se as teses de repercussão

---

ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão. [...] No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito."

[233] BRASIL. *Decreto n.º 8.506, de 24 de agosto de 2015*. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América para melhoria da observância tributária internacional e implementação do FATCA, firmado em Brasília, em 23 de setembro de 2014. *Diário Oficial da União*, Brasília, 2015. Disponível em: http://www. planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/D8506.htm. Acesso em: 17 abr. 2020. Sob este aspecto, cabe que no final de 2014, Brasil e Estados Unidos anunciaram a assinatura do Acordo de Cooperação Intergovernamental (IGA) para adoção do FATCA, Lei de Conformidade Tributária de Contas Estrangeiras, ou *Foreign Account Tax Compliance Act*. O FATCA não trata da proteção de dados pessoais, mas sim do fornecimento de dados por parte de instituições bancárias estrangeiras a autoridades norte-americanas, desde que os correntistas em questão sejam, também, cidadãos dos Estados Unidos. O acordo foi promulgado por meio do Decreto n.º 8.506, de 2015, a partir do Acordo para Melhoria da Observância Tributária Internacional e Implementação do FATCA, firmado em Brasília, em 23 set. 2014.

[234] Apesar da existência de tal acordo com os Estados Unidos envolvendo a transferência, armazenamento e tratamento de dados específicos, o instrumento não se presta à proteção dos dados pessoais, mas sim à troca automática de dados em poder de instituições financeiras.

[235] INTERNETLAB. Pesquisa em Direito e Tecnologia. *Vigilância das comunicações pelo Estado brasileiro.* São Paulo, 2015. p. 13. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf Acesso em: 17 abr. 2020. Tais acordos internacionais em matéria penal podem: (i) exigir dupla incriminação; (ii) exigir dupla incriminação em exceções; ou (iii) não exigir dupla incriminação.

[236] STF. Supremo Tribunal Federal. *Recurso Extraordinário n.º 1055941*. Rel. Min. Dias Toffoli. Julgado em 04/12/2019. "Decisão: O Tribunal, por maioria, aderindo à proposta formulada pelo Ministro Alexandre de Moraes, fixou a seguinte tese de repercussão geral: '1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional. 2. O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios', vencido o ministro Marco Aurélio, que não referendava a tese. Presidência do Ministro Dias Toffoli. Plenário, 04.12.2019."

geral fixadas se aplicam somente a crimes tributários e aduaneiros, ou se poderão ser aplicadas a outros delitos.

Para que os preceitos constitucionais sejam efetivamente respeitados, é necessário determinar a distinção entre investigação fiscal e investigação criminal à revelia do contribuinte, já que a esfera criminal conta com garantias específicas. As teses fixadas não impedem o compartilhamento de informações sigilosas entre a Receita Federal e o Ministério Público, mesmo sem a participação da polícia judiciária ou do juízo penal.

Falharam, porém, ao garantir o direito ao sigilo fiscal, que tem o propósito de impedir a realização de investigações sem a devida observância do princípio do contraditório ou da ampla defesa, tampouco o conhecimento do investigado. Ainda que o objetivo em tese seja combater a corrupção e a lavagem de dinheiro, a decisão é passível de críticas por ampliar o rol dos agentes responsáveis pelo tratamento de dados sigilosos e, principalmente, por abdicar do controle de legalidade prévio pelo Judiciário nas hipóteses ali determinadas. Atualmente, a Receita compartilha relatórios contendo dados sigilosos com a polícia e o Ministério Público, sem a necessidade de ordem judicial prévia, o que é questionável do ponto de vista das garantias penais e constitucionais.

Em segundo lugar, há repetidos julgados acerca do sigilo das comunicações telefônicas para fins de persecução penal, analisando, principalmente, o alcance da norma contida no art. 5º, inc. XII, da Constituição Federal de 1988 (previsão da inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, neste último caso, por ordem judicial nas hipóteses previstas em lei para fins de investigação criminal ou instrução processual penal)[237].

Até a edição da Lei n.º 9.296, em 1996, o entendimento jurisprudencial era no sentido da impossibilidade de interceptação telefônica (mesmo mediante autorização judicial), em investigação criminal ou instrução processual penal, pois não se considerava recepcionado pela Carta Magna o art. 57, inc. II, da Lei n.º 4.117, de 1962 (Código Brasileiro de Telecomunicações)[238].

---

[237] GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. *Revista de Direito Administrativo*, 1997, n. 207, p. 21. "Foi a Comissão de Redação que, exorbitando de seus poderes, acrescentou ao texto as palavras 'comunicações', 'no último caso' e 'penal', limitando consideravelmente o alcance da norma constitucional legitimamente aprovada em plenário. [...] No meu sentir, a redação restritiva do inciso XX do art. 5º da Constituição é formalmente inconstitucional, por vício de competência e afronta ao processo legislativo. [...] resta saber se o vício teria ficado superado pela promulgação. Tudo indica que não: assim como a sanção não sana o defeito de iniciativa, no tocante às normas infraconstitucionais, do mesmo modo parece-me que a promulgação, em bloco, não teve o condão de convalidar a norma, viciada pela competência e pela violação ao processo legislativo (votação em dois turnos)."

[238] STF. Supremo Tribunal Federal. *HC 81.154*. Rel. Min. Maurício Corrêa, publicado em 19/12/01. "Interceptação telefônica. Prova ilícita. Autorização judicial deferida anteriormente à Lei nº 9.296/96, que

Colidem, portanto, os princípios da proibição da prova ilícita que visam à proteção do sigilo das comunicações e da proporcionalidade, e que permitem o afastamento de determinada norma. Importante a discussão relativa à admissibilidade da prova ilícita – já que esta poderá, por exemplo, ser obtida pela violação das comunicações eletrônicas, inexistindo consenso jurisprudencial a respeito.

Se, por vezes, a jurisprudência admite a produção ilícita de provas mediante violação do sigilo das comunicações telefônicas[239], em tese seria possível o julgador afastar a norma do art. 5º, que prevê o sigilo dos demais meios de comunicação[240] – especialmente em casos de crimes cibernéticos graves, como ameaças terroristas ou difusão de conteúdo de pedofilia.

O uso da internet, conforme apontado, estabelece uma série de relações nas quais há possibilidade de dano transnacional. Nesse contexto, a previsão constitucional, de caráter genérico, e os acordos internacionais, demasiado específicos, não são suficientes para garantir a regulação da matéria em todas as esferas da vida. É necessário, portanto, analisar tais normas conjuntamente com outros dispositivos de natureza infraconstitucional.

1.7.2 Legislação infraconstitucional

Infraconstitucionalmente, há uma série de diplomas normativos relacionados à privacidade e à proteção de dados, os quais merecem análise, inclusive para avaliar a sua

---

regulamentou o inc. XII do art. 5º da Constituição Federal. Nulidade da ação penal por fundar-se exclusivamente em conversas obtidas mediante quebra dos sigilos telefônicos dos pacientes."

[239] STF. Supremo Tribunal Federal. *Habeas Corpus 75.261 MG*. Rel. Min. Octávio Gallotti – Julgado em 24/06/1997. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/14700087/habeas-corpus-hc-75261-mg?ref=serp. Acesso em: 17 abr. 2020. "Interceptação telefônica e gravação de negociações entabuladas entre sequestradores, de um lado, e policiais e parentes da vítima, de outro, com o conhecimento dos últimos, recipiendários das ligações. Licitude desse meio de prova. Precedente do STF (HC 74.678, 1ª Turma, 10-6-97). 2. Alegação improcedente de perda de objeto do recurso do Ministério Público estadual. 3. Reavaliação do grau de culpabilidade para fins de revisão de dosagem da pena. Pretensão incompatível com o âmbito do *habeas corpus*. 4. Pedido, em parte, deferido, para suprimento da omissão do exame da postulação, expressa nas alegações finais, do benefício da delação premiada (art. 159, § 4º, do Código Penal), mantidas a condenação e a prisão."

[240] ABREU, Jacqueline de Souza; SMANIO, Gianluca Martins. Compatibilizando o uso de tecnologia em investigações com direitos fundamentais: o caso das interceptações ambientais. *Revista Brasileira de Direito Processual Penal*, 2019, v. 5, n. 3, pp. 1449-1481, pp. 1449-1450. "Avanços tecnológicos oferecem ferramentas para autoridades de investigação que levantam questionamentos à luz da proteção a direitos fundamentais. Este artigo estuda o processo de compatibilização pelo qual uma dessas ferramentas tem passado: as interceptações ambientais de sinais ópticos, acústicos e eletromagnéticos. Ainda hoje, a medida possui breve regulamentação jurídica no ordenamento brasileiro, mencionada no art. 3º, II, da Lei n.º 12.850/2013. Como meio de obtenção de prova caracterizado pelo caráter sigiloso e invasivo ao lar, à intimidade, às comunicações e mesmo à autodeterminação informacional, é fundamental que seja dotado de regramento pormenorizado em lei a fim de evitar arbítrios incompatíveis com direitos fundamentais."

relação com as normas específicas surgidas posteriormente (Marco Civil da Internet e Lei Geral de Proteção de Dados, ambos tratados em maiores detalhes nos tópicos que seguem).

O primeiro deles é a Lei n.º 5.534/68[241], a qual disciplina especificamente a prestação de informações necessárias ao Plano de Estatísticas Básicas e ao Plano Geral de Informações Estatísticas e Geográficas, coletadas pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Nesse sentido, prevê o caráter sigiloso das informações prestadas, bem como as finalidades específicas às quais sua coleta está adstrita.

A LGPD, cuja vigência foi recentemente postergada em decorrência da crise do COVID-19[242], traz uma série de dispositivos que se referem, especificamente, ao tratamento de dados pelo Poder Público (vide Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público), de modo que a interpretação da Lei n.º 5.534, de 1968, deve ser harmônica com o seu conteúdo.

O Código de Defesa do Consumidor[243], por sua vez, também configura legislação pertinente ao tema, já que em determinados dispositivos, disciplina matéria relativa aos "arquivos de consumo". Nesse sentido, cabe atentar aos arts. 43 e 44, os quais cuidam especificamente dos bancos de dados e dos cadastros de consumidores.

De fato, a defesa do consumidor consta no art. 2º do MCI (inc. VI), como um dos fundamentos da disciplina do uso da internet no Brasil. O mesmo ocorre na LGPD (art. 2º, inc. VI), que coloca a proteção do consumidor como um dos fundamentos da disciplina da proteção de dados pessoais.

No Código Civil de 2002 também é possível encontrar dispositivos aplicáveis às relações estabelecidas no meio digital e à responsabilidade das partes, tanto contratual quanto extracontratual, bem como o fato de que os direitos da personalidade são irrenunciáveis[244], cabendo a interpretação conjunta de suas normas com as leis específicas, no caso da LGPD e do MCI.

---

[241] BRASIL. *Lei n.º 5.534, de 14 de novembro de 1968*. Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/ LEIS/L5534.htm. Acesso em: 17 abr. 2020.

[242] BRASIL. Câmara dos Deputados. *Projeto de Lei n.º 1.179/2020*. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?id Proposicao=2247564. Acesso em: 17 abr. 2020.

[243] BRASIL. *Lei n.º 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 17 abr. 2020.

[244] EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Luneca Campos. Op. cit., 2016. Disponível em: http://enpejud.tjal.jus.br/ index.php/exmpteste01/article/view/63/44. Acesso em: 04 jan. 2020. "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária", é o que diz o Código Civil de 2002. Uma interpretação gramatical

As Leis n.º 9.296/96[245] e 9.472/97[246] também são pertinentes ao tema, uma vez que tratam, respectivamente, da regulamentação do art. 5º, inc. XII, da Constituição Federal de 1988 (apontado no início deste tópico), e da organização dos serviços de telecomunicação, além da criação e funcionamento de um órgão regulador e outros aspectos institucionais.

A Lei do Cadastro Positivo (Lei n.º 12.414/11)[247], por sua vez, disciplina a formação e consulta a bancos de dados com informações de adimplemento para formação de histórico de crédito, garantindo acesso a todos os dados armazenados e responsabilidade sobre atualização e correção de informações.

Já a Lei de Acesso à Informação, também de 2011 (Lei n.º 12.527/11)[248], regula o tratamento de informações pessoais em órgãos e entidades vinculadas ao poder público ou que recebem recursos públicos, mencionando a necessidade de transparência, respeito à intimidade, honra, vida privada e imagem, bem como liberdades e garantias individuais, estabelecendo a necessidade de autorização ou consentimento expresso para divulgação ou acesso por terceiros.

A Lei n.º 12.737/2012, por sua vez, ficou conhecida como "Lei Carolina Dieckman" em referência ao roubo de fotos pessoais da atriz e sua divulgação sem autorização. Esta Lei modificou o Código Penal brasileiro a fim de tipificar como crime a invasão de dispositivo informático[249]. Trata-se de norma de natureza penal, que visa tipificar criminalmente delitos informáticos. Os textos do MCI e da LGPD podem ser utilizados como fundamentos complementares a essa Lei, por exemplo, em ações que

---

faria com que este dispositivo negasse efeito ao consentimento do titular no campo dos direitos da personalidade.

[245] BRASIL. *Lei n.º 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 17 abr. 2020.

[246] BRASIL. *Lei n.º 9.472, de 16 de julho de 1997*. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm. Acesso em: 17 abr. 2020.

[247] BRASIL. *Lei n.º 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 17 abr. 2020.

[248] BRASIL. *Lei n.º 12.527, de 18 de novembro de 2011.* Regula o acesso a informações previsto no inc. XXXIII do art. 5º, no inc. II do § 3º do art. 37, e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 abr. 2020.

[249] BRASIL. *Lei n.º 13.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 abr. 2020.

versam sobre a invasão de dispositivo informático, ou sobre a interrupção ou perturbação de serviço informático.

No que tange à Lei das Organizações Criminosas, Lei n.º 12.850/13[250], cumpre apontar que esta possui previsão semelhante ao Marco Civil da Internet no que se refere à obrigação da guarda de dados, bem como à prerrogativa de acesso a dados cadastrais.

Acerca da utilização de dados pelo Poder Público, há que se ressaltar que o Poder Executivo, por meio do Decreto presidencial n.º 8.789/16[251], disciplinou questões ligadas ao compartilhamento de dados pessoais, o qual entrou em vigor no dia 01 de julho de 2016. A medida visa disciplinar a divisão de bases de dados entre órgãos e entidades federais, facilitando o compartilhamento de bancos de dados entre órgãos e entidades do Estado, sem a necessidade de celebração de convênios ou acordos[252] (destacando-se, novamente, que a LGPD apresenta capítulo específico sobre o tratamento de dados pelo Poder Público).

Por fim, cabe apontar, ainda, a Resolução n.º 340/04, do Conselho Nacional de Saúde[253], a qual regulamenta pesquisas com dados genéticos humanos, exigindo consentimento prévio para coleta e armazenamento, direito ao acesso e retirada dos dados do arquivo, além da confidencialidade das informações. A LGPD trata, também, de forma específica, da proteção de dados na saúde, observando especialmente o disposto sobre a proteção de dados pessoais considerados sensíveis, conforme item que segue.

---

[250] BRASIL. *Lei n.º 12.850, de 02 de agosto de 2013.* Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 abr. 2020.

[251] BRASIL. *Decreto n.º 8.789, de 29 de junho de 2016*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 17 abr. 2020.

[252] ABREU, Jacqueline de Souza. O compartilhamento de dados pessoais no Decreto n.º 8.789/16: um Frankenstein de dados brasileiro? *Uol*. 08/07/16. Disponível em: http://jota.uol.com.br/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro. Acesso em: 20 jul. 2016.

[253] BRASIL. *Resolução CNS n.º 340, de 08 de julho de 2004*. Incorpora todas as disposições contidas na Resolução CNS n.º 196/96, do Conselho Nacional de Saúde, sobre Diretrizes e Normas Regulamentadoras de Pesquisas Envolvendo Seres Humanos, da qual é parte complementar da área temática específica, e incorpora também, no que couber, as disposições constantes das Resoluções CNS n.º 251/97, 292/99, 303/2000 e 304/2000. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2004/res0340_08_07_2004.html. Acesso em: 17 abr. 2020.

1.7.3 Legislação específica: Marco Civil da Internet (MCI)

O Marco Civil da Internet (Lei n.º 12.965/14[254]), diploma normativo recente e de grande relevância para o tema, estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, colocando como fundamento principal para sua utilização o respeito à liberdade de expressão (art. 2º, *caput*)[255].

Embora a Lei apresente em seu art. 5º alguns conceitos relevantes à temática (internet, terminal, endereço de protocolo de internet ou IP, administrador de sistema autônomo, conexão à internet, registro de conexão, aplicações de internet e registros de acesso a aplicações de internet), não há uma definição precisa de "dados pessoais" – o que veio a ocorrer somente com a aprovação da LGPD[256], que passa a vigorar em 2020.

No que tange à privacidade, o art. 7º do MCI assegura a sua proteção, prevendo o acesso à internet como parte essencial do exercício da cidadania, e garantindo, em seu inc. I, a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação"[257].

Também é possível observar nos incs. VIII a XI do mesmo artigo, disposições relativas à proteção de dados, os quais tomam por base o princípio da finalidade, de maneira que os dados coletados somente podem ser tratados em condições específicas[258].

---

[254] BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponivel em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 abr. 2020.

[255] COSTA, José Augusto Fontoura; SOLA, Fernanda. Direito das tecnologias de comunicação e informação: uma primeira abordagem do Marco Civil da Internet. *PIDCC*, Aracaju, fev. 2015, ano IV, ed. n.º 08/2015, pp. 336-351, pp. 342-343. "O primeiro grande projeto a respeito da regulação da rede mundial de computadores, denominada normalmente "internet", foi o PL 84/99, conhecido por "Lei Azeredo" por haver sido relatado pelo senador do PSDB mineiro Ricardo Azeredo. Como criminalizava várias condutas comuns, foi objeto de pesadas críticas e originou uma mobilização em prol de um marco regulatório prévio. Em 2009, o Ministério de Justiça iniciou um amplo processo de consulta e discussão públicas, o qual resultou na formulação do marco civil da internet, convertido no PL 2126/2011. Com 25 artigos, o projeto apresenta cinco capítulos: (1) Disposições preliminares, (2) Dos direitos e garantias dos usuários, (3) Da provisão, conexão e aplicações da internet, (4) Da atuação do Poder Público e (5) Disposições finais."

[256] Tal definição surgiu de maneira mais precisa na Lei n.º 13.709/2018, de forma a estabelecer-se um corpo normativo unitário no que tange especificamente à proteção de dados; até então havia somente o MCI, e os mecanismos de proteção da pessoa humana e sua personalidade sob tal aspecto atuavam tão somente de forma fracionada, conforme apontado por Danilo Doneda (DONEDA, Danilo. Os direitos da personalidade no código civil. *In:* TEPEDINO, Gustavo (Coord.). *A parte geral do novo Código Civil:* estudos na perspectiva civil-constitucional. 2. ed. Rio de Janeiro: Renovar, 2003, p. 28).

[257] BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Op. cit. Disponível em: http://www.planalto.gov.br/ccivil_ 03/_ato2011-2014/2014/lei/ l12965.htm. Acesso em: 17 abr. 2020.

[258] Id., ibid. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. "Art. 7º [...] VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X – exclusão

A Seção II do MCI reúne as disposições relativas à Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas, sendo especialmente relevante destacar o art. 12, que prevê sanções que poderão ser aplicadas de forma isolada ou cumulativa em caso de violação. Já a Seção III trata da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros, isentando o provedor de conexão à internet de responsabilização civil por danos ocasionados por conteúdo gerado por terceiros.

Quando apresentado o conceito de Sociedade da Informação nos capítulos anteriores, restou claro para Dario Moura Vicente, que as especificidades de tal sociedade geram a necessidade de regras particulares para disciplinar as situações surgidas. Não obstante, José Augusto Fontoura Costa e Fernanda Sola indagam se é possível, efetivamente, falar em um Direito das Tecnologias de Comunicação e Informação, tendo em vista a existência de dispositivos – por exemplo, no Código Civil – devidamente capazes de regrar as situações da vida[259].

Ainda assim, concluem que seria possível a disciplina do Direito Digital ou Direito Informático[260], considerando a sua vocação para gerar a "reflexão e solução de questões jurídicas projetadas sobre uma problemática própria do desenvolvimento de tecnologias digitais de informação – computadores, *softwares* e redes, por exemplo – e seus impactos sobre a organização social e econômica"[261].

Especificamente sobre a regulação dos conteúdos e responsabilidade dos intermediários, os autores apontam que inexistem determinações específicas no MCI acerca da ilicitude de tais conteúdos, de modo que quaisquer "conteúdos proibidos, em qualquer outro meio público (jornal, revista, rádio ou televisão, por exemplo), em razão de violação de direito autoral, intimidade, moralidade ou outra razão legal, tampouco podem

---

definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet [...]."

[259] COSTA, José Augusto Fontoura; SOLA, Fernanda. Op. cit., fev. 2015, p. 337. Os autores tecem críticas ao Marco Civil, primeiramente por tratar a referida Lei "apenas de internet e, portanto, não abrange todo o universo das questões digitais." E, ainda, "seu caráter precipuamente transversal cria regras específicas para questões de internet em outros ramos – comercial, administrativo e consumerista, p. ex. – mas não chega a constituir um rol de sujeitos e princípios próprios e característicos, capaz de caracterizar um campo jurídico específico."

[260] Id., ibid., p. 351. "A busca pela construção de um ramo, se é que isto é realmente importante, passa mais pela compreensão das necessidades, expectativas e identidades socialmente construídas do que pela estruturação e racionalização de códigos legais; e o MCI sequer tem a pretensão de codificar. Assim como o Direito Comercial permanece intacto à mudança da sede legislativa de parte de sua regulação e o Direito Ambiental independe de um código próprio, um Direito das tecnologias da informação pode vir a se firmar."

[261] Id., ibid., p. 339.

ser veiculados pela internet. Os sujeitos que os puseram à disposição do público, portanto, assumem a responsabilidade"[262].

Interessante a análise realizada nesse artigo acerca de casos submetidos à apreciação do Superior Tribunal de Justiça (STJ): a partir de tais julgados observa-se que, antes do MCI, a orientação jurisprudencial era no sentido de não exigir dos prestadores de serviço o controle sobre os conteúdos disponibilizados por seus usuários, privilegiando a pronta remoção de informações abusivas.

No julgamento do Recurso Especial n.º 1192208/MG[263], por exemplo, restou evidente o atrito entre o interesse coletivo e o potencial ofensivo da divulgação de conteúdo. Entendeu-se, naquela ocasião, que não há obrigação ou necessidade de fiscalização prévia de conteúdo, sendo necessária a notificação do prestador de serviços para ocorrer a exclusão de conteúdo ilícito ou ofensivo[264].

> Em conformidade com a jurisprudência anterior dominante, (o MCI) não estende a responsabilidade ao provedor de conexão (art. 19, § 1º). Contrariamente, afirma, quanto ao provedor de aplicações, que 'somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdos gerados por terceiros se, após ordem judicial específica, não tomar as providências [...].' Não obstante, tal barreira à responsabilização não deve ser tomada por absoluta: certamente não cobre o ato doloso e, no culposo em sentido amplo, dependerá de avaliação do nexo. Fica estabelecido, porém, não haver dever jurídico específico do provedor de aplicações controlar o conteúdo disponibilizado por terceiro (evitando responsabilização objetiva e inversão de *onus probandi*) e retirar o conteúdo sem ordem judicial, a menos que exista razão séria para tanto. Tampouco se deve interpretar a regra como implicando um dever legal de manter o conteúdo postado até que exista ordem judicial, seguindo-se padrões de razoabilidade e conformidade com a regulação contratual da prestação do serviço, a qual pode prever a retirada à demanda do afetado ou a liberdade de retirar[265].

Em outro artigo publicado por José Augusto Fontoura Costa, juntamente com Marcos Wachowicz, são tecidas críticas ao MCI, especificamente quanto à cláusula atentatória à inviolabilidade e ao sigilo, e quanto à cláusula de eleição de foro, observações

---

[262] Id., ibid., p. 343.

[263] STJ. Superior Tribunal de Justiça. *Recurso Especial n.º 1.192.208-MG*. Rel. Min. Nancy Andrighi, Terceira Turma. Julgado em 12/06/2012, publicado em 02/08/2012.

[264] COSTA, José Augusto Fontoura; SOLA, Fernanda. Op. cit., fev. 2015, p. 344. "No REsp. 1.192.208/MG, a Terceira Turma (relatora Min. Nancy Arrighi) esclareceu, com referência à hospedagem de blogs, que não há necessidade de fiscalização prévia dos conteúdos veiculados por usuários, pois, prejudicaria o livre e rápido fluxo e acesso à informação, que é de interesse da coletividade. Por conseguinte, não sendo o conteúdo ofensivo parte do risco inerente da atividade, não cabe responsabilidade objetiva nos termos do art. 927 do Código de Defesa do Consumidor. Não obstante, uma vez notificado pelo interessado, o prestador de serviços deve retirar prontamente o conteúdo ofensivo e atuar com a maior diligência possível para coibir o anonimato e identificar os autores diretos do dano."

[265] Id., ibid., p. 346.

consideradas válidas[266]. Quanto à possibilidade de eleição do foro, cumpre observar o inc. II, parágrafo único do art. 8º do MCI, o qual proíbe em contrato de adesão cláusulas que excluam o foro brasileiro para serviços prestados no Brasil.

Segundo os autores, cumpre observar: (i) a relação entre tal dispositivo e a privacidade e liberdade de expressão; (ii) a restrição aos serviços prestados no Brasil; (iii) a arbitrariedade; e (iv) a relação da norma com as demais normas de competência internacional existentes no CPC[267].

A questão final, portanto, seria saber se houve ou não a revogação do art. 8º do MCI após a promulgação do Código de Processo Civil de 2015, uma vez que se trata de um problema de antinomia entre regras beneficiadas por critérios de solução distintos,

> a primeira pela *lex specialis* e a segunda pela *lex posterior*. Embora seja possível pressupor alguma preponderância da regra especial, uma vez que seu âmbito de aplicação já excluía aplicabilidade de norma geral anterior, a solução não é cabal, restando sempre espaço para discussão[268].

1.7.4 Legislação específica: Lei Geral de Proteção de Dados (LGPD)

Recentemente foi aprovada a Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709/2018)[269], a qual dispõe especificamente sobre a proteção, uso e tratamento de informações[270], alterando disposições pertencentes ao MCI[271]. A LGPD entraria em vigor

---

[266] COSTA, José Augusto Fontoura; WACHOWICZ, Marcos. Cláusulas contratuais nulas no Marco Civil da Internet. *Revista da Faculdade de Direito da UFMG*. Belo Horizonte, jan./jun. 2016, n. 68, pp. 477-496, p. 489. "No que se refere aos países do Mercosul, tem-se o Protocolo de Buenos Aires de 1994, promulgado no Brasil mediante o Dec. 2.095/96. Em relações de consumo, no entanto, as cláusulas de eleição de foro apostas em contratos de adesão são passíveis de declaração de nulidade *ex officio* (art. 112, parágrafo único, CPC 5); regra, aliás, ausente do novo CPC."

[267] Id., ibid., p. 490. "Decerto, o legislador brasileiro do NCPC, conscientemente, passou a ser bastante mais flexível em matéria de jurisdição internacional, inclusive no sentido de dar protagonismo ao papel da vontade. Neste sentido, passou a admitir a competência para qualquer ação em que as partes se submetam à jurisdição brasileira, o que pode ser feito de maneira expressa ou tácita, antes (p. ex. mediante cláusula contratual) ou depois da propositura da ação (art. 22, III 6). No mesmo sentido, resolveu estabelecer claramente a incompetência do juiz brasileiro em face de cláusula de eleição de foro exclusivo estrangeiro, desde que esta seja arguida pelo réu em contestação (art. 257). Resta, então, observar que as hipóteses do art. 63, §§ 3º e 4º do NCPC não são aplicáveis à escolha de jurisdição estrangeira: tratam claramente da situação de eleição de foro sob a jurisdição brasileira, não da opção por juízo estrangeiro. Corrobora tal situação o fato de que, em ambos os casos, a regra é endereçada ao juiz do foro eleito, sendo o remédio do § 3º - remessa dos autos ao foro de domicílio do réu – evidentemente inaplicável às situações internacionais."

[268] Id., ibid., p. 491.

[269] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 abr. 2020.

[270] ABRUSIO, Juliana. Com certo atraso, Brasil finalmente é inserido no rol de países com marco legal em proteção de dados. *Informativo Migalhas*, 2018, v. 1, p. 1. Disponível em: https://www.migalhas.com.br/depeso/286385/com-certo-atraso-brasil-finalmente-e-inserido-no-rol-de-paises-com-marco-legal-em-protecao-de-dados Acesso em: 18 abr. 2020. "Até agora, o Brasil possuía previsão para proteção de dados em leis

em agosto de 2020 – mas foi adiada recentemente, em decorrência da crise do COVID-19[272]. No contexto da atual crise, a vigência da lei foi postergada para 1º de janeiro de 2021[273] – enquanto a possibilidade de aplicação de sanções foi adiada para agosto do mesmo ano[274].

---

esparsas – a exemplo de breves disposições no Código Civil e Código de Defesa do Consumidor, dentre poucos outros textos legais – que não eram suficientes para a realidade do mercado de dados atual. É certo que a economia do *big data*, impulsionada pela internet das coisas, das cidades inteligentes e da inteligência artificial, não poderia resistir ao vácuo das regras jurídicas do jogo. A cultura atual dos algoritmos exige uma posição do Estado para regulamentar o assunto, sob pena de comprometer direitos fundamentais dos cidadãos (liberdade, privacidade, livre desenvolvimento da personalidade). E não apenas isso. A existência de lei específica traz mais segurança jurídica, o que acaba por fomentar a economia e atrair investidores ao país, uma vez que, agora, as regras são mais claras em relação ao tratamento de dados pessoais."

[271] ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. O que está em jogo no debate sobre dados pessoais no Brasil? *Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de Lei de Proteção de Dados Pessoais*. São Paulo, 2016. Disponível em: http:// www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 17 abr. 2020.

[272] BRASIL. *Projeto de Lei 1.179/2020.* Op. cit. Disponível em: https://www.camara.leg.br/proposicoesWeb/ fichadetramitacao?idProposicao=2247564. Acesso em: 17 abr. 2020.

[273] BRASIL. Ministério Público Federal. *Nota Técnica Conjunta – PFDC & Câmara Criminal – Epidemia Covid-19 e PLS (Substitutivo) 1.179/20:* Manutenção do prazo de entrada em vigor da LGPD (ressalvadas as sanções administrativas). PLS (Substitutivo)1179/20, trata do Regime Jurídico Emergencial e transitório das relações jurídicas de Direito Privado no período da pandemia da doença do coronavírus-19 (COVID-19). Art. 25 do PLS ajustado, que adia a *vacatio legis* da LGPD – Lei Geral de Proteção de Dados até 1º de janeiro de 2021, com a ressalva de que os artigos relativos às sanções só entrarão em vigor em agosto de 2021. Disponível em: https://www.conjur.com.br/dl/nota-tecnica-lgpd.pdf. Acesso em: 18 abr. 2020. "Em breve revisão, não custa lembrar que a LGPD, fruto de amplo esforço legislativo, garante a proteção de dados pessoais, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Quase todos esses direitos têm *status* constitucional, a merecer apenas uma sistematização no texto da Constituição, nos termos da PEC 17/2019 sobre proteção de dados pessoais. No plano infraconstitucional, a LGPD, como lei específica e geral, que disciplina a proteção dos dados pessoais, normatiza os procedimentos para assegurar as garantias desses direitos, estrutura o marco regulatório, cria o sistema administrativo e define o regime sancionatório, vem dar maior segurança aos indivíduos e a setores por ela abrangidos. Há de se destacar também que a garantia dos mencionados direitos é necessária tanto em relação ao Estado quanto em relação às grandes companhias, que têm suplantado os Estados na questão de coleta de dados e de seu uso indiscriminado, sem que os usuários tenham ideia do que é feito com seus dados pessoais, que são o grande ativo desta época, servindo até a experimentos sociais com os indivíduos, que os ignoram por completo. Todos esses princípios constitucionais e legais são essenciais, especialmente no contexto da pandemia COVID-19, sendo a LGPD uma importante aliada no desenvolvimento seguro e parametrizado de ações fundamentais para a proteção à saúde, isolamento social e colaboração com atores estrangeiros, na troca de dados essenciais para o enfrentamento da crise. No cenário atual da Pandemia do COVID-19, a garantia da saúde pública e da aplicação de medidas sanitárias não significa abrir mão de direitos de proteção de dados pessoais e de privacidade"

[274] MONACO, Gustavo Ferraz de Campos; CAMARGO, Solano de; SMITH MARTINS, Amanda Cunha e Mello. Sem sanções, LGPD é inócua. *Valor Econômico*, 13 abr. 2020. Disponível em: https://valor.globo.com/legislacao/noticia/2020/04/13/sem-sancoes-lgpd-e-inocua.ghtml. Acesso em: 18 abr. 2020. Sobre a postergação da LGPD, limita-se a expor a seguinte análise que, apesar de criticar o adiamento da *vacatio legis* assim como a nota técnica supramencionada, discorda desta quanto às sanções: "Trata-se de uma curiosa inovação do sistema, posto que o texto atual determina a entrada em vigor e aplicação potencial de sanções em mesma data. Claro que as inovações dependem, ainda, da manutenção do dispositivo pela Câmara dos Deputados por ocasião da análise do projeto de lei. E, mantido o texto do Senado, dependerá ainda de ser sancionado pelo presidente da República. Muito embora a prorrogação do prazo para início da vigência da LGPD seja compreensível, na medida em que muitas empresas não conseguiram ultimar os diversos preparativos decorrentes da nova regulação, sobretudo depois da necessidade do isolamento social, não se compreende porque haveria de ser postergado o exercício do poder sancionatório, a ser exercido pela Autoridade Nacional de Proteção de Dados (ANPD), ainda em fase gestacional, o que não guarda coerência

Independentemente de sua postergação, a lei tem sido objeto de discussões também no que se refere ao seu conteúdo, principalmente no que tange à adaptação e adequação prévia das empresas que realizam tratamento de dados.

A definição de um conceito de "dados pessoais" é indispensável à sua proteção, tendo influência direta sobre o nível de proteção legal que lhes é concedido[275]. No caso específico do Brasil, a LGPD determina em seu art. 5º, inc. I, que se considera "dado pessoal: informação relacionada à pessoa natural identificada ou identificável". São dados entendidos como pessoais e que podem ser fornecidos, por exemplo, a partir do preenchimento de um formulário ou, ainda, a partir da divulgação voluntária de informações em redes sociais, submetidas aos termos e condições elaborados individualmente por cada *website* e aceitos pelos respectivos usuários[276].

Dessa forma, a Lei define como dados pessoais todos aqueles passíveis de permitir a identificação de uma pessoa, inclusive números, características pessoais, qualificação pessoal, dados genéricos, dentre outros. De fato, é possível obter uma grande quantidade de informações detalhadas a respeito de um indivíduo específico a partir de poucos dados, mesmo que numéricos[277].

Destarte, o aparente anonimato ao se navegar na *internet* não passa de ilusão, uma vez que, a partir de dados pessoais genéricos, ou seja, por vezes de caráter numérico, ou sob a forma de códigos, os quais podem ser facilmente obtidos, é possível realizar a

---

com a realidade nem com a teoria do Direito. A quarentena imposta pelas esferas do Poder Público impulsionou as atividades *online* que adquiriram força e volume jamais vistos. [...] Não faz sentido que uma lei que protege direitos individuais (direito de acesso aos dados pessoais; de contestar algoritmos; de ter as informações atualizadas; de controlar o processamento dos dados pessoais; de ser informado sobre a violação dos dados; de transferir as informações a outrem, etc.) seja promulgada sem sanção. Menos, ainda, que as sanções só possam ser aplicadas alguns meses depois. Caso o PL nº 1.179/2020 venha a entrar em vigor da forma como aprovado pelo Senado Federal, dar-se-á o paradoxo de que, durante sete meses, uma importantíssima lei de proteção a direitos individuais vir a protegê-los apenas se houver boa vontade por parte dos personagens a quem se impõe o dever de cuidado na coleta e tratamento dos dados. Sem coercibilidade não há norma jurídica. Haverá, quando muito, imposição de natureza moral. E para tanto, não seriam necessárias as leis."

[275] ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. O que são dados pessoais? [especial]. São Paulo, 2016. Disponível em: http://www.internetlab.org.br/pt/opiniao/especial-o-que-sao-dados-pessoais/. Acesso em: 17 abr. 2020.

[276] BRASIL. *Lei n.º 13.709/2018*. Op. cit. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 abr. 2020. A Lei em questão diferencia "dado pessoal" de "dado pessoal sensível", de modo que os primeiros são considerados "informação relacionada a pessoa natural identificada ou identificável", enquanto os dados sensíveis são assim definidos por serem qualquer "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".

[277] GIBBS, Samuel. Your phone number is all a hacker needs to read texts, listen to calls and track you – Weaknesses within mobile phone network interconnection system allows criminals or governments to remotely snoop on anyone with a phone. *The Guardian*, 18 abr. 2016. Disponível em: https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you. Acesso em: 17 abr. 2020.

identificação de um indivíduo específico – deixando, assim, de existir tanto o caráter anônimo do sujeito, que passa a ser identificável, quanto o caráter genérico dos seus dados, que possibilitam, a princípio, sua identificação[278].

Neste aspecto, a Lei n.º 13.709/18 define no inc. III do art. 5º, os "dados anonimizados" como aqueles dados pessoais "relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Assim, há dados que não estarão atrelados a uma pessoa natural, de modo que não será possível uma eventual identificação do indivíduo[279].

Para tanto, seria utilizado o processo de "anonimização"[280], definido no inc. XI do art. 5º, como a "utilização de meios técnicos razoáveis e disponíveis no momento do

---

[278] Discute-se a (im)possibilidade técnica de exclusão definitiva de dados após a sua transmissão pela rede – no entanto, o desenvolvimento de tecnologias que permitem tornar os dados absolutamente inacessíveis parece suprir tal necessidade de exclusão em sentido estrito.

[279] OHM, Paul. Broken Promises of Privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 2010, v. 57. University of Colorado Law Legal Studies Research Paper n. 9-12. Disponível em: https://ssrn.com/abstract=1450006. Acesso em: 17 abr. 2020, pp. 1735-1746, p. 1701. O autor aborda a história da anonimização de dados e a forma como as leis atuais interpretam "dados pessoais sensíveis", alertando, ainda, sobre o "*accretion problem*", ou "problema do acréscimo" relacionado com tal anonimização: "Embora a anonimização robusta tenha falhado, ainda faz sentido tratar especialmente os tipos de informações que podem ser usadas diretamente para causar danos. Por outro lado, os legisladores geralmente escolhem categorias de dados para tratamento especial sob a crença equivocada de que essas categorias (e somente essas) aumentam a vinculação de dados anônimos. [...] O problema do acréscimo é o seguinte: uma vez que um adversário vinculou dois bancos de dados anônimos, ele pode adicionar os dados recém-vinculados à sua coleção de informações externas e usá-los para ajudar a desbloquear outros bancos de dados anônimos. Sucesso gera mais sucesso. Narayanan e Shmatikov explicam que 'depois que qualquer dado é vinculado à identidade real de uma pessoa, qualquer associação entre esses dados e uma identidade virtual quebra o anonimato dos últimos'. É por isso que devemos nos preocupar até com eventos de reidentificação que parecem expor apenas informações não sensíveis, porque aumentam a capacidade de vinculação dos dados e, portanto, expõem as pessoas a possíveis danos futuros. Por causa do problema do acréscimo, todo evento de reidentificação, por mais que pareça benigno, aproxima as pessoas de danos." (Tradução livre). "*Even though robust anonymization has failed, it still makes sense to treat specially those kinds of information that can be used directly to cause harm. In contrast, lawmakers often single out categories of data for special treatment under the mistaken belief that these categories (and only these) increase the linkability of anonymized data. [...] The accretion problem is this: Once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success. Narayanan and Shmatikov explain that "once any piece of data has been linked to a person's real identity, any association between this data and a virtual identity breaks the anonymity of the latter." This is why we should worry even about reidentification events that seem to expose only nonsensitive information, because they increase the linkability of data, and thereby expose people to potential future harm. Because of the accretion problem, every reidentification event, no matter how seemingly benign, brings people closer to harm."*

[280] YAKOWITZ, Jane. Tragedy of the Data Commons. *Harvard Journal of Law & Technology*, 2011, v. 25, n. 1, p. 4. No artigo, é apresentada a perspectiva sob a qual, por um lado, a divulgação de bancos de dados anonimizados de hospitais, escolas, órgãos públicos e outras instituições torna possível para o público em geral conduzir investigações e pesquisas que beneficiam a sociedade, justificando assim a autorização para a anonimização: "As pessoas começaram a proteger defensivamente informações anônimas sobre si mesmas. Estamos testemunhando um exemplo moderno de uma tragédia dos bens comuns. Cada indivíduo tem um incentivo para remover seus dados dos bens comuns para evitar riscos remotos de re-identificação. Dessa forma, obtém-se o melhor dos dois mundos: seus dados estão seguros e também há os benefícios indiretos de pesquisas úteis sobre saúde e políticas realizadas no restante dos dados deixados nos bens comuns. No entanto, os benefícios coletivos derivados dos dados comuns irão degenerar rapidamente se os titulares de

tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo." Os dados passariam por um tratamento específico, de modo que não seria mais possível atrelá-los ao indivíduo ao qual pertencem[281].

O conceito de anonimização concebida pela Lei, contudo, já se mostra ultrapassado[282]. Se, por um lado, há críticas sobre os limites da anonimização, já que uma pequena quantidade de dados, mesmo que anônimos, pode permitir a identificação do seu titular (dados anonimizados, portanto, porém identificáveis[283]), por outro lado o

---

dados optarem por se proteger. [...] Primeiro, a utilidade social dos bens comuns de dados é mal compreendida e muito subestimada pela maioria dos estudiosos da privacidade. Dados de pesquisa pública produzem contribuições valiosas para nossa busca coletiva de conhecimento e justiça. Segundo, a influente bolsa de estudos de Ohm e outros interpreta mal a literatura de ciência da computação e, como resultado, supera a futilidade do anonimato, mesmo com relação ao risco teórico. E terceiro, os riscos realmente criados pelos dados comuns são insignificantes. Até o momento, não houve ocorrências conhecidas de re-identificação inadequada de um conjunto de dados de pesquisa. Até os riscos hipotéticos são menores do que outros riscos baseados em informações (de derramamentos de dados ou hackers, por exemplo) que nós toleramos rotineiramente por conveniência." (Tradução livre).*"People have begun to defensively guard anonymized information about themselves. We are witnessing a modern example of a tragedy of the commons. Each individual has an incentive to remove her data from the commons to avoid remote risks of re-identification. This way she gets the best of both worlds: her data is safe, and she also receives theindirect benefits of helpful health and policy research performed on the rest of the data left in the commons. However, the collective benefits derived from the data commons will rapidly degenerate if data subjects opt out to protect themselves. [...] First, the social utility of the data commons is misunderstood and greatly undervalued by most privacy scholars. Public research data produces rich contributions to our collective pursuit of knowledge and justice. Second, the influential legal scholarship by Ohm and others misinterprets the computer science literature, and as a result, oversells the futility of anonymization, even with respect to theoretical risk. And third, the realistic risks posed by the data commons are negligible. So far, there have been no known occurrences of improper re-identification of a research dataset. Even the hypothetical risks are smaller than other information-based risks (from data spills or hacking, e.g.) that we routinely tolerate for convenience."*

[281] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. Caderno Especial. São Paulo: RT, dez. 2018, v. 998, pp. 99-128, p. 101. "Em linhas gerais, criptografia 'é a ciência da escrita secreta com o objetivo de esconder o significado de uma mensagem'. [...] Dados criptografados não configuram dados anônimos ou anonimizados pelo só fato de ocorrer operação de cifragem. [...]."

[282] NARAYANAN, Arvind; FELTEN, Edward W. *No silver bullet*: de-identification still doesn't work. 2014. Disponível em: https://www.semanticscholar.org/paper/No-silver-bullet-%3A-De-identification-still-doesn-'-Narayanan-Felten/1df5567c45ac8cb9289411268573aea89e74e542. Acesso em: 17 abr. 2020. O artigo critica severamente a anonimização de dados, apontando que muito embora seja possível desassociá-los da identidade dos respectivos usuários, isto não significa a inviabilidade técnica de posterior re-identificação: "O ponto principal de nossos argumentos é que (i) não há evidências de que a desidentificação funcione na teoria ou na prática; e (ii) as tentativas de quantificar sua eficácia não são científicas e promovem uma falsa sensação de segurança ao assumir irrealistas e artificialmente restritos modelos do que um adversário pode fazer. [...] Correndo o risco de ser pedante, quando dizemos que a desidentificação não funciona, queremos dizer que não é eficaz em resistir às tentativas contraditórias de re-identificação." (Tradução livre). "*The thrust of our arguments is that (i) there is no evidence that de-identification works either in theory or in practice and (ii) attempts to quantify its efficacy are unscientific and promote a false sense of security by assuming unrealistic, artificially constrained models of what an adversary might do. [...] At the risk of being pedantic, when we say that de-identification doesn't work we mean that it isn't effective at resisting adversarial attempts at re-identification.*"

[283] MACHADO, Diego; DONEDA, Danilo. Op. cit., dez. 2018, pp. 99-128, p. 106. "[...] o conceito amplo estende seu alcance para além da pessoa natural meramente identificada: também é informação de caráter pessoal aquela relativa [à] pessoa identificável. Há dado pessoal não apenas quando houver a presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo. Os dados que potencialmente conduzem à individuação da pessoa são igualmente tomados como informação pessoal. Existem dados ou

desenvolvimento da tecnologia de *blockchain* abordada anteriormente permite que as informações sejam criptografadas e permaneçam seguras em uma cadeia de informação, preservando-se seu sigilo (devido à necessidade de chave) e sua correção (pois os dados são inalteráveis)[284].

Consequentemente, se determinada informação é submetida ao protocolo do *blockchain*, seu acesso já será restrito aos que possuem a chave para a criptografia utilizada – de modo que, sendo tecnicamente questionável a possibilidade de exclusão definitiva de dados, é possível torná-los inacessíveis indefinidamente ao se utilizar uma chave à qual não se tem acesso[285].

A LGPD também definiu alguns tipos específicos de dados pessoais, como os "dados sensíveis", os quais implicariam necessidade de maior proteção por serem informações passíveis de utilização de forma discriminatória[286]. O art. 5º, em seu inc. II, define dados sensíveis como todos aqueles

---

identificadores que, apesar de não individuarem efetivamente alguém, caso tratados com técnicas que são acessíveis e em conjunto com dados suplementares, podem levar à identificação de seu titular. Ainda que o agente responsável pelo tratamento dos dados não possa identificar com precisão a pessoa natural a quem se referem as informações processadas, com algum esforço ele, ou terceiro, pode se valer de meios disponíveis para a obtenção dos dados adicionais aptos a fazê-lo."

[284] O mesmo se aplica à exclusão definitiva de dados, os quais podem se tornar inacessíveis por meio do protocolo de *blockchain*. Assim, podem ser considerados excluídos, mesmo que não seja possível fazê-lo em sentido estrito, conforme apontado.

[285] CROSBY, Michael; NACHIAPPAN; PATTANAYAK, Pradan; VERMA, Sanjeev; KALYANARAMAN, Vignesh. *Block Chain Technology*: Beyond Bitcoin. Applied Innovation Review, jun./2016, n. 2. Disponível em: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf. Acesso em: 08 mar. 2020. "Uma *blockchain* é essencialmente um banco de dados distribuído de registros públicos de todas as transações ou eventos digitais que foram executados e compartilhados entre as partes participantes. Cada transação no livro público é verificada por consenso da maioria dos participantes no sistema. Uma vez inseridas, as informações nunca podem ser apagadas. O *blockchain* contém um registro certo e verificável de cada transação já feita. Para usar uma analogia básica, é mais fácil roubar um biscoito de um pote de biscoitos, mantido em local isolado, do que roubar o biscoito de um pote de biscoitos mantido em um mercado, sendo observado por milhares de pessoas. [...] As oportunidades de aplicações não financeiras também são infinitas. Podemos imaginar a prova da existência de todos os documentos legais, registros de saúde e pagamentos de fidelidade na indústria da música, notário, títulos privados e licenças de casamento na *blockchain*. Ao armazenar a impressão digital do ativo digital em vez de armazenar o próprio ativo digital, o objetivo do anonimato ou da privacidade pode ser alcançado." (Tradução livre) "*A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easier to steal a cookie from a cookie jar, kept in a secluded place, than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. [...] Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved*."

[286] CAMARGO, Solano de. LGPD restringe inovações na saúde. *Valor Econômico.* São Paulo, 24 jun. 2019. Disponível em: https://valor.globo.com/legislacao/noticia/2019/06/24/lgpd-restringe-inovacoes-na-saude.html. Acesso em: 05 mar. 2020. "Os modelos algorítmicos de inteligência artificial não produzem resultados adequados quando o treinamento é realizado em amostra de dados não representativa. Por essa razão, a

> dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Todas essas informações são passíveis de serem obtidas por meio da *internet*: o acesso a *websites* ou o cadastro em páginas de instituições religiosas, a utilização de redes sociais voltadas para relacionamentos pessoais[287], informações sobre resultados de exames médicos e uma série incontável de dados sensíveis são fornecidos a todo tempo a empresas responsáveis pelo seu tratamento, muitas vezes desprotegidas quanto ao acesso por particulares, criminosos, agências governamentais ou *hackers*.

Muitas vezes, inclusive, há a coleta automática de dados, sem que o usuário necessite preencher um formulário ou cadastro. Exemplo disso é a identificação obtida por câmeras inteligentes, reconhecimento facial[288], exames de DNA, impressões digitais ou outros dados biométricos, cuja coleta não ocorre de modo explícito e, por isso, independe diretamente do titular dos dados ou do seu consentimento expresso[289].

Por fim, dentre os conceitos de maior relevância apresentados no art. 5º da Lei analisada, cumpre mencionar, ainda, as definições de "banco de dados" e de "tratamento de

---

tecnologia de reconhecimento facial hoje é muito mais eficaz em homens brancos do que em mulheres negras. Assim, se as *startups* de saúde utilizarem exclusivamente o banco de dados de um hospital de elite de São Paulo, por exemplo, capaz de implantar todos os cuidados e procedimentos previstos na LGPD, corre-se o risco de reproduzir esse preconceito na Medicina, marginalizando ainda mais as comunidades pobres de outras regiões."

[287] HARTZOG, Woodrow. There is no such thing as "public" data – and it's not Ok for researchers to scrape information from websites like OkCupid. *Slate*, 19 maio 2016. Disponível em: https://slate.com/technology/2016/05/okcupids-data-leak-shows-theres-no-such-thing-as-public-data.html. Acesso em: 17 abr. 2020.

[288] GOMES, Helton Simões. Reconhecimento facial usado na China é testado no Brasil: saiba como opera. *Uol*, 18 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/18/reconhecimento-facial-usado-na-china-e-testado-no-brasil-saiba-como-opera.htm. Acesso em: 06 jan. 2020. "Deputados e senadores da bancada no Congresso Nacional do PSL, partido do presidente Jair Bolsonaro, viajaram mais de 16 mil km até a China para conhecer um sistema capaz de reconhecer os rostos de qualquer cidadão no meio da multidão. Usada pelo governo chinês na segurança pública, a solução, no entanto, já está sendo testada desde o fim do ano passado, ainda que com menor abrangência, em Campinas, cidade paulista que fica a pouco menos de 100 km de São Paulo. A Bahia também possui o sistema. O reconhecimento facial já é usado com outras finalidades no Brasil, como identificar pessoas suspeitas em aeroportos. [...] Uma ressalva a ser feita é que a adoção do sistema de reconhecimento é muito mais abrangente na China do que em Campinas. O país asiático possui mais de 170 milhões de câmeras e tem conectividade muito mais avançada. Além disso, o poder público chinês tem menos freios institucionais do que no Brasil, onde a proteção de dados pessoais, por exemplo, é assegurada por lei."

[289] ARBULU, Rafael. Novo sistema de vigilância chinês identifica pessoas pelo jeito de andar. *Canaltech*, 07 nov. 2018. Disponível em: https://canaltech.com.br/seguranca/novo-sistema-de-vigilancia-chines-identifica-pessoas-pelo-jeito-de-andar-126421/. Acesso em: 06 jan. 2020. "Mais um método de vigilância do cidadão empregado pelo governo chinês vem causando preocupações em relação à privacidade dos habitantes do país: a empresa Watrix desenvolveu um sistema de câmeras inteligentes capaz de identificar uma pessoa com bastante precisão apenas pela forma como ela caminha, além de avaliar o formato de seu corpo. As autoridades começaram a implementar esse sistema nas cidades de Pequim e Xangai. [...] A implementação vem sendo testada na prevenção de pequenos crimes, como atravessar uma rua com sinal vermelho para pedestres ou identificação de fugitivos em uma multidão. Com a adoção da tecnologia pelo governo, a Watrix já conseguiu angariar cerca de US$ 14,5 milhões."

dados", constantes, respectivamente, nos incs. IV e X. Importante observar que relativo ao conceito de "banco de dados" consta expressamente se tratar de um "conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico", fazendo menção de que pode se tratar de um banco plurilocalizado.

Acerca do "tratamento de dados", a Lei o define como toda e qualquer

> operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Ao mesmo tempo em que a Lei reserva um capítulo inteiro à disciplina da Transferência Internacional de Dados (Capítulo V), há, também, dispositivos específicos que visam regulamentar a responsabilidade e o ressarcimento de danos (Capítulo VI – Seção III).

Os dez princípios elencados na Lei n.º 13.709/2018[290] foram elaborados, principalmente, com base no conteúdo do RGPD, havendo grande sintonia entre ambos os dispositivos[291]. Conforme dispõe o art. 6º da LGPD, os dez princípios relativos à privacidade, proteção e tratamento de dados são: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação; e (x) responsabilização e prestação de contas.

No que tange ao princípio da **finalidade**, este é definido como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Este princípio implica na impossibilidade de utilização dos dados para além daquele fim que foi expressamente acordado entre as partes quando cedidos[292].

---

[290] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Op. cit. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 abr. 2020.

[291] ABRUSIO, Juliana. Op. cit., 2018. Disponível em: https://www.migalhas.com.br/depeso/286385/com-certo-atraso-brasil-finalmente-e-inserido-no-rol-de-paises-com-marco-legal-em-protecao-de-dados. Acesso em: 18 abr. 2020. "A lei aprovada é inspirada no sistema europeu e insere o Brasil, com certo atraso, no rol dos países mundiais que possuem marco legal na área de proteção de dados. [...] A lei sancionada empodera o cidadão brasileiro ao fundamentar as regras do tratamento de dados na autodeterminação informativa (inteligência jurídica criada na Alemanha, na década de 1970): o titular de dados terá maior controle sobre o processamento de seus dados pessoais, de forma que o compartilhamento de suas informações será devido apenas por meio de consentimento explícito. Além disso, o titular de dados passa a ter a garantia legal que suas informações serão utilizadas apenas para as finalidades específicas para as quais foram coletadas, devendo ser eliminadas após o propósito que gerou sua coleta e armazenamento. Ainda, o direito de portabilidade de dados é uma novidade conferida pela lei ao brasileiro."

[292] Neste ponto, são feitas críticas semelhantes ao RGPD, mencionadas anteriormente: há dificuldade de verificar o consentimento do titular dos dados, inexistindo um formato específico para obtê-lo.

O princípio da **adequação**, por sua vez, relaciona-se à "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Nesse sentido, não basta que o uso das informações ou dados seja para o fim para o qual foi informado – é necessário que tal uso seja adequado, compatível com aquilo que foi informado e expressamente acordado no momento da cessão dos dados[293].

O princípio da **necessidade** refere-se à "limitação do tratamento ao mínimo necessário para a realização das suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Os princípios da proporcionalidade e da adequação são frequentemente invocados em matéria de responsabilidade civil, de modo que é imprescindível que o uso dos dados não se dê de forma abusiva, ou além do necessário ou daquilo que foi pactuado ou expressamente informado[294].

O quarto princípio constante na Lei é o princípio do **livre acesso** aos dados, o qual constitui "garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais". Após a cessão dos dados pessoais, o indivíduo deve conhecer os responsáveis pelo seu armazenamento, bem como o prazo em que eles serão tratados. Ainda, é importante que lhe seja possível ter acesso aos dados que foram cedidos, de forma "facilitada e gratuita".

A **qualidade dos dados**, por sua vez, refere-se à clareza, atualidade, precisão e veracidade das informações, em conformidade com a finalidade do tratamento. Sob este aspecto, destaca-se o direito do titular dos dados solicitar a retificação ou correção de

---

[293] CAMARGO, Solano de. Op. cit., 24 jun. 2019. Disponível em: https://valor.globo.com/legislacao/noticia/2019/06/24/lgpd-restringe-inovacoes-na-saude.html Acesso em: 05 mar. 2020. Há de se ressaltar as implicações de disposições nesse sentido nas áreas médica e de pesquisa, por restringir o acesso de dados e o desenvolvimento de inteligência artificial, principalmente no âmbito da saúde, desmotivando a inovação. "Uma das principais críticas à Lei Geral de Proteção de Dados é que ela poderá atrasar os programas de Inteligência Artificial (IA) que, dentre outras soluções, poderiam diagnosticar o câncer e rastrear distúrbios genéticos. Na medida em que o art. 11, parágrafo 3º, da LGPD prevê que a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores (como prontuários) poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, estabeleceu-se uma zona nebulosa no caminho da inovação na área da saúde. [...] Um dos principais efeitos da lei é tornar bem mais difícil que médicos e hospitais compartilhem dados com pesquisadores que podem promover a inovação, como as *startups* (ou *healthtechs*). A lei impõe uma série de restrições e procedimentos, que marca toda a cadeia de uso de dados, ameaçando eventuais incidentes com pesadas multas e interdições. [...] Para que a sociedade colha os benefícios da inteligência artificial e das inovações científicas na área da saúde, é necessário repensar e simplificar o compartilhamento de dados, inclusive com a perspectiva de ganhos financeiros para os investidores. A primeira medida é a edição de salvaguardas para a pesquisa na área da saúde pela Autoridade Nacional de Proteção de Dados, reconhecendo o "legítimo interesse" para o setor (art. 10) e regulando as hipóteses de tratamento sem o consentimento prévio. A segunda medida é o acompanhamento das pesquisas e da própria concepção do negócio em conjunto com especialistas na Lei Geral de Proteção de Dados, evitando-se prejuízos e interrupções."

[294] O objetivo é impedir a má utilização de dados pessoais, impedindo a manipulação de consumidores ou de eleitores por meio da coleta de dados e uso para finalidade diversa.

dados, conforme necessário. Para isso, é imprescindível que tenha acesso aos dados coletados.

O princípio da **transparência** está relacionado ao princípio do livre acesso aos dados, já que prevê a "garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Novamente, trata-se do direito de acesso aos dados que foram cedidos, bem como a informações sobre os agentes ou empresas que possuem acesso a eles, e que podem utilizá-los.

O sétimo princípio – princípio da **segurança –** prevê a "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". Ou seja: visa obstar a utilização inadequada de dados pessoais quando tal tratamento de dados se der em desacordo com os princípios anteriormente elencados.

Já o princípio da **prevenção** necessita que as empresas adotem medidas prévias a fim de evitar a ocorrência de danos decorrentes do tratamento de dados. Desse modo, a privacidade desde a concepção mostra-se indispensável, bem como a adoção de medidas de segurança, o que evita o roubo ou o vazamento de bases de dados.

O penúltimo princípio trata sobre a **não discriminação**, e prevê a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Trata-se de medida essencial para garantir o acesso igualitário aos dados e à informação, em conformidade com os princípios constitucionais, bem como para coibir práticas abusivas e ilícitas, as quais podem ser facilitadas pela utilização de meios de comunicação, como a *internet*.

Por fim, o último princípio elencado é o da **responsabilização e prestação de contas**, que assegura: "demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas". Novamente, trata-se de disposição relevante para garantir a segurança do tratamento conferido aos dados pessoais no ambiente *on-line*, especialmente quando tal tratamento se der por agências governamentais.

A Lei em questão foi elaborada com grande inspiração no Regulamento Geral de Proteção de Dados da União Europeia (RGPD). Além de definir conceitos relevantes sobre a matéria, a LGPD possui dispositivos relativos a aspectos de Direito Internacional Privado, os quais visam determinar a competência internacional e a lei aplicável. Observa-se, nesse sentido, a redação dada ao art. 3º da Lei:

> 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, salvo o tratamento previsto no inciso IV do caput do art. 4º desta Lei;
> 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
> III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. [...].

As sanções previstas na LGPD são passíveis de críticas, pois, nos termos do art. 52 da Lei, essas podem representar multas de até R$ 50 milhões[295]. Como consequência, há a penalização das vítimas nos casos em que há ataques criminosos por parte de *hackers*, o que pode ser especialmente prejudicial às empresas pequenas ou novas, inibindo a inovação[296].

Em maio de 2019, o Congresso Nacional aprovou a Lei de Conversão nº 7, de 2019, a qual consolidou alterações na LGPD, introduzidas pela Medida Provisória 869-B. Na ocasião foi aprovada a criação da Autoridade Nacional de Proteção de Dados brasileira (ANPD), e alteradas algumas disposições sobre o uso de dados[297], com destaque para a

---

[295] O art. 52 da LGPD lista as penalidades às infrações cometidas: "I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões por infração; III - **multa diária, observado o limite total de R$ 50 milhões**; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração. Ainda, em 02/10/2019, o Congresso Nacional rejeitou alguns dos vetos parciais à LGPD, restabelecendo as seguintes penalidades adicionais, as quais somente poderão ser aplicadas em caso de **reincidência** específica: VII - suspensão parcial do funcionamento do banco de dados a que se refere a infração, pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; VIII - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; e IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados." (BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Op. cit. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 out. 2019).

[296] CAMARGO, Solano de. Op. cit., 2019.

[297] ACCIOLY, Dante. Comissão aprova MP que cria órgão para proteção de dados. *Agência Senado*, 07 maio 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/05/07/comissao-aprova-mp-que-cria-orgao-para-protecao-de-dados. Acesso em: 17 abr. 2020. "A ANPD recupera a competência para aplicar punições, como a suspensão do funcionamento de banco de dados e a proibição do exercício de atividades relacionadas a tratamento de informações. A primeira versão do relatório previa a substituição das penalidades de suspensão total e proibição total por intervenções administrativas. Mas, segundo o deputado Orlando Silva, a medida 'imporia um ônus desproporcional sobre o setor produtivo de tratamento de dados'. Na complementação de voto, ele prevê a pena de suspensão das atividades por seis meses, prorrogável por igual período em caso de reincidência. [...] O cidadão que se sentir prejudicado pela análise de dados realizada exclusivamente por computadores pode solicitar a revisão dos resultados por pessoas. A regra vale para os casos em que o tratamento automatizado for usado para fundamentar decisões que afetem os interesses do usuário, como a definição de perfis pessoal, profissional, de consumo ou de crédito."

área da saúde[298]. Se por um lado tais alterações evitaram a negação de acesso ou a seleção para seguros médicos e planos de saúde, por outro lado criaram obstáculos para a inovação e pesquisa científica, conforme já mencionado, e nos termos defendidos por Solano de Camargo, com os quais se concorda.

Há, contudo, há sintonia entre a LGPD e o RGPD, sendo evidente a sua repercussão sobre a Lei brasileira. Assim, é possível chegar a conclusões semelhantes no sentido de que, não obstante a existência de críticas e aspectos que ainda deverão ser esclarecidos, a Lei representa um marco na proteção de dados pessoais e na tutela da privacidade no Brasil.

Existem, todavia, críticas ao conteúdo da Lei brasileira: exemplo disso é o fato de que, em 30 de outubro de 2019, foi apresentado o Projeto de Lei n. 5.762/2019, de autoria do deputado Carlos Bezerra (MDB/MT)[299]. O referido projeto propôs o adiamento do início da vigência da lei sob o argumento de que as empresas ainda não estariam devidamente adaptadas, e de que o governo teria levado muito tempo para criar a Autoridade Nacional de Proteção de Dados (ANPD).

Discorda-se, porém, do referido Projeto, já que a postergação da vigência da LGPD somente representaria maior morosidade na proteção dos dados dos cidadãos, revelando-se prejudicial aos valores protegidos pela Lei. Cumpre destacar, igualmente, o Projeto de Lei 1179/2020[300], o qual, recentemente, trouxe a questão do adiamento do início da vigência da lei e das sanções previstas, e que já foi brevemente abordado no início deste capítulo.

Há, também, críticas no sentido de que alguns dispositivos tratariam de situações já abarcadas por diplomas normativos, como o Código Civil e o Código de Defesa do Consumidor. Exemplo disto é o art. 33, inc. III da LGPD[301], que guarda relação com o já

---

[298] Id., ibid. "É vedada a comunicação ou o uso compartilhado de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica. A intenção é evitar a negação de acesso ou a seleção de risco para seguros médicos e planos de saúde. A primeira versão do relatório só permitia a transferência de informações na hipótese de prestação de serviços de saúde, incluídos os serviços auxiliares de diagnose e terapia. Na complementação de voto, o deputado Orlando Silva incluiu a possibilidade de compartilhamento para garantir a assistência farmacêutica do usuário. O projeto de lei de conversão estabelece critérios para o compartilhamento. A comunicação só pode ocorrer se for 'exclusivamente para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária'."

[299] BRASIL. *Projeto de Lei n. 5.762/2019*. Altera a Lei n. 13.709 de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022.

[300] BRASIL. *Projeto de Lei n.º 1.179/2020.* Op. cit. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2247564. Acesso em: 17 abr. 2020.

[301] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Art. 33. Op. cit. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 abr. 2020. "A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...] III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; [...]."

disposto no art. 181 da Constituição Federal[302]. No caso, a norma constitucional já pretende tratar da regulação da transferência de informações e de dados, embora muito incipiente e focada no âmbito empresarial.

O artigo em questão já previa a criação de um órgão responsável pela autorização e controle da troca de informações por meio de carta rogatória ou de auxílio direto. A carta rogatória representa o instrumento judicial menos célere, sendo recorrentes os pedidos de auxílio direto entre as administrações públicas de diferentes países, principalmente na esfera penal[303].

O caso do Conselho de Controle de Atividades Financeiras (Coaf), órgão criado em 1998 no âmbito do Ministério da Fazenda[304], constitui um exemplo relevante: o órgão de inteligência financeira do Governo Federal atua, principalmente, na prevenção e no combate à lavagem de dinheiro. Assim, o Coaf funciona como uma grande base de dados, na qual são reunidas todas as operações financeiras e transações que, por lei, precisam ser comunicadas por bancos, corretoras, seguradoras, cartórios, entre outros.

No governo de Jair Bolsonaro, o órgão passou à subordinação do Ministério da Justiça e Segurança Pública[305]. O Balanço do Coaf de 2018 revelou que no ano anterior

---

[302] BRASIL. *Constituição da Republica Federativa do Brasil de 1988*. Art. 181. Op. cit. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao compilado.htm. Acesso em: 17 abr. 2020. "O atendimento de requisição de documento ou informação de natureza comercial, feita por autoridade administrativa ou judiciária estrangeira, a pessoa física ou jurídica residente ou domiciliada no País, dependerá de autorização do Poder competente."

[303] GIACOMOLLI, Nereu José; SANTOS, Laura Rodrigues dos. Cooperação Jurídica Internacional em matéria criminal: autoridades centrais, das rogatórias ao auxílio direto. *Revista de Estudos Criminais*, jul./set. 2012, n. 46, (s.p.). "Qualquer abordagem da cooperação jurídica internacional há de partir da consideração dos fenômenos da globalização, do incremento da migração, das novas tecnologias que aumentam a velocidade das comunicações entre pessoas e Estados, da importância dos tratados internacionais, bem como dos binômios soberania nacional e solidariedade internacional, repressão da criminalidade e preservação dos direitos fundamentais. [...] No Brasil, não há uma lei específica regulamentando os procedimentos da Cooperação Jurídica Internacional. O regramento é fragmentário e aparece na Constituição Federal, e de forma superficial, em vários diplomas legais, e em normativas administrativas do Superior Tribunal de Justiça, do Ministério da Justiça e do Ministério das Relações Exteriores. As regras mais consistentes estão contidas em uma normativa administrativa do Superior Tribunal de Justiça, de 2005, a qual prevê os mecanismos e procedimentos da cooperação jurídica internacional, bem como na Portaria Conjunta nº 1, de 27 de outubro de 2005, que dispõe sobre a tramitação de pedidos de cooperação jurídica internacional em matéria penal entre o Ministério da Justiça, o Ministério Público Federal e a Advocacia-Geral da União. Trata-se de normatização administrativa, mas que vem sendo observada na cooperação, inclusive por juízes e Tribunais, diante da inexistência de uma lei específica. [...] O auxílio direto não está previsto em lei específica, mas em normativas administrativas. Há apenas algumas referências na Lei de Proteção Ambiental, na Lei de Lavagem de Dinheiro e na Lei de Tóxicos."

[304] BRASIL. *Lei n. 9.613, de 3 de março de 1998*. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras (Coaf), e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/ leis/l9613.htm. Acesso em: 17 abr. 2020.

[305] BRASIL. *Decreto n.º 9.663/2019, de 1º de janeiro de 2019*. Aprova o Estatuto do Conselho de Controle de Atividades Financeiras (Coaf). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/ 2019/Decreto/D9663.htm. Acesso em: 17 abr. 2020.

foram recebidos 6.915 pedidos de informações de autoridades nacionais, e realizadas 297 trocas de informações com unidades estrangeiras de Inteligência Financeira[306]. Raramente, porém, o titular das informações foi notificado sobre tais pedidos, restringindo a forma como as informações podem ser utilizadas, especialmente no âmbito penal.

O fato de o Coaf ser um órgão de controle e não de investigação limita a utilização das informações para a finalidade à qual foi constituído, restringindo-a ao âmbito fiscal. O fornecimento de informações com finalidade de persecução penal deve observar os princípios do contraditório e da ampla defesa, bem como o devido processo legal[307].

Devido à importância da LGPD, bem como dos órgãos de controle, como o Coaf, devidamente autorizados pela Constituição Federal de 1988, conforme explicado anteriormente neste capítulo, não é possível afirmar que os limites impostos ao uso de dados e informações, bem como os direitos dos titulares dos dados, estavam devidamente garantidos.

O Código de Defesa do Consumidor – CDC (Lei n. 8.078/90), em seu art. 43, trata de direitos e garantias do consumidor, inclusive relativos às informações pessoais constantes em "bancos de dados e cadastros", sendo apontado como a norma brasileira mais moderna atualmente em vigor na proteção de dados. Assim, o CDC preocupou-se com a utilização abusiva de informações dos consumidores a partir da criação de bancos de dados, sendo, no momento, a base normativa para a responsabilização por violações.

O Código, contudo, não trata de conceitos e princípios centrais do tema, como o princípio da finalidade, a definição de dados sensíveis, dentre outros. É evidente a importância da proteção conferida pelo CDC ao consumidor, inclusive no ambiente digital, contudo, também são evidentes as suas limitações, a iniciar pelo fato de que a aplicação é restrita a relações de consumo[308].

---

[306] COAF. Conselho de Controle de Atividades Financeiras. *Relatório de Atividades 2018*. Disponível em: http://www.fazenda.gov.br/centrais-de-conteudos/publicacoes/relatorio-de-atividades/arquivos/relatorio-de-atividades-coaf-2018.pdf. Acesso em: 17 abr. 2020.

[307] MIRON, Rafael Brum. O sigilo bancário e a atuação do Coaf: análise dos critérios definidos pelo STF no julgamento da ADI2390/DF para a transferência de sigilo de dados. *Revista da AJURIS*. Porto Alegre, jun. 2017, v. 44, n. 142, p. 302. Concorda-se com o entendimento do autor, sob o seguinte aspecto: "Acaso as provas/informações sejam efetivamente utilizadas para dar ensejo a uma demanda criminal, se estabelecerá o devido contraditório e haverá ampla possibilidade de controle da prova por parte da autoridade judiciária. Dessa forma, não se pode exigir a aplicação das mesmas regras utilizadas para o acesso por parte do Fisco. No caso do Coaf, a análise deve ser feita com base nesse formato próprio e peculiar de atuação, típico de uma unidade de inteligência financeira."

[308] STJ. Superior Tribunal de Justiça. Terceira Turma. REsp 1316921/RJ, Rel. Min. Nancy Andrighi. Julgado em 26/06/2012. "CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO. 1. A exploração comercial da Internet sujeita as

Cumpre discordar, portanto, das críticas que avaliam a LGPD como mera repetição de outros dispositivos: diante das inquestionáveis transformações observadas na sociedade da informação, normas elaboradas em contextos anteriores podem se revelar inadequadas ou insuficientes, permitindo a ocorrência de violações e abusos. Justifica-se, portanto, a aprovação de lei que objetiva especificamente resguardar tais direitos no contexto social específico criado pela internet.

1.7.5 Novos desafios e oportunidades

Tanto o Marco Civil da Internet (MCI) quanto a Lei Geral de Proteção de Dados Pessoais (LGPD) justificam as mudanças trazidas pela Internet: além de meio de comunicação singular, também representam aumento constante nas transações feitas *on-line* e na troca de dados e informações. A previsão é de que em 2021 haverá mais telefones celulares do que contas bancárias ou linhas de telefone fixo[309].

Desde 2013, quando foi revelado que a então presidente do Brasil, Dilma Rousseff, estava sendo objeto de vigilância por parte da Agência de Segurança Nacional norte-americana (NSA), os temas relacionados à privacidade e segurança de dados (principalmente aqueles armazenados em nuvem) tornaram-se uma preocupação[310].

Por outro lado, as inovações tecnológicas vêm contribuindo de forma positiva, destacando-se, na seara jurídica, a adoção dos processos eletrônicos[311]. Advogados e outros

---

relações de consumo daí advindas à Lei n. 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração", contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor [...]."

[309] CISCO. Relatório Cisco VNI Mobile. Disponível em: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~mobile-forecast. Acesso em: 17 abr. 2020.

[310] G1. *Documentos da NSA apontam Dilma Rousseff como alvo de espionagem*. Publicado em 01 set. 2013. Disponível em: http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acesso em: 17 abr. 2020.

[311] ADORNO JÚNIOR, Helcio Luiz; SOARES, Marcele Carine dos Praseres. Processo judicial eletrônico, acesso à justiça e inclusão digital: os desafios do uso da tecnologia na prestação jurisdicional. *Revista Universitas*. Ano 2, jul./dez. 2013, n.º 11, pp. 65-86, p. 66. Muito embora os autores reconheçam a importância da incorporação, pelo Judiciário brasileiro, da tecnologia da informação, com resultados significativos em termos de celeridade processual e prestação jurisdicional, apontam também possível incompatibilidade prática com o *jus postulandi*: "A Reforma do Judiciário destacou a celeridade processual como princípio a ser almejado pelos órgãos desse Poder. Importante instrumento para se alcançar esse objetivo traçado pelo legislador é o uso de recursos de informática para a prática dos atos processuais. A Lei nº 11.419, de 2006, oficializou a informatização do processo judicial, [...]. A segurança dos atos processuais é importante desafio a ser enfrentado na prática judicial eletrônica, o que passa pelo desenvolvimento de recursos de informática, como a certificação digital e a assinatura eletrônica. Esses recursos já vinham sendo satisfatoriamente utilizados com o peticionamento eletrônico, cuja prática antecedeu ao próprio processo eletrônico nos Tribunais brasileiros. Outro desafio a ser enfrentado na implementação do processo eletrônico trabalhista é a dimensão territorial do país, que dificulta a padronização dos procedimentos. O acesso à

profissionais da área jurídica se beneficiam dos processos judiciais eletrônicos, os quais começaram a ser implementados em 2005, embora se perceba que ainda há espaço para melhorias e para a uniformização dos sistemas utilizados.

De fato, os Estados possuem autonomia para adotar diferentes sistemas de acesso aos processos (e-SAJ, PJe, Projudi, entre outros) e, embora o CNJ tenha adotado numeração única para os processos, não há regra que uniformize a forma como tal número deve constar em publicações, especialmente quanto à utilização de traços, pontos e outros, o que dificulta a programação e utilização de *softwares* jurídicos de Inteligência Artificial.

Apesar da necessidade de melhorias é inegável que a digitalização dos processos judiciais lhes confira maior celeridade, permitindo o peticionamento e a juntada eletrônica de documentos. Trata-se, pois, de mecanismo que facilita e amplia o acesso à Justiça, permitindo que advogados atuem em diversas partes do país sem os custos inerentes ao deslocamento às diferentes comarcas[312].

Trata-se de exemplo de situação em que há coleta e transferência de dados sem que, necessariamente, exista uma relação de consumo. Isto não pode impedir o titular dos dados de resguardar seus direitos, de modo que uma legislação protetiva de dados deve ser igualmente aplicável a tais casos.

Em maio de 2017 um ataque *hacker* a empresas e órgãos do mundo todo atingiu tribunais brasileiros, como os Tribunais de Justiça de São Paulo, Minas Gerais e Santa Catarina, além do Ministério Público de São Paulo, onde alguns computadores da promotoria de São José do Rio Preto foram afetados. Os responsáveis pelo ataque exigiram o pagamento de um "resgate" pelos dados roubados, o que foi descartado[313].

Em função da grande quantidade de dados com os quais os portais dos tribunais e órgãos públicos são alimentados, e embora os processos judiciais eletrônicos tenham trazido inúmeras vantagens, especialmente quanto à economia e celeridade processual, surgem, constantemente, novos desafios à proteção de informações tratadas e armazenadas.

---

justiça, com os meios e recursos a ela inerentes na sua totalidade, deve ser assegurado às partes litigantes, agora com os desafios da inclusão digital, o que tornará necessária a revisão do instituto do *jus postulandi*."

[312] Id., ibid., p. 82. "Os benefícios da celeridade e da transparência dos atos judiciais, que decorrem da implantação do processo judicial eletrônico, são inegáveis. A tecnologia da informação é realidade em todos os aspectos da vida moderna, da qual o mundo jurídico é apenas uma das facetas. Cabe aos operadores do direito constatar essa realidade e a ela se adequar, como entusiastas da nova possibilidade de otimização da prestação jurisdicional e de aprimoramento do tempo e do conhecimento em prol da pacificação dos conflitos."

[313] PERES, Bruno; SALES, Robson; POLITO, Rodrigo. Ataque de *hackers* atinge o Brasil; INSS do Rio e TJ-SP são afetados. *Agência O Globo e Folhapress*, 12 maio 2017. Disponível em: https://www.valor.com.br/empresas/4967124/ataque-de-hackers-atinge-o-brasil-inss-do-rio-e-tj-sp-sao-afetados Acesso em: 17 abr. 2020.

A pesquisa jurisprudencial também foi facilitada pela digitalização de sentenças e acórdãos: o acesso a decisões tornou-se rápido e eficiente, permitindo, ainda, a análise em massa das informações ali contidas. A partir de um banco de dados amplo de decisões, é possível analisar as atuais tendências dos órgãos julgadores como forma de ajudar a prever o resultado e a viabilidade de demandas judiciais.

A jurimetria, análise estatística aplicada ao Direito, tem sido utilizada em conjunto com *softwares* jurídicos que permitem tentativas de previsão de resultados, probabilidades e valores envolvidos. Assim, não apenas advogados são beneficiados por disporem de uma ferramenta adicional para avaliar seus casos, como também magistrados e demais servidores públicos, os quais podem utilizar tais estatísticas para orientar as suas decisões[314].

Tais desafios não estão restritos à administração pública, mas incluem, também, as empresas e os escritórios de advocacia, os quais são beneficiados e se adaptam às mudanças. A LGPD trouxe novas oportunidades com a criação do cargo de "encarregado", ou DPO (*Data Protection Officer*), o qual exige conhecimento multidisciplinar sobre a matéria, e requer formação jurídica específica, criando oportunidades profissionais para aqueles que possuem conhecimento sobre privacidade e proteção de dados.

Além da adaptação das empresas já existentes aos atuais parâmetros de proteção de dados, as novas empresas têm adotado a privacidade como valor desde a sua concepção, o que é conhecido como princípio *privacy by design*, conceito que também consta no texto do RGPD[315].

---

[314] ABRAHAM, Marcus; RICARDO CATARINO, João. O uso da inteligência artificial na aplicação do direito público: o caso especial da cobrança dos créditos tributários-um estudo objetivado nos casos brasileiro e português. e-Pública: *Revista Eletrônica de Direito Público*, 2019, v. 6, n. 2, pp. 188-219. É possível observar duas tendências distintas quanto à utilização da jurimetria em decisões judiciais. Em alguns países, a ferramenta é vista como uma forma de permitir a análise de disputas legais simples, reduzindo a quantidade de demandas. Na Estônia, um sistema está sendo desenvolvido para permitir a tomada de decisões por Inteligência Artificial – sendo permitida a sua revisão por um juiz humano. Outros países descartam a utilização de tal recurso, cumprindo citar o exemplo da França, país que proibiu em meados de 2019 a divulgação de estatísticas sobre decisões judiciais, prevendo pena de até cinco anos de prisão em caso de violação. Tal restrição vai na contramão dos avanços tecnológicos: as mudanças no seio da sociedade da informação não podem ser ignoradas, sob pena de provocar incoerência ou descompasso entre o direito e a sociedade.

[315] MORASSUTTI, Bruno Schimitt. Uma breve crítica ao Privacy By Design e seus "princípios basilares". *In*: SARLET, Ingo Wolfgang (Org.). *Temas Atuais e Polêmicos de Direitos Fundamentais.* Contribuições do XIV Seminário Internacional de Direitos Fundamentais. Porto Alegre: Editora Fi, 2018, pp. 53-54. "[...] o fluxo transfronteiriço sem controle de dados pessoais também leva a uma contínua diminuição na esfera de privacidade e, por consequência, autonomia dos indivíduos. Dentre as diversas propostas elaboradas para atenuar ou corrigir este problema, o *privacy by design* recentemente ganhou força após a promulgação pela União Europeia do *General Data Protection Regulation*. [...] Conforme se depreende do texto do art. 25, inc. I, do GDPR, o *privacy by design* consistiria na implementação de 'medidas técnicas e organizacionais adequadas' que sejam desenvolvidas para implementar 'princípios de proteção de dados [...] de uma forma

Isto significa que desde os primeiros momentos em que a empresa é planejada são levadas em conta questões relacionadas à privacidade e à proteção de dados dos seus clientes ou usuários, o que garante a sua adequação à LGPD e às demais normas pertinentes. A ideia é incorporar salvaguardas de privacidade e dados pessoais em todos os projetos desenvolvidos.

O princípio *privacy by default* decorre do primeiro, e trata da ideia de que o produto ou serviço seja lançado e recebido pelo usuário com todas as garantias e salvaguardas que foram concebidas durante o seu desenvolvimento, atendendo ao princípio do *privacy by design*[316]. Nenhum dos dois princípios ou conceitos é adotado expressamente no Brasil, mas a ideia central já pode ser encontrada nas normas que tratam de medidas técnicas para proteger dados contra acessos não autorizados, destruição, perda, alteração ou danos.

Ignorar as mudanças trazidas pela Internet é fechar os olhos para uma nova gama de desafios e oportunidades: neste contexto, aqueles profissionais preparados e com formação multidisciplinar estão em vantagem, pois são capazes de utilizar as novas tecnologias em seu benefício e de seus clientes, permitindo melhoria na qualidade dos seus serviços. A tendência é de que surjam novas demandas envolvendo o direito digital, sendo imprescindível a existência de profissionais aptos a atuar em tais casos.

Está sendo desenvolvida a ideia de "Advocacia Digital", relacionada à utilização de *softwares* tecnológicos a fim de otimizar os serviços, dando origem às denominações de *lawtechs* e *legaltechs*[317]. A "Advocacia Digital" passa, primeiramente, pela digitalização de documentos, permitindo reunir informações em um único local, com rápido acesso e segurança.

Permite, ainda, maior flexibilidade e autonomia do advogado nos processos, e reduz gastos com transporte, cópias, acompanhamento processual, entre outros. Assim, é

---

efetiva'. Todavia, o legislador deixou em aberto qual seria o significado dessas 'medidas técnicas e organizacionais'. Essa indefinição se torna ainda mais complexa quando se verifica que, ao contrário do texto que serviu de anteprojeto para o GDPR, a redação final do regulamento não atribuiu a nenhum órgão ou entidade a responsabilidade de esclarecer o conteúdo dessas medidas."

[316] AUSLOOS, Jef; KINDT, Els; LIEVENS, Eva; VALCKE, Peggy; DUMORTIER, Jos. Guidelines for Privacy-Friendly Default Settings. February 18, 2013. *ICRI Research Paper n. 12/2013*. Disponível em: https://ssrn.com/abstract=2220454. Acesso em: 08 mar. 2020.

[317] MARANHÃO, Juliano Souza de Albuquerque. A pesquisa em inteligência artificial e Direito no Brasil. *Consultor Jurídico* (Conjur). 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais Acesso em: 18 abr. 2020. "*Lawtechs* incubadas em escritórios de advocacia têm criado para uso próprio ou ofertado ao mercado diferentes geradores de documentos. Suas técnicas podem ir desde simples modelos pré-definidos até ferramentas capazes de selecionar tipos mais adequados de documentos, ou sugerir complementações de textos ou citações, a partir de uma base de dados. O desafio para IA&Direito está em desenvolver ferramentas capazes de construir os próprios modelos ou documentos a partir da indicação de argumentos e teses jurídicas ou por meio de reconhecimento de padrões nos documentos já existentes em uma base."

ampliado o acesso dos cidadãos à Justiça, bem como são abertas novas oportunidades de trabalho para jovens profissionais, permitindo a competitividade[318].

A atuação de escritórios de Advocacia totalmente *on-line* ainda é objeto de discussão no âmbito da Ordem Brasileira dos Advogados, mas sua devida regulamentação parece ser incontornável no contexto da Era Digital. Os desafios e oportunidades continuarão a se apresentar, cabendo aos profissionais do Direito superá-los, conciliando a atuação profissional com as normas protetivas de dados.

1.8 CONCLUSÕES PARCIAIS

Neste capítulo foram apresentadas as diferentes formas de perceber temas relacionados à privacidade e à proteção de dados no ambiente digital. Buscou-se demonstrar quais são as particularidades deste meio, e a forma como diferentes Estados vêm lidando com os conflitos que surgem. O próprio caráter transnacional dos dados implica a necessidade de realizar uma análise abrangente, de modo que não fique restrita ao contexto brasileiro[319].

Assim, além das normas aplicáveis, segundo o Ordenamento Jurídico nacional, também foram apresentadas normas internacionais e estrangeiras, a fim de ilustrar a forma como a legislação vem evoluindo no tratamento adequado dos temas da Sociedade da Informação.

Ao longo desta primeira parte do estudo, alguns pontos se destacam como centrais à discussão. Primeiramente, há de se compreender a natureza jurídica dos dados pessoais, de

---

[318] Não se trata simplesmente da utilização de ferramentas digitais no cotidiano da Advocacia, mas da criação de novas formas de trabalhar e prestar serviços, empregando mão de obra qualificada e otimizando os procedimentos, como forma de atingir um maior número de pessoas. O contato pessoal com o advogado não é mais visto como uma prioridade pelos clientes, que buscam agilidade e rapidez, bem como maior facilidade na comunicação com os profissionais.

[319] POLIDO, Fabrício Bertini Pasquot. *Direito internacional privado nas fronteiras do trabalho e tecnologias:* ensaios e narrativas na era digital. Rio de Janeiro: Lúmen Juris, 2018. pp. 73. "A natureza global e transnacional da Internet – a grande rede mundial de computadores – tem estabelecido novos modelos de regulação normativa, instituições e valores no quadro das vertentes internacionalistas do Direito, revolucionando, dentre elas, o Direito Internacional Privado de modo significativo e irreversível. Do ponto de vista das questões de determinação de lei aplicável, jurisdição e reconhecimento de decisões estrangeiras (caracterizadas, comumente, como centrais ao objeto da 'disciplina', se admitida em seu viés ou domínio especializado), os espaços *online* e transfronteiriços, arquitetados pela circulação de bens informacionais, serviços, capitais e tecnologias, proporcionaram autêntico incremento quantitativo e qualitativo dos conflitos de interesses, de autoridades, políticas normativas e de jurisdições. A Internet também altera a conformação ou o perfil de litígios entre particulares (indivíduos/usuários, empresas), e mesmo entre particulares, Estados e seus órgãos governamentais, fazendo com que distintos regimes normativos – baseados em sistemas jurídicos estatais ou não estatais – sejam levados em consideração no momento das soluções pelos tribunais judiciais. Ali reside a transnacionalidade que é intrínseca às redes informáticas e telemáticas."

modo que, conforme o exposto, o tratamento conferido pela lei será distinto se forem considerados bens imateriais ou parte de um Direito autônomo à privacidade. Neste ponto, foram expostos pontos de vista diversos, polarizados, principalmente, entre a abordagem contratualista estadunidense e o entendimento que prevalece na União Europeia, no sentido da indisponibilidade de um direito autônomo.

Ainda que sejam os dois principais representantes dos respectivos entendimentos sobre dados, restou demonstrado que, atualmente, o tema da privacidade e da proteção de informações veiculadas pela Internet é uma preocupação em escala global – inclusive no Brasil. Após todo o exposto, a impressão é que o Ordenamento Jurídico nacional conduz à indisponibilidade do direito à intimidade, à privacidade e à proteção de dados pessoais.

A distinção feita por alguns doutrinadores, contudo, entre direitos fundamentais no âmbito constitucional e direitos de personalidade, inseridos na esfera cível, não parece clara. A análise da legislação infraconstitucional, à luz do texto da Constituição, aparenta levar ao entendimento de que tais esferas não são excludentes, e que, em muitos dos casos tratados nesta pesquisa, uma distinção feita de tal modo não é viável, ou sequer necessária.

Conclui-se pela natureza constitucional do direito à privacidade no Brasil, bem como pela necessidade de analisar, caso a caso, se o objeto da demanda tem natureza cível, ou se está restrito a garantias constitucionais. Uma demanda que verse sobre proteção de dados, com origem em uma relação contratual, possivelmente será enquadrada sob o âmbito cível, sem que isto afaste a natureza constitucional de direitos ali discutidos.

As mudanças legislativas são constantes, de modo que nos últimos anos não apenas foi aprovado o *Privacy Shield*, em substituição à *Safe Harbor Decision*, como, também, foram aprovados o Regulamento Geral de Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados brasileira, que se inspirou significativamente no texto do Regulamento, e que entrará em vigor proximamente, trazendo novos desafios a empresários e operadores do Direito.

De fato, a aprovação da LGPD, de forma complementar ao MCI, já está produzindo impactos sobre as atividades empresariais no país, as quais estão se adaptando aos novos requisitos para coleta e tratamento de dados, anterior à sua vigência em agosto de 2020. Não se sabe, contudo, como as normas serão interpretadas pelo Judiciário brasileiro, principalmente se for considerada a tendência de redução de multas e condenações em sede recursal, sobre a qual tratou esta parte do estudo.

O RGPD, por sua vez, é especialmente relevante ao influenciar a produção normativa de diferentes países, dentro e fora da União Europeia. Neste ponto, destaca-se a

distinção feita entre o papel das diretivas e dos regulamentos no contexto da União, de modo que, enquanto as primeiras têm por escopo orientar a produção legislativa dos Estados-membros, os regulamentos (assim como decisões) são diretamente aplicáveis em toda a União, na data de sua entrada em vigor.

Resta, assim, evidente, a razão pela qual o RGPD é visto como um marco distintivo entre os entendimentos da União Europeia e dos Estados Unidos sobre a proteção de dados: ainda que tal distinção tenha sido delineada nos anos anteriores, com destaque às Diretivas de 1995 e 1997, e a decisão de 2000, proferida pela Comissão das Comunidades Europeias, foi somente a partir do RGPD que, em termos normativos, passou a haver clareza na oposição.

A esse respeito parece que a tendência, após este marco, será de gradual convergência, ou ao menos harmonização entre as visões de privacidade adotadas pelos Estados Unidos e pela União Europeia, sendo o *California Consummer Privacy Act* exemplo disto.

A seguir serão suscitados questionamentos relevantes acerca da proteção de dados e da privacidade no meio digital, com vistas a expor temas relevantes à discussão, normas de direito material aplicáveis, e sanções já aplicadas ou previstas.

CAPÍTULO 2 – PROTEÇÃO DE DADOS: QUESTÕES CONTROVERSAS E DIREITO MATERIAL

Conforme apontado anteriormente, a privacidade e a proteção de dados sofreram mudanças significativas nas últimas décadas, em especial a partir da democratização da Internet no contexto da Sociedade da Informação. Esta sociedade se caracteriza, fundamentalmente, pelo fato de que tem a informação, ao mesmo tempo, como bem de consumo, fator de produção e instrumento de poder.

A relevância conferida à informação em tal sociedade se justifica pelo fato de se encontrar "acessível através de redes de comunicações eletrônicas com âmbito mundial – as chamadas *autoestradas da informação* –, entre as quais sobressai a Internet"[320]. Muito embora a Internet seja um meio de comunicação, ela é dotada de especificidades, não podendo ser igualada aos demais meios existentes.

Alguns fatores diferenciam a Internet dos demais meios de comunicação, entre eles, o seu caráter descentralizado, que não se submete a uma autoridade central; sua natureza pública ou aberta; e, por fim, o fato de permitir que um número ilimitado de utilizadores acesse o conteúdo no momento de sua escolha[321].

No Brasil, o conceito de Sociedade da Informação já foi incorporado, como é possível observar no documento divulgado pelo Ministério da Ciência e da Tecnologia no ano de 2000, intitulado *Sociedade da Informação no Brasil – Livro Verde*. Na apresentação do documento, assinada pelo então ministro de Estado da Ciência e Tecnologia, é possível identificar que: "O advento da Sociedade da Informação é o fundamento de novas formas de organização e de produção em escala mundial, redefinindo a inserção dos países na sociedade internacional e no sistema econômico mundial"[322].

---

[320] VICENTE, Dário Moura. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, p. 89 (grifo no original).

[321] Id., ibid., p. 93. "[...] uma vez que a informação disponibilizada num sítio Internet, por exemplo, fica acessível em todos os países onde exista acesso a esta, o ilícito porventura consubstanciado na disponibilização desta informação (v.g. violadora de direitos autorais ou com conteúdo difamatório) é, em rigor, cometido em qualquer desses países, sendo por isso, *prima facie*, aplicáveis as respectivas leis e competentes os tribunais locais. [...] A diferença entre estes e a Internet está, no entanto, na circunstância de que, em razão do âmbito universal desta, o número de países em que o elemento de conexão relevante pode considerar-se concretizado é muito superior, embora não raro o número de utilizadores efetivos da informação disponibilizada em cada um deles seja muito inferior. O que, do ponto de vista do equilíbrio dos interesses em presença, torna, em tais casos, menos justificável uma opção pela lei do país de destino da informação."

[322] TAKAHASHI, Tadao (Org.). *Sociedade da Informação no Brasil. Livro Verde*. Brasília: Ministério da Ciência e Tecnologia, set. 2000, p. v. "A Sociedade da Informação está sendo gestada em diversos países. [...]. O advento da Sociedade da Informação é o fundamento de novas formas de organização e de produção em escala mundial, redefinindo a inserção dos países na sociedade internacional e no sistema econômico mundial. Tem, também, como consequência, o surgimento de novas demandas dirigidas ao Poder Público no

Para José Augusto Fontoura Costa e Fernanda Sola, o desenvolvimento recente da informática pode ser designado como "revolução da informação", e vem afetando profundamente as maneiras como o conhecimento é produzido e distribuído[323]. Os impactos dessa revolução sobre a sociedade vêm sendo estudados há decênios: nas décadas de 1970 e 1980, o desenvolvimento da microeletrônica suscitou discussões sobre a automação das fábricas e uma "sociedade do lazer" em que ocorreria o suposto "fim do trabalho"; neste contexto, a informação assumiu posição de destaque[324].

Os temas atualmente em discussão "se relacionam com a expansão e aumento da funcionalidade da Internet, inclusive democracia eletrônica, relações virtuais, redes sociais, modelos de difusão e proteção de obras artísticas e técnicas e direito à intimidade, entre outros"[325], e têm sido objeto de análise por juristas, bem como por acadêmicos de outras áreas do conhecimento, onde demonstram a sua abrangência:

> Já há muito que se fala em sociedade da informação, Frank Webster (2003), por exemplo, analisa o conceito e aspectos da sociedade de informação a partir do cotejamento das teorias de Daniel Bell (sociedade pós-industrial), Manuel Castells (sociedade em rede e capitalismo informacional), Herbert Schiller (manipulação da informação), Jürgen Habermas (declínio da esfera pública) Anthony Giddens (função de controle e vigilância da informação em face da modernização reflexiva) e os pós-modernistas Jean Baudrillard e Zygmunt Bauman, que analisam a profusão dos signos na atualidade. O autor estabelece uma perspectiva de análise que contrapõe aqueles que acreditam que as transformações são realmente estruturais e profundas, de um lado, e aqueles mais céticos, que enfatizam a continuidade, do outro lado[326].

---

que respeita ao seu próprio funcionamento. Na era da Internet, o Governo deve promover a universalização do acesso e o uso crescente dos meios eletrônicos de informação para gerar uma administração eficiente e transparente em todos os níveis. [...]. Ao mesmo tempo, cabe ao sistema político promover políticas de inclusão social, para que o salto tecnológico tenha paralelo quantitativo e qualitativo nas dimensões humana, ética e econômica. A chamada "alfabetização digital" é elemento-chave nesse quadro. [...]. Essa iniciativa permitirá alavancar a pesquisa e a educação, bem como assegurar que a economia brasileira tenha condições de competir no mercado mundial."

[323] COSTA, José Augusto Fontoura; SOLA, Fernanda. Direito das tecnologias de comunicação e informação: uma primeira abordagem do Marco Civil da Internet. *PIDCC*. Aracaju, fev. 2015, ano IV, ed. nº 08/2015, pp. 336-351.

[324] ABRUSIO, Juliana. O uso do link patrocinado como prática de conduta desleal no comércio da internet. *Pensamento Jurídico*, 2018, v. 12, pp. 291-311, pp. 293-294. "Com a consagração da internet, o comércio invadiu a grande rede, alargando as opções tanto dos empresários de praticarem a mercancia, como dos consumidores em adquirirem produtos e serviços. A internet revolucionou a forma tradicional de produção. [...] Em consequência desse novo sistema social, novo poder foi criado, o poder tecnológico. Não à toa, constata-se que a competitividade pelo domínio tecnológico é agressiva. As companhias que alcançam domínio tecnológico terão maior vantagem frente ao mercado e seus clientes. E, nessa corrida pela liderança de mercado, alguns agentes econômicos desviam-se das regras da concorrência leal, estabelecidas pelo ordenamento jurídico, e salutares para a dinâmica do mercado."

[325] Id., ibid., pp. 339-340.

[326] Id., ibid., p. 340.

Se, por um lado, a Internet oferece grande potencial econômico em termos de desenvolvimento, por outro há que se considerar que as suas especificidades fazem surgir problemas igualmente particulares, relacionados à sua essência internacional[327]. Ao mesmo tempo em que a Internet globaliza o mercado, ela também aumenta os locais nos quais danos podem ocorrer[328]. E, ainda que a Sociedade da Informação se baseie em um espaço de liberdade – a Internet –, há que se considerar o risco oferecido por sua *hiper-regulação*, perigo para o qual alerta Dário Moura Vicente:

> Com efeito, ela assenta num espaço de liberdade – a Internet –, no qual se facultam ao público recursos informativos numa escala sem precedentes na história da humanidade e se possibilita a cada um a expressão e a divulgação quase instantânea do seu pensamento através de um meio de comunicação de âmbito universal. No entanto, o risco de uma hiper-regulação da Internet, por via da aplicação à atividade através dela desenvolvida de uma multiplicidade de leis com os conteúdos mais diversos, assim como da prolação de sentenças contraditórias por tribunais de diferentes países que se tenham por competentes para julgar os litígios dela emergentes, é susceptível de coarctar aquela liberdade, restringindo o fluxo da informação através das fronteiras e o acesso do público a esta[329].

---

[327] CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999, v. I, p. 46. Manuel Castells apresenta reflexão interessante acerca da expressão "sociedade da informação", diferenciando-a do que entende como "sociedade informacional": "O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo, por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolasticismo, ou seja, no geral uma infraestrutura intelectual. Ao contrário, o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial. [...] Meu emprego dos termos sociedade informacional e economia informacional tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades."

[328] KESSEDJIAN, Catherine. Dispute resolution on-line (Symposium on Jurisdiction and the Internet). *The International Lawyer*, 1998, v. 32, n.º 4, pp. 977-990, (s.p.). "Mas, embora a Internet seja vista como uma ferramenta para uma melhor administração do sistema judicial, é preciso reconhecer que ela mesma cria novas causas de disputa. De fato, a Internet, por sua essência internacional, gerou novos riscos. [...] Daqui resulta que as partes contratantes pela Internet serão confrontadas, como nunca antes, com situações bastante desconfortáveis; serão processadas em uma jurisdição estrangeira ou em várias jurisdições simultaneamente; serão expostas a uma lei estrangeira; ou terão que entrar com uma ação em uma jurisdição estrangeira para garantir seus direitos, ou entrar com uma ação simultaneamente em várias jurisdições. De fato, a Internet globaliza o mercado, mas também aumenta o número de lugares em que podem ocorrer danos." (Tradução livre). "*But while the Internet is thought of as a tool for a better administration of the judicial system, one must recognize that the Internet itself creates new causes for dispute. Indeed, the Internet, by its international essence, has generated new risks. [...] It follows that parties contracting over the Internet will be faced, move than ever before, with rather uncomfortable situations; they will be sued in a foreign jurisdfiction, or several jurisdictions, simultaneously; they will be exposed to a foreign law; and they will also have to bring suit in a foreign jurisdiction to enforece their rights, or to bring suit simultaneously before several jurisdictions. Indeed, the Internet globalizes the maket, it also increases the number of places where damages can be incurred*."

[329] MOURA VICENTE, Dário Manuel Lentz de. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, p. 95.

Observam-se, portanto, valores em conflito, além da questão da liberdade em oposição à regulação. Ademais, são considerados outros interesses sociais relevantes, como a proteção da ordem pública e dos consumidores, ressaltando-se que, por vezes, as tecnologias acentuam e não atenuam as desigualdades sociais.

Não obstante, há que se reconhecer o papel por elas exercido no desenvolvimento econômico e social, fazendo-se necessário um "quadro jurídico apropriado que, além do mais, assegure a liberdade de estabelecimento e a livre circulação dos serviços da sociedade da informação através das fronteiras"[330].

A seguir, são abordados alguns dos principais temas relacionados ao direito à privacidade e à proteção de dados na Era Digital[331]. A proposta não é exaurir as temáticas ligadas ao assunto, mas demonstrar a relevância prática da discussão e delinear a relação existente entre as questões controversas abordadas e o tratamento conferido pelo Direito Material, já assinalando alguns pontos de discussão relevantes ao Direito Conflitual.

O tratamento conferido pelo Direito Material depende necessariamente da qualificação do objeto do conflito em questão. Tratou-se, anteriormente, da abordagem contratualista dos dados pessoais, cujo maior exemplo são os Estados Unidos, bem como a visão que coloca o direito à privacidade e os direitos à personalidade na condição de direitos constitucionais indisponíveis, ligados essencialmente à dignidade humana.

Igualmente, delineou-se que o posicionamento adotado pelo Brasil parece ser, em geral, mais coerente com esta segunda visão, a qual cita, como exemplo, a União Europeia, com destaque para o RGPD que, conforme tratado a seguir, traz implicações quanto à questão da qualificação.

---

[330] Id., ibid., p. 96.

[331] MARANHÃO, Juliano Souza de Albuquerque. A pesquisa em inteligência artificial e Direito no Brasil. *Consultor Jurídico* (Conjur), 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais Acesso em: 18 abr. 2020. "[...] em relação à proteção de dados, deve-se atentar para o fato de que sistemas de IA baseados não só tomam decisões com base em dados como a cada interação recolhem dados para a futura tomada de decisões. Há preocupação sobre como esses dados são colhidos, processados e empregados. Além disso, tais sistemas podem tomar decisões com base em 'perfis' individuais ou de grupos desenvolvidos pelos próprios sistemas, ou ainda com base em correlações derivadas de um modelo de aprendizado de máquina sobre enorme gama de dados, de difícil compreensão teórica. Como os dados processados podem ser enviesados, as decisões automáticas decorrentes podem interferir em direitos individuais, sem que o programa ou os desenvolvedores consigam sequer apresentar justificativas humanamente compreensíveis sobre quais foram as razões de sua decisão. Portanto, além da preocupação de a IA poder extrair o conhecimento por trás de decisões baseadas em algoritmos complexos envolvendo aprendizado de máquina, existe a preocupação jurídica com a regulação e garantia dos direitos daqueles que são afetados por tais decisões."

2.1 QUALIFICAÇÃO

O método do Direito Internacional Privado no Brasil é composto por três fases, sendo a primeira delas a qualificação[332], que significa enquadrar juridicamente os fatos pertinentes ao caso[333], compreendendo a questão objeto da lide e procedendo a subsunção dos fatos à regulamentação jurídica, seguida da identificação do objeto de conexão e da definição da lei aplicável e sua aplicação, levando, por fim, à solução material do conflito[334]. Este conceito, em verdade, reflete a ideia de que existe uma pluralidade de culturas, de forma que os Estados acabam por construir normas jurídicas distintas, segundo critérios próprios[335].

Antes, porém, de identificar o tribunal competente e o direito por ele aplicado, é preciso qualificar a situação analisada de acordo com um dos critérios supra-apontados[336]. Trata-se do enquadramento da questão jurídica[337], passando pela conceituação e pela

---

[332] MONACO, Gustavo Ferraz de Campos. *Conflitos de Leis no Espaço e Lacunas (Inter)Sistêmicas.* São Paulo: Quartier Latin, 2019, pp. 79-80. "Apesar de não ter sido ainda explicitado, entende-se por qualificação [...] o processo mental de conceituação e classificação de uma relação jurídica plurilocalizada e que não depende exclusivamente, como se verá, dos conceitos jurídicos vigentes em um ou em outro dos ordenamentos presentes. Por outras palavras, trata-se do ajuste da situação juridicamente relevante a uma das instituições normativamente construídas pelo legislador com a finalidade de dar-lhe jurídico enquadramento, porém, partindo-se da *lex fori* e chegando-se a utilizar, muitas das vezes, de conceitos da *lex causae* (qualificação-subsunção). Isso significa que nas situações relativas aos bens e às obrigações, o intérprete brasileiro deverá, por explícita disposição legal, tomar em consideração, para proceder à subsunção do fato à norma, a mesma lei que tomará para fins de determinação dos aspectos estruturais e materiais da *questio iuris decidenda*. Ao assim dispor, o legislador brasileiro reconhece [...] a possibilidade de que uma obrigação que no ordenamento nacional é estabelecida apenas e tão somente por meio do acordo de vontades entre as partes seja, no ordenamento alienígena, estabelecida por determinação legal caso as partes não concretem sua vontade em determinado sentido, observadas tais ou quais condições ou certo prazo, por exemplo."

[333] AUDIT, Bernard. Qualification et droit international privé. *Droits*, 1993, n. 18, p. 55. "Operação fundamental do raciocínio jurídico, a qualificação cumpre duas funções principais. Como em qualquer matéria, ele é um facilitador do idioma, no qual um termo (hipotético...) permite sintetizar uma longa definição. Mais específico é o fato de que a quaificação define um regime, como ilustra a distinção mais fundamental do direito francês: aquela do direito público e o direito privado. Esta distinção em si influencia a delimitação do objeto da matéria abordada: as relações privadas internacionais." (Tradução livre). "*Opération fondamentale du raisonnement juridique, la qualification remplit deux fonctions principales. Comme en toute matière, ele est une facilité du langage, en ce qu'um mot (hypothèque...) permet de synthétiser une longue définition. Plus spécifique est le fait que la qualification définit um régime, comme l'illustre la distinction la plus fondamentale du droit français: celle du droit public et droit privé. Cette distintction même intervient dans la délimitation de l'objet de la matière abordée: les relation privées internationales*."

[334] DOLINGER, Jacob; TIBURCIO, Carmen. *Direito Internacional Privado*. 15. ed. Rio de Janeiro: Forense, 2020.

[335] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 52-53. "As múltiplas culturas levaram – muitas vezes – os Estados soberanos a construir normas jurídicas distintas em sua estrutura e/ou em seu conteúdo material, reunindo-as por razões de política legislativa, segundo critérios que fazem sentido no sistema ali instituído, pelo que se pode afirmar a viabilidade de se fazer ao menos uma etnologia da cultura jurídica em consideração."

[336] MAGALHÃES COLLAÇO, Isabel Maria de. *Direito internacional privado*. Lisboa, 1958-1963.

[337] MONACO, Gustavo Ferraz de Campos. Competência internacional (limites à jurisdição nacional) em matéria de ação revisional de prestação alimentícia e partilha de bens. *Revista de Processo*, 2017, v. 266, pp. 365-391, p. 377. "Em DIP, a subsunção da relação fática à norma que indicará a lei aplicável se faz por meio

classificação[338], havendo, ainda, a possibilidade de ocorrência de conflitos de qualificação[339].

O legislador brasileiro fez duas esparsas referências à lei a que se deve recorrer para fins de qualificação, mencionando a necessidade de se valer da *lex causae* sempre que se tratar de qualificar os bens (lei do local de situação dos bens)[340] e as obrigações (lei do local de constituição)[341]. Silenciou, contudo, quanto ao estabelecimento de uma regra geral, de modo que a maior parte da doutrina invoca as disposições da Convenção

---

de um importante exercício hermenêutico denominado 'qualificação'. A qualificação é assim, o exercício interpretativo dos fatos que tem por escopo permitir o enquadramento da relação jurídica apresentada, em uma das grandes categorias jurídicas tratadas pelas normas de DIP, permitindo que se encontre o elemento de conexão e, consequentemente, o direito aplicável."

[338] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 57-58. "Com efeito, no âmbito das relações privadas com elementos estrangeiros, a interpretação do Direito material interno apresenta particularidades que obrigam a alargar os conceitos utilizados nas normas de conflito, como forma de se garantir a desejável coordenação entre os sistemas. Isso não quer significar, necessariamente, que a mesma situação da vida mereça uma apreensão por normas jurídicas diversas, provenientes de sistemas jurídicos distintos. Mas, sim, que se possa garantir que na 'categoria normativa própria a cada regra de conflitos', para falar com António Ferrer Correia, seja possível enquadrar os 'múltiplos preceitos e os numerosos institutos estrangeiros', os quais, em seus ordenamentos de origem, cumprem o mesmo papel: propõem-se a 'realizar a mesma função social que o legislador do foro teve em vista ao aludir a tal categoria, ou uma função substancialmente análoga'. O que ocorre, em suma, é que os elementos fatuais são apreendidos pelas normas jurídicas consideradas a partir de conceitos qualificadores próprios a cada um dos ordenamentos colidentes. E isso porque o que se busca com o estabelecimento de normas jurídicas amplas e generalizantes no Direito Internacional Privado é justamente evitar repetições, [...]. Nesse processo de generalização que visa colocar em evidência o que é essencial, os conceitos de que se valem as normas de conflitos acabam por ser preenchidos por conceitos de seu próprio ordenamento [...]."

[339] MAGALHÃES COLLAÇO, Isabel Maria de. *Da qualificação em direito internacional privado.* Lisboa: s/e, 1964, p. 215, 261. "Toda a qualificação supõe a prévia interpretação da categoria legal a que vai reconduzir-se o objecto a qualificar, mas envolve, para além disto, a caracterização desse objecto, em ordem a decidir finalmente da possibilidade da sua subsunção no conceito em causa. [...] Na disciplina da vida privada internacional prosseguida por um dado sistema de normas de conflitos, pode acontecer que duas regras materiais, dimanadas de ordens jurídicas diferentes, e aplicáveis por força de normas e conflitos distintas a uma mesma situação fundamental da vida, venham a revelar-se em radical dissonância, por uma delas tutelar um interesse que a outra incondicionalmente sacrifica. O fenômeno que assim se desenha destaca-se claramente das figuras de concurso de normas de conflitos que ficaram evocadas nos números anteriores."

[340] BRASIL. *Decreto-Lei n.º 4.657 de 04 de setembro de 1942*. Lei de Introdução às Normas do Direito Brasileiro (LINDB). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 17 abr. 2020. Bens imóveis são qualificados a partir do art. 8.º, *caput*, da LINDB. Bens móveis que se destinam ao transporte, por sua vez, são qualificados pela lei do local de domicílio do proprietário, nos termos do § 1º do mesmo artigo. Nos demais casos envolvendo bens, aplica-se a referida regra geral, conduzindo à qualificação pela *lex fori*. "Art. 8º. Para qualificar os bens e regular as relações a eles concernentes, aplicar-se-á a lei do país em que estiverem situados. § 1º. Aplicar-se-á a lei do país em que for domiciliado o proprietário, quanto aos bens moveis que ele trouxer ou se destinarem a transporte para outros lugares. § 2º. O penhor regula-se pela lei do domicílio que tiver a pessoa, em cuja posse se encontre a coisa apenhada."

[341] Id., ibid. Importante distinguir a regra do *caput* do art. 9º, que se refere ao local em que são constituídas as obrigações, e o § 2º do mesmo artigo, que se aplica a obrigações contratuais entre ausentes, conduzindo à lei do local de residência do proponente. "Art. 9º. Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem. § 1º. Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato. § 2º. A obrigação resultante do contrato reputa-se constituída no lugar em que residir o proponente."

Interamericana sobre normas gerais de Direito Internacional Privado[342] (CIDIP), as quais vão no mesmo sentido do art. 6º do Código Bustamante, estatuindo a qualificação pela *lex fori*[343].

Consequentemente, é possível identificar nos casos, segundo o Direito brasileiro, ao menos duas possibilidades de qualificação envolvendo privacidade e proteção de dados plurilocalizados: primeiramente, há a possibilidade de qualificação pela *lex causae*, ou do local onde foi constituída a obrigação, conforme consta expressamente no *caput* do art. 9º. Em seguida, em se tratando de obrigação resultante de contrato celebrado entre os ausentes, reputa-se o local de residência do proponente, sendo a lei utilizada para fins de qualificação, nos termos do § 2º do mesmo artigo[344].

Há, contudo, ainda outras possibilidades a serem consideradas e avaliadas caso a caso, como os que envolvem contratos de consumo. Cláudia Lima Marques defende a

---

[342] BRASIL. *Decreto n.º 1.979, de 09 de agosto de 1996*. Promulga a Convenção Interamericana sobre Normas Gerais de Direito Internacional Privado, concluída em Montevidéu, Uruguai, em 8 de maio de 1979. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1996/D1979.htm. Acesso em: 17 abr. 2020. Destacam-se os seguintes artigos da mencionada Convenção: "Art. 1º. A determinação da norma jurídica aplicável para reger situações vinculadas com o direito estrangeiro ficará sujeita ao disposto nesta Convenção e nas demais convenções internacionais assinadas, ou que venham a ser assinadas no futuro, em caráter bilateral ou multinacional, pelos Estados Partes. Na falta de norma internacional, os Estados Partes aplicarão as regras de conflito do seu direito interno. Art. 2º. Os juízes e as autoridades dos Estados Partes ficarão obrigados a aplicar o direito estrangeiro tal como o fariam os juízes do Estado cujo direito seja aplicável, sem prejuízo de que as partes possam alegar e provar a existência e o conteúdo da lei estrangeira invocada."

[343] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 77-78. "Seja como for, o fato é que as normas brasileiras de conflito não enunciam uma regra geral apta a construir um modelo de qualificação dos casos fáticos plurilocalizados, muito embora o façam em dois dispositivos específicos como adiante se verá, restando à doutrina a tentativa de forjar o modo pelo qual se deva, no foro brasileiro, proceder à qualificação. E ainda assim, por exemplo, Jacob Dolinger e Haroldo Valladão extraem das regras específicas expressas a regra geral oculta de modo diametralmente oposto: para Dolinger a regra geral é a qualificação segundo os critérios da *lex fori*; para Valladão, pelos da *lex causae*."

[344] OLIVEIRA, Elsa Dias. *A proteção dos consumidores nos contratos celebrados através da Internet*. Coimbra: Almedina, 2002, p. 345. A respeito da celebração de contratos entre ausentes no espaço (embora presentes no tempo, o que se torna possível pelo meio digital), o momento da celebração do contrato é questão que assume especial relevância. Tal aspecto é analisado por Elsa Dias Oliveira sob a ótica do Direito do Consumidor no seguinte excerto: "A determinação do momento da celebração do contrato é outra questão que pode assumir especial relevância para o consumidor, já que, v.g., em alguns contratos o prazo para exercício do direito de rescisão se inicia no momento da celebração do contrato. Contudo, as teorias seguidas nos diversos Estados, para determinação deste momento, não são uniformes. Nos contratos celebrados através da Internet, as dificuldades agudizam-se face à ainda novidade do meio, à possibilidade de celebrar contratos entre presentes e entre ausentes e à própria falta de uniformidade doutrinária e jurisprudencial sobre esta matéria. Entendemos que, à luz do ordenamento jurídico português, e nos contratos entre ausentes, deverá, por regra, prevalecer a teoria da recepção e o contrato ser considerado celebrado no momento em que o proponente pode aceder à aceitação, ainda que não tenha transferido para o sistema informático do seu computador. Nos contratos entre presentes, não se suscitam especiais questões, já que entre a proposta e a aceitação não se verifica um lapso de tempo juridicamente relevante. Ainda atenta à diversidade de orientações seguidas nos vários ordenamentos jurídicos, considerou-se importante tratar a questão de saber qual seja a lei aplicável à determinação do momento da celebração do contrato e concluímos que, nos termos da Convenção de Roma, essa será a *lex contractus*."

proteção da parte mais fraca da relação[345], de forma similar ao que dispõe o art. 5º da Convenção de Roma, de 1980, no âmbito da União Europeia.

Mesmo após a promulgação da LGPD, ainda não há normas que tratam especificamente da qualificação no meio digital, como, por exemplo, definir o que se entende por localização do proponente *online*. Pressupõe-se, conforme já apontado, que o contrato seja considerado como celebrado entre ausentes.

De todo o modo, o entendimento acerca de contratos eletrônicos firmados por aceitante domiciliado no Brasil, e proponente domiciliado em outro país, é de que cumpre observar o art. 9º da LINDB, aplicando-se a lei estrangeira para fins de qualificação do caso analisado. Ou seja: como regra geral, as obrigações contratuais implicam a qualificação pela lei do país do proponente e, excepcionalmente, aplica-se a lei brasileira sobre as formalidades essenciais do contrato, na hipótese de obrigação a ser cumprida no país (§ 1º do art. 9º).

Enquanto o art. 435 do Código Civil determina que "Reputar-se-á celebrado o contrato no local em que proposto"[346], o Código de Defesa do Consumidor[347] é, por vezes, utilizado como base legal para afastar a norma estrangeira sob o argumento de desequilíbrio da relação jurídica quando o consumidor for domiciliado no Brasil[348]. Enquanto o art. 51, inc. IV, do CDC veda a aplicação de cláusulas que coloquem o consumidor em vantagem exagerada, é possível considerar que o contrato celebrado por meio eletrônico tem como local de contratação o domicílio do consumidor, tido como país de destino do serviço ou produto.

---

[345] MARQUES, Cláudia Lima. A insuficiente proteção do consumidor nas normas de direito internacional privado – da necessidade de uma convenção interamericana (CIDIP) sobre a lei aplicável a contratos e relações de consumo. *Revista dos Tribunais*. São Paulo, 2001, v. 788, pp. 11-56, (s.p.). "Mister superar as conexões tradicionais para proteger o contratante mais fraco. [...] Esta realidade faz com que as normas brasileiras do art. 9º, § 2º da LICC/42 e art. 9º, § 1º LICC/42 estejam superadas. O § 2º do art. 9º dispõe que a obrigação resultante do contrato reputa-se constituída no lugar onde residir o proponente, determinando, assim, a aplicação da lei do lugar de residência do fornecedor para reger os contratos entre ausentes, mesmo os de consumo. Necessário, pois, superar esta regra e escolher, para os contratos de consumo, diferentemente dos contratos internacionais comerciais, uma conexão mais favorável ao consumidor, como a do art. 5º da Convenção de Roma, de 1980, que dá preferência à lei do país onde o consumidor tem sua residência habitual como conexão rígida (art. 5,3 Conv. de Roma de 1980), se não há expressa manifestação da vontade."

[346] BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 17 abr. 2020.

[347] BRASIL. *Lei n.º 8.708, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 17 abr. 2020.

[348] OLIVEIRA, Elsa Dias. Op. cit., 2002, p. 59. "A ausência física dos contraentes no processo de formação dos contratos e em especial no momento das trocas de consentimento, propícia ao contacto impessoal e anónimo, pode colocar problemas pertinentes quanto à identificação das pessoas e, mais concretamente, quanto à percepção da capacidade contratual da parte pelo seu co-contratante."

Se entendidos, contudo, como contratos celebrados entre ausentes no espaço (mesmo que presentes no tempo), há de se considerar a existência de lapso temporal entre a proposta e a respectiva aceitação, bem como o fato de que os locais de proposta e de aceitação serão distintos em grande parte dos casos[349]. Destarte, se for considerado o local de residência do proponente como critério de qualificação, nos termos do art. 9º da LINDB, pouco importará o país no qual está o consumidor, ou no qual está o provedor, ou registrado o domínio, já que assim dispõe claramente o texto da lei.

Se um consumidor brasileiro, domiciliado e residente no Brasil, contrata bem ou serviço de uma pessoa jurídica do país A, cujos provedores estão no país B, e cujo domínio está registrado no país C, reputar-se-á como aplicável a lei estrangeira do país A, local da residência do proponente. Tal análise não impede, contudo, que sejam suscitados conflitos de qualificação[350], com base nos argumentos tratados anteriormente[351].

Outro conflito de qualificação que poderá ser suscitado após a vigência da LGPD é relativo ao legítimo interesse. Com linguagem similar ao GDPR, a LGPD dispõe, no seu art. 7º, que dados pessoais podem ser objeto de tratamento

> 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, [...] o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, [...] somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados[352].

---

[349] CONSELHO DE JUSTIÇA FEDERAL. III Jornada de Direito Civil. *Enunciado n.º 173 ao Código Civil*. 2004. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/311. Acesso em: 17 abr. 2020. "A formação dos contratos entre pessoas ausentes, por meio eletrônico, completa-se com a recepção da aceitação pelo proponente."

[350] MAGALHÃES COLLAÇO, Isabel Maria de. *Da qualificação em direito internacional privado.* Lisboa: s/e, 1964, pp. 2433-2434. "A aplicação concorrente de duas ou mais normas de um dado sistema local de conflitos de leis pode desenhar-se em termos de fazer surgir na titularidade do mesmo interessado, duas ou mais pretensões, fundadas em normas materiais distintas, por forma a que tais pretensões devem ter-se por independentes e cumuláveis, apesar de se reconduzirem pelo menos em parte aos mesmos factos ou situações da vida."

[351] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 68 e ss. "Um equívoco de qualificação empurra a situação da vida que se encontra sob o império do foro E1 para uma lei que não foi considerada pelo legislador de Direito Internacional Privado de E1 como a mais próxima e, por isso, a lei com eficácia para dirimir os conflitos dentre todas as leis presentes e, por isso, competentes. Da mesma forma, a qualificação realizada por meio da incidência de critérios relativos à suposta *lex causae* – como no exemplo anteriormente desenhado – pode levar, por vezes, a que a lei aplicável seja uma lei diferente daquela que – por algum motivo – foi considerada como tal, criando um círculo vicioso de difícil justificação como foi afirmado acima."

[352] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/ L13709.htm. Acesso em: 17 abr. 2020.

Enquanto a LGPD utiliza o termo "interesse", no RGPD optou-se por "finalidade", conceitos que, embora próximos, são distintos. Enquanto a finalidade se relaciona com o propósito específico do tratamento de dados, o interesse mostra-se mais amplo, "sendo aquilo que o controlador, ou terceiro, pretende auferir com o tratamento de dados; em outras palavras, é o benefício que se espera decorrer da atividade de tratamento, seja para o controlador, para o próprio titular dos dados ou, ainda, para a sociedade em geral"[353].

Considerando que ambos os diplomas normativos têm amplo âmbito de aplicabilidade, as chances de conflito de qualificação em termos de legítimo interesse são uma questão a ser levada em conta.

Primordialmente, no Brasil, a qualificação é realizada a partir do critério da *lex fori*, excetuando-se conflitos que envolvam bens ou obrigações, conforme arts. 8º e 9º da LINDB e respectivos critérios supra-apontados. A partir de tal regra poderá ser aplicada a lei do foro ou a lei estrangeira, conforme cada caso concreto.

Para fins de reflexão, traz-se o seguinte exemplo: um estrangeiro, nacional de X e residente no Brasil, deseja ajuizar uma demanda por não ter sido atendida sua solicitação de exclusão de dados ou informações, coletados em Y por empresa sediada em Z. Pelo fato de o indivíduo ser residente no Brasil, o Judiciário nacional será potencialmente competente a partir da leitura do art. 21, inc. I, do CPC. Por se tratar de relação de consumo, e sendo o consumidor aqui domiciliado, seria igualmente aplicável o art. 101, inc. I, do CDC, conduzindo, também, à competência do juiz nacional.

Ao ser chamado a dirimir o conflito, o juiz deverá, necessariamente, proceder à qualificação. Conforme exposto, neste caso seria aplicável a regra geral que institui a qualificação pela *lex fori*. Se, porém, os dados foram coletados a partir de uma relação contratual, a qualificação será feita, potencialmente, pela lei do local de constituição da obrigação, ou do local de residência do proponente (considerando-se a contratação entre ausentes).

---

[353] SOARES, Pedro Silveira Campos. Legítimo interesse como hipótese para tratamento de dados. *Conjur*, 18 jun. 2019. Disponível em: https://www.conjur.com.br/2019-jun-18/pedro-soares-tratamento-dados-baseado-legitimo-interesse. Acesso em: 07 jan. 2020. "Uma ressalva deve ser feita: apesar de sua amplitude conceitual, a experiência europeia demonstra que somente interesses claramente definidos e vinculados ao escopo de atividades praticados pelo controlador poderão servir de base para tratamento de dados que pretenda encontrar fundamento da hipótese aqui discutida. Remete-se ao caso dos aplicativos de controle de atividades físicas. Neste exemplo, o interesse do controlador pode ser proporcionar maior transparência e controle sobre as atividades físicas desempenhadas pelo usuário, com intuito de proteger a saúde e aprimorar o condicionamento físico. A finalidade específica perseguida pelo controlador, de outro lado, pode envolver a implementação de um meio instantâneo e de fácil acesso para registro de atividades com uso de georreferenciamento."

Na primeira hipótese, a qualificação deverá se dar pela lei de Y, por ser o local onde os dados foram coletados na ocasião em que foi estabelecida a relação contratual. Tal lei poderá conferir, ao direito alegado pelo autor da ação, tratamento jurídico distinto daquele conferido pela lei brasileira, quando aplicável a *lex fori* à qualificação.

Na segunda hipótese, por sua vez, haverá de ser considerado o momento em que foi constituída a relação contratual entre as partes[354]: é possível que o proponente tenha sido a empresa, localizada no país Z, sem filiais ou representantes em outros países. Novamente, considerada a *lex causae* para fins de qualificação, poderá conduzir a resultados distintos daqueles advindos da aplicação da *lex fori*.

Tratando-se, portanto, de dever legal, a qualificação será feita pela *lex fori*, entretanto, se for de obrigação contratual, esta poderá ser entre presentes, considerando-se o local em que foi constituída a obrigação, seja ele qual for (no exemplo, Y), ou entre ausentes, considerando-se o local de residência do proponente (no exemplo, Z). Nesses dois últimos casos, será necessária a análise caso a caso para avaliar como o objeto da ação será qualificado.

É possível, portanto, que o estrangeiro ajuíze a demanda perante o Judiciário brasileiro, e que este proceda à qualificação segundo uma lei estrangeira. Em casos de qualificação pela *lex causae*, deverá proceder-se à requalificação da instituição jurídica conforme a lei indicada[355]. Em tais hipóteses, poderá haver ou não coincidência entre as instituições (estruturas) nos ordenamentos.

Importante ressaltar, por fim, que se a obrigação for exequível no Brasil, e a demanda versar sobre questões relativas a formalidades essenciais, segundo a lei brasileira, esta será aplicada nos termos do art. 9º, § 1º, da LINDB[356]. Igualmente, a lei brasileira será aplicada a casos nos quais a parte for aqui domiciliada, e que versarem questões de capacidade, já que a estas aplica-se a lei de domicílio da pessoa, conforme art. 7º, *caput*, da LINDB[357].

---

[354] JUNQUEIRA, Miriam. *Contratos eletrônicos*. Rio de Janeiro: Mauad, 1997, p. 23 "A formação do consenso ocorrerá quando a proposta e a aceitação coincidirem no conteúdo."

[355] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019.

[356] BRASIL. *Decreto-Lei n.º 4.657 de 04 de setembro de 1942*. Lei de Introdução às Normas do Direito Brasileiro (LINDB). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 17 abr. 2020. "Art. 9º. [...] § 1º. Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato. [...]."

[357] Id., ibid. "Art. 7º. A lei do país em que domiciliada a pessoa determina as regras sobre o começo e o fim da personalidade, o nome, a capacidade e os direitos de família."

Nos casos aqui analisados, por outro lado, as demandas versam principalmente sobre direitos de personalidade (enfatizando-se a privacidade); contratos eletrônicos (sejam de consumo ou não); e de responsabilidade civil (ocorrência de danos, sejam considerados no âmbito da responsabilidade contratual ou extracontratual); aplicando-se o art. 9º da LINDB ou a regra geral da CIDIP.

Numa tentativa de delinear as ideias propostas por Gustavo Ferraz de Campos Monaco acerca da qualificação e requalificação no Direito Internacional Privado, anteriormente citadas, é possível chegar à seguinte esquematização[358]:

Quadro 1. Qualificação no Direito Internacional Privado

1º. Observação das normas de qualificação do ordenamento jurídico brasileiro	Possibilidade a): qualificação pela ***lex fori***
	Possibilidade b): qualificação pela ***lex causae***
2º. Aplicação das normas de qualificação	Possibilidade a): em caso de qualificação pela ***lex fori***: prosseguir com o método de DIP
	Possibilidade b): em caso de qualificação pela ***lex causae***: proceder à requalificação da instituição jurídica conforme a lei indicada
3º. Requalificação (ou qualificação-subsunção) pela *lex causae* (se necessário)	Possibilidade a): **coincidência** entre as instituições (estruturas) nos dois ordenamentos: prosseguir com o método de DIP
	Possibilidade b): instituições **distintas**: proceder à **requalificação** conforme a lei indicada e, então, prosseguir com o método de DIP.

Fonte: adaptado de Monaco (2019)[359].

Ainda não é clara, contudo, a forma como as relações digitais devem ser classificadas de acordo com as normas vigentes no Direito brasileiro[360]. Há, também, a

[358] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019.
[359] Id., ibid.
[360] POLIDO, Fabrício Bertini Pasquot; SILVA, Lucas Sávio Oliveira da. Contratos Internacionais eletrônicos e o Direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. *Sequência*. Florianópolis, abr. 2017, n. 75, pp. 157-188, p. 162. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000100157&lng=en&nrm=iso. Acesso em: 17 abr. 2020. "Ainda como observa Draetta (2005, p. 58), todas as normas que têm um 'lugar' como referência acabam por não serem apropriadas à natureza deslocalizada da Internet. Daí a dificuldade em se legislar a respeito de direito eletrônico, bem como a inadequação das normas de conflito tradicionais (e respectivas regras de conexão determinadoras de direito aplicável às obrigações contratuais nas redes digitais). De fato, normas que têm /como referência o lugar da prática do ato ilícito, o lugar de residência, do principal estabelecimento do negócio, ou ainda, normas conflituais de Direito Internacional Privado intimamente relacionadas ao direito dos contratos, tais como as que levam em consideração para indicação do direito aplicável o lugar de conclusão do contrato, a exemplo do art. 9º da Lei de Introdução às Normas do Direito Brasileiro (LINDB), ou mesmo de execução da obrigação, terminam por ter sua aplicação dificultada nos casos em que a internet seja base para as relações jurídicas. Trata-se, na verdade, de um problema de qualificação dada a patente dificuldade, sem a existência de normas apropriadas para tanto, de se caracterizar com exatidão, por exemplo, o lugar de conclusão de um contrato realizado pela internet. A determinação do 'lugar' nas relações travadas em ambientes de internet (portanto 'globais' por natureza) é uma questão de atribuição de efeitos jurídicos. Dessa forma, o que interessa é que existam maneiras seguras de imputar efeitos jurídicos às relações havidas em meio eletrônico."

necessidade de avaliar se a demanda envolve questão contratual ou extracontratual[361]. Caso fique entendida a primeira opção, há de se estabelecer se a qualificação das relações jurídicas entre o usuário e a empresa de tecnologia representa relação de consumo, ou, alternativamente, prestação de serviços[362].

2.2 VIOLAÇÕES DE SEGURANÇA E SANÇÕES APLICADAS

Inicialmente, e considerando a vigência do Regulamento Geral de Proteção de Dados da União Europeia, serão expostas algumas das sanções já aplicadas em decorrência de violações de segurança (roubo ou vazamento de dados, especialmente). Até o momento, menos de 150 multas foram aplicadas no âmbito do RGPD[363], o que equivale a menos de

---

[361] Id., ibid. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000100157& lng= en&nrm=iso. Acesso em: 17 abr. 2020. "Outra característica da internet que tem consequências diretas quando se analisa a contratação por meio eletrônico é a natureza imaterial deste meio. [...] Os contratos eletrônicos, por sua vez, fazem total abstração do suporte em papel. Oferta e aceitação são mensagens transmitidas eletronicamente e, mesmo que possa haver posterior impressão em papel, ainda restaria dúvida quanto à autenticidade do documento. Além do mais, a assinatura, modo confiável de atribuição de autoria, também não pode ser, em meio eletrônico, da mesma maneira como tradicionalmente o foi no mundo físico. Tais questionamentos geram a discussão sobre a necessidade de adoção de regras específicas, as quais venham estabelecer parâmetros para a segurança das partes."

[362] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. *Governança global da internet, conflito de leis e jurisdição*. Instituto de Referência em Internet e Sociedade (IRIS). Belo Horizonte: 2018, pp. 144 e ss. "No direito brasileiro, a relação jurídica de consumo é estabelecida pela composição de fornecedor e consumidor em lados opostos, e tendo como objeto produto ou serviço, conforme se depreende da análise dos arts. 2º e 3º do CDC. [...] A categoria de produto ou serviço é desenvolvida no art. 3º, parágrafos 1º e 2º do CDC com ampla abrangência, considerando todo bem ou atividade fornecida no mercado de consumo, mediante remuneração. Cláudia Lima Marques defende a proteção do consumidor enquanto direito fundamental no ordenamento jurídico brasileiro, nos termos do art. 5º, inc. XXXII, da Constituição Federal. Essa proteção se materializa por intervenção do Estado, no sentido de garantir o equilíbrio entre as partes no contrato. [...] Uma das formas de intervenção do Estado com o objetivo de garantir o equilíbrio contratual é a limitação da autonomia da vontade por meio de norma imperativa e de ordem pública, como o Código de Defesa do Consumidor. Como defendem alguns autores, a consequência dessa abordagem é de que a legislação consumerista compõe-se de normas de aplicação imediata, como espécie de privilégio da lei do foro (*lex fori*). Impede que o consumidor, enquanto parte de comunidade econômica, sofra qualquer diminuição de seus direitos por parte do contratante economicamente mais forte, quando a aplicação da lei estrangeira for manifestamente incompatível: [...]. No entanto, a qualificação das relações enquanto consumeristas é ainda mais questionável no âmbito dos contratos eletrônicos, principalmente no que diz respeito ao objeto ser ou não considerado bem ou serviço."

[363] CAMARGO, Solano de. As sanções da LGPD e o Inferno de Dante. *Revista do Advogado* (AASP), nov. 2019, v. 1, nº 144, pp. 220-232, (s.p.). "Até agora, a maior multa aplicada foi de US$ 228 milhões (183 milhões de libras esterlinas) contra a companhia aérea British Airways, equivalente à 1,5% da receita mundial da companhia em 2017. Até o momento, menos de 150 multas foram aplicadas – menos de 0,25% das violações relatadas, por conta do grande número de procedimentos que devem ser analisados pelas autoridades nacionais dos Estados que compõem a União Europeia. E a maioria dessas multas está na faixa de € 20 mil ou menos. Segundo o relatório DLA Piper, esse quadro deve mudar nos próximos anos, pois as agências regulatórias europeias ainda se encontram sobrecarregadas, havendo um grande estoque de notificações em seus balcões de reclamação. Com isso, pode-se intuir que, no Brasil, haverá um início tímido na aplicação de sanções, até o aculturamento da sociedade ante os novos tempos, tal qual ocorreu com a vigência do Código de Defesa do Consumidor, em 1990. O relatório DLA Piper contabilizou 59.430 notificações de incidentes, com os Países Baixos, a Alemanha e o Reino Unido no topo da lista, com

0,25% das violações relatadas[364], sendo que a maioria dessas multas está na faixa de vinte mil euros ou menos[365]. A maior multa aplicada até o momento ocorreu em 2017, no valor de US$ 228 milhões (183 milhões de libras esterlinas) contra a companhia aérea British Airways, equivalente a 1,5% da receita mundial da companhia[366].

A segunda maior multa foi aplicada à empresa de tecnologia Google: a Comissão Nacional de Informações e Liberdade (CNIL), autoridade francesa de proteção de dados, determinou o pagamento de sanção no valor de 50 milhões de euros com base no RGPD[367]. Na ocasião, entendeu-se que a empresa teria violado os princípios da transparência, da informação e do consentimento.

Outras empresas, como a rede de hotéis Marriott e a empresa de transporte Uber também já foram multadas em decorrência de incidentes de vazamento de dados – a primeira, também no âmbito do RGPD[368], e a segunda, a partir de ação judicial movida nos Estados Unidos, o que resultou em acordo[369].

---

aproximadamente 15.400, 12.600 e 10.600 casos, respectivamente. Os Países Baixos acusaram o maior número de incidentes per capita, com 89,8 impactados para cada grupo de 100.000 pessoas, seguidos pela Irlanda e pela Dinamarca."

[364] DLA Piper GDPR Data Breach Survey: February 2019. Disponível em: https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf. Acesso em: 17 abr. 2020. O relatório contabilizou 59.430 notificações de incidentes com os Países Baixos, a Alemanha e o Reino Unido no topo da lista, com cerca de 15.400, 12.600 e 10.600 casos cada, respectivamente. Os Países Baixos acusaram o maior número de incidentes per capita, com 89,8 impactados para cada grupo de 100.000 pessoas, seguidos pela Irlanda e pela Dinamarca.

[365] PORTUGAL. *Relatório de Atividades da Comissão Nacional de Proteção de Dados, 2017-2018.* Disponível em: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf. Acesso em: 17 abr. 2020. "[...] A CNPD (Comissão Nacional de Protecção de Dados) desenvolve ainda atividade fiscalizadora por todo o território nacional, realizando inspeções, seja no âmbito de queixas ou de participações, seja no contexto de averiguações específicas ou de auditorias mais gerais, por sua iniciativa. [...] A CNPD tem ainda competência para aplicar sanções, quando a prática dos responsáveis pelos tratamentos de dados, públicos ou privados, constituir contraordenação. Em 2017, foram abertos 1.381 processos de contraordenação, e até 24 de maio de 2018, 494 processos da mesma natureza, tendo-se registado um ligeiro aumento em relação ao ano anterior. No que diz respeito ao ano de 2017, destacam-se as queixas que deram origem a cerca de 600 processos. [...]. Em relação à parte de 2018, deram entrada 166 queixas e um total de 328 processos de participação. No quadro desta atividade em 2017, a CNPD aplicou 160 coimas, num valor total de 266 602,39 EUR. No primeiro período de 2018, a CNPD aplicou 50 coimas, num valor aproximado de 80 mil EUR."

[366] REINO UNIDO. Information Comissioner's Office (ICO). *Intention to fine British Airways £183.39m under GDPR for data breach,* 08 jul. 2019. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/. Acesso em: 17 abr. 2020. No Reino Unido, a ICO (*Information Commisioner's Office*) é a entidade responsável pela salvaguarda do RGPD e privacidade dos cidadãos. Por meio deste comunicado foi anunciada a intenção de aplicar multa de 183,39 milhões de libras (cerca de 204,7 milhões de euros) à empresa British Airways, por infrações ao regulamento europeu em decorrência da notificação de um incidente de vazamento de dados em setembro de 2018, envolvendo o direcionamento de tráfego de utilizadores do site da British Airways para um site fraudulento. Assim, em média, 500 mil clientes da British Airways foram afetados pela situação.

[367] GOMES, Helton Simões. Google recebe maior multa já aplicada por violar dados pessoais na Europa. *Uol*, 21 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/21/google-e-multado-na-franca-por-violar-de-dados-pessoais.htm. Acesso em: 06 jan. 2020.

[368] REINO UNIDO. Information Comissioner's Office (ICO). *Statement:* intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 09 jul. 2019. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-

Também no ano de 2018, o Tesco Bank (banco de varejo de rede de supermercados do Reino Unido) foi multado em 16,4 milhões de libras pela *Financial Conduct Authority* (FCA) do Reino Unido, após roubo realizado dois anos antes, de mais de US$ 3 milhões de nove mil contas de clientes do banco[370].

---

marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/. Acesso em: 17 abr. 2020. A autoridade de proteção de dados do Reino Unido multou a rede hoteleira Marriott em US$ 123 milhões (equivalente a quase 500 milhões de reais), por conta de violação de dados que expôs cerca de 383 milhões de hóspedes, a partir do vazamento, em 2014, de banco de dados central com informações de reservas de quartos, descoberto somente em novembro de 2018, afetando aproximadamente 30 milhões de moradores da União Europeia. Sob o regime do RGPD, o ICO tem o direito de multar uma empresa em um valor equivalente a até 4% do seu faturamento anual; a Marriott faturou US$ 3,6 bilhões em 2018, de modo que a multa aplicada representa cerca de 3% da receita global da rede hoteleira.

[369] SOMERVILLE, Heather. Uber to pay $148 million to settle data breach cover-up with U.S. states. *Reuters*, 26 set. 2018. Disponível em: https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ. Acesso em: 17 abr. 2020. A ação judicial em questão tem por objeto vazamento de banco de dados da empresa Uber em outubro de 2016, afetando a privacidade de milhões de usuários do aplicativo; cerca de 50 milhões de passageiros e 7 milhões de motoristas foram prejudicados. A fim de evitar que o vazamento fosse noticiado, a empresa optou por pagar US$ 100 mil (cem mil dólares) aos invasores, descumprindo dever legal de informação de vazamento ou roubo de dados pessoais. Apenas em 2017 o vazamento veio à tona, quando Dara Khosrowshahi, CEO da empresa, relevou o ocorrido, demitindo seu diretor de segurança à época, Joe Sullivan. Por fim, como resultado, foi celebrado acordo entre a empresa Uber e os 50 estados que moveram a ação, equivalente a US$ 148 milhões – o maior valor de acordo envolvendo violação da privacidade nos Estados Unidos até o momento.

[370] SWINHOE, Dan. Os oito maiores vazamentos de dados de 2018. Hacks e roubos de dados custaram um total de quase US$ 280 milhões para empresas. *Computerworld*. Disponível em: https://computerworld.com.br/2018/10/31/os-8-maiores-vazamentos-de-dados-de-2018/. Acesso em: 17 abr. 2020. "[...] **Tesco Bank**: US$ 21 milhões. O Tesco Bank, braço de banco de varejo da rede de supermercados do Reino Unido, foi multado em 16,4 milhões de libras (US$ 21,2 milhões) pela *Financial Conduct Authority* (FCA) do Reino Unido, depois que pouco mais de US$ 3 milhões foram roubados de nove mil contas de clientes em 2016. A FCA acusou o Tesco de 'deficiências' no *design* de seus cartões de débito, controles de crimes financeiros e sua equipe de operação de crimes financeiros. **Anthem**: US$ 16 milhões. A seguradora de saúde norte-americana Anthem sofreu uma violação, em 2015, que afetou 79 milhões de pessoas. A violação incluía nomes, aniversários, números da Previdência Social e identificações médicas. Em outubro, a empresa foi multada em US$ 16 milhões pelas violações do Departamento de Saúde e Serviços Humanos dos Estados Unidos pela *Health Insurance Portability and Accountability Act* (HIPAA). Essa multa foi além dos US$ 115 milhões que a empresa teve que pagar em 2017 para resolver uma ação coletiva relacionada à violação. **University of Texas MD Anderson Cancer Center**: US$ 4,3 milhões. Em junho, um juiz confirmou a decisão de multar a University of Texas MD Anderson Cancer Center em US$ 4,3 milhões por violações do HIPAA. O centro de câncer sofreu três violações de dados entre 2012 e 2013: um caso de roubo de um *laptop* não criptografado da residência de um funcionário e dois USB não criptografados foram perdidos. As informações de saúde de mais de 33.500 pessoas foram perdidas. **Fresenius Medical Care North America**: US$ 3,5 milhões. Em fevereiro, a *Fresenius Medical Care North America* (FMCNA) recebeu US$ 4,3 milhões por conta de cinco infrações em diferentes locais da empresa entre fevereiro e julho de 2012. Uma investigação do Escritório de Direitos Civis concluiu que a FMCNA não havia 'conduzido uma análise precisa e completa dos riscos potenciais e vulnerabilidades à confidencialidade, integridade e disponibilidade de todas as informações de saúde que estava armazenando em suas diferentes entidades'. Essas falhas incluem não impedir o acesso não autorizado a instalações e equipamentos, não criptografar dados de saúde, não governar a remoção de mídia eletrônica que armazena dados de saúde e não ter procedimentos de incidentes de segurança. **Equifax e Facebook**: US$ 650.000. A Equifax e o Facebook podem se considerar sortudos. O Escritório do Comissário de Informações do Reino Unido multou as duas empresas por falhas nos dados sob a Lei de Proteção de Dados pré-GDPR, na qual a multa mais alta possível é de apenas £ 500.000 (aproximadamente US$ 650.000). Sob GDPR, as penalidades poderiam ter sido muito maiores. Em outubro, o Facebook recebeu a multa sobre o escândalo de dados da Cambridge Analytica, enquanto a Equifax recebeu a multa máxima em setembro pela violação de 2017, que permitiu o vazamento de dados de 147 milhões de clientes. [...]."

Se antes do RGPD já havia multas e condenações por conta de vazamentos de dados, na conjectura posterior à sua vigência a tendência é aumentar o número de denúncias e multas. Por outro lado, é possível observar uma preocupação maior por parte das empresas com questões relativas à segurança e privacidade dos dados dos usuários: a transparência quanto ao uso e armazenamento dos dados, assim como na ocorrência de incidentes envolvendo roubo ou vazamento de dados é incontornável na busca pela tutela dos valores discutidos.

Espera-se que tais efeitos prossigam quando a LGPD passar a ser vigente no Brasil, comprovando a valiosa análise das sanções já aplicadas em outros países, assim como dos impactos positivos gerados pela regulamentação. Neste aspecto, cumpre questionar a forma como as sanções previstas na Lei serão de fato aplicadas pelo Judiciário brasileiro, considerando o valor elevado das multas dispostas na norma[371].

[371] ANTUNES, Júlia Caiuby de Azevedo. A previsibilidade nas condenações por danos morais: uma reflexão a partir das decisões do STJ sobre relações de consumo bancárias. *Revista Direito GV*. São Paulo, jun. 2009, v. 5, n. 1, pp. 169-184. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322009000100009&lng=en&nrm=iso. Acesso em: 09 mar. 2020. O artigo traz reflexão sobre o arbitramento de danos morais, com base na jurisprudência do STJ. Muito embora trate especificamente sobre relações de consumo bancária, as observações feitas acerca da tendência de redução do valor das condenações arbitradas pelas instâncias inferiores mostram-se úteis para ilustrar a problemática aqui proposta, a fim de questionar a forma como as multas impostas pela LGPD serão de fato aplicadas pelo Judiciário brasileiro. A respeito destacam-se os seguintes trechos: "No universo pesquisado, o Superior Tribunal de Justiça optou pela redução do *quantum* indenizatório em 74,23% dos processos. Tão elevado percentual de revisão indica que o Superior Tribunal Federal percebe os valores arbitrados nas instâncias anteriores como exorbitantes ou desarrazoados, merecendo, portanto, sua diminuição a patamares considerados como adequados. Uma vez que não existe um cálculo matemático das repercussões negativas da violação, as instâncias inferiores têm liberdade para aferir a quantia devida. A possível ocorrência de exacerbação nas pretensões indenizatórias [...], com a consequente banalização do instituto do dano moral, parece ser a principal preocupação do Superior Tribunal de Justiça ao rever o valor indenizatório. O voto do Min. Sálvio de Figueiredo Teixeira, no julgamento do REsp 265.133, denota claramente tal temor ao afirmar que, 'em face de manifestos e frequentes abusos na fixação do *quantum* indenizatório, no campo da responsabilidade civil, com maior ênfase em se tratando de danos morais, é lícito ao Superior Tribunal de Justiça exercer o respectivo controle'. A Corte Especial parece não acreditar que a proximidade do juiz de primeiro grau com a realidade fática apresentada no processo lhe empresta melhores condições de aferir o valor adequado ao caso concreto. Em 99,17% dos casos em que a Corte interveio para reduzir a condenação, foi sustentado que o valor era excessivo, o que poderia ser entendido como uma visão de que os julgadores das instâncias inferiores não atuaram com a devida prudência e bom senso na tarefa de quantificação da indenização. Ao lado da revisão dos valores em quase 80% dos casos, em regra, para diminuí-los, nota-se que há uma aparente padronização dos valores. [...] A redução do valor indenizatório é sintomática, sendo observada em mais de 70% dos casos levados à apreciação do Superior Tribunal de Justiça. A diminuição tende a ser efetivada sem preciso aclaramento de quais elementos do caso concreto foram decisivos para a interferência excepcional da corte, muitas vezes com a mera indicação de que o 'valor é excessivo'. Nos casos em que houve manutenção do *quantum* determinado pelas instâncias inferiores, aquele já se encontrava em conformidade com o padrão médio dos valores por ela controlados, [...]. A interferência do Superior Tribunal de Justiça no arbitramento do valor condenatório denota a tentativa de conceder valores condenatórios aproximados para situações que cuidam de temas assemelhados, independentemente das circunstâncias de cada caso levado a juízo. Tal constatação leva ao questionamento se, na prática, o Superior Tribunal de Justiça não adotou um tabelamento da quantia condenatória, diferentemente do que ocorre nas instâncias inferiores."

O RGPD, assim como as demais normas que regulam a circulação de dados no ambiente digital, gera um impacto positivo sobre as políticas de privacidade e transparência das empresas. Exemplo disso é a adoção da ideia de *privacy by design* mencionada anteriormente[372], o que demonstra uma preocupação tanto por parte das empresas que já atuam no mercado em termos de *compliance*, quanto das novas empresas e *start ups* que vêm surgindo[373].

Outra conclusão possível a partir da aplicação das sanções mencionadas é o fato de que mesmo em situações nas quais os dados são utilizados de forma distinta daquela finalidade inicialmente apontada, a transparência surge como um valor de extrema relevância, sendo necessário não apenas tomar medidas para prevenir roubos e vazamentos, mas, também, comunicar devidamente os titulares dos dados sobre a ocorrência de episódios do gênero, conhecidos como *data breaches*[374].

---

[372] MOTA, Joana. Proteção de dados desde a concepção e por defeito. Avaliação de impacto e segurança. *In*: CORDEIRO, António Menezes *et al. FinTech II:* novos estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 138-139. "A abordagem baseada no risco encontra também algum grau de criticidade quando se trata de interpretar e concretizar os princípios da proteção de dados desde a conceção e por defeito. Apesar de só agora expressamente consagrados, os mesmos não são, tal como o princípio da responsabilidade, uma inovação do RGPD. Na verdade, estes conceitos foram desenvolvidos pela primeira vez na década de 90 pelo Comitê de Informação e Privacidade de Ontario (*Information and Privacy Comissioner*), tendo-se tornado um referencial internacionalmente reconhecido para a proteção dos dados pessoais. Concretamente, e de acordo com aquela entidade reguladora, para que os objetivos do conceito de privacidade desde a conceção (*privacy by design*) se materializem, é necessário antecipar e prevenir situações que possam ser violadoras da privacidade antes que as mesmas ocorram, sendo necessário que os responsáveis pelo tratamento se certifiquem de que os dados pessoais são protegidos automaticamente em qualquer sistema de informação ou prática comercial, de forma a que se um utilizador nada fizer, a sua privacidade permanece intacta. Acresce que a privacidade desde a conceção deve ser uma soma positiva, o que significa que a abordagem deve procurar acomodar todos os interesses e objetivos legítimos numa estratégia de '*win-win'*. Por outro lado, a privacidade desde a conceção estende-se por todo o ciclo de vida dos dados envolvidos e deve assegurar a todas as partes interessadas que, independentemente da prática comercial ou da tecnologia utilizada, as mesmas são, de facto, feitas de acordo com os objetivos declarados, de forma visível e transparente e sujeitos a verificação. Por último, os interesses das pessoas singulares devem ser colocados no centro das preocupações, quer dos responsáveis pelo tratamento, quer dos arquitetos das soluções tecnológicas, devendo oferecer-se informação apropriada e níveis de privacidade fortes."

[373] Id., ibid., p. 146. "Esta alteração paradigmática trazida pelo RGPD terá reflexos, desde logo, no funcionamento interno das organizações, que devem deixar de ver o cumprimento da lei aplicável como um mero exercício de rotina de *box ticking*, devendo passar a assumir um compromisso sério de gestão dos dados pessoais que estão sob o seu controlo de forma lícita, leal e transparente."

[374] CAMARGO, Solano de. Op, cit., nov. 2019, (s.p.). "As novas diretrizes de proteção de dados, as graves sanções (que podem ser aplicadas concomitantemente pelas autoridades regulatórios de diversos países) e a possibilidade de litígios em massa, parecem confirmar a advertência contida na entrada do inferno na Divina Comédia: aqueles que não se prepararem para os novos tempos – em que a privacidade *online* passou a merecer a tutela jurídica em caráter transnacional – devem deixar toda a esperança para trás."

2.3 CONSENTIMENTO E UTILIZAÇÃO DE *COOKIES*

Conforme apontado anteriormente, o consentimento e o legítimo interesse são centrais à licitude no tratamento de dados. O conceito de "consentimento" pode ser extraído do art. 4º do RGPD, consistindo em "uma manifestação de vontade, livre, específica, informada e explícita pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[375].

Em 1º de outubro de 2019, o Tribunal de Justiça da União Europeia (TJUE) decidiu, no caso C-673/2017[376], que o mero "*click*" autorizando a instalação de *cookies*[377] é insuficiente para provar o consentimento do usuário à coleta de seus dados pessoais[378].

Não foi, porém, determinada com clareza a forma como deve ocorrer o consentimento para a coleta de dados por meio dos *cookies*[379]. Como resultado, por vezes,

---

[375] PINHEIRO, Alexandre Sousa *et al*. (Coords.). *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018, p. 167. "O consentimento é uma condição de legitimidade para o tratamento de dados pessoais especialmente desenvolvida nos arts. 6º e 9º. São, também, relevantes as relações com os princípios previstos no art. 5º, especialmente quando se pretende proceder ao tratamento de dados não incompatíveis com os que presidiram à recolha."

[376] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia (TJUE). *Bundesverband der Verbraucherzentralen und Verbraucherverbände* – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH. Processo C-673/17, 01 out. 2019. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=D5DC4CA415C605B28E70747FD3C5158C?text&docid=218462&pageIndex=0&doclang=PT&mode=req&dir&occ=first&part=1&cid=1458627. Acesso em: 08 mar. 2020. "*Cookies*" são arquivos de Internet que armazenam temporariamente o que o internauta está visitando na rede, podendo armazenar praticamente qualquer tipo de informação, como endereços de e-mail, preferências de pesquisa, cidade de conexão, I.P., dentre outras informações.

[377] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 144. "Os *dados pessoais* – [...] – podem hoje, com efeito, ser recolhidos, transmitidos e tratados com grande facilidade por meios informáticos, com finalidades comerciais, administrativas, políticas ou outras. Elucidativa disso é a amplitude com que são actualmente utilizados os chamados 'testemunhos de conexão' (*cookies*) e dispositivos análogos, amiúde instalados nos terminais dos utentes das redes electrônicas sem o consentimento prévio destes, com o intuito, nomeadamente, de obter, transmitir e armazenar informação relativa à utilização de um terminal de computador, e até informação [...] nele registrada, que permita traçar o 'perfil' daqueles sujeitos enquanto cidadãos ou consumidores."

[378] CAMARGO, Solano de. Op. cit., nov. 2019. "Como exemplo dos novos tempos, após a promulgação da GDPR e posteriormente da LGPD, os usuários passaram a ter que decidir, a todo momento, se autorizaram os sites a instalar os chamados *cookies*. *Cookies*, por sua vez, são pequenos arquivos criados pelos sites visitados e que são salvos no computador ou no *smartphone* do usuário, por meio do navegador. Esses arquivos contêm informações que servem para identificar o visitante, tanto para personalizar a página de acordo com o perfil do usuário como para facilitar o transporte de dados entre as páginas de um mesmo site. Ocorre que, em 1º de outubro de 2019, o Tribunal de Justiça da União Europeia (TJUE) decidiu, no caso C-673/2017, que o mero click autorizando a instalação de *cookies* demonstrou ser um mecanismo insuficiente para provar o consentimento do usuário à coleta de seus dados pessoais. Os juízes do TJUE não propuseram alternativas às caixas de texto, tais como a necessidade de rolagem completa da página da web ou outro meio qualquer, de forma que a questão permanece em aberto. Com isso, não há uma resposta adequada sobre o funcionamento dos *cookies*, que movimentam um sem número de fluxos de dados em quase 2 bilhões de páginas de internet, em todo o mundo."

[379] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. Caderno Especial.

o tratamento de dados é feito com base no legítimo interesse, em detrimento do consentimento expresso, muito embora, em tese, este último devesse representar a regra[380].

A definição de consentimento trazida pelo RGPD é composta por três elementos: uma manifestação de vontade, livre, específica, informada e explícita, por meio da qual o titular de dados aceita, mediante declaração ou ato positivo inequívoco, que os dados que lhe digam respeito sejam objeto de tratamento. O Regulamento cala, contudo, sobre as formas pelas quais o consentimento seria considerado válido, e consonante tais requisitos[381].

É possível questionar se o consentimento dado pelos usuários da Internet é consciente, e se de fato implicaria uma restrição no uso dos dados[382]. Como consequência, o consentimento é tido como ficcional, envolvendo uma falsa ideia de controle sobre os dados[383]. É preciso entender o consentimento como uma das etapas necessárias à

São Paulo: Ed. RT, dez. 2018, v. 998, pp. 99-128, p. 109. "[...] os *cookies* [...], uma vez enviados por websites e armazenados nos computadores dos usuários a partir do navegador utilizado, funcionam como identificadores eletrônicos. Esses arquivos são notadamente empregados com o propósito de monitorar hábitos de navegação dos usuários, ou proporcionar-lhes uma experiência personalizada de navegação no sítio eletrônico."

[380] PINHEIRO, Alexandre Sousa *et al.* (Coords.). Op. cit., 2018, p. 172. "Relativamente a tratamentos de *big data analytics* e à exigência do consentimento nos termos em que o RGPD o prevê, já se procedeu à crítica de que o novo regime "não condiz com a realidade da *big data*". São conhecidas as dificuldades de articular esta espécie de tratamentos massivos, provenientes habitualmente de informação contida na Internet, com as regras do consentimento, com o direito de informação e com a definição de finalidades. Estamos em crer que a realização de tratamentos extensos de *big data* completamente à margem da autodeterminação informacional contribuiu para a alteração do regime jurídico do consentimento no RGPD."

[381] CORDEIRO, A. Barreto Menezes. O consentimento do titular dos dados no RGPD. *In*: CORDEIRO, António Menezes *et al. FinTech II:* novos estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 56-57. "O dever de consentimento é acompanhado, naturalmente, pelo dever de provar o cumprimento de todas as exigências formais e substantivas das quais depende um válido e legítimo consentimento. [...] Quanto mais informal for a forma pela qual o consentimento tiver sido manifestado, mais difícil será, naturalmente, a sua demonstração. O RGPD deixa ao critério do responsável os meios como este utiliza para demonstrar a prática do consentimento. A prova pode, por princípio, ser feita através dos vários mecanismos disponibilizados no Estado-Membro em que a questão se suscita."

[382] Id., ibid., pp. 35-36. "Koops, sublinhando não ser o consentimento o meio mais adequado de legitimação de tratamento de dados, recorre a argumentos igualmente empíricos: a maioria das pessoas limita-se a consentir sem o fazer conscientemente, quer por falta de paciência, porque os meios de avaliação são muito pesados e complexos. Estes pontos voltam a ser explorados por Solove, para quem os titulares não têm capacidade para avaliar o que é vantajoso ou desvantajoso nem o alcance exato das consequências associadas ao consentimento. Os estudos comportamentais e econômicos disponíveis sobre a realidade da Internet são inequívocos: a maioria das pessoas não lê as condições *online*, não tem capacidade ou conhecimentos para compreender o que lê e, se todos os utilizadores o decidissem fazer, os custos económicos seriam elevadíssimos."

[383] Id., ibid., p. 35. "Spiros Simitis, um dos mais reconhecidos autores do Direito dos Dados Pessoais, há muito que descreve o consentimento como uma ficção: o reconhecimento deste direito ao consentimento traduz uma falsa ideia de controle na esfera jurídica do titular – daí a ideia de ficção. Pouco importa, prossegue Simitis, que o titular consinta formalmente, quando, na esmagadora maioria das vezes, (i) não tem hipótese de não o fazer sem incorrer em pesados riscos – os dados são pedidos por um superior hierárquico ou por um sujeito que detenha uma enorme ascendência, p.ex.: área da saúde; ou (ii) o consentimento é necessário para aceder a bens e serviços indispensáveis – emprego, energia, comunicação, contas bancárias, etc. Simitis conclui a sua análise afirmando que, distintamente do que o legislador parece considerar, a

legitimação do tratamento de dados (ou uma das suas bases), o qual deve ser associado às demais medidas previstas no RGPD a fim de garantir a licitude do tratamento.

A questão, portanto, permanece em aberto, inexistindo resposta adequada sobre o funcionamento dos *cookies* que movimentam um enorme fluxo de dados em páginas de Internet por todo o mundo. Se, por um lado, o RGPD condiciona a coleta dos dados ao consentimento válido do titular, por outro silencia quanto à forma de obtenção de tal consentimento, dificultando o cumprimento do Regulamento pelas empresas.

Parece ser necessária certa evolução do Direito Material para que seja possível regulamentar de forma mais clara e completa o ambiente digital, inclusive a utilização de *cookies*. Resta evidente que a instalação não autorizada de *cookies* pode acarretar violação ao direito à privacidade do usuário da Internet, cujos dados pessoais estão sendo coletados e tratados sem o devido consentimento.

A mesma crítica pode ser feita à LGPD: se, por um lado, a Lei prevê a necessidade de consentimento como base para o tratamento de dados, por outro poderia ter indicado mais precisamente requisitos para considerar válido tal consentimento, principalmente quando se tratar de contratos automáticos, os quais serão abordados mais cuidadosamente no tópico que segue.

2.4 CONTRATOS ELETRÔNICOS

Contratos são celebrados constantemente no meio digital, de forma global e massificada, e se diferenciam dos contratos entre ausentes tradicionalmente conhecidos[384]. Sempre que produtos ou serviços são adquiridos por meio da Internet, ou produtos são licenciados, por exemplo, há um **contrato eletrônico**[385] estabelecendo os elementos essenciais àquela relação[386].

---

imposição do consentimento não restringe o uso dos dados pessoais: pelo contrário: representa uma chave para um acesso virtualmente ilimitado a um sem fim de informações."

[384] MELO, Milena Barbosa de; LUCENA, Elis Formina; TEIXEIRA, Ana Luiza Figueiredo Quirino. Contratos eletrônicos internacionais: uma análise sobre a lei aplicável e competência. *Revista Dat@venia*, jan./abr. 2015, v. 7, n. 1, pp. 70-96, p. 91: "[...] não podendo a justiça brasileira deixar de apreciar uma situação jurídica celebrada por meio da Internet, a doutrina majoritária se utiliza da analogia com fulcro nos artigos 425 e 434 do Código Civil, que vêm enquadrando os contratos eletrônicos como atípicos, por não estarem inseridos no rol de classificação de contratos típicos, considerando quanto à formação deste contrato celebrado entre ausentes, desde que a aceitação seja expedida."

[385] MARANHÃO, Juliano Souza de Albuquerque. Op. cit., 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 18 abr. 2020. "Outra área promissora é a pesquisa sobre *smart contracts*. Há uma série de softwares para a gestão e execução automática de contratos. Normalmente, aplicam contratos simples, traduzidos pelo programador por uma série de instruções procedimentais. Hoje, há interesse em ligar *smart contracts* a tecnologias de

A formação da vontade na **contratação eletrônica** baseia-se na transmissão das declarações mediante recurso a meio eletrônico. Não há, contudo, grandes desvios às regras gerais de formação do negócio jurídico, mas tão somente uma adaptação ao meio em que as declarações passaram a ser emitidas: o ambiente digital[387].

De fato, a celebração de **contratos entre ausentes** já era conhecida pelo Direito mesmo antes da Internet[388]: por exemplo, por meio da troca de cartas era possível identificar precisamente o momento da formação do contrato, a partir da apresentação e aceitação da proposta final. Os contratos eletrônicos, contudo, permitem declarações negociais entre ausentes no espaço – embora presentes no tempo – suscitando questões sobre validade, formação, eficácia[389], autonomia da vontade, competência e lei aplicável[390].

---

blockchain. O desafio para IA&Direito nesse campo está em criar ferramentas que não se limitem a instruções procedimentais, mas sejam capazes de entender contratos cada vez mais complexos e inferir as posições individuais das partes a serem executadas."

[386] CUNHA JÚNIOR, Eurípedes Brito. Os contratos eletrônicos e o Novo Código Civil. *Revista CEJ*. Brasília, out./dez. 2002, n. 19, pp. 62-77, p. 67: "Mostra-se importante a classificação dos contratos eletrônicos porque, a depender do respectivo enquadramento, ter-se-á respondido acerca: a) do local de formação contratual para definição da legislação aplicável ao contrato objeto de exame e, a depender da situação específica, do foro competente para processar e julgar feitos que cuidem sobre as controvérsias entre as partes, que decorram da inexecução contratual, etc.; b) do momento da formação contratual, instante em que passa a existir a relação jurídica, obrigações são constituídas, passam a ser contados os prazos prescricionais e decadenciais. Os contratos eletrônicos classificam-se quanto: ao grau de eletronização; à natureza da relação tutelada; ao grau de interação homem/máquina; à simultaneidade proposta/aceitação; e à subforma."

[387] ALVES, Hugo Ramos. Smart contracts: entre a tradição e a inovação. *In*: CORDEIRO, António Menezes *et al*. *FinTech II:* novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019, pp. 191-192. "Como conclusão provisória, temos que, neste particular, a contratação eletrônica não concita particulares desvios às regras gerais de formação do negócio jurídico: apenas houve lugar a uma adaptação destes ao meio em que as declarações de vontade são emitidas, pese embora o contrato telemático tenha sido erigido a nova categoria negocial. Em rigor, a contratação através de redes de comunicação já era conhecida, motivo pelo qual tais asserções podem ser consideradas apressadas. A contratação eletrônica concitou apenas aspectos específicos relativamente à contratação com consumidores, traduzidos na imposição de deveres específicos ao prestador de serviços em rede [...]. Apesar de a Internet ter sido considerada a terceira revolução industrial, as principais questões suscitadas pelo comércio eletrônico em sede de contratação eletrônica foram devidamente enquadradas pela dogmática tradicional, que apenas se adaptou ao meio em que o contrato é celebrado."

[388] CUNHA JÚNIOR, Eurípedes Brito. Op. cit., out./dez. 2002, pp. 62-77. "A definição do momento e do local de constituição do contrato têm relevância para o Direito, na medida em que são determinantes para a verificação da existência da relação jurídica, das obrigações constituídas, dos prazos prescricionais e decadenciais, da legislação aplicável e do foro competente para processar e julgar eventuais feitos entre as partes. Quando entre presentes, por dedução lógica, o contrato se forma no local em que se encontram os contratantes. Já em relação ao momento da formação, este ocorre no instante em que se dá a aceitação, ou seja, quando o oblato aceita a proposta a ele dirigida. [...] Quando entre ausentes, o contrato se forma no local onde foi proposto (art. 435 do novo Código Civil, 1.087 do antigo). A norma guarda pertinência com os preceitos da Lei de Introdução ao Código Civil, que no *caput* do art. 9º consigna que regerá as obrigações a lei do país em que se constituírem e, no § 2º do mesmo dispositivo que a obrigação resultante do contrato reputa-se constituída no lugar em que residir o proponente."

[389] RAMOS, Victor de Moraes. A validade dos contratos celebrados pela internet (contratos eletrônicos). *Revista de Direito UNIFACS*, 2009, n. 105, ISSN 1808-4435. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/539. Acesso em: 07 jan. 2020. "Em que desde logo, pode-se afirmar que em relação à formação, validade e eficácia dos contratos, as regras e normas que regem a teoria geral também

Neste estudo será adotada uma divisão entre os contratos eletrônicos[391], considerando, principalmente, as partes envolvidas nas declarações negociais[392]: assim, os

---

dão embasamento aos contratos eletrônicos. Em uma concepção simplista, contrato eletrônico pode ser conceituado como negócio jurídico que é fonte de obrigação, em que as partes criam vínculos recíprocos, mediante o uso da comunicação em rede, criando, modificando, ou extinguindo direitos. [...] Como visto anteriormente, os contratos eletrônicos apresentam algumas características que são comuns a todos os contratos desta espécie, tais quais a liberdade de uso, a escassa legislação, a flexibilização dos conceitos de tempo e de espaço e também a dispensabilidade, em regra, de documentos físicos, escritos em papel. Porém, alguns contratos apresentam características peculiares, em que é possível classificar os contratos eletrônicos em três espécies: intersistêmicos, interpessoais e interativos. [...] Assim, como exemplo, podem ser objetos de um contrato eletrônico desde produtos e serviços comuns, adquiridos comumente em qualquer estabelecimento físico, como eletrodomésticos, livros, carros, produtos em geral. Até bens e serviços incorpóreos, como informações, o acesso a determinados *sites*, *softwares*, serviços de turismo, serviços financeiros, serviços profissionais, dentre muitos outros. Curioso é como podem ser utilizados determinados serviços através do meio eletrônico, que podem ocorrer das seguintes maneiras: com o serviço de correspondência eletrônica (envio de *e-mails*); hospedagem de informações (em *homepages*, *blogs*); transferências de arquivos (ou seja, *downloads* de textos, fotos, jogos etc.); dentre outras formas."

[390] MELO, Milena Barbosa de; LUCENA, Elis Formina; TEIXEIRA; Ana Luiza Figueiredo Quirino. Op. cit., jan./abr. 2015, v. 7, n. 1, pp. 70-96, p. 82. "[...] essa possibilidade de realizar contratos eletrônicos entre partes em países distintos põe em discussão a clássica noção de territorialidade, já que ao ser realizado um contrato eletrônico além das fronteiras de um estado, existirá o contato com mais de um ordenamento jurídico, suscitando conflitos de lei, originando questionamentos acerca da lei de qual país será aplicado em caso de conflitos, bem como a escolha do tribunal competente para julgar tais casos."

[391] CUNHA JÚNIOR, Eurípedes Brito. Op. cit., out./dez. 2002, pp. 62-77, p. 71. "Essa classificação foi proposta por Mariza Delapieve Rossi e adotada por Érica Brandini Barbagalo. Outros autores propuseram classificações assemelhadas às presentes [...]. De acordo com tal classificação, os contratos podem ser interpessoais, interativos ou intersistêmicos."

[392] BARBAGALO, Érica Brandini; DE MATTIA, Fábio Maria. Contratos eletrônicos: contratos formados por meio de redes de computadores peculiaridades jurídicas da formação do vínculo. Universidade de São Paulo, São Paulo, 2000. Neste aspecto mostra-se esclarecedora a distinção feita no texto entre contratos eletrônicos *intersistêmicos*, contratos eletrônicos *interpessoais* (simultâneos ou não), e contratos eletrônicos *interativos*: "A especificidade dos contratos eletrônicos deriva da utilização das redes de computadores para sua formação, que pode dar-se de modos distintos, permitindo a classificação dos contratos eletrônicos em três categorias: contratos eletrônicos intersistêmicos, formados através da interação entre dois sistemas computacionais, programados para comunicação entre si; contratos eletrônicos interpessoais, caracterizados pela existência de pessoas em cada extremo da relação, admitindo duas subcategorias: contrato eletrônico interpessoal simultâneo e contrato eletrônico interpessoal não simultâneo, diferenciando-se estas subcategorias quanto à existência de lapso temporal entre a emanação da declaração de vontade e a percepção desta pela outra parte; e, por fim, contratos eletrônicos interativos, que se caracterizam pela interação entre uma pessoa e um sistema computacional de processamento de dados. O exemplo mais conhecido desta última categoria de contrato eletrônico são os contratos celebrados através de websites que contenham em suas páginas propostas ou convites a fazer propostas. [...], verificamos que as declarações de vontade expressas por meios eletrônicos são válidas, acolhidas pelo Código Civil, têm como regra a forma livre para declaração de vontade, excetuando-se esta regra por determinação expressa de lei, bem como dispõe que se atenda mais à intenção contida na declaração de vontade que ao sentido literal de sua expressão. No que tange ao local de formação dos contratos eletrônicos, aplica-se a regra constante do art. 1.087 do Código Civil quando ambas as partes residirem no território nacional, ao passo que, se as partes - ou uma delas – tiver residência em outro país, a regra contida na Lei de Introdução ao Código Civil, artigo 9º, parágrafo 2º, é a aplicável. Ambos os dispositivos consideram formado o contrato no local onde for feita a proposta. Resguarda-se, todavia, a autonomia da vontade na escolha da lei de regência do contrato, desde que respeitados os limites do âmbito das leis imperativas. Para os contratos eletrônicos celebrados através de websites, sugerimos uma interpretação diferenciada do artigo 9º, parágrafo 2º, da Lei de Introdução ao Código Civil, aplicável àqueles "web sites" cujos titulares, embora residentes no estrangeiro, claramente direcionem suas atividades ao mercado de uma localidade específica, demonstrando a intenção de ali exercerem suas atividades de forma constante, portanto sujeitando-se à legislação desta localidade. Quanto ao momento de formação, nos contratos eletrônicos intersistêmicos, esse momento estará regulado no contrato prévio firmado entre as partes. No que diz respeito aos contratos eletrônicos interpessoais simultâneos, o momento de formação rege-se pelos mesmos princípios aplicáveis aos contratos firmados entre presentes, tendo-se por celebrado o

contratos eletrônicos poderão ser **automatizados** ou não. No primeiro caso estão compreendidos tanto os contratos **intersistêmicos** (dos quais participam dois sistemas de computador)[393] quanto os contratos **interativos** (nos quais há um sistema e um ser humano envolvidos diretamente).

Enquanto alguns contratos, mesmo que celebrados eletronicamente, assumem a forma tradicional, outros consistem em termos e condições previamente elaborados, resultando em contratações automatizadas[394], podendo ocorrer entre dois sistemas, ou entre um ser humano e um sistema, conforme apontado anteriormente. São, a cabo, termos e condições aceitos pelo cliente[395], os quais podem ser considerados contratos de adesão por não permitirem a alteração das cláusulas ali contidas[396].

Ainda no caso da contratação automatizada, verificam-se situações nas quais a contratação é celebrada exclusivamente por meio de computadores (contratos intersistêmicos, conforme mencionado anteriormente): há, em tais casos, a intervenção por parte de máquinas ou sistemas na fase de emissão da declaração de vontade e na fase de

---

contrato no momento em que a aceitação é emitida. Já aos contratos eletrônicos interpessoais não simultâneos, aplicam-se, por analogia, os preceitos do artigo 1.086 do Código Civil, tendo-se por celebrado o contrato no momento em que a aceitação é enviada ao proponente. Finalmente, no tocante aos contratos eletrônicos interativos, em existindo uma proposta que possa ser acessada pela outra parte, considerar-se-á celebrado o contrato no momento em que o oblato expedir a aceitação, valendo as regras aplicáveis aos contratos firmados entre ausentes."

[393] RAMOS, Victor de Moraes. Op. cit., 2009. Disponível em: https://revistas.unifacs.br/index.php/ redu/ article/view/539. Acesso em: 12 mar. 2020. "Nos contratos eletrônicos intersistêmicos, a Internet é utilizada apenas para ratificar e executar o que as partes já estipularam previamente, geralmente em contratos escritos. Assim, o computador não estará interferindo na formação das vontades dos contratantes [...]. Esta forma de contratação é inerente às pessoas físicas e, geralmente, utilizadas para estabelecer relações comerciais de atacado."

[394] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 142. "Termos de uso são geralmente tratados como contratos no Brasil. É necessário analisar se os termos de uso possuem, de fato, validade contratual segundo o ordenamento jurídico brasileiro. No campo do Direito Civil, os contratos estão inclusos na categoria de negócios jurídicos que, segundo Caio Mário da Silva Pereira, são 'declarações de vontade destinadas à produção de efeitos jurídicos queridos pelo agente'. Essa definição é essencial para que os termos de uso sejam considerados negócios jurídicos, já que o usuário deve assentir (declarar sua vontade) para que possa utilizar um serviço de Internet, que produz efeitos previstos no contrato pelo agente (usuário). Definidos os termos de uso como negócios jurídicos, eles apresentam alguns requisitos para que sejam considerados válidos. De acordo com Código Civil brasileiro de 2002, negócios jurídicos apresentam requisitos de validade de ordem subjetiva (capacidade) e objetiva (objeto e forma): capacidade dos agentes, objeto lícito, possível, determinado ou determinável; e forma prescrita ou não defesa em lei (art. 104)."

[395] Id., ibid., pp. 143. "Como esclarecem as próprias empresas quanto à utilização de um serviço de internet, os termos de uso devem ser entendidos como documentos, o que lhes dá validade de acordo com Código Civil brasileiro. Portanto, analisando-se exclusivamente os requisitos de validade de um negócio jurídico de acordo com o direito civil brasileiro, os termos de uso devem ser considerados válidos. Outro poderia ser o resultado se os termos de uso são analisados segundo o direito estrangeiro indicado aplicável (e.g. os termos de uso adotados pela Amazon e Ebay), [...]."

[396] Importante ressaltar que havendo qualquer grau de individualização na elaboração dos termos, condições ou cláusulas, isto a princípio afastaria o caráter de contrato de adesão.

sua transmissão[397], sem que um ser humano participe diretamente. Mesmo em tais casos, em que a declaração de vontade é emitida por uma máquina[398], não é possível afastar ou desconsiderar o elemento volitivo (vontade das partes contratantes) que surge no momento em que há programação para emissão de declarações negociais[399].

Seja um contrato eletrônico intersistêmico, celebrado exclusivamente entre dois sistemas, ou um contrato eletrônico interativo, no qual há um sistema e um ser humano como partes na contratação, o elemento volitivo permanece presente, já que o sistema está, em ambos os casos, meramente reproduzindo declarações negociais para as quais foi programado.

Por fim, ainda no âmbito dos contratos eletrônicos automatizados, cumpre esclarecer o conceito de "*Smart contracts*", ou "**contratos inteligentes**"[400], os quais envolvem a "tradução informática" dos contratos, a partir da utilização de recursos como a criptografia e a *blockchain*[401], a fim de garantir a observação de postulados básicos, ao

---

[397] ALVES, Hugo Ramos. Op. cit., 2019, pp. 192-194. "Estamos perante situações em que existe uma interposição de uma máquina, quer na emissão da declaração, quer na respectiva transmissão, nada obstando a que, quer do lado do oferente, quer do lado do aderente, sejam máquinas a produzir e transmitir as declarações negociais. Mais concretamente, existe uma automatização, *i.e.*, recorre-se a um processo técnico, de modo a dispensar a interação humana. Estamos, pois, perante uma situação distinta da contratação electrônica [...], em virtude de esta ainda poder ser reconduzível diretamente a pessoas, enquanto na contratação automatizada tal vontade depende da programação. [...] Por ora, importa referir que, conquanto não seja, diretamente, uma pessoa a emitir uma declaração negocial, esta não pode deixar de lhe ser imputável: a vontade negocial é expressa através da programação da máquina, a qual é preparada para emitir declarações negociais. O que equivale dizer que a declaração emitida pela máquina tem um autor: o programador, funcionando o autômato como uma *longa manus* da vontade humana."

[398] MARANHÃO, Juliano Souza de Albuquerque. Op. cit., 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 18 abr. 2020. "No âmbito do Direito Contratual, deve-se refletir sobre como lidar com o fato de que sistemas de IA podem participar da negociação, formação e execução de contratos. Para todas essas etapas, o Direito Civil baseia-se em conceitos que pressupõem intencionalidade das partes: expectativas, crenças, vontades, objetivos, boa-fé, etc. Como aplicar o Direito Contratual a negócios firmados por agentes autônomos sem atribuir-lhes intencionalidade? Devemos entender que agentes autônomos têm intenções? Ou devemos reconstruir o Direito Civil sem o conceito de intencionalidade?"

[399] CUNHA JÚNIOR, Eurípedes Brito. Op. cit., out./dez. 2002, pp. 62-77, p. 72. Observe-se que mesmo quando operados por máquinas, os contratos refletem a vontade do responsável pela programação: "Dizem-se 'intersistêmicos' os contratos operados entre máquina e máquina, em que os empresários programam previamente suas máquinas, de modo a executar o que foi antes avençado."

[400] ALVES, Hugo Ramos. Op. cit., 2019, p. 205. "Nesta sede, assentaremos na definição de *smart contract* como um acordo, vertido em formato digital, autoexecutável e autoimplementável na *blockchain*. Desta definição avulta o elemento digital: o *smart contract* carece de programação. [...] Por si só, o *smart contract* não é um contrato: depende do contexto em que o código é executado, carecendo a vinculatividade deste de um acordo prévio entre as partes."

[401] Id., ibid., p. 201. "Em termos práticos, a *blockchain* é um banco de dados distribuído. Mais concretamente, uma forma específica de armazenar dados, como, por exemplo dados de transações ou pagamentos. Estes dados são escritos num "bloco". Uma vez alcançada a capacidade do bloco, os dados são escritos no bloco seguinte e assim sucessivamente. O novo bloco reporta-se ao anterior, de modo que uma cadeia de blocos seja criada, ou seja, a *blockchain*."

mesmo tempo em que são obtidos ganhos de eficiência com a tradução de contratos em algoritmos informáticos[402].

A ideia dos contratos inteligentes é permitir o cumprimento ou a execução de um negócio jurídico sem a necessidade de negociação direta entre as pessoas envolvidas. São, portanto, **contratos digitais** que utilizam código de programação para a sua execução, dispensando a impressão de um contrato em linguagem jurídica.

A relação entre contratante e contratado é estabelecida por meio de um código – inclusive as disposições relativas ao possível descumprimento do instrumento[403]. O uso de tecnologias como criptografia, assinaturas ou certificados digitais e *blockchain* agrega segurança jurídica ao contrato inteligente, pois impede a sua alteração, reduzindo riscos de fraude. Trata-se, portanto, de uma forma segura de celebrar contratos eletronicamente, mesmo de forma automatizada.

Já no caso dos contratos eletrônicos **não automatizados**, esses são considerados contratos **interpessoais**, ou seja, celebrados entre dois seres humanos, pelo meio digital – podendo ser simultâneos ou não[404].

Além da questão do caráter massificado dos contratos eletrônicos, os instrumentos celebrados no ambiente digital por vezes reúnem partes localizadas em territórios de países

---

[402] Id., ibid., pp. 194-196. "É comum apontar Nick Szabo como o teorizador do *smart contract*. [...] o jurista norte-americano sustenta que o recurso a algoritmos é suscetível de ser traduzido informaticamente. Partindo do pressuposto de que um contrato obedece a postulados próprios e de que a respectiva "tradução" informática os exponencia, Szabo apresenta um conjunto de postulados essenciais da figura. [...] Para Szabo, os objetivos primaciais da construção de clausulados contratuais podem ser exponenciados pelo recurso à criptografia e a chaves eletrônicas, pois não só seriam observados os postulados referidos supra, como, adicionalmente, seriam obtidos ganhos de eficiência em virtude de o recurso a processos informáticos permitir uma aceleração da execução dos contratos devidamente traduzidos em algoritmos informáticos. [...] Sem prejuízo da manifesta incipiência terminológica, *in radice*, no atual contexto o *smart contract* apenas será um contrato na eventualidade de cumprir os requisitos gerais da formação e conclusão do negócio jurídico, salvo, naturalmente, a eventual adoção de legislação específica. Em qualquer caso, o próprio adjetivo "inteligente" é enganador, pois, em rigor, a figura assenta na execução de uma ordem programada."

[403] GONÇALVES, Pedro Vilela Resende; CAMARGOS, Rafael Coutinho. Blockchain, Smart Contracts e "Judge as a Service" no Direito Brasileiro. II Seminário Governança das Redes e o Marco Civil da Internet: globalização, tecnologias e conectividade. *Anais...* Belo Horizonte: Instituto de Referência em Internet e Sociedade-IRIS, 2017, pp. 207-212. Os contratos inteligentes dispensam a existência de um intermediário para negociações, sendo um exemplo as transações ou compras realizadas *on-line*, nos quais há redução dos riscos e custos das operações da empresa, diante de sua rapidez, segurança, autonomia e integração. Também são utilizadas ferramentas de criptografia, restringindo o acesso a pessoas devidamente autorizadas.

[404] RAMOS, Victor de Moraes. Op. cit., 2009. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/539. Acesso em: 12 mar. 2020. "Contratos eletrônicos interpessoais seriam aqueles firmados em decorrência da interação de duas pessoas, simultaneamente ou não, através da internet. Pode-se exemplificar tal classificação, nos casos de contratos firmados através de troca de e-mails, de videoconferência ou em programas de mensagem instantânea, ou ainda, no caso de leilão virtual. A principal característica desta forma contratual é a necessidade de uma manifestação ativa das partes, ou seja, é necessária a ação humana tanto para enviar uma proposta através de mensagem, quanto para emitir mensagem de resposta de aceitação. Assim, [...], as duas manifestações volitivas essenciais ao preenchimento dos requisitos de existência da relação jurídica ocorrem, cada uma ao seu turno, no momento em que seus autores transmitem a mensagem eletrônica."

diferentes. Assim, um brasileiro poderá celebrar um contrato enquanto estiver em Portugal, com uma empresa com sede na Espanha, registro na França e servidores em Malta. A relação contratual estabelecida entre as partes estará, em tais casos, permeada por elementos transnacionais, revelando-se plurilocalizada e atraindo, consequentemente, a aplicação de normas conflituais[405].

Novamente, a validade do consentimento e a sua forma de obtenção surgem como questões relevantes, principalmente quando se trata de uma relação de consumo, ou qualquer relação na qual uma das partes é hipossuficiente. Se, por um lado, a Internet otimiza e dinamiza o encontro entre oferta e procura, por outro há um aumento dos riscos e incertezas envolvidos nas transações, sejam de compra e venda, ou de prestação de serviços[406], podendo, inclusive, envolver questões de capacidade, que é a dificuldade em verificar se a parte contratante é efetivamente apta e capaz para o ato.

Observa-se nos contratos eletrônicos (automatizados ou não) o espelhamento dos requisitos e dos elementos que constituem a declaração de vontade nos demais contratos,

[405] MELO, Milena Barbosa de; LUCENA, Elis Formina; TEIXEIRA, Ana Luiza Figueiredo Quirino. Op. cit., jan./abr. 2015, pp. 70-96, p. 80. "[...] os contratos com caráter meramente automatizados, [...] que suscitam maior discussão jurídica pelo afastamento da intervenção humana; além do que, se celebrados no âmbito internacional, trazem grandes conflitos, pois nem sempre se consegue estabelecer o local, o momento da celebração do contrato, assim como a identificação das partes, criando imensas dificuldades quanto à Lei aplicável e ao Tribunal Competente. Em Portugal, por exemplo, os contratos eletrônicos estão regulamentados no art. 9º da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, que foi transposta para o ordenamento nacional pelo Decreto Lei de Portugal 7/2004, onde se encontram dispostos da seguinte forma: 'Os Estados-Membros assegurarão que os seus sistemas legais permitam a celebração de contratos por meios eletrônicos. Os Estados-Membros assegurarão, nomeadamente, que o regime jurídico aplicável ao processo contratual não crie obstáculos à utilização de contratos celebrados por meios eletrônicos, nem tenha por resultado a privação de efeitos legais ou de validade desses contratos, pelo fato de serem celebrados por meios eletrônicos'."

[406] OLIVEIRA, Elsa Dias. Op. cit., 2002, p. 29 "O acesso à rede permite uma rápida e ampla divulgação de bens ou serviços que se pretendem vender, a custos muito baixos, o que leva a que entidades que, através de outro meio de comunicação, não teriam possibilidade de o fazer, aqui o façam. Em consequência, os consumidores têm conhecimento de serviços e bens de consumo provenientes de todos os países do mundo. Este conhecimento não aparece, por regra, de uma forma isenta, antes é transmitido pela publicidade, nem sempre muito honesta, com os inerentes atrativos e métodos de sedução ao consumidor e, assim, as necessidades fictícias têm grande probabilidades de aumentar. As cores, os sons, os recursos áudio-visuais, permitem difundir mensagens publicitárias especialmente atraentes, as quais, associadas ao efeito de surpresa, a técnicas de condicionamento da vontade, à pressão para a fidelização e cadastração dos clientes, influenciam o consumidor para adquirir no sentido de fornecer os seus dados pessoais e, inclusive, uma lista das suas preferências. Importa, ainda, sublinhar que a maioria dos consumidores desconhece as potencialidades técnicas oferecidas pelos meios informáticos, não tendo sequer noção da utilização que deles pode fazer o fornecedor: assim, poderá ficar admirado se, ao entrar num sítio da Internet que já antes havia visitado, e ao qual tinha fornecido alguns dos seus dados, for surpreendido por uma mensagem eletrônica em que são indicados alguns dos bens que estão de acordo com as suas preferências. Acresce, ainda, que os sítios a que o consumidor acede não expressam necessariamente a sua mensagem numa língua que aquele domina, o que dificulta inequivocamente a compreensão das informações que lhe são dadas. Além disso, a celebração de contratos com fornecedores estrangeiros pode levar à aplicação de regras estrangeiras, sem que o consumidor se aperceba dessa possibilidade e sem que tome consciência dos efeitos daí decorrentes."

diferenciados pelo meio utilizado para a celebração[407]. Importa adaptar os mecanismos de celebração dos contratos pelo meio digital para, assim, garantir a sua validade, com o cumprimento tanto dos requisitos necessários à formação e declaração da vontade, quanto com os princípios relativos à transmissão e armazenamento dos dados ali contidos.

Como resultado, a formação dos contratos eletrônicos pode ser dividida em momentos distintos: negociações preliminares; oferta (ou policitação); e aceitação ou oblação. A formação do contrato inicia, efetivamente, a partir da oferta, com manifestação de vontade inequívoca de contratar por uma das partes[408].

Além disso, há sempre a questão de fundo, que envolve o fornecimento e o tratamento de dados – neste caso, pertencentes ao consumidor, sujeito vulnerável, hipossuficiente e merecedor de proteção específica. É sob este aspecto específico que o tema dos contratos eletrônicos interessa ao presente estudo.

Neste contexto, valores como a transparência adquirem importância ainda maior. Os princípios da transparência, consentimento e do legítimo interesse já eram objeto de preocupação do legislador anterior à Sociedade da Informação, de modo que analogias e adaptações vêm sendo utilizadas para aplicá-los ao ambiente digital.

Dado o caráter transnacional de tais relações contratuais, surgem questões relacionadas aos critérios de conexão aplicáveis a cada caso. Neste momento, retoma-se a questão inicialmente proposta acerca da possibilidade de analogia com os contratos celebrados entre ausentes para avaliar, por exemplo, o momento e o local de celebração do

---

[407] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 144. "Ou seja, caso o usuário alegue não leitura dos termos de uso, seja por não entendimento da linguagem utilizada ou outro motivo referente às circunstâncias do negócio, é possível a anulação do contrato celebrado, por não haver efetiva declaração de vontade no momento de estabelecimento do negócio jurídico. [...] Em vista dos dispositivos do Código Civil vigente no Brasil, quando aplicáveis à relação jurídica entre o usuário e a empresa provedora de serviços, os termos de uso podem ter sua validade jurídica questionada, sobretudo naqueles casos em que são anuídos por meio de declaração de vontade defeituosa."

[408] RAMOS, Victor de Moraes. Op. cit., 2009. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/539. Acesso em: 12 mar. 2020. Concorda-se com o autor no sentido de que, de forma geral, os contratos eletrônicos podem ser considerados como celebrados entre ausentes no espaço (independentemente de sua presença ou não no tempo): "As ofertas feitas através da internet geralmente ocorrem por meio de sites especializados em divulgar e intermediar contratos de venda de produtos e serviços ou através de lojas virtuais. As ofertas e propostas são, nestes casos, permanentes, ou seja, acessíveis a qualquer tempo. [...] A aceitação ou oblação é a fase em que uma parte assente com as condições estabelecidas na oferta. A partir desta concordância, geram-se direitos e obrigações para ambas as partes, que devem dar cumprimento aos deveres pactuados. Há um embate doutrinário, em que se discute se os contratos celebrados por meio da internet seriam formados entre presentes ou entre ausentes. [...] algumas características são inerentes a todos os contratos eletrônicos: a primeira característica observada é que tais contratos são firmados entre pessoas que não estão fisicamente presentes; a segunda característica observada é de que a simultaneidade no momento compreendido entre a oferta e a aceitação pode existir ou não. Portanto, com todo o respeito em relação aos que apresentam entendimento em contrário, diante destas conclusões adota-se o posicionamento de que o contrato eletrônico, em regra geral, é firmado entre ausentes. Já que as partes não se encontram fisicamente no mesmo espaço físico, bem como, não há, necessariamente, simultaneidade."

contrato, a serem considerados para fins de determinação da jurisdição internacionalmente competente e da lei aplicável a um eventual conflito[409].

Além do local e da possibilidade de celebração entre ausentes, o conceito de tempo também é relativizado, já que existem diferenças entre fusos horários, ou intervalos de tempo entre as etapas da formação do contrato, tornando-se dificultosa a sua precisa determinação. Não obstante os contratos eletrônicos, "deve ser atribuído o mesmo reconhecimento jurídico que se atribui aos contratos tradicionais. Ou seja, não é só porque um contrato foi celebrado via eletrônica que se deve negar-lhe os efeitos jurídicos referentes à validade e de eficácia"[410].

Por fim, há que se considerar, no momento do ajuizamento de eventual ação, se o seu objeto envolve questões de natureza contratual ou extracontratual. É possível que a controvérsia tenha sido firmada quanto ao cumprimento do contrato, após certo produto não ter sido entregue, por exemplo. É igualmente possível, contudo, que a partir da relação contratual tenham se revelado violações relativas a direitos fundamentais e de natureza extracontratual, não estando diretamente relacionados ao objeto do contrato. Revela-se essencial, novamente, a adequada qualificação a fim de garantir a subsunção dos fatos à norma jurídica efetivamente relevante e aplicável.

2.5 CRIPTOMOEDAS E MOEDAS DIGITAIS

Os *smart contracts* abordados anteriormente apresentaram desenvolvimento substancial a partir do surgimento da Bitcoin e de outras criptomoedas. Criptomoedas são, essencialmente, meios de troca[411]. Na maior parte dos casos, são utilizadas a criptografia

[409] Id., ibid. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/539. Acesso em: 12 mar. 2020. "O momento em que um sistema desta natureza é colocado à disposição em um ambiente eletrônico de rede, é o momento da oferta, para efeitos jurídicos. Ao passo que, no momento em que o futuro adquirente acessa o sistema, e com ele interage, preenche os seus dados e expressa a aceitação aos termos e condições de fornecimento constantes da oferta, seria o momento da celebração do contrato de adesão."

[410] RAMOS, Victor de Moraes. Id., ibid. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/539. Acesso em: 07 jan. 2020. "Neste sentido, o art. 5º da Lei Modelo da Uncitral estabelece 'reconhecimento jurídico das mensagens de dados' e, também, afirma que 'Não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica'. Este princípio fora abordado, no âmbito nacional, no Projeto de Lei n. 1.589/99 da OAB de São Paulo, que dispôs que 'o simples fato de ser realizada por meio eletrônico não sujeitará a oferta de bens, serviço e informação a qualquer tipo de autorização prévia'."

[411] MARANHÃO, Juliano Souza de Albuquerque; FERRAZ JÚNIOR, Tércio Sampaio; FINGER, Marcelo. O desafio do Whatsapp ao Leviatã. *Folha de São Paulo, Tendências/Debates*, 16 ago. 2016. Disponível em: https://www1.folha.uol.com.br/opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml. Acesso em: 18 abr. 2020. "O interessante é que essa tecnologia de encriptação, ao proporcionar inviolabilidade, torna o Estado impotente e, no limite, dispensável – os bitcoins, por exemplo, usam a criptografia para proporcionar a todos os usuários um sistema seguro de geração de moedas, de sua propriedade e de trocas."

de dados e a tecnologia *blockchain* para assegurar a validade das transações, criando novos meios de troca, semelhantes a moedas, os quais podem ser centralizados[412] ou descentralizados[413]. Moedas digitais, diferentemente das criptomoedas inicialmente cunhadas, podem ser centralizadas ou dispensar o uso de *blockchain.*

A Bitcoin é a mais conhecida dentre as criptomoedas, especialmente por ter sido a primeira criptomoeda descentralizada, criada em 2009 por Satoshi Nakamoto (pseudônimo)[414]. A ideia é diferente dos sistemas bancários centralizados: a tecnologia de

---

[412] ORTEGA, João. Moeda digital oficial da China está pronta para lançamento. *StartSe*, 12 ago. 2019. Disponível em: https://www.startse.com/noticia/ecossistema/criptomoeda-oficial-china. Acesso em: 07 jan. 2020. "A China está prestes a lançar uma moeda digital oficial do país. Mu Changchun, executivo do Banco Popular da China, anunciou neste sábado (10) que o projeto, desenvolvido durante os últimos cinco anos, está pronto para entrar em operação. [...] Sabe-se que, **diferente de uma criptomoeda, no entanto, a emissão e o controle da moeda chinesa não serão descentralizados**, e sim divididos entre o banco central e outras instituições financeiras. **Além disso, a moeda não é gerida pela *blockchain***, como é típico das criptografadas, como o Bitcoin. Hoje, transações com criptomoedas são proibidas na China. [...] Embora não seja uma criptomoeda e tenha sido desenvolvida desde 2014, o *timing* da novidade do Banco Popular da China a coloca no cenário internacional como uma resposta à Libra, a criptomoeda do Facebook. [...] Além do Facebook, outras gigantes estão por trás da Libra, como Uber, Visa, Paypal e Mastercard." (grifamos).

[413] COLOMÉ, Jordi Pérez. Facebook lança Libra, uma moeda própria para "reinventar o dinheiro". *El País*, 18 jun. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/06/18/tecnologia/1560851467_183722.html. Acesso em: 07 jan. 2020. "O Facebook lançará em 2020 a sua própria moeda: a Libra. Os usuários do WhatsApp e Messenger poderão trocar dinheiro a partir de sua carteira digital e o Facebook também vai oferecer o serviço como um aplicativo independente. [...] 'Uma criptomoeda de baixa volatilidade, com base em *blockchain* **descentralizado** com o objetivo de criar uma nova oportunidade para a inovação de serviços financeiros responsáveis'. O Facebook criou sua própria tecnologia *blockchain* para gerenciar a Libra. [...] A Libra estará atrelada a uma reserva real – a reserva Libra – e poderá ser trocada por outras moedas reais com base em uma taxa de câmbio estável. 'Para ajudar a dar confiança a uma nova moeda e alcançar uma maior adoção no início, tradicionalmente as notas do país podiam ser trocadas por recursos reais, como o ouro. Em vez de embasar a Libra com o ouro, ela será apoiada por um conjunto de recursos de baixa volatilidade, tais como depósitos bancários e valores públicos de curto prazo de moedas de bancos centrais estáveis e de reputação'. **Este detalhe é o que mais distancia a Libra das criptomoedas comuns, como o bitcoin, que não têm uma reserva por trás e cuja taxa de câmbio varia com facilidade**. [...]." (grifamos).

[414] NAKAMOTO, Satoshi. *Bitcoin:* a Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 17 abr. 2020. Os princípios que regem a tecnologia *blockchain* foram elaborados em texto divulgado no ano de 2008, por autor desconhecido, cujo pseudônimo é Satoshi Nakamoto. O texto expõe um sistema baseado na construção de uma alternativa ao sistema financeiro e meios de pagamento convencionais. "O comércio na Internet passou a depender quase exclusivamente de instituições financeiras que servem como terceiros confiáveis para processar pagamentos eletrônicos. Embora o sistema funcione bem o suficiente para a maioria das transações, ele ainda sofre com os pontos fracos inerentes ao modelo baseado em confiança. [...] O custo da mediação aumenta os custos de transação, limitando o tamanho mínimo prático da transação e cortando a possibilidade de pequenas transações casuais, e há um custo mais amplo na perda da capacidade de fazer pagamentos não reversíveis por serviços não reversíveis. Com a possibilidade de reversão, a necessidade de confiança se espalha. [...] O que é necessário é um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança, permitindo que duas partes dispostas a fazer transações diretamente entre si, sem a necessidade de terceiros confiáveis. Transações que são computacionalmente impraticáveis para reverter protegeriam os vendedores de fraudes, e mecanismos rotineiros de custódia poderiam ser facilmente implementados para proteger os compradores." (Tradução livre). "*Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. [...]. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. [...]. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing*

blockchain permite a criação de uma cadeia de registro de dados, semelhante a um livro-registro, a partir do qual todos possuem uma cópia idêntica e impassível de alterações do completo histórico de transações. Assim, restam impedidas alterações no registro por parte de uma entidade central, como ocorre tradicionalmente com as transações bancárias.

Além de oferecer um meio seguro de registro das transações, pela própria característica técnica das tecnologias que envolvem a criptografia e a *blockchain*, a Bitcoin adquiriu popularidade devido à sua capacidade de ser utilizada sem vinculação ao sistema bancário tradicional, possibilitando a realização de transações sob maior sigilo[415], estabelecendo neste ponto a sua relação com o tema da privacidade no ambiente digital.

Uma criptomoeda pode ser entendida, portanto, como um sistema que atende a seis condições específicas: (i) não requer uma autoridade central; (ii) mantém uma visão geral das unidades de criptomoeda e sua propriedade; (iii) define se novas unidades de criptomoeda podem ser criadas (se forem, o sistema define as circunstâncias de sua origem e como determinar a sua propriedade); (iv) a propriedade de unidades de criptomoeda pode ser provada exclusivamente por criptografia; (v) permite transações, com alteração da propriedade das unidades criptográficas, mediante comprovação da propriedade atual das unidades; e (vi) se duas instruções diferentes para alterar a propriedade de uma unidade criptográfica foram inseridas simultaneamente, no máximo uma delas será executada [416].

Em 2017 ocorreram as primeiras *Initial Coin Offerings (ICO)*, ou seja, a obtenção de financiamento por meio da emissão de criptomoedas: trata-se de um meio não

---

any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse wouldprotect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers."

[415] ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. *Revista Brasileira de Políticas Públicas UniCEUB*, dez. 2017, v. 7, n. 3, pp. 44-59, p. 46. "A ideia de utilizar o dinheiro na forma digital já é uma realidade, o que se verifica desde as operações mais simples como o depósito em uma conta bancária por sistemas de internet *banking*, em que um *software* identifica o proprietário e cria um crédito de acordo com o valor do depósito; até compras e transações que envolvem o fluxo internacional da moeda."

[416] SANTOS, João Vieira dos. Desafios jurídicos e regulatórios das *Initial Coin Offerings*. *In*: CORDEIRO, António Menezes *et al. FinTech II:* novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019, p. 303. "A ascenção da *blockchain* deveu-se, em grande medida, ao sucesso das *bitcoins* e aos princípios definidos no artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", publicado em 2008, cuja autoria pertence ao desconhecido, ou grupo de desconhecidos, chamado "Satoshi Nakamoto". A partir desse artigo, emitiram-se pela primeira vez, em 2009, as *bitcoins*, e permitiu-se, destarte, resolver o problema da dupla alienação (*double spending*), sem que seja necessária a intervenção de um intermediário. Este problema da dupla alienação advém do envio de cópias através da *internet*. Quando se envia um documento ou um *email*, o que estamos a enviar é uma cópia desse documento ou *email*. [...] Por outro lado, a tecnologia *blockchain* permite que se faça esta verificação da transação de uma forma automática, reduzindo drasticamente os custos normalmente associados a essa verificação, e permite, ainda, resolver este problema de uma forma mais segura e eficiente: [...]."

regulamentado, que permite a um novo empreendimento ou projeto de criptomoeda realizar a venda de moedas criptográficas "recém-cunhadas"[417].

As ofertas têm tido grande sucesso entre investidores, especialmente no contexto das *start ups*, demonstrando a existência de uma lacuna no sistema societário que vem sendo preenchido pelas ICO. Além da Bitcoin, há uma grande variedade de criptomoedas sendo transacionadas atualmente: calcula-se que existem mais de 1.300 criptomedas/*tokens* diferentes em que é possível investir.

Não obstante a grande variedade de criptomoedas e moedas digitais, este é um meio de pagamento novo, existente há apenas uma década. Assim, é evidente que surgirão questionamentos sobre as normas aplicáveis e sua regulação[418]. Há, por exemplo, problemática envolvendo a qualificação das criptomoedas e moedas digitais conforme a lei aplicável: se forem entendidas como um valor mobiliário, há obrigações legais relativas ao registro. Tais obrigações, contudo, podem ser afastadas, a depender da qualificação realizada.

Há, igualmente, questões envolvendo as estruturas nas quais as criptomoedas podem ser negociadas, como a necessidade de cumprimento dos requisitos de transparência, integridade e reporte, além daqueles específicos. De todo modo, o crescimento constante dos utilizadores e proprietários de criptomoedas e moedas digitais é inevitável, o que denota o início de um "processo de digitalização da economia que, de forma célere e irrefreável, tem transformado todos os modelos de negócio"[419], embora o seu estudo no Brasil ainda seja incipiente[420].

---

[417] Id., ibid., pp. 299-301. "No ano de 2017, as *Initial Coin Offerings* – obtenção de financiamento através da emissão de criptomoedas – envolveram mais de 3 mil milhões de dólares, espoletando cada vez o interesse de investidores, regulares e não só, para conhecerem melhor este fenômeno. [...] Ao passo que a posição institucional da China tem sido a de proibir a transação de criptomoedas e a dos Estados Unidos da América de regular as *Initial Coin Offerings* por recurso às normas relativas a valores mobiliários – através do trabalho de investigação da SEC (*Securities Exchange Comission*) –, na Europa as posições têm sido mais incentivadoras."

[418] CAMARGO, Solano de. *Homologação de sentenças estrangeiras:* Ordem Pública Processual e Jurisdições Anômalas. São Paulo: Quartier Latin, 2019, p. 113. "À vista das características típicas do comércio eletrônico, ou seja, valores nem sempre expressivos, transnacionalidade das relações econômicas e manutenção do anonimato, iniciou-se uma progressiva necessidade de resolução de disputas envolvendo as operações celebradas em bitcoins."

[419] SANTOS, João Vieira dos. Op. cit., 2019, p. 324.

[420] ANDRADE, Mariana Dionísio de. Op. cit., dez. 2017, p. 28. Disponível em: https://www.arqcom.uniceub.br/RBPP/article/viewFile/4897/3645. Acesso em: 07 jan. 2020. "Na medida em que as características típicas do uso dessa modalidade se materializam pela descentralização e ausência de instituições reguladoras que impõem tributação, as operações por meio das bitcoins são anônimas e de difícil identificação dos usuários, o que propicia espaço para todos os tipos de pessoas, inclusive as que utilizam o ciberespaço para a realização de práticas delitivas."

2.6 INTELIGÊNCIA ARTIFICIAL (IA) E SENTENÇAS CIBERNÉTICAS

O uso da Inteligência Artificial (IA) para analisar situações, prever resultados e, inclusive, prever decisões, tem sido frequente e com resultados cada vez mais precisos. Integrada em todas as áreas da vida, a IA merece especial atenção à forma como tem sido utilizada por operadores jurídicos, escritórios de advocacia, tribunais, órgãos legislativos e administrativos[421].

Por um lado, a IA permite aos advogados e demais operadores do Direito analisarem o conjunto de decisões judiciais já existentes sobre um tema específico. Assim, é possível avaliar a tendência jurisprudencial, as chances de êxito de uma demanda e, ainda, encontrar novos nichos de atuação.

A França já se posicionou contrária à análise de decisões judiciais e à utilização de jurimetria. O país foi o primeiro a criar normas criminalizando a publicação de análises feitas a partir de decisões judiciais, prevendo pena de até cinco anos de prisão aos infratores[422]. A lei, portanto, proíbe a indexação de decisões dos tribunais franceses e os respectivos nomes dos magistrados, evitando a sua utilização.

A lei francesa foi objeto de diversas críticas, principalmente no sentido da publicidade das decisões judiciais e do princípio da transparência no Poder Judiciário. Uma alternativa considerada é a retirada do nome do magistrado, restringindo a análise ao

---

[421] MARANHÃO, Juliano Souza de Albuquerque. Op. cit., 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 18 abr. 2020. "Diversos centros de pesquisa têm sido criados para dar suporte ao florescimento à inteligência artificial (IA) ligada ao Direito em seus países, por meio do fomento e desenvolvimento de pesquisa acadêmica. Por exemplo, o Codex, da Universidade de Standford; o Cirsfid, Centro de Informática Jurídica da Universidade de Bologna; o programa de Sistemas Inteligentes, da Universidade de Pittsburgh; o centro de Direito e Tecnologia da Informação do King's College. As principais universidades do mundo têm criado não só centros congêneres de pesquisa, como também novos cursos de Direito aliados ao ensino de lógica jurídica e lógica de programação, além de incubadoras de *lawtechs*. A Associação Internacional de Inteligência Artificial e Direito (Iaail) promove, bienalmente, a Conferência Icail, atualmente a mais relevante da área, que reúne pesquisadores dos principais centros internacionais de Inteligência Artificial e Direito. Ainda há poucos brasileiros nessa comunidade acadêmica, mas o país começa a ganhar reconhecimento, valendo mencionar que a Universidade de São Paulo está na disputa com a Universidade de Montreal para sediar o próximo Icail, a ocorrer em 2019. De todo modo, para inserir o Brasil nesta nova fronteira tecnológica, é fundamental que não só a USP como também as principais universidades do país comecem a engajar pesquisadores nesse ramo. Dentro desse espírito, um grupo de professores de Engenharia, Ciência da Computação, Filosofia e Direito da USP criou um *think tank*, chamado *Lawgorithm*, para articular a pesquisa acadêmica e a formação universitária com as iniciativas práticas, nos setores público e privado, de desenvolvimento de ferramentas computacionais para a atividade jurídica, bem como para refletir sobre as implicações jurídicas, sociais, econômicas e culturais da inteligência artificial em geral."

[422] FRANÇA. *Lei de Reforma da Justiça* (Réforme de la justice et renforcement de l'organisation des juridictions), 25 de março de 2019. Disponível em: http://www.senat.fr/espace_presse/actualites/201810/reforme_de_la_justice.html. Acesso em: 17 abr. 2020. "Art. 33. Os dados de identidade dos magistrados e dos membros do poder judiciário não podem ser reutilizados com a finalidade ou o efeito de avaliar, analisar, comparar ou prever as suas práticas profissionais reais ou alegadas." (Tradução livre).

conteúdo das decisões. Há de se ressaltar, contudo, que esta opção não se mostra totalmente apta a permitir o tratamento de dados do Judiciário sem implicar violações à lei.

Importante relembrar que a mera supressão do nome do magistrado não impede a sua identificação: a existência de dados e informações sobre o órgão responsável pelo julgamento, data e horário, pautas de audiência, dentre outros, reunidos em bancos de *big data*, possibilita que um sistema de IA identifique o magistrado responsável por uma decisão.

No Brasil, as decisões judiciais são publicadas e amplamente divulgadas, com exceção dos casos de ações que tramitam sob segredo de Justiça, nas quais os nomes das partes são ocultados. Isto permite o desenvolvimento de programas de Inteligência Artificial voltados especificamente à análise das decisões judiciais como ferramenta complementar à atividade de advogados ou outros operadores do Direito, como é o caso dos sistemas Watson[423], Sapiens[424], Sinapses[425] e Victor[426].

---

[423] A plataforma cognitiva "Watson" foi desenvolvida pela empresa IBM, tendo aplicação em áreas diversas, inclusive no âmbito do Direito. No entanto, a mera utilização do robô para a realização de atividades repetitivas e automáticas, como preenchimento de dados automatizados, não significa necessariamente a utilização de Inteligência Artificial, que implica o aprendizado pela própria máquina a partir das tarefas inicialmente programadas e conforme a alimentação de novos dados. Mais informações disponíveis em: IBM Watson. *Coloque a Inteligência Artificial para trabalhar*. Disponível em: https://www.ibm.com/watson/br-pt/. Acesso em: 17 abr. 2020.

[424] AGU. Advocacia Geral da União. *Advocacia-Geral aposta em inteligência artificial e automação de processos para agilizar trabalhos jurídicos*, 26 fev. 2013. Disponível em: http://www.agu.gov.br/page/content/detail/id_conteudo/230719. Acesso em: 15 dez. 2019. O Sistema de Apoio à Procuradora Inteligente (Sapiens) foi criado no âmbito da Advocacia Geral de União (AGU), permitindo a implementação de rotinas de inteligência baseadas em técnicas de análise de critérios de similaridade, permitindo a leitura de acórdãos pela máquina e indicação da peça jurídica mais adequada. "[...] O Sistema de Automação Processual (SAP), também conhecido como 'robozinho', distribui processos e cadastra tarefas no Sistema Integrado de Controle das Ações da União (Sicau) em segundos. A expectativa é que ele atinja a marca de um milhão de registros no mês de março. Já o Sistema de Apoio à Procuradoria Inteligente (Sapiens) vai além, lê o processo e indica a melhor peça jurídica a ser usada. [...] Da evolução e aperfeiçoamento do SAP foi desenvolvido o Sapiens. O projeto executa as mesmas informações do 'robozinho' e ainda implementa rotinas de inteligência por meio de técnicas de análise de similaridade, o que permite que o computador 'leia' um acórdão e sugira a melhor peça jurídica a ser utilizada. [...] O sistema é dividido em dois módulos distintos: o primeiro módulo (Módulo Administrativo) é responsável pela integração do Sapiens com os demais sistemas informatizados existentes (Sicau, Tribunais, etc.). O Módulo Administrativo é uma ferramenta de auxílio exclusivo da equipe de apoio administrativo da Procuradoria, sendo por esta equipe operado. Ele realiza a migração automática das intimações eletrônicas da Justiça, em um primeiro instante, para o sistema Sapiens e, após, para o Sicau. Neste processo, ele recupera informações completas do processo (autor, réu, partes, etc.). Ele também é responsável pela sincronização das bases de tarefas do Sicau e Sapiens, realizando a migração e o eventual encerramento das mesmas, quando necessário. O segundo módulo (Módulo Judicial) constitui ferramenta de auxílio ao trabalho desenvolvido pelo procurador. Ele auxilia no controle de prazos, na produção da peça jurídica (com a indicação de prováveis modelos para o caso em análise e controle do fluxo de produção de minutas de peças por estagiários), na sistematização do serviço de natureza jurídica (com a prévia de quais processos seriam prioritários, quais conteriam pedido de cumprimento de tutela, etc.), no controle e acompanhamento de pedidos de cumprimento de decisões judiciais, no controle e acompanhamento dos pedidos de carga. [...]. O sistema trabalha com o conceito de inteligência social, que reúne e combina o apoio fornecido por ferramentas de inteligência artificial com o *feedback* humano. [...]."

[425] CNJ. Conselho Nacional de Justiça. *Inovações em Inteligência Artificial para o PJe são apresentadas no CNJ*, 22 maio 2019. Disponível em: https://www.cnj.jus.br/inovacoes-em-inteligencia-artificial-para-o-pje-

A Inteligência Artificial ainda é escassamente utilizada pelo Poder Judiciário brasileiro, apesar das iniciativas mencionadas anteriormente e seus benefícios, como ganhos em termos de celeridade e duração razoável do processo. Em alguns países, programas do gênero já são utilizados por magistrados como ferramenta auxiliar na tomada de decisões. Nos Estados Unidos, ela é utilizada no âmbito do sistema criminal para avaliação de perfis e níveis de risco[427], enquanto na Estônia[428] ela será brevemente adotada

---

sao-apresentadas-no-cnj/. Acesso em: 17 abr. 2020. "[...] A plataforma Sinapses, desenvolvida pelo Tribunal de Justiça de Rondônia (TJ/RO), constitui-se num modelo unificado para construir soluções e prover IA. Por meio de um termo de cooperação técnica, servidores daquela unidade estão no CNJ para desenvolvimento e funcionamento de IA num ambiente de nuvem para atendimento de todos os tribunais do país. O passo seguinte foi o chamamento público, por meio de edital, para que os tribunais trabalhem com o CNJ por meio de propostas, desenvolvimento e produção de IA. Atualmente, o Inova PJe trabalha em uma solução para identificar decisões similares para que o magistrado, com essa informação, possa utilizar o tempo na produção de decisão; identificação de demandas repetitivas; análise de prevenção em parceria com o Tribunal Regional Federal da 3ª Região (TRF3) e o Gabinete do Magistrado, uma solução de IA que veio de Rondônia e que, em breve, será colocada à disposição dos juízes. [...]."

[426] STF. Supremo Tribunal Federal. *Inteligência artificial vai agilizar a tramitação de processos no* STF, 30 maio 2018. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038. Acesso em: 17 abr. 2020. "Batizado de 'Victor', a ferramenta de Inteligência Artificial é o resultado da iniciativa do Supremo Tribunal Federal, sob a gestão da ministra Cármen Lúcia, em conhecer e aprofundar a discussão sobre as aplicações de IA no Judiciário. Cuida do maior e mais complexo Projeto de IA do Poder Judiciário e, talvez, de toda a Administração Pública brasileira. Na fase inicial do projeto, 'Victor' lerá todos os recursos extraordinários que sobem para o STF e identificará aqueles vinculados a determinados temas de repercussão geral. [...] Como toda tecnologia, seu crescimento pode se tornar exponencial e já foram colocadas em discussão diversas ideias para a ampliação de suas habilidades. O objetivo inicial é aumentar a velocidade de tramitação dos processos por meio da utilização da tecnologia para auxiliar o trabalho do Supremo Tribunal. A máquina não decide, não julga, isso é atividade humana. Está sendo treinado para atuar em camadas de organização dos processos para aumentar a eficiência e velocidade de avaliação judicial. [...]."

[427] O algoritmo "Compas" é utilizado no âmbito do sistema criminal dos Estados Unidos, com a finalidade principal de avaliação de riscos de pessoas no sistema carcerário a fim de determinar, por exemplo, se o réu poderá aguardar o julgamento em liberdade. O algoritmo não pode, contudo, ser revisado por um humano ou questionado publicamente. As críticas ao algoritmo são no sentido de que ele seria tendencioso, apontando indivíduos de determinados perfis como de maior risco, levando à discriminação contra grupos específicos. Há, ainda, críticas direcionadas ao fato de se tratar de ferramenta de avaliação de risco desenvolvida por uma companhia privada. Mais informações disponíveis em: EQUIVANT. Disponível em: https://www.equivant.com/northpointe-suite/. Acesso em: 17 abr. 2020. "O Northpointe Suite é um pacote de software de suporte a decisões automatizadas das principais ferramentas de gerenciamento de riscos, avaliação de necessidades e gerenciamento de casos. Os instrumentos abordam o conjunto complexo de riscos, necessidades e gerenciamento de casos que melhoram a precisão das decisões de custódia, supervisão e programação com base nas necessidades criminogênicas subjacentes." (Tradução livre). "*The Northpointe Suite is an automated decision support software package of industry leading risk, needs assessment and case management tools. The instruments address the complex set of risk, need and case management considerations that improve decision accuracy in custody, supervision and programming based on underlying criminogenic needs*."

[428] NILLER, Eric. Can al be a fair judge in court? Estonia Thinks so. *Wired*, 25 mar. 2019. Disponível em: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/. Acesso em: 17 abr. 2020. A Estônia está desenvolvendo um "juiz robô", apto a tomar decisões em causas de menor valor (até sete mil euros). Neste caso, haveria a possibilidade de revisão, posteriormente, por um juiz humano, se necessário. "No projeto mais ambicioso até hoje, o Ministério da Justiça da Estônia pediu a Velsberg e sua equipe que projetassem um 'juiz robô' que pudesse julgar disputas por pequenas causas, inferiores a € 7.000 (cerca de US $ 8.000). As autoridades esperam que o sistema possa ajudar a eliminar uma lista de casos para juízes e funcionários do tribunal. O projeto está em fase inicial e provavelmente começará ainda este ano com um piloto focado em disputas contratuais. Em teoria, as duas partes enviarão documentos e outras informações relevantes, e a AI emitirá uma decisão que pode ser apelada a um juiz humano. Muitos detalhes ainda

na tomada direta de decisões, resguardando o direito de revisão da decisão por um humano[429].

Ainda que os algoritmos possam ser tendenciosos (e certamente podem), pois são programados a partir de seres humanos que, por sua vez, refletem seus valores e preconceitos, é possível corrigir facilmente a programação para que a IA seja menos tendenciosa. Essa tarefa, por vezes, pode ser mais árdua quando se trata de seres humanos cujas ideias não podem ser reprogramadas a partir de um código. É possível calibrar um sistema de IA desde que observados a transparência, os procedimentos e os protocolos específicos para sua programação[430]. Parece, no entanto, ser imprescindível a possibilidade da revisão de sentenças e decisões proferidas via IA por um ser humano, a fim de garantir a observação dos princípios da ampla defesa e do devido processo legal.

Em resumo, há quatro situações nas quais é possível perceber a atuação de robôs no âmbito jurídico[431]: (i) algoritmos utilizados para classificação (análise de precedentes); (ii)

---

precisam ser elaborados. Velsberg diz que o sistema pode ter que ser ajustado após o feedback de advogados e juízes." (Tradução livre). "*In the most ambitious project to date, the Estonian Ministry of Justice has asked Velsberg and his team to design a 'robot judge' that could adjudicate small claims disputes of less than €7,000 (about $8,000). Officials hope the system can clear a backlog of cases for judges and court clerks. The project is in its early phases and will likely start later this year with a pilot focusing on contract disputes. In concept, the two parties will upload documents and other relevant information, and the AI will issue a decision that can be appealed to a human judge. Many details are still to be worked out. Velsberg says the system might have to be adjusted after feedback from lawyers and judges."*

[429] CAMARGO, Solano de. O reconhecimento e a execução de sentenças cibernéticas no Direito Internacional Privado. *In*: MALHEIROS, Clara; MONTE, Mário Ferreira; PEREIRA, Maria Assunção; GONÇALVES, Anabela (Orgs.). *Direito na Lusofonia*. Direito e novas tecnologias. Braga: Escola de Direito da Universidade do Minho, 2018, v. 1, pp. 477-484. O autor defende que decisões judiciais ou sentenças proferidas por *softwares* de Inteligência Artificial representariam uma violação à ordem pública brasileira, ao princípio do devido processo legal, e à ética humana, de forma que não seriam passíveis de homologação no Brasil. Isto porque, no seu entendimento, o princípio do devido processo legal e do livre convencimento motivado do julgador condicionam que as decisões judiciais sejam proferidas por seres humanos. Cumpre questionar, contudo, se ainda haveria violação à ordem pública nacional caso a decisão sujeita à homologação tenha sido revisada por um ser humano em sede recursal.

[430] ARBIX, Glauco. Inteligência artificial ainda sofre com algoritmos enviesados. *Jornal da USP*, 18 nov. 2019. Disponível em: https://jornal.usp.br/radio-usp/colunistas/inteligencia-artificial-ainda-sofre-com-algoritmos-enviesados/. Acesso em: 17 abr. 2020. "Um estudo publicado na revista Science fez com que cientistas acompanhassem a evolução de um *software* voltado para a área da saúde, que indicava a ordem de prioridade dos pacientes em fila para receber atendimento. O resultado foi que existia um viés racial, que desfavorecia pessoas negras nos algoritmos do sistema. É possível diminuir as tendências dos algoritmos, corrigindo distorções que possam prejudicar pessoas, mas é preciso que o problema apareça, que alguém aponte o problema, caso contrário, o *software* continuará trabalhando."

[431] MARANHÃO, Juliano Souza de Albuquerque. Op. cit., 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 18 abr. 2020. "A partir dessas convicções, é importante separar duas perspectivas da interação entre Inteligência Artificial (IA) e Direito. Da perspectiva da aplicação da Inteligência Artificial ao Direito (que chamo de IA&Direito), é importante promover a pesquisa sobre sistemas lógicos que sirvam de base a ferramentas computacionais capazes de tornar mais eficiente a atuação de juristas (juízes, advogados, promotores, professores de Direito, etc.) e gerar informações sobre as atividades legislativa e jurisdicional. Da perspectiva da disciplina jurídica da Inteligência Artificial (que chamo de Direito da IA), a pesquisa jurídica deve buscar compreender tecnicamente o que são e qual o significado de agentes digitais em suas relações com humanos de modo a refletir sobre seus impactos sociais e sobre novas questões jurídicas delas

algoritmos de mineração de dados em grande volume (identificação de fatos relevantes dentro de um contexto amplo de informações e dados); (iii) algoritmos capazes de tomar decisões de baixa complexidade; e (iv) análise de decisões anteriores para prever o resultado de demandas atuais.

Existem diferenças entre robôs, Inteligência Artificial (IA), *Machine Learning* (ML) [432] e *Deep Learning* (DL). Os *robôs* são programados para reduzir ou otimizar o trabalho de seres humanos. No âmbito do Direito, podem ser programados para elaborar procurações e instrumentos simples, como contratos padronizados ou até mesmo de forma a auxiliar na elaboração de petições.

A automatização de tarefas, a otimização da produtividade e a redução da margem de erros estão entre os principais objetivos da utilização de robôs, no entanto, devem ser programados para atividades específicas, sendo incapazes de desenvolver novas tarefas a partir da realização de tarefas anteriores. Em outras palavras, robôs podem ser programados, mas não podem aprender de forma autônoma.

A Inteligência Artificial (IA), por sua vez, pode ser considerada um termo genérico, relacionada à capacidade de um sistema autonomamente gerir e agir de acordo com suas próprias regras. Ainda que todo *Machine Learning* (ML) seja uma espécie de IA, nem toda a Inteligência artificial é baseada no ML.

Já o *Machine Learning* (ML) é utilizado, por exemplo, pelo Facebook, para programar as postagens que são exibidas no *feed* de notícias de cada usuário, de forma individualizada, e com base naquilo que o sistema já aprendeu sobre determinada pessoa. Em outras palavras, trata-se de um sistema capaz de evoluir conforme for sendo alimentado com novos dados, estando em constante mudança e adaptação.

O *Deep Learning* (DL), finalmente, representa um passo além do ML, pois conta com o aprendizado de novas habilidades e com ajustes daquelas já existentes[433]. Trata-se

---

derivadas. Para essas duas linhas, tanto para a Ciência da Computação quanto para o Direito devem ser dirigidos esforços para a pesquisa teórica e para a pesquisa aplicada."

[432] Id., ibid. "Técnicas de processamento de linguagens naturais e *machine learning* são treinados a partir de um *corpus* de dados relevantes, sobre os quais são construídas ontologias que representem as relações semânticas entre os termos e conceitos empregados. Uma vez treinados, esses sistemas podem interagir com textos aos quais ainda não foram expostos, generalizando os conceitos representados nas ontologias e as interações entre eles."

[433] NILLER, Eric. Op. cit., 25 mar. 2019. Disponível em: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/. Acesso em: 17 abr. 2020. "[...] Siim Sikkut, diretor de informações da Estônia, começou a dirigir diversos projetos baseados em IA em agências em 2017, antes de contratar Velsberg no ano passado. Velsberg diz que a Estônia implantou IA ou *machine learning* em 13 lugares onde um algoritmo substituiu os funcionários do governo. Por exemplo, os inspetores não checam mais os agricultores que recebem subsídios do governo para cortar seus campos de feno a cada verão. Imagens de satélite tiradas pela Agência Espacial Europeia todas as semanas de maio a outubro são inseridas em um algoritmo de

de uma das técnicas utilizadas para que uma máquina interprete dados e aprenda com eles de forma autônoma. Sistemas únicos, tanto ML quanto DL são formas de IA, executadas por máquinas que utilizam sistemas programados para desempenhar funções cognitivas associadas à aprendizagem intuitiva.

No ML, contudo, há necessidade de designar, manualmente, os recursos que serão processados, enquanto o *DL* implica em um aprendizado mais intuitivo. O DL permite a generalização a partir de dados parciais, facilitando a identificação de objetos, mesmo quando obstruídos em partes. Pode ser utilizado, por exemplo, no reconhecimento facial ou de fala[434], tradução automática, pesquisa por voz, relatórios de performance, gestão de investimentos[435], dentre outras incontáveis oportunidades de aplicação[436].

---

aprendizado profundo desenvolvido originalmente pelo Observatório Tartu. As imagens são sobrepostas em um mapa de campos em que os agricultores recebem os subsídios para cortar o feno para impedir que vire florestas ao longo do tempo. O algoritmo avalia cada pixel nas imagens, determinando se o trecho do campo foi cortado ou não. A pastagem de gado ou o corte parcial podem prejudicar o processamento da imagem; nesses casos, um inspetor ainda se dirige para verificar. Duas semanas antes do prazo de corte, o sistema automatizado notifica os agricultores por texto ou e-mail que inclui um link para a imagem de satélite de seu campo. O sistema economizou € 665.000 (US $ 755.000) em seu primeiro ano porque os inspetores fizeram menos visitas ao local e se concentraram em outras ações de fiscalização, de acordo com Velsberg. Em outra aplicação, currículos de trabalhadores demitidos são inseridos em um sistema de aprendizado de máquina que combina suas habilidades com os empregadores. Cerca de 72% dos trabalhadores que obtêm um novo emprego através do sistema ainda estão no cargo após seis meses, um aumento de 58% antes da implantação do sistema de correspondência por computador. Em um terceiro caso, as crianças nascidas na Estônia são automaticamente matriculadas nas escolas locais ao nascer, para que os pais não precisem se inscrever em listas de espera ou ligar para os administradores das escolas. Isso ocorre porque os registros hospitalares são automaticamente compartilhados com as escolas locais. O sistema não exige realmente IA, mas mostra como os serviços automatizados estão se expandindo." (Tradução livre). *"[...] Siim Sikkut, Estonia's chief information officer, began piloting several AI-based projects at agencies in 2017, before hiring Velsberg last year. Velsberg says Estonia has deployed AI or machine learning in 13 places where an algorithm has replaced government workers. For example, inspectors no longer check on farmers who receive government subsidies to cut their hay fields each summer. Satellite images taken by the European Space Agency each week from May to October are fed into a deep-learning algorithm originally developed by the Tartu Observatory. The images are overlaid onto a map of fields where farmers receive the hay-cutting subsidies to prevent them from turning forests over time. The algorithm assesses each pixel in the images, determining if the patch of the field has been cut or not. Cattle grazing or partial cutting can throw off the image processing; in those cases, an inspector still drives out to check. Two weeks before the mowing deadline, the automated system notifies farmers via text or email that includes a link to the satellite image of their field. The system saved €665,000 ($755,000) in its first year because inspectors made fewer site visits and focused on other enforcement actions, according to Velsberg. In another application, resumes of laid-off workers are fed into a machine learning system that matches their skills with employers. About 72 percent of workers who gain a new job through the system are still on the job after six months, up from 58 percent before the computer-matching system was deployed. In a third case, children born in Estonia are automatically enrolled in local schools at birth, so parents don't have to sign up on waiting lists or call school administrators. That's because hospital records are automatically shared with local schools. The system doesn't truly require AI, but it shows how automated services are expanding."*

[434] SOPRANA, Paulo. Analistas veem risco à privacidade com tecnologia de reconhecimento facial. *Folha de São Paulo*, 17 jan. 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/01/analistas-veem-risco-a-privacidade-com-tecnologia-de-reconhecimento-facial.shtml. Acesso em: 17 abr. 2020. "No sistema chinês, empresas como a Dahua oferecem ao Partido Comunista um software de inteligência artificial capaz de identificar rostos e relacioná-los com outras informações, como sexo, idade e números identificadores. É possível detectar quantas vezes uma pessoa passa por um determinado local, se tem um comportamento

Do ponto de vista jurídico, resta clara a necessidade de regulamentar de forma adequada os sistemas de IA, inclusive ML e DL, de forma a garantir a transparência e os mínimos padrões de segurança no tratamento de dados. Não é possível concordar, no entanto, com a posição proibitiva francesa, que vai na contramão dos avanços tecnológicos mais recentes, e dificilmente perdurará no contexto da Sociedade da Informação[437].

---

considerado suspeito pelas autoridades e com quem está acompanhada, por exemplo. O sistema reconhece essas características e, em tempo real, transmite as imagens e informações em painéis."

[435] TOLEDO, Letícia. Como a Inteligência artificial está guiando o mercado financeiro. *InfoMoney*, 17 jan. 2019. Disponível em: https://www.infomoney.com.br/mercados/como-a-inteligencia-artificial-esta-guiando-o-mercado-financeiro/. Acesso em: 17 abr. 2020. "[...] Para trazer apenas um dado, o valor de ativos financeiros ao redor do mundo administrados por robôs chegou a US$ 222 bilhões em 2017 — mais do que o dobro do ano anterior. 'Automação, inteligência artificial e *machine learning* estão prestes a transformar o setor de serviços financeiros', afirma Shawn Edwards, diretor-chefe de tecnologia (CTO) da Bloomberg. Empresas mais sofisticadas usam o *machine learning* para processos como a análise de risco de contraparte, previsão do risco de falência, previsão de retornos e de lucros. Para fundos de investimentos, a tecnologia ajuda ainda na construção de portfólio e análise de sentimentos de notícias financeiras. No caso do *trading*, a aplicação mais óbvia dessas tecnologias é a utilização de robôs que, com parâmetros pré-definidos, conseguem operar a compra e venda de ativos. Mas, além disso, a era do *big data* e das tecnologias como *machine learning* pode ajudar os operadores a obter muito mais valor das informações, incluindo dados relacionados a clientes, *holdings*, negociações e até eventos que não foram negociados. Há ganhos, também, ao automatizar os processos de *compliance* e alavancar os dados que os reguladores exigem que as empresas capturem. [...]."

[436] RAJPUKAR, Pravan *et al.* CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning. Computer Vision and Pattern Recognition. *Cornell University*. 14 nov. 2017. Disponível em: https://arxiv.org/abs/1711.05225. Acesso em: 17 abr. 2020. O artigo traz exemplo de utilização de algoritmo e *deep learning* na área da saúde: foi realizada pesquisa a fim de desenvolver algoritmo capaz de detectar pneumonia a partir da análise de exames de raio-X com performance superior à de radiologistas. "Conclusão. [...] Desenvolvemos um algoritmo que detecta pneumonia a partir de radiografias de tórax de vista frontal em um nível superior aos radiologistas. Também mostramos que uma extensão simples de nosso algoritmo [que pode ser aplicada] para detectar várias doenças supera o estado da arte anterior no ChestX-ray, o maior conjunto de dados de raio X de tórax publicamente disponível. Com a automação no nível de especialistas, esperamos que essa tecnologia possa melhorar a prestação de serviços de saúde e aumentar o acesso ao conhecimento em imagens médicas em partes do mundo onde o acesso a radiologistas qualificados é limitado." (Tradução livre). "*Conclusion. [...] We develop an algorithm which detects pneumonia from frontal-view chest X-ray images at a level exceeding practicing radiologists. We also show that a simple extension of our algorithm to detect multiple diseases outperforms previous state of the art on ChestX-ray, the largest publicly available chest Xray dataset. With automation at the level of experts, we hope that this technology can improve healthcare delivery and increase access to medical imaging expertise in parts of the world where access to skilled radiologists is limited."*

[437] GUEDES, Anielle. Inteligência artificial no tribunal: da análise de dados ao algoritmo juiz. *Uol*, 21 nov. 2019. Disponível em: https://anielleguedes.blogosfera.uol.com.br/2019/11/21/inteligencia-artificial-no-tribunal- da-analise-de-dados-ao-algoritmo-juiz/. Acesso em: 15 dez. 2019. "Os cidadãos de Pequim contam com tecnologia de ponta para receber aconselhamento jurídico: a robô Xiaofa fica alocada no Tribunal Popular Intermediário nº 1, de Pequim, ajudando o público a entender a terminologia legal. Ela sabe a resposta para mais de 40.000 questões de litígio e pode lidar com 30.000 questões legais. E ela não é a única – a China já possui mais de 100 robôs nos tribunais, reduzindo a carga de trabalho dos funcionários. Alguns deles têm até especialidades e vão ainda mais longe: utilizam inteligência artificial para filtrar mensagens privadas ou comentários nas mídias sociais que podem ser utilizados como evidência no tribunal. Enquanto isso, a polícia de trânsito usa a tecnologia de reconhecimento facial para identificar e condenar infratores. Um aplicativo chamado *Intelligent Trial* 1.0 já está reduzindo as cargas de trabalho dos juízes, ajudando-os a filtrar o material do processo e produzindo arquivos eletrônicos dos casos. Por enquanto, a ênfase está em ajudar os profissionais da lei, não substituí-los. Além disso, a IA também pode ajudar a resolver crimes antes de um juiz ser envolvido. A "Valcri", por exemplo, realiza os aspectos de trabalho intensivo de um investigador, percorrendo textos, relatórios de laboratório e documentos da polícia para destacar áreas que justificam uma investigação mais aprofundada e possíveis conexões que os humanos possam perder."

2.7 REALIDADE VIRTUAL E *GAMES*

Dados pessoais e metadados são coletados constantemente: a utilização de dispositivos de realidade virtual[438] ou de *games*[439], também conhecidos como "esportes eletrônicos"[440] ou *e-sports*[441], não é uma exceção. Uma imensidão de informações pode ser obtida acerca do usuário, a começar pelos metadados, que envolvem data e hora de utilização, chegando a detalhes sobre os movimentos físicos do usuário, suas dimensões, altura ou mesmo registro de movimento dos olhos, especificamente no caso da realidade virtual[442].

---

[438] HENRIKSSON, Emil Albihn. Data protection challenges for virtual reality applications. *Interactive Entertainment Law Review.* Jun. 2018. Disponível em: https://www.elgaronline.com/abstract/journals/ielr/1-1/ielr.2018.01.05.xml. Acesso em: 15 dez. 2019. "*Virtual reality technologies necessitate the collection and processing of more – and more intimate – personal data than other media. This gives rise to some particular considerations under data protection regulations and not least the EU General Data Protection Regulation."*

[439] EVANGELISTA, Rafael de Almeida; SOARES, Tiago; SCHIMIDT, Sarah Costa; LAVIGNATTI, Felipe. DIO: um jogo em dispositivos móveis para mapear câmeras de vigilância. *Liind em Revista.* Privacidade e vigilância nos meios digitais. Rio de Janeiro, nov. 2016, v. 12, n. 2, pp. 322-333, p. 322 e ss. Disponível em: http://revista.ibict.br/liinc/article/view/3731. Acesso em: 06 jan. 2020. "Na sociedade contemporânea, as câmeras de vigilância são tecnologias de uso rápido e crescente. As razões dadas para essa proliferação estão principalmente relacionadas a preocupações com segurança. [...]. DIO é um jogo para celulares, ainda em desenvolvimento, que tematiza a proliferação das câmeras em áreas urbanas, promovendo um mapeamento colaborativo de sua localização geográfica. [...]. O acúmulo de pontos permite a aquisição de novos itens jogáveis, que aumentam as potencialidades de cada jogador, a contribuição que pode dar ao seu grupo. Pretendemos, também, que o jogador possa administrar seus dados de vigilância coletados pelo jogo. Por exemplo: que cada usuário possa visualizar os trajetos que fez, em quais dias e horários, e passando por quais câmeras, e perceber e refletir que essas informações podem ser armazenadas também por outros aplicativos. Essa funcionalidade nos permite abordar a questão do uso econômico dos dados pessoais coletados por meio de vigilância. Do mesmo modo, como pensamos a visibilidade dos dispositivos de videovigilância no contexto do jogo, pretendemos dar visibilidade também para a coleta de dados, necessária para o funcionamento do próprio jogo. O uso econômico de dados pessoais na internet se constitui, assim como as câmeras de vigilância, uma questão social polêmica e que tem sido alvo de novas propostas legislativas. Ela coloca em cena três atores principais: os cidadãos, usuários de serviços na internet; as empresas provedoras desses serviços, que utilizam os dados como matéria prima de análises de inteligência voltadas para o comércio e fonte de lucros; e os governos, que utilizam os dados coletados para a prestação de serviços públicos e práticas de repressão política e de segurança."

[440] MOREIRA, André de O. Schenini. Propriedade intelectual e esportes: o premente conflito entre o direito de exclusividade e a liberdade desportiva. *Lei em campo*, 25 nov. 2019. Disponível em: https://leiemcampo.com.br/propriedade-intelectual-e-esports-o-premente-conflito-entre-o-direito-de-exclusiva-e-a-liberdade-desportiva/. Acesso em: 17 abr. 2020. "A chegada dos esportes eletrônicos (esports) no mundo da prática desportiva profissional já é uma realidade inegável. Apenas em 2017, conforme relatório feito pela empresa de consultoria Newzoo, o mercado competitivo profissional de jogos eletrônicos fez girar cerca de US$ 700 milhões ao redor do mundo, incluindo nesta monta valores de publicidade, patrocínio, direitos de transmissão, consumo dos espectadores e investimentos das próprias *publishers*. A expectativa é que esse mercado, até 2020, atinja o patamar de US$ 1,5 bilhão."

[441] CAMARA, Dennys Eduardo Gonsales; LAZZARINI, Giuseppe Mateus Boselli; GHERINI, Pamela Michelena de Marchi. *E-sports:* visão geral e desafios jurídicos. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2018/10/artigo-baptista-luz-pt-E-sports.pdf. Acesso em: 17 abr. 2020. "O cenário do e-sport ainda se encontra em crescimento e desenvolvimento. A novidade do tema apresenta desafios para institutos do Direito, seja pelo papel único na cadeia desportiva desempenhado pelas *publishers*, seja pela relação da matéria com o Direito esportivo."

[442] HENRIKSSON, Emil Albihn. Op. cit., jun. 2018. Disponível em: https://www.elgaronline.com/abstract/journals/ielr/1-1/ielr.2018.01.05.xml. Acesso em: 17 abr. 2020. "As tecnologias de realidade virtual, em

Dificilmente, porém, o jogador consente de maneira efetiva com a coleta de tais dados, fazendo-o de forma automática e desinformada, assim como ocorre com os *cookies* e com os termos e condições de uso, tratados nos tópicos anteriores, havendo igualmente risco de violação de seu direito à privacidade.

Dada a natureza desses dados, cumpre indagar se seriam, no âmbito do RGPD e das demais normas acerca da proteção de dados pessoais, considerados dados biométricos (nos termos do art. 4º do referido Regulamento) e, consequentemente, dados sensíveis, merecedores de proteção específica. Importante considerar, ainda, que muitas vezes os usuários de dispositivos de realidade virtual ou de *games* são menores de idade, e seus dados devem receber, igualmente, proteção específica[443].

Para que o usuário, no entanto, possa usufruir da melhor experiência possível, é incontornável a coleta e análise de uma série de dados. O cerne da questão, mais uma vez, está na forma como os dados são coletados, armazenados e tratados, e o respeito aos

---

particular fones de ouvido de ponta, como Oculus e HTC Vive, coletam dados sobre movimentos físicos e dimensões do usuário, incluindo, por exemplo, a direção, velocidade e ângulo do movimento da mão do usuário. Outros exemplos incluem a determinação da distância entre os olhos de uma pessoa e a altura relativa do fone de ouvido, a fim de proporcionar uma experiência imersiva e confortável. Em essência, os dados pessoais capturados são muito mais íntimos do que em um jogo normal. No horizonte há um processamento adicional, por exemplo, para permitir o rastreamento ocular e o rastreamento de gestos faciais. Este último foi especialmente considerado vital para os aspectos sociais da RV. Oculus já demonstrou a capacidade de expressar emoções através de gestos faciais. Embora isso tenha sido alcançado pelo uso de controladores, e não pelo rastreamento facial, o rastreamento facial real provavelmente não está longe. Como exemplo, a empresa britânica Emteq está desenvolvendo um sistema que pode rastrear as expressões faciais e emoções dos usuários usando sensores no revestimento interno de um fone de ouvido VR. O sensor Emteq lê a atividade muscular elétrica, frequência cardíaca, resposta da pele, detecção de movimento ocular e posição da cabeça. Olhando para o futuro, os avanços tecnológicos provavelmente permitirão o processamento de ainda mais dados e, por exemplo, já existem aplicativos disponíveis com sensores EEG. Continuamos nos estágios iniciais dessa nova geração de tecnologias de realidade virtual, mas já podemos ver que a coleta e o processamento de dados pessoais de natureza mais íntima do que antes são impulsionados por essas novas tecnologias." (Tradução livre). "*VR technologies, in particular higher end headsets such as Oculus and HTC Vive, collect data on physical movements and dimensions of the user, including for instance the direction, speed and angle of the user's hand motion. Other examples include determining the distance between a person's eyes and the relative height of the headset in order to provide an immersive and comfortable experience. In essence the personal data captured is much more intimate than with a normal game. On the horizon is further processing, for example to enable eye tracking and tracking of facial gestures. The latter especially has been posited as vital for the social aspects of VR. Oculus has already demonstrated the ability to express emotions through facial gestures. Although this was achieved by use of controllers rather than facial tracking, real facial tracking is likely not far away. As na example, UK company Emteq is developing a system that can track users' facial expressions and emotions using sensors on the inside lining of a VR headset. The Emteq sensor reads electrical muscle activity, heart-rate, skin response, eye movement detection and head position. Looking further into the future, technological advances will likely enable processing of even more data and there are, for instance, already applications out there with EEG sensors. We remain in the early stages of this new generation of VR technologies, but we can already see that collection and processing of personal data of a more intimate nature than before are driven by these new technologies."*

[443] Id., ibid. Disponível em: https://www.elgaronline.com/abstract/journals/ielr/1-1/ielr.2018.01.05.xml. Acesso em: 17 abr. 2020.

princípios da transparência, consentimento e finalidade[444] para que não se verifiquem violações ao direito à privacidade, passíveis de reparação.

2.8 *DEEP WEB* E *DARK WEB*

Ainda relacionado ao tema da privacidade, uma das formas mais simples de se evitar a coleta de dados e as informações de navegação é a utilização de janelas anônimas, recurso disponível, por exemplo, no navegador Google Chrome. Além dos sites convencionais, os quais fazem parte da *surface web*, ou internet de superfície, contudo,

[444] As mesmas questões são suscitadas quanto a sensores eletroencefalográficos, e dispositivos que registram, de uma forma geral, dados físicos sobre o usuário, como, por exemplo, batimentos cardíacos, associando-os a outros dados como horário e localização, permitindo, assim, identificar hábitos do indivíduo, como horário de sono, atividades realizadas, e lugares frequentados. Há estudos que apontam falhas de segurança em tais dispositivos. Nesse sentido: CHING, Ke Wan; SINGH, Manmeet Mahinderjit. Wearable technology devices security and privacy vulnerability analysys. *International Journal of Network Security & Its Applications (IJNSA)*, maio 2016, v. 8, n. 3. Disponível em: https://pdfs.semanticscholar.org/ed59/579757a718715ef61c3346a667257464d312.pdf. Acesso em: 17 abr. 2020. "Os dispositivos ou sensores 'vestíveis' [*wearable sensors*] são frequentemente combinados com os outros sensores para detectar atividades humanas da vida diária (ADL), como caminhar, correr, sentar e comer. Existem muitas aplicações possíveis para o reconhecimento de atividades com tais sensores, por exemplo, nas áreas da saúde, assistência a idosos, condicionamento físico, entretenimento ou artes cênicas. Diferentes sensores são implantados em dispositivos com sensores que podem ser vestidos [*relógios, pulseiras, colares, entre outros*], dependendo do tipo de informação de monitoramento de atividade a ser coletada. [...] O Samsung Smartwatch é outro *wearable sensor* que oferece funcionalidades inovadoras significativas que aprimoram a vida diária das pessoas. De fato, o maior ponto de venda são os recursos de notificação no Android Wear Smartwatch. Ele permitiu sincronizar dados com o telefone e todos os alertas e notificações importantes serão mostrados diretamente no pulso. No entanto, de acordo com um estudo recente da HP [...] dentre os 10 principais Smartwatches mais populares do mercado, 100% dos dispositivos testados contêm vulnerabilidades significativas, incluindo má autenticação, falta de criptografia e problemas de privacidade. [...] Três em cada dez relógios ficaram vulneráveis à coleta de contas [*harvesting*], que é um ataque que obtém acesso ao dispositivo e aos dados, procurando senhas fracas e sem bloqueio de conta. [...] questões de segurança e privacidade podem ser as principais razões disso. Isso pode levar a sérias violações e perdas se a vulnerabilidade de segurança não for tratada adequadamente. A perda pode ser um ativo estático, como arquivos ou documentos, ou um ativo dinâmico, como o número do cartão de crédito. No final, isso causará perda de dados e perda financeira, ou mesmo problemas de segurança." (Tradução livre). "*Wearable sensors are often combined with the other sensors to detect human activities of daily living (ADL) such as walking, running, sitting and eating. There are many possible applications for activity recognition with wearable sensors, for instance in the areas of healthcare, elderly care, personal fitness, entertainment, or performing arts. Different sensors are deployed on wearable devices depending on what kind of activity monitoring information to be collected. [...] Samsung Smartwatch is another wearable device that offers significant innovative functionalities that makes the enhancement of people's daily life. In fact, the biggest selling point is the notification features in Android Wear Smartwatch. It has enabled to synchronize data to the phone and all the important alert and notifications will get pushed directly on the wrist. However, according to an HP recent study […] on top 10 popular Smartwatches in the market, found that 100 percent of the tested Smartwatches contain significant vulnerabilities, including poor authentication, lack of encryption and privacy issues. […]. 3 in 10 watches were vulnerable to account harvesting, which is an attack that gain access to the device and data by looking for weak passwords and lack out account lockout. [...] Security and privacy issues could be the major reasons of it. It can lead to the serious breach and loss if the security vulnerability is not handled properly. The loss could be either static assets such as files, documents or dynamic asset like credit card number. At the end, it will cause data and financial loss or even safety issues."*

existem, também, a *deep web* e a *dark web*, que permitem um nível maior de anonimato do usuário.

A *surface web* corresponde a toda a parte da Internet indexada, ou seja, abarca quaisquer domínios que possam ser encontrados por sites de busca, os quais podem ser acessados livremente por todo o público. Não obstante, estima-se que estes sites correspondam a, efetivamente, menos de cinco por cento de todo o conteúdo disponibilizado *online*: o restante do conteúdo somente pode ser acessado por meio da *deep web* ou da *dark web*, com a utilização de redes específicas criptografadas, as quais permitem que a identidade do usuário seja ocultada, como é o caso dos softwares Tor[445], i2p e FreeNet.

Os endereços hospedados na *deep web* não estão indexados, e não podem ser encontrados a partir de sites de busca, como o Google, Bing ou outros. O número de IP (*Internet Protocol*) do usuário, por sua vez, é ocultado, assim como as suas demais informações e dados. Existe uma infinidade de informações disponíveis na *deep web*, de modo que seus usuários não estão necessariamente envolvidos em situações ilegais, ao contrário do que se pensa. É possível encontrar todo o tipo de dados e de informações – inclusive alguns duvidosos ou mesmo ilegais.

A *deep web* permite o armazenamento de dados importantes à manutenção da própria rede, bem como de informações sigilosas, cujo acesso é restrito àqueles que possuem tanto o endereço quanto as credenciais necessárias. Alguns exemplos são registros médicos, bancos de dados acadêmicos, informações de interesse ou segurança nacional, registros financeiros, entre muitos outros. O objetivo é, muitas vezes, proteger ou restringir o acesso a informações e dados específicos[446].

---

[445] A palavra "Tor" é, em verdade, uma sigla que corresponde a "*The Onion Router*": trata-se de um *software* livre que, ao criar uma cadeia de redes abertas, permite ao usuário navegar de forma oculta (criptografada). Enquanto na *surface web* os domínios costumam acabar com "*.com*", na rede Tor eles se caracterizam pela finalização "*.onion*". Ao acessar um domínio, o pedido do usuário passa por vários servidores, localizados em diferentes países, criando uma teia que impede o rastreamento. A rede surgiu a partir de um projeto financiado pelo governo dos Estados Unidos, e visa à transmissão de informações sigilosas.

[446] Mesmo *softwares* que visam o sigilo ou anonimato, como o Tor, são questionáveis do ponto de vista da segurança: FARQUHAR, Peter. An FOI request has revealed 'anonymous' browser Tor is funded by US government agencies. *Business Insider Australia*, 02 mar. 2018. Disponível em: https://www.businessinsider.com.au/claims-tor-funded-by-us-government-agencies-2018-3. Acesso em: 17 abr. 2020. "O navegador anônimo Tor pode não ser de fato anônimo, depois que um jornalista recebeu uma solicitação de informações de 2.500 páginas, no qual alega-se que receberia financiamento do governo dos EUA. A jornalista investigativa norte-americana, Yasha Levine, ex-repórter do Pando Daily e autora de um novo livro, 'Surveillance Valley: The Secret Military History of the Internet', está em uma missão para expor as alegações de anonimato de Tor desde o final de 2015. Desenvolvido pelo The Tor Project e lançado em 2002, o Tor defende o sistema de 'roteamento de cebola' - basicamente devolvendo sua solicitação de conexão à Internet através dos computadores de muitos outros usuários antes de finalmente ligar através de um 'nó de saída'." (Tradução livre). "*Anonymous web browser Tor might not be anonymous at all, after a journalist was*

A *dark web*, por sua vez, corresponde à parcela da *deep web* que de fato envolve situações ilegais ou criminosas, desde tráfico de drogas, pessoas e órgãos, até pedofilia e assassinatos[447]. A chamada "zona escura da Internet" conta com uma criptografia especialmente complexa com vistas a evitar que usuários leigos possam chegar até ela. A maioria dos domínios possui um nome aleatório, formado por sequências de letras e números sem sentido ou ordem específica (*strings*), o que evita qualquer identificação.

Ainda no sentido de evitar o rastreamento ou a identificação, as transações feitas pela *deep web* e, principalmente, da *dark web*, costumam ser realizadas com o uso de criptomoedas, como as já mencionadas Bitcoins. Em resumo, a *deep web* (*dark web*, inclusive) é uma forma de navegação segura e anônima, pois visa à proteção da identidade do usuário e das informações e dados compartilhados – sejam eles ilegais ou não.

Neste ambiente há obstáculos à localização das partes devido ao mencionado sistema de redirecionamento, bem como à sua identificação, consideradas as medidas de segurança para o acesso a tais redes. Resta dificultada, portanto, a responsabilização por atos cometidos na *deep web* ou *dark web*, embora existam precedentes nesse sentido, como o caso do criador do mercado *Silk Road* (vide nota anterior).

Em caso de violação da privacidade por meio da *deep web*, há dificuldade na responsabilização, identificação e localização das partes envolvidas, justamente por se tratar de modo de navegação, cuja característica é a segurança das informações dos usuários. Conforme demonstra o caso da *Silk Road*, ainda que a identificação e a responsabilização sejam difíceis, ela não é impossível ou inviável tecnicamente. Em situações que fogem ao âmbito criminal, contudo, e que ficam cingidas a violações de direitos de personalidade, como o direito à privacidade, há obstáculos significativos à responsabilização.

---

granted a 2500-page Freedom of Information request that claims it receives funding from the US government. Russian-born US investigative journalist Yasha Levine, a former reporter for Pando Daily and author of a new book, Surveillance Valley: The Secret Military History of the Internet", has been on a mission to expose Tor's claims of anonymity since late 2015. Developed by The Tor Project and launched in 2002, Tor champions the system of 'onion routing' – basically bouncing your internet connection request through many other users' computers before finally hooking up through an 'exit node'."

[447] ESTADOS UNIDOS. USA x Ross William Ulbricht. Case 1:14-cr-00068-KBF, 02 maio 2015. Disponível em: https://www.docketalarm.com/cases/New_York_Southern_District_Court/1--14-cr-00068/USA_v.Ulbricht/183/. Acesso em: 17 abr. 2020. O mercado *Silk Road* operava atividades ilegais (principalmente tráfico de drogas) por meio da *deep web*, utilizando a rede Tor para garantir o anonimato do seu criador e usuários. Apesar das medidas de segurança a fim de evitar a identificação, o criador do site, Ross William Ulbricht (conhecido pelo pseudônimo *Dread Pirate Roberts*), foi condenado à prisão perpétua, e o site foi fechado pelo FBI. Ulbricht foi acusado, em agosto de 2014, dos crimes de lavagem de dinheiro, invasão de computadores e conspiração para traficar drogas. Em sede de sentença foram incluídas, também, evidências relativas a assassinatos encomendados.

2.9 DANOS E RESPONSABILIDADE CIVIL NO BRASIL: PRIVACIDADE E PROTEÇÃO DE DADOS

Os temas relacionados à privacidade e à proteção de dados passaram a ser discutidos no Brasil, principalmente a partir de 2014, ano da Lei n.º 12.965, conhecida como Marco Civil da Internet – primeiro diploma normativo a tratar especificamente sobre a *internet* no país. Mas foi apenas na LGPD que os dados foram efetivamente conceituados e regulamentados, de modo que, com a iminência da vigência da Lei, a perspectiva é de que seus princípios já comecem a ser incorporados[448].

Cumpre mencionar que o Projeto de Lei n.º 3.420/2019, atualmente na Câmara dos Deputados, aguarda parecer do Relator na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI). O PL propõe a alteração da LGPD, a fim de modificar o critério da multa aplicada às entidades de direito privado em casos de vazamento de dados pessoais. Em outras palavras, a ideia é limitar a multa aplicada a empresas em tais hipóteses a 2% do faturamento no país em seu último exercício, excluídos os tributos até o limite de R$ 50 milhões. O texto do PL elimina a expressão "por infração" que atualmente consta n LGPD[449].

O PL, apresentado em junho de 2019, foi elaborado no contexto do caso da Atlas Quantum, empresa de criptomoedas responsável pelo episódio de vazamento de dados pessoais. O Ministério Público do Distrito Federal e Territórios (MPDFT) ajuizou ação civil pública por danos morais coletivos em face da empresa no âmbito do seu Tribunal de Justiça[450]. O MP formulou, na petição inicial, pedido de condenação das empresas

---

[448] Como exemplo de demanda que envolve a proteção de dados e o consentimento, é possível mencionar decisão proferida nos autos de Ação Civil Pública, determinada pela Justiça Federal de São Paulo, no sentido de orientar a Microsoft a adequar o Sistema Operacional Windows 10, com a finalidade de proporcionar ao usuário, de forma simples e fácil, a optar pelo não fornecimento de dados à empresa: "Ante o exposto, DEFIRO em parte e, em menor extensão, a tutela antecipada requerida, para determinar que a Microsoft adote procedimentos específicos, no prazo de 30 (trinta) dias, de modo a permitir que o usuário do Sistema Operacional Windows 10, em caso de não autorizar o uso de seus dados, tenha ferramenta operacional e de interface que permita o exercício de tal opção e tanto quanto a interface operacional que permite a atualização do sistema com a forma simples, fácil e direta, sem autorização da coleta de dados do usuário." (TRF3. Justiça Federal da 3ª Região. 9ª Vara Cível Federal de São Paulo. *Ação Civil Pública n.º 5009507-78.2018.4.03.6100.* Sentença proferida em 27 abr. 2018, por Cristiane Farias Rodrigues dos Santos).

[449] BRASIL. Câmara dos Deputados. *PL 3.420/2019*. Altera o a Lei nº 13.709, de 14 de agosto de 2018, a fim de alterar o critério da multa aplicada às entidades de direito privado em caso de vazamento de dados pessoais. Autoria de Heitor Freire (PSL/CE), apresentado em 11 jun. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2207337. Acesso em: 09 mar. 2020.

[450] DINHEIRO DIGITAL. *Atlas não quis acordo, agora é com o Ministério Público.* Petição inicial. Disponível em: https://www.mpdft.mp.br/portal/pdf/A%c3%a7%c3%a3o_civil_por_danos_ coletivos_Atlas.pdf. Acesso em: 21 dez. 2019.

pertencentes ao grupo econômico ao pagamento de R$ 10 milhões em decorrência do vazamento de dados de mais de 260 mil clientes em agosto de 2018[451].

A Lei Geral de Proteção de Dados prevê, como apontado, sanções às empresas responsáveis por episódios de vazamento de dados, as quais passarão a ser aplicáveis a partir de agosto de 2020, cumprindo às empresas se adaptarem com antecedência aos requisitos de segurança da Lei a fim de evitar a aplicação de tais sanções.

A LGPD criou parâmetros que devem ser observados tanto por empresas públicas quanto privadas, a fim de garantir a segurança da informação, uma vez que, até então, a regulamentação do tema era escassa, embora os conflitos envolvendo a Internet viessem crescendo constantemente[452].

Exemplo disso é a investigação iniciada pela Comissão de Dados Pessoais do Ministério Público do Distrito Federal e Territórios para apurar a possível má utilização que farmácias estão fazendo dos dados de seus clientes[453]. Os dados seriam fornecidos em troca de descontos, CPF, principalmente, e poderiam estar sendo repassados ou vendidos. Assim, as compras feitas por cada consumidor estariam sendo divulgadas a empresas de planos de saúde e análise de crédito[454].

---

[451] BRASIL. Ministério Público do Distrito Federal e Território (MPDFT). *Vazamento de dados leva MPDFT a ajuizar ação contra grupo que explora criptomoedas*, 26 abr. 2019. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10794-vazamento-de-dados-leva-mpdft-a-ajuizar-acao-contra-grupo-que-explora-criptomoedas. Acesso em: 17 abr. 2020.

[452] BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel da. A coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral de Proteção de Dados. *RJLB*, ano 5, 2019, nº 6, pp. 473-514, p. 483 e ss. "Após a Internet ter chegado no Brasil em 1988, surgiram algumas condutas nocivas aos usuários do ambiente virtual que não eram abordadas pela legislação nacional. Começaram, então, a surgir Projetos de Lei que versavam sobre a criminalização e a tutela da privacidade na internet, como por exemplo, o PL 84/1999, que propunha a criminalização de ataques praticados por *crackers* e *hackers* e a utilização indevida de senhas; e o PL 151/2000, que cuidava do acesso à internet e a guarda de dados de usuários brasileiros em *datacenters* instalados no Brasil. Isso demonstra que já existia uma preocupação emergente àquela época sobre a tutela de novas situações decorrentes do avanço tecnológico da sociedade. Hodiernamente, o número de pessoas conectadas à *web* cresce a cada ano. Conforme pesquisa realizada com dados de 2016 e divulgada em fevereiro do ano em curso pelo Instituto Brasileiro de Geografia e Estatísticas – IBGE, cerca de 70% dos domicílios no país têm acesso à Internet, sendo o celular o equipamento mais utilizado para tal acesso em 97,2% desses domicílios. Ademais, 116 milhões de brasileiros estão conectados à rede, o que equivale a 64,7% de toda a população (acima de 10 anos). Cerca de 95% dos brasileiros utilizam a Internet com o objetivo de trocar mensagens de texto, voz e imagens por aplicativos. [...]. Porém, em contrapartida ao avanço do número de usuários com acesso à rede mundial de computadores, bem como essa tendência em garantir o acesso aos cidadãos, alguns problemas críticos de violação à privacidade passaram a ser também cada vez mais corriqueiros."

[453] LUIZ, Gabriel. *CPF em troca de desconto:* MP investiga venda de dados de clientes por farmácias, 16 mar. 2018. G1. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 17 abr. 2020.

[454] BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel da. Op. cit., 2019, p. 495. "Por exemplo, até mesmo o fato de um cidadão informar seu CPF numa farmácia pode lhe custar muito caro. Isso porque todos os medicamentos que ele adquire ficarão atrelados ao seu CPF. E se a farmácia fornecer os dados desse cidadão a uma empresa de plano de saúde? Com base no tratamento dos dados sobre os

O Ministério Público do Rio de Janeiro, por sua vez, ajuizou ação civil pública por danos morais coletivos à empresa Decolar.com, a qual realiza a venda de passagens aéreas. A acusação trata da prática de *geoblocking*, ou seja, o bloqueio da oferta de passagens com base na origem geográfica do consumidor, bem como *geopricing*, implicando a precificação diferenciada com base na localização do usuário, com caráter discriminatório[455].

A ação ainda não foi julgada, contudo, a prática de *geoblocking* é comumente aceita por ser uma forma de levar em conta custos associados à localização de cada consumidor, como, por exemplo, custos de natureza fiscal, não sendo necessariamente discriminatória, como aduzido pelo MPRJ[456].

Em agosto de 2018 ocorreu um caso que envolveu a Linha Amarela do Metrô de São Paulo (SP) e o Instituto Brasileiro de Defesa do Consumidor (IDEC), em que o Tribunal de Justiça de São Paulo determinou o fim da coleta de dados faciais pela concessionária responsável (ViaQuatro). Houve, assim, a retirada das câmeras e dos painéis publicitários, os quais permitiam o reconhecimento facial dos passageiros. Neste caso, embora a LGPD ainda não estivesse vigente, ela foi utilizada como uma das bases legais para o ajuizamento da Ação Civil Pública pelo Idec[457].

É preciso levar em consideração, ainda, a utilização da Internet por crianças e adolescentes[458] – consideradas pessoas em desenvolvimento e vulneráveis, as quais

---

medicamentos adquiridos, tal plano poderia, porventura, traçar um perfil desse cidadão e, inclusive, identificá-lo como pertencente a algum grupo de risco, com o intuito de cobrar um valor de mensalidade mais alto."

[455] MIGALHAS. *MP/RJ acusa Decolar.com de manipular preços para discriminar brasileiros:* ACP requer reparação de R$ 57 milhões por danos morais coletivos. 2018. Disponível em: https://www.migalhas.com.br/Quentes/17,MI273955,91041-MPRJ+acusa+Decolarcom+de+manipular+precos+para+discriminar+brasileiros. Acesso em: 17 abr. 2020.

[456] VAINZOF, Rony. Geopricing é ilegal? *JOTA*. Disponível em: //www.jota.info/opiniao-e-analise/colunas/direito-digital/geopricing-e-ilegal-12012017. Acesso em: 01 jul. 2020.

[457] IDEC. Instituto Brasileiro de Defesa do Consumidor. *Ação Civil Pública com Pedido de Tutela de Urgência.* Petição inicial. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 17 abr. 2020.

[458] VAAS, Lisa. Two schoolkids sue Google for collecting biometrics. *Naked Security,* 07 abr. 2020. Disponível em: https://nakedsecurity.sophos.com/2020/04/07/two-schoolkids-sue-google-for-collecting-biometrics/. Acesso em: 18 abr. 2020. Merece destaque a utilização da Internet por crianças e adolescentes para fins educacionais, muitas vezes por intermédio ou por orientação da própria escola: "Mesmo antes de o COVID-19 enviar as escolas para um curso intensivo sobre aprendizado remoto, e para a adoção das ferramentas que as empresas oferecem para que isso aconteça, o Google estava analisando uma ação legal sobre as implicações de privacidade dos estudantes que usam Chromebooks que utilizam o G Suite for Education. Em fevereiro, o procurador-geral do Novo México, Hector Balderas, processou o Google por suposto mau uso de dados com os laptops. Como o processo do BIPA aberto na semana passada, Balderas acusou o Google de coletar secretamente informações, incluindo informações de localização geográfica dos alunos, histórico da Internet, termos que os estudantes pesquisaram no Google, vídeos que assistiram no YouTube, listas de contatos pessoais, senhas salvas, gravações de voz e mais, violando a COPPA. O Google já havia sido multado por agredir a privacidade de crianças alguns meses antes do processo do Novo México.

merecem a proteção específica da Lei. Conforme estudo elaborado pelo Internetlab, as crianças constituem cerca de um terço dos usuários de Internet no mundo e, no Brasil, 82% das crianças acessam a rede[459].

Nestes casos, o consentimento para a coleta e tratamento de dados é especialmente importante, e a sua forma de obtenção deve observar o respeito às garantias constitucionais e àquelas constantes no Estatuto da Criança e do Adolescente[460]. Tais questões se mostram problemáticas, especialmente em relação à verificação da validade do consentimento[461].

Justifica-se, portanto, o fato de a LGPD haver dedicado uma seção exclusivamente aos dados de crianças e adolescentes: a Seção III da Lei evidencia o princípio do melhor

---

Em setembro de 2019, a Federal Trade Commission (FTC) multou a empresa em US $ 170 milhões por sugar ilegalmente os dados das crianças para que pudesse segmentá-las com anúncios." (Tradução livre). "*Even before COVID-19 sent schools reeling into a crash course on remote learning and an embrace of the tools companies offer to make it happen, Google was looking at legal action over the privacy implications of students using its free G Suite for Education-loaded Chromebooks. In February, New Mexico Attorney General Hector Balderas sued Google over alleged data slurping with the laptops. Like the BIPA lawsuit filed last week, Balderas accused Google of secretly collecting information including students' geolocation information, internet history, terms that students have searched for on Google, videos they've watched on YouTube, personal contact lists, saved passwords, voice recordings, and more, in violation of COPPA. Google had already been fined over blowing kids' privacy a few months prior to New Mexico's suit. In September 2019, the Federal Trade Commission (FTC) fined the company $170 million for illegally sucking up kids' data so it could target them with ads."*

[459] INTERNETLAB. *Especial Apps para crianças*. Disponível em: http://www.internetlab.org.br/pt/projetos/especial-apps-para-criancas/. Acesso em: 17 abr. 2020.

[460] BRASIL. *Lei n.º 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 17 abr. 2020.

[461] MOZETIC, Vinícius Almada; BABARESCO, Daniele Vedovatto Gomes da Silva. Lei Geral de Proteção de Dados de Crianças e Adolescentes no Brasil: coleta de dados e o problema da obrigatoriedade do consentimento dos pais. *A Era Digital e os direitos das crianças e adolescentes*, 2020. Disponível em: https://www.academia.edu/42044798/LGPD_E_A_OBRIGATORIEDADE_DO_CONSENTIMENTO_NA_COLETA_DE_DADOS_DE_CRIAN%C3%87AS_E_ADOLESCENTES_NO_BRASIL. Acesso em: 17 abr. 2020. "[...] crianças estão menos conscientes dos riscos e consequências do compartilhamento de dados e de seus direitos e qualquer informação endereçada de maneira específica a uma criança ou adolescente deve ser adaptada para ser facilmente acessível e com transparência de informações. [...] Em relação à privacidade e à proteção de dados de crianças e adolescentes, a questão é ainda mais polêmica. Os problemas advindos do uso abusivo dos dados pessoais, relacionados à assimetria informacional, são potencializados quando o sujeito está em uma situação de vulnerabilidade [...]. Os serviços *online*, atualmente e na sua grande maioria, exigem o consentimento dos pais ou responsáveis para processar os dados pessoais de uma criança com base no consentimento até certa idade. No Brasil, o limite estabelecido, segundo o Estatuto da Criança e do Adolescente, são pessoas com até 12 (doze) anos de idade incompletos. Por esta razão, o tratamento de dados pessoais de crianças e adolescentes, bem como a transferência de dados a terceiros só podem ocorrer com o consentimento especial, ou seja, por pelo menos 01 (um) dos pais ou responsável legal. Existe uma grande dificuldade, mesmo com toda a tecnologia à disposição, sobre a verificação deste consentimento e se ele está realmente em consonância com a lei. [...] Não está claro quanto esforço e prova em relação à obtenção de consentimento podem ser solicitados aos controladores em situações em que há dificuldade para adquirir o consentimento parental. [...] O fato de a LGPD não se referir à verificação da idade não é surpreendente em si. Num primeiro momento, o tema da verificação de idade levanta uma temática importante: questões sensíveis e não resolvidas relacionadas com o anonimato *online*, liberdade de expressão e expressão, e privacidade de crianças e adultos *online*. A ideia de que todos os usuários de internet em todos os sites pudessem ser convidados a fornecer sua idade (ou ainda se identificar) poderia não só levar ao aumento da coleta de dados pessoais, mas também pode ser visto como *des*-proporcional."

interesse do menor, bem como o consentimento específico necessário em tais casos (concedido pelos pais ou representante legal).

Os parágrafos do art. 14 trazem, portanto, as condições específicas para o tratamento de dados de menores, ressaltando que as informações a respeito devem ser fornecidas de "maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado [...]"[462].

Além do Estatuto da Criança e do Adolescente (ECA) e das disposições específicas trazidas pela LGPD, cumpre ressaltar, ainda, a Convenção sobre os Direitos das Crianças[463], devidamente internalizada no Brasil, e cujas normas protetivas dos menores devem ser igualmente levadas em consideração ao se interpretar o conteúdo da Seção III da LGPD.

Por vezes, a coleta de dados é de interesse do próprio usuário: diversos programas utilizam algoritmos capazes de avaliar as opções e interesses dos usuários e realizar sugestões de sua preferência – seja para a venda de produtos ou para personalizar a experiência do usuário, como ocorre com o *Spotify* (plataforma musical), *YouTube* (plataforma de vídeos) ou com o *Netflix* (plataforma de filmes e séries). Em todos esses casos o usuário consente com a coleta e tratamento de seus dados, o que permite que tenha uma experiência melhor com o site ou aplicativo.

Existe, portanto, tanto o consentimento do indivíduo quanto a transparência sobre a coleta dos dados. O problema e, consequentemente, a ocorrência do dano, está nas situações em que não houve consentimento, ou este foi falho ou, ainda, quando falta transparência acerca da finalidade do tratamento dos dados[464].

---

[462] BRASIL. Op. cit. *Lei n.º 13.709, de 14 de agosto de 2018,* art. 14, § 6º.

[463] BRASIL. *Decreto n.º 99.710, de 21 de novembro de 1990*. Promulga a Convenção sobre os Direitos da Criança. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm. Acesso em: 17 abr. 2020.

[464] Há, ainda, possibilidade de utilização indevida de dados ou informações por outros indivíduos, como no caso de divulgação não autorizada de imagens, já mencionado anteriormente (cuja sanção penal não afasta condenação na área cível, mas, pelo contrário, a corrobora) ou, também, no caso de divulgação de mensagens ofensivas. Nesse sentido, veja: STJ. Superior Tribunal de Justiça. I*nformativo n.º 495, de 9 a 20 de abril de 2012*, 3ª Turma, REsp 1.306.066-MT, rel. Min. Sidnei Beneti. "RESPONSABILIDADE CIVIL. SITE DE RELACIONAMENTO. MENSAGENS OFENSIVAS. A responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC, não se aplica à empresa hospedeira de site de relacionamento no caso de mensagens com conteúdo ofensivo inseridas por usuários. O entendimento pacificado da Turma é que o dano decorrente dessas mensagens não constitui risco inerente à atividade dos provedores de conteúdo. A fiscalização prévia do teor das informações postadas pelo usuário não é atividade do administrador de rede social, portanto seu dever é retirar do ar, logo que for comunicado, o texto ou a imagem que possuem conteúdo ilícito, apenas podendo responder por sua omissão. Precedentes citados: REsp 1.186.616-MG, DJe 31/8/2011, e REsp 1.175.675-RS, DJe 20/9/2011. REsp 1.306.066-MT, Rel. Min. Sidnei Beneti, julgado em 17/4/2012. (g.n.)"

Presentes os elementos necessários à responsabilização civil, há o dever de reparação ou indenização da vítima. Nesse sentido, cumpre salientar que a função da responsabilidade civil no Direito brasileiro é, principalmente, reparatória – não havendo dispositivo legal que autorize ou indique função punitiva em qualquer sentido.

O dano, seja ele transnacional ou não, é apenas um dos elementos da responsabilidade civil[465]. Assim, para que exista o dever de reparação há uma série de elementos que devem ser identificados e levados em consideração de forma geral: (i) dano; (ii) conduta (ação ou omissão); (iii) relação de causalidade (ou nexo causal); e (iv) culpa do agente (ressalvadas as hipóteses de responsabilidade objetiva).

Constatada a ocorrência do dano, e sempre que se tratar de uma situação transnacional ou que estiverem em questão dados plurilocalizados, cumpre determinar a lei aplicável às partes, bem como o tribunal competente, ensejando, assim, a abordagem pela ótica do Direito Internacional Privado.

2.10 CONCLUSÕES PARCIAIS

Nos tópicos anteriores foram expostas algumas questões centrais às discussões que envolvem a Internet e a proteção da infinidade de dados coletados, tratados e armazenados constantemente[466]: observe-se, por exemplo, que a classificação de contratos eletrônicos surge como um aspecto importante em termos do Direito Internacional Privado devido, principalmente, à sua relação com a qualificação do objeto da lide. Igualmente, se tratando de um contrato, importante saber se relativo a bem ou a serviço.

Interessa, ainda, conhecer o Direito Material aplicável à matéria segundo cada ordenamento, uma vez que o caráter transnacional da transferência e o tratamento de dados

---

[465] BITTAR, Carlos Alberto. *Responsabilidade civil* – Teoria e prática. 5. ed. Rio de Janeiro: Forense Universitária, 2005; CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil*. 7. ed. São Paulo: Atlas, 2007; PEREIRA, Caio Mário da Silva. *Instituições de Direito Civil*. 11. ed. Rio de Janeiro: Forense, 2004. v. III.

[466] ABRUSIO, Juliana. O direito ao esquecimento na Internet e a (im)possibilidade de recomeçar. *CESA – Anuário*, 2013, v. 1, pp. 17-26, pp. 22-23. "Assim como predito também no romance de George Orwel "1984", na atualidade, é constante a sensação de sempre estarmos sendo vistos. Constantemente nos deparamos com registros a respeito do que fazemos ou deixamos de fazer, expostos na Internet, sem nunca termos tido a chance de autorizar tal divulgação. Somos, de certa forma, vigiados. Não por um vigia apenas, constituído para essa função, mas para quem bem entender nos observar, pelo governo, por entidades privadas ou outros indivíduos – basta o acesso à Internet (que digam os *yankees*). As ferramentas e serviços da Internet acarretam novos níveis de indiscrição. Muito do que escrevemos ou daquilo que dizem a nosso respeito na Internet fica em arquivos digitais públicos e permanentes. Os vários dispositivos eletrônicos móveis e serviços informáticos são capazes de capturar nossas palavras e ações, registrando-as de modo perene e compartilhando-as em segundos. Assim, ao invés de serem esquecidos, os registros do passado se mantêm em armazenamentos digitais, a menos, ou até, que sejam apagados por alguém."

agrega internacionalidade aos conflitos gerados, e a lei aplicável pode ser mais ou menos favorável às partes. Nesse sentido, resta clara a importância, igualmente, sobre consentimento, *cookies* e termos de uso gerados automaticamente: o domicílio da empresa e o local de seu registro ou de seus servidores poderá influir diretamente sobre a jurisdição competente e sobre a lei aplicável, cujas questões são tratadas com mais detalhes na próxima parte desta pesquisa.

Em tais situações vislumbra-se a possibilidade de *forum shopping*, que nada mais é do que a escolha (direta ou indireta) do tribunal ou jurisdição mais favorável para solucionar um litígio[467]. O benefício pode ser em termos de custos do processo, ou mesmo para facilitar a incidência de normas processuais ou materiais mais favoráveis. Em muitos casos, tal escolha é lícita e permitida, constituindo estratégia contenciosa; em outros, contudo, configura-se abusividade[468].

Assim, podem resultar verdadeiros "paraísos jurisdicionais": plataformas seguras do ponto de vista legislativo e institucional, nas quais uma regulação mais leniente atrairia empresas destinadas a oferecer determinados produtos e serviços *online*[469]. As questões

[467] TIBURCIO, Carmen. *Extensão e limites da jurisdição brasileira:* competência internacional e imunidade de jurisdição. Salvador: JusPodivm, 2006, p. 143 e ss. "O fato de um litígio ser submetido ao juiz brasileiro, e não ao juiz inglês, poderá acarretar uma substancial diferença na solução da lide. O juiz brasileiro irá solucioná-la em conformidade com as regras de conexão brasileiras – caso não haja escolha da lei pelas partes; já o juiz inglês irá resolver o litígio com base nas regras de conexão inglesas, que não são necessariamente idênticas às brasileiras. Assim, o local do julgamento irá influir no seu desfecho, já que a lei substantiva a ser aplicada em cada caso poderá ser diferente. Ou seja, a jurisdição influi na determinação da lei aplicável. Nesse sentido, como o desfecho pode variar em função do local da propositura da ação, antes do seu ajuizamento deve-se verificar qual a melhor jurisdição, dentre aquelas que são competentes no plano internacional, para conhecer o litígio. Isso significa que, antes de uma ação ser ajuizada, o autor deverá analisar as vantagens e as desvantagens de cada jurisdição potencialmente competente para conhecer do litígio em questão e, diante das soluções vislumbradas, deverá escolher o melhor lugar para a demanda. [...] Vale notar que nem todos os países necessariamente vislumbram o *forum shopping* como uma inconveniência. Alguns vêem nesta procura um sinal de que os estrangeiros reconhecem que o sistema judiciário local é bastante desenvolvido e célere."

[468] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 119-120. "No domínio da internet, essas práticas são comuns, embora as cláusulas de eleição de foro sejam frequentemente limitadas pelas normas do ordenamento jurídico do Estado de destino, evitando, assim, abusividades. Mais preocupante e relevante para as questões de jurisdição e internet são as hipóteses em que um determinado serviço ou conteúdo sediado em um país de legislação menos restritiva seja acessível em todo o mundo, por indivíduos em países distintos. A viabilidade da prática de *forum shopping* em litígios envolvendo Internet requer que as regras de escolha de jurisdição estejam exclusivamente concentradas no país de origem das atividades *online* em questão. A abordagem do país de origem é uma das várias propostas para a resolução de conflitos de jurisdição, e é favorecida, principalmente, por provedores de conteúdo *online*, que apontam a previsibilidade e a segurança jurídicas para todos os atores envolvidos como as principais vantagens do método."

[469] Id., ibid., pp. 119-120. "A indústria de jogos de azar via Internet é o caso mais concreto do surgimento desses paraísos, com exemplos muito claros de países, territórios ou regiões, que reduziram padrões normativos e regulatórios, em seus respectivos sistemas jurídicos domésticos, para atrair empreendimentos dessa natureza. Destacam-se, nesse sentido, a Ilha de Man, a cidade de Gibraltar, ambos territórios do Reino Unido. De forma análoga aos chamados 'paraísos fiscais', os paraísos jurisdicionais favorecem, de maneira desequilibrada, as empresas ou indivíduos que buscam realocar seus bens, ativos, negócios, para outros

relativas à competência ou jurisdição internacional e lei aplicável ganham, consequentemente, especial relevância.

Além dos aspectos de Direito Material e questões controversas expostas, há duas questões que parecem ser centrais no desenvolvimento desta segunda parte do estudo. Primeiramente, devido às implicações em termos de qualificação, há necessidade da retomada da discussão acerca da natureza dos dados transmitidos e armazenados com o uso da Internet. Justifica-se a análise da natureza jurídica dos dados como bens imateriais ou como direitos se consideradas as consequências de qualificar-se de uma ou de outra forma.

Assim, em casos nos quais a qualificação se dá pela *lex causae*, o ordenamento estrangeiro poderá conferir tratamento jurídico distinto à questão, o que deverá ser levado em consideração, mesmo quando o juiz nacional for considerado competente para decidir o conflito. A qualificação e o tratamento jurídico resultante poderão coincidir ou não entre os ordenamentos, evidenciando a sua relevância ao Direito Internacional Privado.

Conclui-se, ao final desta segunda parte, que quando a qualificação se der pela *lex fori*, atendendo à regra geral, ou mesmo em consequência da aplicação dos arts. 8º ou 9º da LINDB, os temas relacionados à proteção de dados, privacidade e intimidade serão enquadrados como direitos. Por outro lado, ao qualificar-se pela *lex causae*, o resultado dependerá das previsões específicas do ordenamento estrangeiro, sendo possível que a lei aplicável para reger um bem (imaterial) seja distinta daquela que rege uma obrigação.

Além de tal distinção, constatou-se, também, a importância da análise do momento da formação dos contratos, o que permite classificar, de forma adequada, as suas obrigações decorrentes, sejam contratos entre presentes ou entre ausentes.

Embora haja entendimento sobre a qualificação dos contratos celebrados entre ausentes, é imprescindível considerar a possibilidade de que as partes estejam ausentes no espaço, mas presentes no tempo – situação que não ocorria anterior à Sociedade da Informação e ao desenvolvimento de novas tecnologias de comunicação – e que, após,

---

países, diferentemente daqueles de sua nacionalidade, sede ou residência habitual, como forma de evasão regulatória ou de minimizar efeitos de políticas regulatórias de outros Estados. Com essa estratégia, as partes incorrem em ações de *law shopping*, que se difere de *forum shopping*, pois o objetivo daquele é o de buscar sistemas legais que sejam mais favoráveis do ponto de vista regulatório, e não necessariamente tribunais mais eficientes ou especializados para adjudicação de litígios privados. Fator adicional que contribui para o surgimento e fortalecimento desses paraísos é a dificuldade de execução de decisões proferidas na jurisdição do domicílio ou residência habitual de um possível demandante. Em diversos casos, tribunais locais afirmaram sua jurisdição sobre atos e condutas originados no estrangeiro, mas encontraram sérias dificuldades para fazer cumprir suas decisões. Em certos litígios privados transfronteiriços, foram utilizados mecanismos que permitiram a devida execução de sentenças por meio da responsabilização de subsidiários ou outros tipos de ativos na jurisdição do tribunal em questão."

passou a ser verificada de forma massiva e generalizada por meio de contratos eletrônicos (intersistêmicos, interpessoais, ou interativos).

Conclui-se que os contratos eletrônicos podem ser considerados celebrados entre ausentes no espaço (mesmo se presentes no tempo), atraindo para fins de qualificação a norma do art. 9º, § 2º da LINDB, que prevê a aplicação da lei no local de residência do proponente, uma vez que oferta e aceitação poderão ou não ocorrer no mesmo momento.

No próximo capítulo tais questões serão analisadas sob o viés do Direito Internacional Privado, buscando, ao final, propor critérios de conexão adequados às lides, envolvendo o mundo digital, reconsiderando as ideias de soberania e de fronteira e, por fim, adaptando-se a um contexto fluido e descentralizado[470].

[470] RIBEIRO, Marilda Rosado de Sá; ALMEIDA, Bruno. A cinemática jurídica global: conteúdo do direito internacional privado contemporâneo. *Revista da Faculdade de Direito da UERJ*, 2011, v. 1, n. 20, (s.p.). ISSN 22363475. Disponível em: file:///C:/Users/anadi/Downloads/1516-8697-2-PB.pdf. Acesso em: 17 abr. 2020. Para compor tal viés, os autores trazem o entendimento de JAYME, Erik. O Direito Internacional Privado do novo milênio: a proteção da pessoa humana face à globalização. *In*: ARAUJO, Nadia de; MARQUES, Cláudia Lima (Orgs.). *O novo Direito Internacional* – estudos em homenagem a Erik Jayme. Rio de Janeiro: Renovar, 2005, pp. 2-15, e de MARQUES, Cáudia Lima, Ensaio para uma introdução ao Direito Internacional Privado. *In*: DIREITO, Carlos Alberto Menezes; PEREIRA, Antonio Celso Alves; TRINDADE, Antônio Augusto Cançado. *Novas perspectivas do Direito Internacional Privado Contemporâneo*. Rio de Janeiro: Renovar, 2008, pp. 315-340: "Por outro lado, se a globalização não se traduz como elemento absolutamente novo e inexplorado pela disciplina, a conjuntura contemporânea contribui para a vertiginosa exacerbação não só da velocidade e da ubiquidade, mas, também, da própria liberdade dos diversos indivíduos no espaço fragmentado e conturbado da atualidade (JAYME, 2005, p. 4). Dessa forma, por conta da crescente internacionalização das relações privadas, o Direito Internacional Privado é uma ferramenta de grande utilidade para os juristas contemporâneos, pois lhes permitirá adotar uma abordagem dinâmica, pluralista e dialética na busca pela solução mais justa para as situações jurídicas multiconectadas." (MARQUES, 2008, pp. 321-322).

CAPÍTULO 3 – DANOS TRANSNACIONAIS E DIREITO INTERNACIONAL PRIVADO: PROTEÇÃO DE DADOS PLURILOCALIZADOS

A descentralização característica da Internet dificulta a atribuição de responsabilidade pelo conteúdo difundido naquele ambiente, gerando incerteza e dúvida também a respeito da jurisdição competente para dirimir conflitos que envolvem diversos ordenamentos jurídicos – devido, precisamente, a tal dispersão internacional do conteúdo na rede[471].

Uma das premissas aqui adotadas é a de que os critérios de conexão tradicionalmente adotados se mostram, por vezes, inadequados no âmbito específico da Internet e da Sociedade da Informação[472]. Não obstante, isto não significa a sua total inaplicabilidade, fazendo-se útil a sua análise, bem como de princípios já outrora aceitos e adotados, como o da proximidade[473].

Quaisquer conflitos envolvendo dados pessoais e empresas como o *Facebook*, por exemplo, de sede estadunidense, recairão sobre questões de Direito Internacional Privado, e determinarão a sua jurisdição competente e respectiva lei aplicável. Necessária, portanto, a análise de tais elementos no âmbito da privacidade e proteção de dados na Internet[474].

---

[471] CASTRO, Emília Lana de Freitas; WINTER, Patrícia Pereira. O conflito de jurisdições em caso de violação de direitos da personalidade por publicação na internet. *Revista de Estudos Jurídicos - Unesp*, 2014, v. 18, p. 3.

[472] BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. The datasphere and the law: new space, new territories. *Revista Brasileira de Políticas Públicas (Brazilian Journal of Public Policy).* Direito e o Mundo Digital, dez./2017, v. 7, n.º 8, p. VII. "Construções legais ainda não reconhecem a datasfera como um novo espaço. Diferentemente das outras esferas (como a litosfera, a hidrosfera, a atmosfera), a datasfera ainda não é considerada como criadora de um campo específico de atividades humanas sobre o qual a lei pode intervir e organizar. No entanto, esta área merece reflexão e exame, particularmente sobre a relação global entre o surgimento de um novo espaço e a definição de novas relações com os territórios. A perspectiva de um novo espaço permite estabelecer um conceito abrangente, não abordado atualmente na literatura sobre o assunto, e que melhoraria a nossa compreensão das relações clássicas ou potencialmente recém-formadas com os territórios." (Tradução livre).

[473] ARAÚJO, Nadia de. *Direito Internacional Privado:* teoria e prática brasileira. 6. ed. Porto Alegre: Revolução eBook, 2016, (s.p.). "Um problema de DIPr (para a concepção clássica) não é um problema de justiça material, e sim de escolha da lei aplicável indicada pela norma de conflito. O seu objetivo consiste em promover e garantir a continuidade e a estabilidade das situações jurídicas multinacionais através da uniformidade da respectiva valoração por parte dos diversos sistemas interessados. Com isso, evita-se a frustração das partes e terceiros. Esse sistema não cuida da utilização de suas normas, mas sim das conectadas à questão. Ainda, segundo Ferrer Correa, não se trata de escolher a melhor lei, mas a melhor colocada para intervir – em razão da localização dos fatos, ou da relação dela com as pessoas a que estes respeitam. Os valores predominantes são os da segurança e certeza jurídica, cuidando de atingir uma justiça formal, pois seu objetivo é garantir a continuidade e estabilidade das situações jurídicas."

[474] OLIVEIRA, Carlos Eduardo Elias de. *Aspectos principais da Lei nº 12.965, de 2014, o Marco Civil da Internet:* subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, abr./2014 (Texto para Discussão nº 148). Disponível em: www.senado.leg.br/estudos. Acesso em: 17 abr. 2020. Neste ponto, cumpre desde já esclarecer aspecto relevante acerca do Marco Civil da Internet e da Lei de Introdução às Normas do Direito Brasileiro, especialmente no que tange ao art. 11 daquela primeira lei: "[...] não é qualquer norma brasileira que atingirá os provedores estrangeiros sem filial no Brasil, mas apenas as normas que tratam de coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de

José Augusto Fontoura Costa e Geraldo Miniuci destacam, em artigo que trata do direito ao esquecimento, que tem se observado dificuldades em manejar a distinção entre os campos privado e público na rede – que, por sua vez, conduzem a situações de violação da intimidade e privacidade por falta de habilidade e conhecimentos, além de incapacidade de embaralhar as esferas[475].

Não importa a qual espécie de dados seja feita referência – dados genéricos, metadados ou dados pessoais – pois todos são passíveis de transferência e armazenamento em bancos de dados. A transferência de dados poderá ocorrer entre servidores localizados em territórios pertencentes a Estados distintos e, consequentemente, submetidos a diferentes regimes jurídicos[476].

A partir do momento em que as ideias de território e de soberania se distanciam daquilo que se entende como uma concepção mais tradicional ou clássica, a percepção das fronteiras físicas se altera, de modo que é necessário pensar sobre as regras que determinam o exercício da jurisdição do Estado em um determinado território[477].

---

comunicações, pois, pelo que se constata do *caput* do art. 11 e do seu parágrafo 3º, o interesse do legislador foi apenas de submeter essas operações à legislação nacional. [...] Primeira conclusão: o Marco Civil não cuida de definir a legislação que disciplinará o contrato celebrado por um brasileiro que adquire um produto em um site estrangeiro, salvo no tocante à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações. Para isso, seguem vigentes os elementos de conexão previstos na LINDB e na jurisprudência do STJ. Em outras palavras, para definir qual a legislação disciplinará os contratos celebrados pelos brasileiros em compras à distância, não se invocará o Marco Civil, que nada diz a respeito, e sim a LINDB e a jurisprudência. [...] Se, porém, o site não pertencer a uma empresa com esse perfil (ou seja, não houver filial no Brasil nem *marketing* direcionado ao mercado brasileiro), somente será aplicável a lei estrangeira para a disciplina do contrato, nos termos do art. 9º, § 2º, da LINDB. O CDC não poderá ser invocado aí. Segunda conclusão: o art. 11 do Marco Civil cuida de elemento de conexão específico e exclusivo para aplicação da legislação brasileira relativa à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações."

[475] COSTA, José Augusto Fontoura; MINIUCI, Geraldo. Não adianta nem tentar esquecer: um estudo sobre o direito ao esquecimento. *Revista Brasileira de Políticas Públicas (Brazilian Journal of Public Policy).* Direito e Mundo Digital, dez./2017, v. 7, n.º 3, p. 429. "Há, nesse aspecto, interesses (i) dos indivíduos em não deixarem escapar informações íntimas e privadas; (ii) da sociedade em ter informações e canais disponíveis a baixo custo e de utilização livre; e (iii) dos provedores de acesso, aplicações, busca e conteúdos em evitar o incremento de seus custos operacionais."

[476] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico.* Joaçaba, jul./dez. 2011, n. 12, n. 2, pp. 91-108, pp. 92-93. "A ferramenta que possibilita a sistematização de volumes que podem chegar a ser gigantescos de informação e que teve seu potencial exponencialmente incrementado com o advento da informática foi, propriamente, o banco de dados. Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações."

[477] RIBEIRO, Marilda Rosado de Sá; ALMEIDA, Bruno. Op. cit., 2011. "As circunstâncias atuais da Sociedade Internacional, marcadas pelos signos da globalização econômica (velocidade, ubiquidade e liberdade) apontam para a necessidade da cooperação entre os Estados soberanos, especialmente porque o atributo da soberania deixa de ser considerado em sua forma absoluta e ilimitada, por força da consagração de outros sujeitos de Direito Internacional, como os organismos internacionais, as empresas transnacionais e, principalmente, a pessoa humana, cuja dignidade constitui o eixo epistemológico do Direito Internacional Contemporâneo, consagrado pela convergência dos ramos do Direito Internacional Público, do Direito Internacional Privado e de todas as áreas correlatas ao estudo da complexidade da vida internacional."

> Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar receber e difundir, **sem consideração de fronteiras**, informações e ideias por qualquer meio de expressão[478].

A ausência de fronteiras no mundo *online* cria dificuldades para o Estado exercer o seu papel de regulador físico (em contraposição à virtual), abrindo espaço para possíveis conflitos de jurisdições. Conforme os efeitos reais do uso de uma ferramenta virtual ocorrem em outro (ou outros) ponto do planeta, atos praticados por indivíduos com acesso à Internet podem estar submetidos a uma jurisdição distinta daquela onde os dados foram acessados, fato do qual raramente os usuários de tais *websites* possuem conhecimento.

> O distanciamento de territórios institucionais tradicionais levanta a questão da manutenção dos mecanismos legais existentes que atualmente estabelecem ligações entre as circunstâncias que a lei pretende governar e os territórios que produzem a lei. A fim de localizar uma circunstância em um espaço global composto por diversos territórios, a lei define regras de aplicabilidade espacial que estabelecem um fator de conexão entre o estado de direito produzido por uma certa autoridade normativa (um Estado, uma cidade, uma organização internacional ou regional) e as circunstâncias concretas. Este fator de conexão é baseado em um conjunto extremamente diversificado de critérios de localização, sejam eles factuais (localização de um ativo ou de uma pessoa em um território em um dado momento) ou a consequência de uma construção normativa (nacionalidade, domicílio, registro). No entanto, tais critérios de localização são distorcidos quando considerados sob a perspectiva da datasfera. Se as circunstâncias devem ser consideradas como à parte dos territórios institucionais convencionais, outros critérios de conexão devem ser desenvolvidos, ou mesmo concebidos, entre a circunstância de ser governada e o estado de direito.[479] (tradução livre).

---

[478] ONU. Organização das Nações Unidas. *Declaração Universal dos Direitos Humanos*. 1948, art. 19. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 05 mar. 2020 (grifamos).

[479] BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. Op. cit., dez./2017, p. VIII. "O desapego dos territórios institucionais tradicionais levanta a questão da manutenção dos mecanismos legais existentes que atualmente estabelecem vínculos entre as circunstâncias que a lei deseja governar e os territórios que a produzem. Para localizar uma circunstância em um espaço global composto por vários territórios, a lei define regras de aplicabilidade espacial que estabelecem um fator de conexão entre o estado de direito produzido por uma determinada autoridade normativa (um Estado, uma cidade, uma organização internacional ou regional) e as circunstâncias concretas. Esse fator de conexão é baseado em um conjunto extremamente diversificado de critérios de localização, seja factual (localização de um ativo ou pessoa em um território em um determinado momento) ou a consequência de uma construção legal (nacionalidade, domicílio, registro). No entanto, esses critérios de localização são distorcidos quando considerados da perspectiva da esfera de dados. Se a circunstância deve ser considerada desapegada dos territórios institucionais convencionais, outros critérios de conexão devem ser desenvolvidos, ou mesmo criados, entre a circunstância a ser governada e o Estado de Direito." (Tradução livre). "*Detachment from traditional institutional territories raises the issue of the maintenance of existing legal mechanisms that currently establish links between circumstances the law wants to govern and the territories producing the law. In order to localize a circumstance in a global space comprised of several territories, the law defines spatial applicability rules that establish a connecting factor between the rule of law produced by a given normative authority (a State, a town, an international or regional organization) and the concrete circumstances. This connecting factor is based on an extremely diverse set of localization criteria, whether factual (location of an asset or a person on a territory at a given moment) or the consequence of a legal construction (nationality, domicile, registration). However, these localization criteria are distorted when considered from the datasphere perspective. If the circumstance to be*

Conforme explicam Emília Lana de Freitas Castro e Patrícia Pereira Winter, em artigo no qual discutem questões ligadas ao conflito de jurisdições em caso de violação de direitos da personalidade por publicação na Internet, num contexto em que há de fato um grande fluxo na rede, é inevitável que surjam conflitos jurídicos. Isto posto, é imprescindível combater tais dissídios de forma tão ágil quanto as relações e tratativas que se dão via Internet – o desafio reside, em verdade, em fazê-lo de forma eficaz, sem comprometer o equilíbrio e a eficiência do sistema[480].

Justifica-se, portanto, a abordagem do tema pela ótica do Direito Internacional Privado, considerando que o crescente uso da Internet não produziu mudanças somente quanto aos conceitos de privacidade e de dados pessoais, mas, também, em relação ao próprio conceito de fronteiras e de soberania[481].

> Dentre as inúmeras rupturas institucionais nas estruturas jurídicas do Estado, geradas pelo convencionalmente denominado fenômeno da globalização econômica, destaca-se, sem dúvida, como pondera José Eduardo Faria, o esvaziamento da soberania e da autonomia dos Estados nacionais. Ao longo do tempo, uma nova concepção de soberania, embasada na crescente aceitação de uma ordem jurídica supranacional, foi-se sobrepondo ao conceito clássico-tradicional, que teve sua origem na necessidade de consolidação da territorialidade do Estado moderno[482].

Considerando que "os cidadãos afetados pelas informações contidas em sítios eletrônicos ou por relações mantidas no ambiente virtual não podem ser tolhidos do direito de acesso à justiça para a análise de eventuais danos ou ameaças de lesões decorrentes de

---

considered as detached from conventional institutional territories, other connecting criteria must be developed, or even devised, between the circumstance to be governed and the rule of law."

[480] CASTRO, Emília Lana de Freitas; WINTER, P. P. Op. cit., 2014, p. 3.

[481] BASILIEN-GAINCHE, Marie-Laure. Les frontières européennes – Quand le migrant incarne la limite. *Revue de l'Union Européene*, jun. 2017, n.º 609, pp. 5-6. No artigo é ressaltado o papel central desempenhado pelas novas tecnologias desenvolvidas no controle das fronteiras físicas no âmbito da União Europeia e do Espaço Shengen, de modo que há a virtualização das fronteiras físicas em tal contexto: "Todos os aspectos do controle de fronteiras são alimentados por novas tecnologias, desde o monitoramento das passagens pelas fronteiras, conduzindo operações de inteligência, desenvolvendo análises de risco, garantindo a cooperação entre autoridades envolvidas (alfândega, polícia, justiça, defesa etc.), para coordenar as atividades das autoridades europeias, dos Estados-Membros e dos países vizinhos." (Tradução livre). "*Tous les aspects du contrôle des frontières se nourrissent des nouvelles technologies, qu'il s'agisse de surveiller les franchissements des frontières, de conduire des opérations de renseignements, d'élaborer des analyses de risques, d'assurer la coopération entre les autorités impliquées (douanes, police, justice, défense etc.), de coordonner les activités des instances européennes, des États membres et des pays voisins."*

[482] CELLI JÚNIOR, Umberto. Solução de conflitos na União Européia: lições para o Mercosul? *Revista da Faculdade de Direito. Universidade de São Paulo*. São Paulo, 2002, v. 97, pp. 415-434.

direitos de privacidade, intimidade, consumidor, dentre outros"[483], é preciso buscar definir quais critérios seriam aplicáveis a fim de permitir efetivamente essa tutela[484].

Há, por outro lado, limites à responsabilidade do provedor, seja ele de conteúdo, de hospedagem, de acesso ou de correio eletrônico. Nos termos do CDC, os provedores são considerados fornecedores (arts. 12 e 14), sendo responsáveis, portanto, pelos defeitos decorrentes da respectiva atividade, inclusive aqueles relativos a falhas de segurança e pela reparação dos danos causados.

Aplicam-se, contudo, as excludentes de responsabilidade previstas no Ordenamento brasileiro, sendo afastadas em caso fortuito ou força maior, por fato de terceiro ou, ainda, por culpa exclusiva da vítima. Há entendimento jurisprudencial no sentido de que usuários que navegam sem tomar as devidas precauções (seja a instalação de programas antivírus, *firewalls*, criptografia ou dupla verificação) implicam o reconhecimento de fato exclusivo da vítima, podendo afastar a responsabilidade civil do fornecedor.

Há, ainda, há questões controvertidas no que se refere à classificação do provedor como mero intermediário, afastando-se a obrigação quanto ao conteúdo transmitido, bem como quanto ao mecanismo de *notice and take down*, o qual implica a necessidade de notificação prévia para que possa haver a responsabilização do provedor, caso o conteúdo não seja indisponibilizado quando solicitado[485].

---

[483] STJ. Superior Tribunal de Justiça. *Resp. 1168546/RJ*. Rel. Ministro Luis Felipe Salomão. Quarta Turma, julgado em 11 maio 2010, DJE em 07 fev. 2011, p. 15.

[484] POLIDO, Fabrício Bertini Pasquot. *Direito internacional privado nas fronteiras do trabalho e tecnologias:* ensaios e narrativas na Era Digital. Rio de Janeiro: Lúmen Juris, 2018, pp. 120 e ss. "Nesse sentido, parece ser de interesse para o Direito Internacional Privado a delimitação conceitual e normativa de regras de conexão determinadoras de direito aplicável aos atos de violação transfronteiriça de direitos de personalidade na Internet. Tanto nos sistemas de tradição romano-germânica como os de '*common law*', o modelo clássico de imputação de responsabilidade civil extracontratual requer a identificação dos elementos do ato delitual, os danos ocorridos e a relação causal existente entre o ato praticado e os danos. Ainda que se trate de atos ilícitos ou delitos de internet, o Direito admite o dever pré-existente das partes – não exaustivamente, de usuários, servidores, criadores e provedores de conteúdo, de abstenção de toda e quaisquer práticas infrativas direcionada a direitos de titularidade de terceiros, dentro da coletividade. Da mesma forma, a metodologia para a qualificação da responsabilidade civil (por imputação ou atribuição) está justificada nos casos de violação positiva da lei ou do contrato e da prática de atos cujos resultados podem ser individualizados em danos específicos, com prejuízos sentidos pelo titular dos direitos tutelados."

[485] TJ/RJ. Tribunal de Justiça do Rio de Janeiro. *Apelação Cível n.º 0022893-68.2014.8.19.0202*. 26ª Câmara Cível. Consumidor Rel. Des. Natacha Nascimento Gomes Tostes Gonçalves de Oliveira. Julgado em 27 jul. 2017. "Apelação. Responsabilidade do Provedor. Postagens ofensivas. Sistema *notice and take down*. Ação de obrigação de fazer c/c indenização por danos morais c/c pedido de tutela antecipada. Palavras ofensivas contra autor em site hospedado pela ré. [...] Apesar de não se exigir controle prévio do conteúdo publicado pelos usuários, o provedor, após ser notificado, tem o dever de retirar do ar o conteúdo ofensivo veiculado. Falha na prestação do serviço configurada eis que o autor logrou êxito em comprovar o conteúdo ofensivo à sua honra constante no blog mencionado e ter entrado em contato com a ré solicitando a retirada imediata do conteúdo ofensivo da internet, sem que a providência fosse tomada. Responsabilidade objetiva da ré pautada na Teoria do Risco do Empreendimento nos termos do art. 14 do CPC. Os fatos ocorreram antes da vigência do Marco Civil da Internet, não se aplicando o art. 19 (exigência de determinação judicial). Dano moral configurado e majorado para o valor de R$ 15.000,00, já que o autor é portador de transtorno psiquiátrico

O art. 20 do Marco Civil da Internet, em seu parágrafo único, prevê a obrigação de indisponibilizar conteúdos quando solicitado pelo usuário, de modo que

> [...] o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização[486].

O art. 19, por sua vez, prevê que

> [...] o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente [...][487].

Há, contudo, dificuldade em fazer valer sentenças no caso de empresas estrangeiras, as quais, por vezes, optam por manter suas sedes em jurisdições favoráveis. Enquanto, porém, o art. 19 exclui a responsabilidade se não houver ordem judicial para remoção do conteúdo, os provedores desempenham atuação neutra, de modo a preservar o interesse coletivo na disponibilização de informações pela Internet[488], e retirá-lo somente se determinado judicialmente.

---

comportamental, com pior após os fatos agravado pela resistência da ré em excluir os comentários ofensivos. [...] Recursos conhecidos, desprovido o apelo do réu e provido em parte o do autor." TJ/RJ. Tribunal de Justiça do Rio de Janeiro. *Apelação Cível n.º 0031762-47.2012.8.19.0054.* 5ª Câmara Cível. Rel. Des. Heleno Ribeiro Pereira Nunes. Julgado em 10 dez. 2019. "Apelação Cível. Responsabilidade civil de site de buscas. Sentença de procedência parcial que se mantém. Não cabe aos provedores de hospedagem exercer juízo de valor prévio acerca da natureza ofensiva das páginas de Internet, sendo-lhes, todavia, imposto o dever de acolher os pedidos de remoção de conteúdo em prazo razoável. Precedentes jurisprudenciais. Desse modo, sem a prova de que o apelado efetivamente tomou ciência acerca do equívoco da notícia e, não obstante, quedou-se inerte, sua responsabilidade se circunscreve à remoção do conteúdo ofensivo em prazo razoável, não sendo cabível impor-lhe o dever de reparar o dano moral porventura sofrido pelo lesado. Recurso ao qual se nega provimento."

[486] BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2014/lei/ l12965.htm. Acesso em: 17 abr. 2020.

[487] Id., ibid.

[488] STJ. Superior Tribunal de Justiça. REsp 1306157/SP, Rel. Ministro Luis Felipe Salomão, Quarta Turma, julgado em 17 dez. 2013, DJe 24 mar. 2014. "DIREITO CIVIL. OBRIGAÇÃO DE FAZER E NÃO FAZER. VÍDEOS DIVULGADOS EM SITE DE COMPARTILHAMENTO (YOUTUBE). CONTRATAÇÃO A ENVOLVER A MARCA E MATERIAL PUBLICITÁRIO DOS AUTORES. OFENSA À IMAGEM E AO NOME DAS PARTES. DEVER DE RETIRADA. INDICAÇÃO DE URL'S. DESNECESSIDADE. INDIVIDUALIZAÇÃO PRECISA DO CONTEÚDO DO VÍDEO E DO NOME A ELE ATRIBUÍDO. MULTA. REFORMA. PRAZO PARA A RETIRADA DOS VÍDEOS (24 H). MANUTENÇÃO. 1. Atualmente, saber qual o limite da responsabilidade dos provedores de internet ganha extrema relevância, na medida em que, de forma rotineira, noticiam-se violações à intimidade e à vida privada de pessoas e empresas, julgamentos sumários e linchamentos públicos de inocentes, tudo praticado na rede mundial de computadores e com danos substancialmente potencializados em razão da natureza disseminadora do veículo. [...]. 2. [...] o presente recurso especial cinge-se à obrigação remanescente relativa aos vídeos com o título difamante, tenham sido eles indicados precisamente pelas autoras (com a menção das URL's), ou não, mas

3.1 DETERMINAÇÃO DA JURISDIÇÃO COMPETENTE

Conforme mencionado anteriormente, a Internet interfere diretamente nos conceitos tradicionais, tais como a soberana territorial estatal[489]. Ao considerar que a soberania e as fronteiras estão diretamente relacionadas, e que no mundo digital as fronteiras assumem caráter fluido ou flexível, frequentemente descentralizado, as regras de conexão baseadas em critérios geográficos ou territoriais podem ser de difícil aplicação[490], tanto em relação à lei aplicável, quanto ao Tribunal internacionalmente competente.

Para fins de determinação da competência (ou jurisdição) internacional, cumpre analisar o disposto nos arts. 21 a 25 do Código de Processo Civil, fonte interna[491]

---

desde que existentes no site, com aquele preciso título, depois de o provedor ter sido formalmente notificado de sua existência. 3. Por outro lado, há referência nos autos acerca de perícia já realizada na qual se constatou a viabilidade técnica de controle dos vídeos no site youtube, [...]. 4. Com efeito, [...], reafirma-se entendimento segundo o qual o provedor de internet - administrador de redes sociais -ainda em sede de liminar, deve retirar informações difamantes a terceiros manifestadas por seus usuários, independentemente da indicação precisa, pelo ofendido, das páginas em que foram veiculadas as ofensas (URL's). 5. [...] a responsabilidade dos provedores de Internet, quanto a conteúdo ilícito veiculado em seus sites, envolve também a indicação dos autores da informação (número de IP). 6. Multa cominatória reajustada para que incida somente a partir deste julgamento, no valor de R$ 500,00 (quinhentos reais) por dia de descumprimento, mantido o prazo de 24 (vinte e quatro) horas para a retirada dos vídeos difamantes. 7. Recurso especial parcialmente provido, apenas no tocante ao valor das astreintes."

[489] MOURA VICENTE, Dario Manuel Lentz de. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, pp. 111-112. "É, de todo o modo, ao Estado do foro que pertence, no exercício da sua soberania, definir os pressupostos e limites a que se subordina a aplicação na ordem interna de Direito estrangeiro. A lei desse Estado é, por isso, a ordem jurídica de referência no juízo acerca da tolerabilidade do resultado da aplicação da lei designada pelas regras de conflitos. Não pode, por outro lado, negar-se a importância que contemporaneamente assume o primado das normas internacionalmente imperativas do Estado do foro sobre as da *lex causae* – [...] –, porquanto numa economia 'globalizada' essas normas são indispensáveis à implementação das políticas econômicas de cada Estado e dos regimes locais sobre concorrência. Uma rigorosa igualdade entre a *lex fori* e o Direito estrangeiro aplicável às situações da vida privada internacional, não se afigura, vistas as coisas sob este ângulo, desejável ou sequer viável."

[490] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. *Governança global da internet, conflito de leis e jurisdição*. Instituto de Referência em Internet e Sociedade (IRIS). Belo Horizonte: 2018, pp. 80-81. "O modelo westfaliano de Estado-nação, baseado na soberania territorial, contrasta com o modelo da Internet, fundamentado na descentralização, na abertura, na colaboração e nos movimentos transfronteiriços – ou que ocorrem no ciberespaço. [...]. A internet é estruturada especialmente por linguagem computacional (código) e infraestrutura física (computadores, cabos e satélites, entre outros). O Estado, por sua vez, organiza e controla seu território e uma população por meio de uma constituição, leis, instituições e costumes. Conectar geografia e ciberespaço, então, é uma tarefa complexa, em plena construção e mudança nos tempos atuais."

[491] DOLINGER, Jacob. Supreme Court Solutions for Conflicts between Domestic and International Law: An Exercise in Eclecticism. *Capital University Law Review*, 1993, v. 22, n. 1041, pp. 1043-1045: "Ambas as autoridades de Direito Internacional públicas e privadas vinculam o conflito entre fontes de direito internas e internacionais às doutrinas clássicas do monismo e do dualismo, cada uma propondo uma solução diferente. Charles Rousseau explica que ou a ordem jurídica é independente, distinta, separada e impenetrável (dualismo) ou que uma deriva da outra, o que implica uma concepção unitarista do direito (monismo). De acordo com a escola dualista, o Direito Internacional e o Direito Interno são dois sistemas independentes e diferentes, as fontes e as regras do Direito Internacional não têm relação com questões jurídicas internas e as normas do Direito Interno não influenciam os assuntos jurídicos internacionais. As leis internacional e nacional são dois círculos que não se cruzam, são meramente contíguos. Quando um Estado assina e ratifica

delimitadora da jurisdição estatal, seja a competência exclusiva ou concorrente[492]. Demonstrada a transnacionalidade da questão a partir da presença de um elemento estrangeiro, cumpre tratar dos princípios gerais de incidência e reconhecimento da jurisdição internacional[493].

Primeiramente, há os princípios que levam à admissão do uso da jurisdição de um determinado Estado, e nele Solano de Camargo agrupa os princípios[494]: (i) do acesso à

---

uma convenção, o aprova como uma fonte de Direito Internacional, sem qualquer repercussão em seu sistema jurídico interno. Para converter um tratado em uma fonte de Direito Interno, o Estado precisa aprovar um novo estatuto que reproduza as regras do tratado para que ele se aplique às relações jurídicas internas. Isso é conhecido como o processo de adoção, [internalização] ou transformação. Os dualistas, portanto, defendem a primazia da lei municipal em cada Estado. A escola monista começou com Hans Kelsen, que não aceitava a possibilidade de dois sistemas jurídicos diferentes e totalmente independentes. Segundo ele, há uma convergência ou superposição desses sistemas. [...] Kelsen estabelece um certo senso de hierarquia no Direito Internacional e Municipal." (Tradução livre). "*Both public and private international law authorities link the conflict between internal and international sources of law to the classical doctrines of monism and dualism, each proposing a different solution. Charles Rousseau explains that either both legal order are independent, distinct, separate and impenetrable (dualism) or that one derives from the other, which implies a unitarist conception of law (monism). According to the dualist school, international law and domestic law are two different independent, inconnected systems, the sources and rules of international law have no bearing on internal legal matters and the norms of internal law have no influence over international legal subsjects. International and national law are two circles that do not intersect, they are merely contiguous. When a state signs and ratifies a convention, it approves it as a source of international law, without any repercussion in its internal legal system. To convert a treaty into a source of internal law, the state has to enact a new statute that reproduces the treaty's rules in order to have it applies to internal legal relations. This is known as the process of adoption or transformation. Dualists, therefore, assert the primacy of municipal law within each state. The monist school started with Hans Kelsen who did not accept the possibility of two different, totally independent legal systems. According to him, there is a convergence or superposition of these systems. […] Kelsen establishes a certain sense of hierarchy in international and municipal law.*"

[492] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, pp. 95 e ss. "No sistema de Direito Internacional Privado brasileiro, normas unilaterais definem imediatamente a competência dos tribunais domésticos aos casos com conexão internacional, na esteira do que estabelece o art. 12 da Lei de Introdução às Normas do Direito Brasileiro (LINDB) e arts. 21 a 24 do Código de Processo Civil de 2015 (que tratam, fundamentalmente, da competência concorrente, competência exclusiva e litispendência processual internacional). [...] Por outro lado, como o art. 12 da LINDB indica a competência internacional, em duas etapas deve o juiz nacional analisar o caso que lhe é submetido: em um primeiro momento, ele observa os limites espaciais da jurisdição brasileira, como nas competências concorrente e exclusiva, respectivamente endereçadas pelos arts. 21, 22 e 23 do Código de Processo Civil e, em seguida, proceder à análise da competência interna, que será aferida pelas normas de organização judiciária do Direito Processual brasileiro. A primeira etapa desse exame, portanto, reside em saber quais os limites da jurisdição doméstica, a saber, se a causa apreciada se inclui dentro dos limites que fixam a extensão da jurisdição nacional. A segunda etapa será a delimitação, pelo juiz, da competência interna, a partir da qual a causa que lhe foi apresentada será julgada. [...] a eleição de foro em contratos internacionais também está assegurada como critério definidor da exclusividade da jurisdição escolhida pelas partes, por força do art. 25 do CPC. Daí resulta ser possível a submissão de um litígio envolvendo contratos internacionais eletrônicos a tribunais estrangeiros."

[493] MOURA VICENTE, Dario Manuel Lentz de. Op. cit., 2005, p. 77. "Uma adequada unificação internacional das regras sobre a competência judiciária internacional e o reconhecimento de sentenças estrangeiras reclama, por isso, a prévia ou concomitante unificação das regras sobre conflitos de leis no espaço, sob pena de a primeira se transmutar num incentivo ao *forum shopping*."

[494] CAMARGO, Solano de. *Forum shopping:* modo lícito de escolha de jurisdição? Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de São Paulo. Orientador: Prof. Dr. Gustavo Ferraz de Campos Monaco. São Paulo, 2015, p. 35. Para o autor, "[...] parece clara a necessidade de se superar a distinção baseada exclusivamente em espécies normativas (quer baseada em nacionalidade, domicílio ou qualquer outra), em favor de uma distinção baseada no caráter pluridimensional dos enunciados."

Justiça; (ii) do *forum necessitatis*[495]; (iii) da *plenitudo jurisdictionis*; (iv) da *commitas gentium*; e (v) da autonomia da vontade. No segundo grupo foram alocados os princípios que levam à vedação do uso da jurisdição de um determinado Estado[496]: (i) da imunidade de jurisdição; (ii) da efetividade; e (iii) da jurisdição exorbitante.

Quanto aos princípios positivos que conduzem à competência internacional, o princípio de acesso à Justiça e inafastabilidade do controle jurisdicional surge como argumento relevante[497], utilizado, por vezes, em decisões judiciais brasileiras que envolvem elementos estrangeiros, como, por exemplo, em ações relativas a empresas com sede no exterior.

O princípio da *plenitudo jurisdictionis* também é especialmente relevante, pois determina a soberania do Estado para definir a sua própria competência (ou jurisdição) sobre uma lide, fazendo com que os aspectos processuais e procedimentos sejam regidos exclusivamente pela *lex fori*.

O princípio da autonomia da vontade pode ser aplicado para reconhecer a validade de cláusulas contratuais de eleição de foro, como manifestação da vontade das partes quando da sua celebração, ou então, pode ser afastado, especialmente no caso de demandas que envolvem direito do consumidor, de modo que a abusividade eventual de cláusulas de eleição de foro demanda, necessariamente, a análise de elementos fáticos[498].

---

[495] Id., ibid. O princípio do *forum necessitatis* leva à indicação de critério positivo de fixação da competência internacional quando houver conflito negativo de jurisdições em situações como guerras civis, calamidade pública, ou outras de grande ordem, que impeça o ajuizamento na demanda de um foro em particular.

[496] Id., ibid.

[497] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 154. "No Brasil, a prestação jurisdicional pelo Estado é, segundo Fredie Didier Jr., imperativa e inevitável, tendo em vista se tratar da manifestação de um poder previsto no art. 5º, inc. XXXV, da Constituição Federal. O dispositivo prevê que "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito". É imperativa porque o Estado não pode se esquivar da apreciação da lide quando provocado, mesmo quando a lei for omissa, como dispõe o art. 4º da Lei de Introdução às Normas do Direito Brasileiro (LINDB). Assim, 'todo problema que for submetido ao tribunal precisa ser resolvido, necessariamente [...] ainda que a situação concreta não esteja prevista expressamente na legislação'. Como decorrência dos direitos fundamentais do processo, a prestação jurisdicional é inevitável, tendo em vista ser obrigatória e indeclinável a apreciação da lide pelo Estado, mesmo quando houver outros recursos administrativamente disponíveis. [...] Assim, tanto do ponto de vista internacional quanto do direito interno, é do Estado brasileiro o ônus de oferecer aos seus cidadãos o devido acesso a um recurso jurisdicional eficiente, que vai além do ponto de vista meramente formal, provendo meios jurídicos necessários para o acesso de todos ao Judiciário e assegurando a efetiva proteção de direitos."

[498] STJ. Superior Tribunal de Justiça. *REsp 1.089.993-SP*. Rel. Ministro Massami Uyeda, julgado em 18 fev. 2010. "COMPETÊNCIA. FORO. ELEIÇÃO. ABUSIVIDADE. A Turma decidiu que, na hipótese em que uma empresa com filiais em diversas localidades firma contrato com consumidores nelas domiciliados, com cláusulas prévias, elegendo sua sede como o foro para futuras e eventuais demandas, é possível avaliar, desde logo, a intenção do fornecedor de restringir a defesa do consumidor aderente. Daí que o fundamento adotado pelas instâncias ordinárias, i.e., a existência de relação jurídica regida pelo CDC, por si só não determina que seja abusiva a cláusula de eleição de foro. Assim, provido em parte o recurso para determinar que o tribunal de origem analise o foro eleito pelas partes nos termos propostos, no sentido de melhor examinar se tal cláusula dificulta o acesso da parte hipossuficiente ao Poder Judiciário. Ademais, é vedado, na via especial,

Isto porque, ainda que conste eleição de foro diverso no contrato celebrado entre as partes, aplicar-se-á o art. 101, inc. I do Código de Defesa do Consumidor, o que permite o ajuizamento da ação no domicílio do autor. Deste modo, se o autor for consumidor domiciliado no Brasil, o Judiciário brasileiro poderá ser reconhecido como competente para solucionar controvérsias decorrentes do contrato, independentemente do foro previsto no contrato[499].

A proteção assegurada pelo CDC é essencial para garantir o acesso à Justiça dos consumidores que contratam produtos ou serviços pela Internet. Por vezes, enquanto o consumidor é brasileiro e está aqui domiciliado, o site pelo qual é feita a contratação está registrado em outro país, seus servidores localizados em outro e a sede da empresa ainda em outro.

Soma-se a isto o fato de que muitas contratações são feitas a partir da assinatura de termos automáticos, termos de aceite ou de uso e condições – os quais raramente são lidos e compreendidos em sua integridade pelo consumidor. Ainda que conste cláusula expressa elegendo foro estrangeiro, não é possível afirmar que se trata de vontade comum das partes ou expressão de sua autonomia, já que o consumidor, parte hipossuficiente, dificilmente estava ciente de tal aspecto quando realizou a contratação.

Tal princípio esbarra, por vezes, com o princípio da efetividade, disposto entre os princípios negativos de incidência da jurisdição internacional do Estado. Isto porque, mesmo que seja possível o ajuizamento da demanda perante o Judiciário brasileiro, a jurisdição nacional encontra limites quanto à possibilidade de cumprimento de decisões[500].

O princípio da jurisdição exorbitante, por sua vez, parece ser mais relevante nas demandas relacionadas à Internet como forma de se afastar alegações de incompetência da Justiça brasileira pelo réu demandado, sob o pretexto de que seria outra a jurisdição

---

aferir a abusividade da cláusula de eleição de foro nos termos propostos, por demandar a análise de elementos fáticos. Precedentes citados: REsp 56.711-SP, DJ 20/3/1995; CC 64.524-MT, DJ 9/10/2006; REsp 403.486-SP, DJ 12/8/2002, e CC 30.712-SP, DJ 30/9/2002."

[499] O Código de Processo Civil admite expressamente a eleição do foro brasileiro para dirimir controvérsias internacionais, nos termos do art. 22, III; por outro lado, determina o não conhecimento de demandas propostas no Brasil quando estas forem decorrentes de contrato com eleição de foro estrangeiro, no art. 25. Em casos envolvendo relações de consumo cumpre observar, contudo, o disposto no art. 101, inc. I, o qual contém previsão de ajuizamento da ação de responsabilidade civil no foro do domicílio do autor da ação.

[500] CAMARGO, Solano de. Op. cit., 2015, p. 56. "Vera Jatahy vai no mesmo sentido, definindo o princípio da efetividade pelo aspecto negativo, na medida que o Estado deve abster-se de julgar a demanda, caso a sentença que vier a produzir não tenha como ser reconhecida onde deva produzir seus efeitos. Assim, segundo a autora, o fundamento do princípio encontra-se na inutilidade de um julgamento prolatado em tais circunstâncias. [...] O princípio da efetividade, dentro do contexto da jurisdição internacional, parece estar ligado à própria condição da ação: o interesse de agir em um litígio envolvendo parte ou partes estrangeiras. [...] Em tempos em que se busca dar maior efetividade ao processo, enfatizando sua instrumentalidade, deve-se evitar e impedir que o processo inviável exista."

competente, evidentemente mais favorável a si. Trata-se de princípio que permite obstar o acúmulo de competências em Estados que guardam pouca relação com a lide, mas cujos ordenamentos contêm disposições mais benéficas a uma das partes[501].

É possível, ainda, a aplicação do princípio da efetividade ou do princípio do *forum non conveniens*, abstendo-se o julgador de apreciar o litígio que lhe foi submetido, o qual foi declarado incompetente por não ser o mais adequado em razão da ausência do réu e da dificuldade de acesso a elementos do caso. Ou, então, por haver tribunal mais apropriado para julgar o caso, com garantias processuais semelhantes, relacionado às ideias de boa-fé processual e abuso do direito de litigar[502].

Importante ressaltar, neste momento, que a jurisdição é tradicionalmente tida como um conceito relacionado ao poder do Estado de "legislar, administrar e julgar afetando diretamente as pessoas, bens e fatos sob sua influência, sendo um corolário dos princípios internacionais da soberania, da igualdade e da não interferência em assuntos internos"[503]. No contexto das relações digitais, contudo, tais características tradicionalmente atribuídas à jurisdição estatal devem ser reavaliadas.

No âmbito da União Europeia, Anabela Susana de Sousa Gonçalves analisou o tratamento conferido pelo Tribunal da Justiça da União Europeia a casos de violação transfronteiriça a direitos de personalidade, apontando uma tendência pela adoção da *delict oriented approach*, interpretação que "varia em função do delito em causa, tendo em conta a natureza do direito violado, o âmbito de proteção geográfica desse direito e a análise da extensão do dano"[504].

---

[501] Id., ibid., p. 62. "Por fim, a competência internacional baseada na existência de 'negócios' do demandado no foro, sem que tais negócios tenham qualquer relação com a demanda, é encontrada em certos Estados federativos dos Estados Unidos, baseados em regras denominadas '*long arm statutes*'. A partir dessas regras, tais Estados exercem a jurisdição internacional sobre demandas em que o réu tenha qualquer atividade econômica no foro, mesmo que tais atividades não tenham qualquer relação com a causa."

[502] TIBURCIO, Carmen. Op. cit., 2006, pp. 208 e ss.

[503] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 104.

[504] GONÇALVES, Anabela Susana de Sousa. O caso *Bolagsupplysningen* e o lugar da ocorrência do facto danoso *online* na violação transfronteiriça de direitos de personalidade. *Direito na Lusofonia.* Direitos e novas tecnologias. Minho, Portugal: Escola de Direito da Universidade do Minho, 2018, p. 20. "A ocorrência de delitos *online* obrigou o TJUE a novo esforço interpretativo, agora tendo em atenção as características específicas da Internet, que se assumem como um meio de divulgação de informação rápido, difuso e de acesso global. [...] Essas características da Internet levaram o TJUE a adotar, especialmente na interpretação do lugar da ocorrência do dano quanto a delitos *online* uma *delict oriented approach*, ou seja, uma interpretação que varia em função do delito em causa, tendo em conta a natureza do direito violado, o âmbito de proteção geográfica desse direito e a análise da extensão do dano. A ideia de partida da *delict oriented approach* é a de que a ocorrência do dano em determinado local depende da condição de o direito em questão ser protegido no território desse Estado. Logo, a *delict oriented approach* tem em consideração a área de proteção geográfica do Direito, pela necessidade de identificar o tribunal mais bem colocado para avaliar a violação do direito em questão."

Além do caso *Bolagsupplysningen*, principal objeto do artigo da autora, também são mencionados outros casos nos quais o TJUE ensaiou a *delict oriented approach* em relação a delitos *online*: o caso *Wintersteiger*[505] sobre violação de propriedade intelectual; o caso *Peter Pinckney*[506] sobre direitos autorais; o caso *Concurrence SARL*[507] sobre direitos de distribuição exclusiva e, ainda, os casos *Shevill*[508] e *eDate*[509], sobre divulgação de conteúdo difamatório ou lesivo.

Em alguns casos, como no *Shevill*, o TJUE adotou posição conhecida como *mosaic approach* (*Mosaikbetrachtung*), permitindo ao lesado propor uma ação no Tribunal de cada lugar ou país onde sofreu danos. Esses, por sua vez, irão reconhecer apenas aqueles danos sofridos em seu território, ou seja: "o atentado feito por uma publicação difamatória à honra, à reputação e à consideração de uma pessoa singular ou colectiva manifesta-se nos lugares onde a publicação é divulgada, quando a vítima é aí conhecida".

Em decisões posteriores, contudo, o TJUE reviu a sua posição, tendo em conta a previsibilidade do foro de ajuizamento da ação a fim de conferir segurança e confiança às partes. Seu propósito também foi no sentido de evitar a multiplicação de foros potencialmente por todos os Estados-membros, em um cenário de incerteza[510].

Afastada a abordagem do *mosaic approach*, a autora conclui que a seu ver, e aplicando as disposições do Regulamento Bruxelas I *bis* para a apreciação dos danos resultantes da violação de direitos de personalidade por colocação de conteúdos na Internet, o tribunal deve ter competência para conhecer a totalidade dos danos ocorridos.

---

[505] Wintersteiger AG c. Producuts 4USoundermachinenbau GmbH, C-523, CJ, 2012.
[506] Peter Pinckney v. KDG Mediatech AG, Processo C-170/12, 2013.
[507] Concurrence SARL contra Samsung Electronics France SAS, Amazon Services Europe Sàrl, Processo C618/15, 21 dez. 2016.
[508] TJUE, Fiona Shevill, Ixora Trading INC., Chequepoint SARL e Chequepoint Interational LTD contra Presse Alliance AS., C-68/93, 07 maio 1995.
[509] eDate Advertising GmbH c. X (C-509/09), 2011.
[510] GONÇALVES, Anabela Susana de Sousa. Op. cit., 2018, p. 23. "Ou seja, o fato de o dano não ser cindível geograficamente e da Internet ter um alcance mundial, o que significa que o conteúdo aí colocado pode ser consultado em qualquer Estado, levou o tribunal a recuar na aplicação da *mosaic approach*, ensaiada anteriormente, quando está em causa a violação *online* dos direitos de personalidade."

Destarte, somente terão competência: os tribunais do local de domicílio do réu[511], os tribunais no lugar do evento causal[512] e os tribunais do centro de interesses do lesado[513].

Tal abordagem, contudo, é restrita à União Europeia, com base na existência de Regulamentos: importante a ressalva de que nos demais casos, como o brasileiro, o *mosaic approach* será, muitas vezes, a única forma para se obter a devida reparação, em conformidade com os danos sofridos em diferentes locais, e em respeito ao nexo de causalidade como um dos elementos essenciais da responsabilização.

Com o Regulamento Geral de Proteção de Dados, a jurisdição internacionalmente competente em demandas que envolvem o meio digital ficou mais clara. Especialmente relevantes tais disposições, já que a localização geográfica dos dados armazenados, por exemplo, em nuvem (*cloud*), poderá determinar o cumprimento de regulação específica de um país ou grupo de países[514]. Existe, portanto, certa flexibilidade na definição da jurisdição competente[515].

---

[511] UNIÃO EUROPEIA. *Regulamento (EU) n.º 1215/2012*. Parlamento Europeu e do Conselho de 12 de dezembro de 2012 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial. Regra geral do art. 4º do Regulamento Bruxelas I *bis*: "Art. 4.º 1. Sem prejuízo do disposto no presente regulamento, as pessoas domiciliadas num Estado-Membro devem ser demandadas, independentemente da sua nacionalidade, nos tribunais desse Estado-Membro. 2. As pessoas que não possuam a nacionalidade do Estado-Membro em que estão domiciliadas ficam sujeitas, nesse Estado-Membro, às regras de competência aplicáveis aos nacionais."

[512] Id., ibid. Art. 7º, n.º 2, do Regulamento Bruxelas I *bis*: "Art. igo 7.º As pessoas domiciliadas num Estado-Membro podem ser demandadas noutro Estado-Membro: [...] 2) Em matéria extracontratual, perante o tribunal do lugar onde ocorreu ou poderá ocorrer o fato danoso; [...]."

[513] Ressalte-se que o centro de interesses do lesado geralmente irá coincidir com o seu local de residência habitual; não obstante, poderá ser, alternativamente, o local onde exerce suas atividades profissionais, por exemplo, desde que demonstrado que há maior proximidade com tal lugar do que com o país de sua residência.

[514] RESINA, Fernando *et al. Cloud – a lei e a prática:* guia e perguntas frequentes. Coimbra: Almedina, 2016, pp. 109-110: "Por exemplo, dependendo da localização da *Cloud* poderão ser equacionadas as regras de transferências internacionais de dados aplicáveis (note-se que dentro da União Europeia/Espaço Econômico Europeu a transferência de dados é livre). Alguns prestadores de serviços *cloud* permitem aos clientes dos seus serviços *cloud* a opção de armazenamento dos dados numa determinada geografia, sem custo adicional, podendo ser selecionada a União Europeia. [...] A transferência de dados pessoais para países terceiros (isto é, países localizados fora da União Europeia/Espaço Econômico Europeu) é possível desde que para um país com um nível de proteção adequado. Caso o país em questão não tenha um nível de proteção adequado, a transferência de dados é permitida, designadamente, se tiverem sido celebrados contratos com o conteúdo das cláusulas contratuais-tipo aprovadas pela Comissão Europeia com as entidades destinatárias dos dados."

[515] Id., ibid., p. 33. "As partes envolvidas num contrato podem estabelecer cláusulas de eleição da lei aplicável ao contrato e escolha do tribunal. [...] Por seu turno, em princípio, os tribunais competentes estão igualmente indicados no contrato e podem resultar da escolha das partes. Contudo, e uma vez mais, pode suceder que um Estado se considere competente para julgar um determinado processo que resulte de incumprimento contratual mesmo que as partes tenham atribuído competência a um tribunal de outro Estado. [...] Veja-se a Lei n.º 41/2013, de 26 de junho (Código de Processo Civil), o Regulamento EU n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial – aplicável apenas às ações judiciais intentadas, aos instrumentos autênticos formalmente redigidos ou registrados e às transações judiciais aprovadas ou celebradas em 10 de janeiro de 2015 ou em data posterior, continuando a aplicar-se o Regulamento (CE) nº 44/2011, de 16 de janeiro, relativo à mesma matéria (Regulamento Bruxelas I) [...]

Em casos que envolvem responsabilidade de autoridades de um Estado-Membro no exercício dos seus poderes públicos, ou seja, envolvendo uma agência de controle governamental, a ação deverá necessariamente ser ajuizada perante os tribunais daquele Estado-Membro, nos termos do art. 78. Já os casos que visam reparação por violações ao Regulamento, cuja responsabilidade é de empresas privadas, devem observar o art. 79.

Em tais hipóteses, há a possibilidade de diversos tribunais serem efetivamente competentes, o que poderá suscitar questões de litispendência (abordadas, por sua vez, no art. 81). Conforme mencionado, o art. 79 dispõe sobre a jurisdição ou a competência internacional, determinando que será competente, em princípio, o Tribunal do local onde o responsável pelo tratamento, ou subcontratante, tenha estabelecimento.

Abre-se a possibilidade de ajuizamento, portanto, em qualquer Estado-Membro no qual a empresa esteja estabelecida, não havendo distinção, segundo o Regulamento, entre estabelecimento e estabelecimento principal. Há, ainda, o reconhecimento da competência do Tribunal do local de residência habitual do demandante, inclusive na hipótese de a empresa não possuir estabelecimento em território da União Europeia[516].

As possibilidades de foros competentes para ajuizar demandas do gênero no âmbito do RGPD são, portanto, múltiplas. Verificada a ocorrência de litispendência, a ação poderá ser suspensa ou extinta, mas em ambos os casos visa evitar que sejam prolatadas decisões conflitantes ou inconciliáveis (art. 81).

Para além do âmbito da responsabilidade civil, o RGPD é aplicável ao tratamento de titulares de dados que se encontrem no território da União, mesmo se o responsável pelo tratamento dos dados ou subcontratante não estiver estabelecido na U.E.[517], nas hipóteses referidas no art. 3º do Regulamento[518].

---

antes de 10 de janeiro de 2015 e abrangidas pelo âmbito de aplicação daquele Regulamento – e a Convenção sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras, celebrada em Nova Iorque a 10 de junho de 1958 [...]. No domínio da relação com o consumidor, refira-se ainda o regime da Lei n.º 144/2015, de 8 de setembro, que estabelece o enquadramento jurídico dos mecanismos de resolução extrajudicial de litígios de consumo [...].”

[516] PINHEIRO, Alexandre Sousa *et al*. (Coords.). *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018, p. 626 e ss.

[517] Id., ibid., p. 112 e ss: “Com este *Marktortprinzip* baseado na *lex loci* pretende-se eliminar a não aplicação do Direito Europeu caso não exista estabelecimento ou sede localizados na UE. A doutrina considera que a estabilidade da instalação pode ser obtida através da instalação de um servidor, da abertura de um apartado ou de uma conta bancária, desde que se verifique uma ação ativa na matéria do tratamento de dados. O n.º 1 estabelece um âmbito territorial de aplicação do RGPD que transcende a UE na medida em que quando o (i) estabelecimento ou o (ii) contexto de atividades se situe em território da UE, se aplica a tratamentos de dados pessoais efetuados na UE ou fora dela. [...] A expressão ‘independentemente de estarem associados a um pagamento’ não significa a gratuidade dos bens ou serviços. O que está em causa é a não ligação necessária a um pagamento financeiro. O pagamento neste caso pode fazer-se através da transação de dados pessoais do próprio ou de terceiros. [...] Relativamente à alínea b) do n.º 2 do artigo sob comentário está em causa o controle do comportamento dos titulares dos dados, caso tenha lugar na UE. Esta ação pode manifestar-se

No caso do Brasil, quando suscitados conflitos entre jurisdições, importam especialmente os arts. 21 a 25 do Código de Processo Civil[519], os quais tratam dos limites da jurisdição nacional[520], bem como o art. 63 do mesmo diploma normativo, que prevê a possibilidade de modificação da competência internacional pelas partes mediante cláusula de eleição de foro.

O legislador interno realizou alteração terminológica no Novo Código de Processo Civil de 2015, ao substituir o título "Capítulo II – da competência internacional" por "Título II – dos limites da jurisdição nacional e da cooperação internacional; Capítulo I – dos limites da jurisdição nacional". Observa-se que houve a substituição da expressão "*competência internacional*" por "*jurisdição*", conferindo caráter mais técnico à norma[521].

---

através da colocação de 'gostos' em redes sociais, e da utilização de formas de vigilância e controle como *webtracking, cookies* ou *social plug-ins*. [...] Existe uma relação evidente entre a necessidade de cumprir os direitos previstos no RGPD e a aplicação da disposição em causa. Esta matéria apresenta-se especialmente sensível na definição de perfis."

[518] UNIÃO EUROPEIA. *Regulamento 2016/679*. Regulamento Geral sobre a Proteção de Dados. Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/45/CE. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC. Acesso em: 08 mar. 2020. "Art. 3º. Âmbito de aplicação territorial. 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. 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. 3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.".

[519] BRASIL. *Lei n.º 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 17 abr. 2020.

[520] TIBURCIO, Carmen. *Extensão e limites da jurisdição brasileira:* competência internacional e imunidade de jurisdição. Salvador: JusPodivm, 2006, p. 101 e ss: "A doutrina discute se as normas sobre jurisdição são taxativas ou exemplificativas. Parte da doutrina entende que os arts. 88 e 89 do CPC de 1973 trazem hipóteses taxativas de exercício da função jurisdicional. Consequentemente, se a causa não estiver dentre aquelas ali enumeradas, a autoridade judiciária não poderá conhecer dela. Já outra corrente doutrinária denomina as normas sobre competência internacional previstas no CPC como 'limites da jurisdição brasileira', mas admite algumas adições às hipóteses previstas nos arts. 88 e 89, nas quais seria absurdo negar o exercício da função jurisdicional no Brasil." Parece ter sido esta segunda corrente aquela adotada pelo Novo Código de Processo Civil, conforme alteração do título do capítulo, tratada a seguir.

[521] Id., ibid., pp. 25-26: "Gaetano Morelli, ao analisar a natureza das normas sobre jurisdição sob outro aspecto, cita duas teorias existentes sobre o tema, com abordagem ligeiramente distinta da citada acima: i) as normas sobre jurisdição no plano internacional restringem o seu exercício, limitando as situações que podem ser julgadas pelo Judiciário nacional; e ii) as normas sobre jurisdição servem também para delimitar a esfera de eficácia do ordenamento jurídico material nacional, pois segundo Chiovenda não pode haver jurisdição se não há aplicação da lei. A primeira teoria parte do pressuposto de que a jurisdição preexiste e, portanto, as normas sobre exercício da função jurisdicional limitam este exercício àqueles casos enumerados. Nas situações não expressamente mencionadas, existe a jurisdição, mas esta não deve, em princípio, ser exercida, seja por não ser do interesse do Estado, seja em razão do princípio da efetividade, tendo em vista a existência de outros Estados, que também exercem validamente a sua jurisdição. A segunda teoria, por sua vez, resulta de confusão entre lei aplicável e exercício da função jurisdicional. [...] Como regra geral, cronologicamente,

Em termos gerais, as previsões relativas aos limites da jurisdição nacional são aquelas elencadas nos arts. 21, 22 e 23 do Código de Processo Civil brasileiro[522].

O termo "jurisdição" determina o "poder de julgar em abstrato, definindo que dada questão com elementos de estraneidade pode ser julgada por um juiz nacional. A jurisdição internacional define, portanto, se o Estado em questão tem poder para alcançar, com suas normas, determinada hipótese; decorre da soberania do Estado"[523].

O entendimento predominante é o de que, em casos que envolvem danos transnacionais por meio da Internet, os tribunais brasileiros possuem competência internacional concorrente quando ocorrer qualquer uma das hipóteses do art. 21 do CPC[524].

---

em primeiro lugar se fixa a jurisdição para, posteriormente, se determinar a lei aplicável. A teoria defendida por Chiovenda inverte a ordem lógica, pois em primeiro lugar se determinaria a lei aplicável e, posteriormente, caso o ordenamento nacional fosse aplicável, se concluiria pela possibilidade de exercício da função jurisdicional. O CPC de 2015 parece referendar o que se vem de dizer, denominando um de seus capítulos "Dos limites da jurisdição nacional". Assim, a lógica adotada, tal como aqui se sustentou, é a de que a jurisdição preexiste, mas é limitada pelas normas previstas no referido capítulo. A premissa é verdadeira, mas isso não significa que é imune a dificuldades: o não exercício da jurisdição em hipóteses previstas na legislação (em razão, por exemplo, do *forum non conveniens* ou da eleição de foro) e o exercício da jurisdição em hipóteses não expressamente previstas são temas que apresentam sutilezas teóricas, como se verá oportunamente. Desde já, contudo, vale registrar a conclusão geral de que não há como se negar que há princípios que podem impedir o exercício da jurisdição em casos expressamente previstos (e.g, soberania – imunidade de jurisdição – e boa administração da justiça – *forum non conveniens*, efetividade, coisa julgada) e, da mesma forma, há princípios que podem determinar o exercício da jurisdição em hipóteses não listadas na legislação (e.g. soberania, vedação à denegação de justiça)."

[522] MONACO, Gustavo Ferraz de Campos. Competência internacional (limites à jurisdição nacional) em matéria de ação revisional de prestação alimentícia e partilha de bens. *Revista de Processo*, 2017, v. 266, pp. 365-391: "Como é sabido – e deflui do conceito de soberania – o legislador brasileiro estabelece normas para que componham o ordenamento jurídico brasileiro. A aplicação da lei brasileira no exterior, quando ocorrer – e é disso que trata o conflito das leis no espaço enquanto objeto do DIP –, ocorre por determinação do legislador de DIP estrangeiro que entendeu por bem determinar, naquele caso, a aplicação da lei brasileira. Não obstante, é incorreto afirmar que o legislador brasileiro estabeleça uma regra pensando no julgador estrangeiro. [...] nosso legislador não se dirige ao juiz estrangeiro impedindo-o, proibindo-o de decidir. A atribuição de competência ao juiz estrangeiro cabe ao legislador estrangeiro, que a avocará se entender que seus magistrados se encontram em condições de bem desempenhar tal competência. Nesse sentido, as normas ditas de competência internacional não são normas que limitam, *a contrario sensu*, o exercício da jurisdição brasileira. Ao avocar as competências que o legislador considera que o julgador brasileiro é capaz de desempenhar, a verdade é que o legislador brasileiro parece deixar de avocar outras competências e, nesse sentido, estabelece limites ao exercício da jurisdição do Estado brasileiro. [...] Assim agindo, tais legisladores criam hipóteses de competência concorrente entre diversos julgadores e o fazem, no mais das vezes, de modo não intencional. [...] Outras vezes – em situações muito limitadas – o legislador desenha a competência jurisdicional e estabelece que as mesmas serão desempenhadas com exclusão de quaisquer outras competências de jurisdições estrangeiras. Nesses casos, o legislador constrói as chamadas competências exclusivas da jurisdição brasileira. No entanto, seria esdrúxula e histriônica eventual posição do legislador de qualquer Estrado soberano que tendesse a distribuir competências judiciárias entre os cerca de 200 Estados soberanos existentes no mundo."

[523] CASTRO, Emília Lana de Freitas; WINTER, Patrícia Pereira. Op. cit., 2014, v. 18, p. 3,5.

[524] TIBURCIO, Carmen. As regras sobre o exercício da jurisdição brasileira no novo Código de Processo Civil. *Revista Interdisciplinar de Direito.* Faculdade de Direito de Valença, jan./jun. 2018, v. 16, n. 1, pp. 67-90, pp. 68-69. "Em primeiro lugar, cumpre observar que o Código de Processo Civil de 2015 não trouxe qualquer alteração às hipóteses de competência concorrente já previstas no CPC de 1973, quais sejam: (i) réu domiciliado no Brasil; (ii) obrigação a ser cumprida no Brasil; e (iii) ação que decorra de ato ou fato ocorrido no Brasil. Salvo algumas alterações redacionais, o art. 21 do novo Código basicamente reproduziu o art. 88 do CPC 1973. [...] As reais inovações foram reservadas para o artigo subsequente, no qual foram previstas

Por conseguinte, o réu de qualquer nacionalidade que estiver domiciliado no Brasil atrairá o reconhecimento da jurisdição brasileira, ainda que o *website* utilizado como veículo para a produção do dano esteja hospedado no exterior[525].

Mesmo com a alteração do Código de Processo Civil (CPC), ocorrida em 2015, conservou-se a previsão do reconhecimento da concorrência entre jurisdições sempre que o evento danoso aos direitos ocorrer em território brasileiro, ou quando o ato ilícito for praticado no Brasil, segundo consta no inc. III do art. 21 do mesmo diploma.

Já o art. 25 do CPC de 2015 trouxe inovação ao

> estabelecer regra explícita determinante do afastamento da jurisdição brasileira em razão da vontade das partes no processo. Sendo certo que tal solução já encontrava precedentes na jurisprudência, embora minoritária, sua inclusão no texto não apenas afasta quaisquer dúvidas pendentes, mas também auxilia no balizamento dos caminhos solucionadores de questões relevantes, ao mesmo tempo em que abre novas oportunidades para interpretação e debate[526].

Interessante, pois, trazer a definição de "contratos internacionais" apresentada por Irineu Strenger[527], para quem "um contrato é internacional, desde que seja conectado a

---

novas hipóteses de competência concorrente relativamente a ações de alimentos – (a) domicílio ou residência do autor; e (b) existência de vínculos entre o réu e o país; e consumo – domicílio ou residência do consumidor. O dispositivo também inovou ao tratar dos efeitos positivos da cláusula de eleição de foro, tema que será abordado em outro tópico do presente trabalho. [...] A inclusão dessas duas hipóteses privilegiando tanto o alimentando quanto o consumidor deixou evidente a intenção do legislador de beneficiar a parte mais fraca das relações jurídicas em questão, visando atender ao princípio do acesso à justiça. Em que pese o acerto dessa decisão de trazer as referidas regras ao CPC, dotando-as de maior clareza e segurança, é preciso reconhecer que não se trata propriamente de uma novidade: essas já constavam de convenções internacionais ratificadas pelo Brasil e já eram aplicadas pela jurisprudência."

[525] ROBERTO, Wilson Furtado. *Dano transnacional e internet:* direito aplicável e competência internacional. Curitiba: Juruá, 2010.

[526] COSTA, José Augusto Fontoura; SANTOS, Ramon Alberto dos. Contratos internacionais e a eleição do foro estrangeiro no Novo Código de Processo Civil. *Revista de Processo*, mar. 2016, v. 253, (s.p.). "O texto legal, ao mesmo tempo em que autoriza a exclusão da jurisdição brasileira baseada no acordo de vontades entre as partes, estabelece limites para tanto. Um deles é a exclusividade do foro estrangeiro escolhido, ou seja, este deve ser indicado como uma possibilidade única, sem dar a qualquer das partes o condão de escolher unilateralmente. Outro é o caráter contratual, excluindo-se a possibilidade de estender os efeitos a quaisquer situações que não possam ser objeto de contratação. Além disso, a cláusula de eleição deve ser escrita e aludir claramente ao âmbito material de sua cobertura. Não poderá ser abusiva, o que pode ser declarado de ofício pelo juiz ou alegado pelo réu na contestação. Por fim, o contrato onde se insere a cláusula de eleição de foro deve ser internacional."

[527] STRENGER, Irineu. Aspectos da Contratação Internacional. *Revista da Faculdade de Direito, Universidade de São Paulo.* São Paulo, jan./2001, v. 96, pp. 455-474, pp. 456-457. "À diferença dos contratos tradicionais, os internacionais identificam-se com as exigências nascidas do caráter setorizante e profissionalizante dos negociantes transnacionais, cujas relações exigem soluções complexas, geralmente traduzidas em técnicas próprias, e correlatas às peculiaridades do comércio envolvido. Tarefa das mais árduas será a procura dos conceitos no plano do comércio internacional, pela incipiência de suas formas de expressão. O comércio internacional, identificado com a *lex mercatoria*, explica-se como trajetória cheia de percalços, pela alta fecundidade de seus agentes reveladores, os quais põem, inevitavelmente, em constante interação, os fatores da prática e da teoria. Tentar conceituações abrangentes, em relação aos contratos do comércio internacional, seria lançar-se em densa floresta, na qual as picadas continuam sendo abertas, sem que o ponto de chegada tenha sido determinado. Deste modo, a conceituação dos contratos internacionais do

normas jurídicas emanadas de vários Estados, em razão, notadamente, de seu lugar de conclusão ou execução, da localização de seu objeto, da nacionalidade ou do domicílio das partes"[528]. O autor expressa ainda que:

> São contratos internacionais do comércio todas as manifestações bi ou plurilaterais da vontade livre das partes, objetivando relações patrimoniais ou de serviços, cujos elementos sejam vinculantes de dois ou mais sistemas jurídicos extraterritoriais, pela força do domicílio, nacionalidade, sede principal dos negócios, lugar do contrato, lugar da execução, ou qualquer circunstância que exprima um liame indicativo do Direito aplicável[529].

Quanto à interpretação do art. 21, inc. III, do CPC, vale trazer como referência o caso submetido ao julgamento do Superior Tribunal de Justiça, no qual restou claro que "o direito de resguardo à imagem e à intimidade é autônoma em relação ao pacto firmado, não sendo dele decorrente"[530].

Ao analisar o referido acórdão, Emília Lana de Freitas Castro e Patrícia Pereira Winter entendem que há certa flexibilidade no Direito brasileiro no que diz respeito ao critério do acesso à mensagem lesiva pelo usuário-vítima[531]. Nesse sentido, considerar o local onde o ilícito promoveu maiores efeitos negativos à vítima evita que a jurisdição competente para o caso nada tenha a ver com o conflito que se pretende dirimir[532].

O conceito tradicional de soberania, assim como o de privacidade, vem sofrendo transformações substanciais[533], criando desafios para a determinação do exercício da jurisdição do Estado em um determinado território. "A Internet torna mais difícil o controle regulador físico do Estado em razão da ausência de fronteiras"[534]. Dessa forma, ao utilizarem a Internet, os indivíduos raramente estão cientes de que praticam atos sob as leis de outra jurisdição, diferente daquela do local de acesso[535].

---

comércio parte dos pressupostos fáticos, encaminhando-se, na medida do possível, para a sintetização, tecnicamente assimilada, de seus principais elementos."

[528] Id., ibid., pp. 470-471.

[529] Id., ibid., p. 472.

[530] STJ. Superior Tribunal de Justiça. *Resp. 1168546/RJ*. Rel. Ministro Luis Felipe Salomão. Quarta Turma, julgado em 11 maio 2010, DJE em 07 fev. 2011, p. 15.

[531] CASTRO, Emília Lana de Freitas; WINTER, Patricia Pereira. Op. cit., 2014, p. 3,7.

[532] ROBERTO, Wilson Furtado. Op. cit., 2010.

[533] MONACO, Gustavo Ferraz de Campos. A globalização entre o passado e o futuro da soberania. *Revista da Faculdade de Direito do Sul de Minas*, v. extra, 2008, pp. 45-53.

[534] COSTA, Ligia Maura. *Direito Internacional Eletrônico.* Manual das Transações *On-Line*. São Paulo: Quartier Latin, 2008, p. 32, *apud* CASTRO, Emília Lana de Freitas; WINTER, Patricia Pereira. Op. cit., 2014, p. 3.

[535] Id., ibid., p. 3.

Diante desse cenário, há critérios específicos para determinar a competência de casos que envolvem a *web*[536]. A primeira característica de tais critérios de conexão é o fato de que demonstram vinculação objetiva ou territorial do problema a um Estado (seja quanto ao local de execução de obrigação, local de celebração de contrato, nacionalidade ou domicílio das partes envolvidas, local de produção do dano, entre outros)[537].

O segundo aspecto está relacionado com o fato de que os critérios clássicos do Direito Internacional Privado são rígidos e neutros, fazendo referência a conceitos jurídicos definidos legalmente[538]. A neutralidade pode desempenhar um papel favorável na solução de conflitos em casos práticos – contudo, a rigidez desses mesmos critérios, confrontada com a fluidez das questões que envolvem a Internet, por vezes pode representar um óbice à sua efetiva solução.

Nem sempre, contudo, tais critérios tradicionais bastam para identificar a adequada solução dos conflitos de jurisdições (assim como dos conflitos entre leis aplicáveis) quando tratados casos no âmbito *online*. E, ainda que Dolinger[539] defenda a determinação da lei aplicável, conforme o princípio da proximidade[540], e que isso confira certa flexibilização ao Direito Internacional Privado, o alcance global da Internet possui impacto direto sobre os critérios clássicos até então utilizados[541], aspecto que não pode ser ignorado[542].

3.2 DETERMINAÇÃO DA LEI APLICÁVEL

A identificação dos critérios de conexão aplicáveis, e consequente determinação da lei aplicável, é igualmente desafiadora[543]. As regras de conflitos, por serem baseadas em

---

[536] CASTRO, Emília Lana de Freitas; WINTER, Patricia Pereira. Op. cit., 2014, p. 3.
[537] Id., ibid., p. 3.
[538] Id., ibid., p. 3.
[539] DOLINGER, Jacob; TIBURCIO, Carmen. *Direito Internacional Privado*. 15. ed. Rio de Janeiro: Forense, 2020.
[540] DOLINGER, Jacob. Direito Internacional Privado – O princípio da proximidade e o futuro da humanidade. *Revista Brasileira de Direito Administrativo*. Rio de Janeiro, 2004, v. 235, pp. 139-149.
[541] ROBERTO, Wilson Furtado. Op. cit., 2010, p. 26. "Os princípios tradicionais do Direito Internacional Privado se relacionam com atividades que tenham uma localização física, e não, virtual, com exceção do princípio da nacionalidade, que é típico no Direito Internacional de Família, e o sucessório, pelo menos nos sistemas jurídicos que adotam a *civil law*. [...]. Vale salientar que, na Internet, tudo o que se refira a lugar, território ou cadeira estará perdendo sentido, pois a eletrônica acelera a desterritorialização do Direito."
[542] VICENTE, Dário Moura. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005, p. 101. "As relações jurídicas respeitantes à produção, utilização e transmissão de informação através de redes electrônicas de comunicação não se eximem, pois, à regulação estadual. O ideal de liberdade que se acha associado à Internet carece, por isso, de ser compatibilizado com o exercício das soberanias nacionais. Eis por que a principal dificuldade [...] não deriva, a nosso ver, da inexistência de uma lei aplicável, mas antes [...] a uma pluralidade de leis nacionais."
[543] POLIDO, Fabrício Bertini Pasquot. *Direito internacional privado nas fronteiras do trabalho e tecnologias:* ensaios e narrativas na era digital. Rio de Janeiro: Lúmen Juris, 2018, pp. 127-128. "Casos

normas clássicas e/ou vigentes de conexão, com caráter essencialmente localizado (em oposição à deslocalização da Internet), poderiam mostrar-se, por vezes, inadequadas – o que não significa, contudo, que sejam inaplicáveis em conflitos relacionados ao meio digital[544].

Enquanto os limites geográficos tradicionais não se enquadram à realidade da rede mundial de computadores[545], os princípios tradicionais do Direito Internacional Privado se relacionam com atividades que tenham uma localização física e não virtual (com exceção do princípio da nacionalidade, típico do Direito de Família, de inspiração manciniana, frequentemente adotado na Europa continental). Os elementos de conexão, portanto, como a *lex rei sitae* e a *lex loci delicti commissi*, podem se tornar inconsistentes e inadequados em um mundo desterritorializado[546].

Cumpre esclarecer que uma das premissas da pesquisa realizada é a possibilidade de solucionar questões e conflitos surgidos no âmbito da Sociedade da Informação a partir de teorias e princípios elaborados em contextos anteriores ou estranhos a ela. Desta forma, se o problema atualmente proposto oferece novos desafios, impondo-se, por vezes, a

---

envolvendo atos delituais no espaço virtual, dentre eles aqueles relacionados à violação de direitos de personalidade (direito ao nome, honra, imagem e privacidade), indicam, portanto, a enorme dificuldade prática e metodológica na aplicação da regra *lex loci delicti*. A primeira crítica da doutrina aparece quanto à dependência normativa do DIP, nessas situações, do critério espacial ou de localização territorial para identificação do direito aplicável às obrigações delituais. Isso porque, em ambientes digitais a noção clássica de territorialidade cai por terra, na exata medida em que o amplo domínio da rede mundial de computadores é - por natureza e contingência – multilocalizado e multiterritorial. [...] Não somente isso. O fluxo de informações também relacionado ancilarmente à atividade cibernética (aqui compreendida como conjunto de atos praticados por usuários de internet, servidores e provedores de acesso e conteúdo) indica uma dificuldade de precisar sua localização em um único território formalmente considerado, inclusive ofuscando o que é público do privado e vice-versa. Os métodos do direito internacional privado passariam invariavelmente por uma necessária reconsideração."

[544] BOYLE, James. Foucault in Cyberspace: Surveillance, Sovereignty and Hardwwired Censors. *University of Cincinnati Law Review,* 1997, n.º 66, pp. 179-180. "Quanto aos obstáculos tecnológicos que a Internet levantou contra a filtragem de conteúdo imposta externamente, é preciso acrescentar os obstáculos geográficos levantados por sua extensão global. Como um documento pode ser recuperado tão facilmente de um servidor a cinco mil milhas de distância ou de um arquivo de servidor a milhas de distância, a proximidade geográfica e a disponibilidade de conteúdo são independentes uma da outra. Se o mandato do rei atingir apenas a espada do rei, presume-se que grande parte do conteúdo da Internet esteja livre da regulamentação de qualquer soberano em particular." (Tradução livre). "*To the technological obstacles the Internet raised against externally imposed content filtration, one must add the geographic obstacles raised by its global extent. Because a document can be retrieved as easily from a server five-thousand miles away or a server file miles away, geographical proximity and content availabilty are independent of each other. If the king's writ reaches only as far as the king's sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular soverein."*

[545] KESSEDJIAN, Catherine. *Le temps du droit au XXIe siècle.* Compatibilité avec la codification? Les Cahiers de droit. Faculté de droit de l'Université Laval, 2005, v. 46, n.º 1-2, pp. 547-560, p. 551. "Um dos elementos próprios ao século XXI é certamente a aceleração do tempo, aceleração em relação à qual o tempo jurídico não representa exceção." (Tradução livre). *"Un des éléments propres au XXI° siècle est certainement l'accélération du temps, accélération à laquelle le temps juridique ne fait pas exception*."

[546] ROBERTO, Wilson Furtado. Op. cit., 2010, p. 16. "A possibilidade de o resultado danoso, decorrente da conduta ilícita, verificar-se em vários Estados nacionais desencadeia um complexo problema acerca da lei aplicável e do foro de competência".

necessidade de buscar soluções igualmente inovadoras, também será possível fazer uso de critérios de conexão e princípios tradicionalmente utilizados pelo Direito Internacional Privado, assim como de conceitos e princípios já consolidados no âmbito do Direito Civil, em especial no que tange à responsabilidade civil[547].

No domínio das redes digitais e bens informáticos, há duas orientações divergentes no que tange à política legislativa a ser adotada: por um lado, é sustentada a "livre circulação dos serviços da Sociedade da Informação, e um reconhecimento tão amplo quanto possível de direitos de exclusivo uso sobre os bens informáticos"[548]. Neste caso, é postulada a aplicação da *lex originis* aos bens e serviços em questão, preponderando a autorregulação e a utilização de meios extrajudiciais para a composição de litígios[549].

Por outro lado, é possível sustentar a imposição de limites a tais atividades, tendentes a "salvaguardar os interesses do Estado e de certos grupos sociais carecidos de proteção"[550] – hipótese na qual a preferência é pela aplicação da *lex destinationis*, prevalecendo a regulação estadual e a solução de controvérsias pelo Poder Judiciário.

Dário Moura Vicente ressalta que, em um caso ou em outro, há de se levar em conta a tutela do princípio da confiança, de maneira que uma "aplicação demasiado extensa da *lex destinationis* comprometerá, pois, inevitavelmente este valor e o próprio reforço da liberdade individual que muitos auguraram com o advento da Internet"[551].

Se em caso analisado pelo Judiciário for reconhecida a competência internacional, deverá ser levada em consideração, ainda, a possibilidade do surgimento de conflitos entre

---

[547] A discussão acerca da necessidade de desenvolver uma disciplina normativa específica para a matéria é objeto, particularmente, da obra de Dário Moura Vicente anteriormente citada, bem como do artigo de José Augusto Fontoura Costa e Fernanda Sola (VICENTE, Dário Moura. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005; COSTA, José Augusto Fontoura; SOLA, Fernanda. Direito das tecnologias de comunicação e informação: uma primeira abordagem do Marco Civil da Internet. *PIDCC.* Aracaju, fev/2015, ano IV, ed. nº 08/2015, pp. 336-351; POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018).

[548] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 97.

[549] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, pp. 115-116. "Outro importante tema no Direito Internacional Privado da Internet diz respeito à interface com os aspectos da qualificação e lei aplicável em matéria de obrigações extracontratuais (delituais) nas redes. [...] é importante ter em mente que o tema se desdobra em duas grandes abordagens: de um lado, permite reconhecer que relações intersubjetivas na Internet têm se desenvolvido ancoradas no exercício de direitos e garantias fundamentais, como a liberdade de expressão, proteção da privacidade, livre iniciativa, autonomia privada, proteção do consumidor e das relações laborais. De outro, constata-se a existência de autênticos conflitos de concepções e de interesses sobre os objetivos sistêmicos envolvidos na própria 'Governança da Internet', entre a proteção da privacidade e de dados pessoais de usuários, e flexibilidades associadas aos modelos de negócio, atividade empresarial nas redes, governo eletrônico e papeis constritivos do Big Data."

[550] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 97.

[551] Id., ibid.

leis potencialmente aplicáveis[552]. Ainda que o problema dos limites das leis[553] seja entendido por parte da doutrina como o principal problema trabalhado no âmbito do Direito Internacional Privado, João Baptista Machado o aponta como problema secundário e subordinado, decorrente do primeiro, a "colisão entre leis"[554], referindo-se ao conflito de leis[555].

No caso de relações plurilocalizadas, como ocorre com aquelas estabelecidas por meio da Internet, ou seja, relações nas quais entram em contato mais do que um único ordenamento jurídico, torna-se necessário coordenar a aplicação das várias leis, a fim de prevenir o concurso de normas[556].

Baptista Machado destaca que, em matéria de conflito de leis, há um primeiro e fundamental problema: nas palavras do próprio autor, trata-se do "problema da limitação (da autolimitação intrínseca) da esfera de eficácia da lei por força do seu carácter de regra de dever-ser"[557]. Nesse sentido, defende que o critério delimitador do possível âmbito de eficácia de uma lei deve se referir apenas a fatos, atendendo unicamente às suas concretas ligações (ou ausência de ligações) com o sistema jurídico, cujo âmbito de aplicabilidade trata de delimitar.

---

[552] ARAUJO, Nadia de. Op. cit., 2016, (s.p.). "Berço da teoria do conflito de leis, com os estatutários italianos, e depois com a tese savigniana, incorporada nas grandes codificações, a Europa encontra-se mais uma vez na liderança do movimento precursor de uma nova era do DIPr. Ao invés de considerá-lo um mero direito de remissão, encara-o como um verdadeiro direito de decisão. Seu objetivo maior é promover a regulamentação adequada e materialmente mais justa da questão plurilocalizada. A disciplina é mais do que a designação formal de uma lei, preocupando-se com a justiça material na própria formulação das normas de conflitos. Esse desenvolvimento fez surgir novos tipos de regras de DIPr: as materiais, as narrativas e as de aplicação imediata. Não houve um abandono do método conflitual tradicional, mas um maior ecletismo para se obter a solução do problema, tornando o pluralismo de métodos uma das características do DIPr atual."

[553] MACHADO, J. Baptista. *Âmbito de eficácia e âmbito de competência das leis.* Coimbra: Almedina, 1998, p. 3. Para o DIP, "qualquer lei é aplicável a todos e quaisquer fatos que apenas estejam em contato com essa lei (casos meramente internos)" e "qualquer lei é aplicável a todos e quaisquer fatos que apresentem em relação a ela uma qualquer conexão ou contato".

[554] Id., ibid., p. 3 e ss.

[555] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 80. "Optaremos, [...] por examinar, primeiramente, os problemas postos pela determinação do Direito aplicável e só depois os que suscitam a fixação do tribunal ou dos tribunais internacionalmente competentes. Por duas ordens de razões. Por um lado, porque a complexidade daquela primeira categoria de problemas, bem como a sua especificidade no domínio em apreço, são inequivocamente superiores [...]. Por outro lado, porque, podendo as regras de conflito de leis operar como verdadeiras regras de conduta, ainda que indiretas, a sua atuação em concreto não depende necessariamente de um ato judicial de aplicação; além de que a determinação do órgão jurisdicional competente para este efeito pode pressupor, como referimos acima, a determinação de lei aplicável ao mérito da causa. Nada impõe, por conseguinte, a subordinação do estudo científico ao das regras de conflitos de jurisdições."

[556] DOLINGER, Jacob; TIBURCIO, Carmen. *Direito Internacional Privado*. 15. ed. Rio de Janeiro: Forense, 2020 (E-book), p. 278. "Estas normas *[normas indiretas de direito internacional privado]* não solucionam a questão jurídica propriamente dita, não dizem se a pessoa é capaz ou incapaz, se o contrato é válido ou não, [...] e assim por diante. As regras de conexão do DIP apenas escolhem, dentre os sistemas jurídicos de alguma forma ligados à hipótese, qual deve ser aplicado. São normas instrumentais."

[557] MACHADO, J. Baptista. Op. cit., 1998, p. 13 e ss.

Em obra distinta, o autor apresenta sua visão sobre a teoria da Regra de Conflitos, em que destaca um elemento da situação de fato suscetível de apontar para uma, e apenas para uma das leis em concurso, por ele designadas "leis interessadas"[558]. Este seria o elemento de conexão apresentado conjuntamente com a ideia de "conceito-quadro".

As principais conexões são apresentadas a seguir, dentre as quais se destacam: a nacionalidade, o domicílio, residência habitual ou simples, ou sede de uma pessoa coletiva; a situação de uma coisa (*lex rei sitae*); o local de prática do ato (*lex loci actus, lex loci delecti commissi*); o local de cumprimento de uma obrigação; a convenção entre as partes sobre a lei aplicável; e o nexo de interligação com uma outra relação jurídica.

Ferrer Correia aponta que cada Estado possui o seu próprio Direito Internacional Privado para uso interno, ou seja, normas próprias, com interpretação própria[559]. Nesse sentido, as regras de conflitos do DIP se propõem a resolver um problema de concurso entre preceitos jurídico-materiais procedentes de diversos sistemas de Direito.

No seu entendimento, as regras de conexão podem ser divididas em: (i) regras que se referem à pessoa dos sujeitos da relação jurídica; (ii) que se referem ao ato ou fato jurídico encarado em si mesmo; ou (iii) que se referem à coisa objeto do negócio jurídico[560].

Destarte, as regras de Direito Internacional Privado teriam caráter meramente instrumental, já que se limitam a indicar a lei que fornecerá o regime da situação e não se prestam a compor elas mesmas os conflitos interindividuais de interesses. Ainda que contribuam para a resolução da questão jurídico-privada, não dizem elas próprias qual é de fato a relação[561].

---

[558] MACHADO, J. Baptista. *Lições de Direito Internacional Privado*. 3. ed. Coimbra: Almedina, 2006, p. 57.
[559] CORREIA, António Ferrer. *Lições de Direito Internacional Privado*. Coimbra: Almedina, 2000, p. 19.
[560] Id., ibid., p. 21.
[561] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, p. 119 e ss. "Existe significativa dificuldade, do ponto de vista do Direito Internacional Privado para definição de regras de conexão determinadoras de lei aplicável às obrigações delituais com conexão internacional. Em particular, essa tarefa, ao menos à primeira vista, dependerá de duas variáveis centrais: a primeira diz respeito à adequada qualificação dos casos em contato com uma pluralidade de ordens jurídicas e eventual dissociação geográfica ou espacial entre a ocorrência do fato delitual e o dano; a segunda, por seu turno, refere-se às escolhas de política regulatória sobre responsabilidade civil, mecanismos de apuração dos danos e padrões de indenizações aplicáveis, levando a distintas visões dos ordenamentos jurídicos domésticos sobre o problema. A escolha de lei aplicável, portanto, é decisiva para que as partes visualizem e estimem as consequências da responsabilidade extracontratual, particularmente nos casos em que os tribunais tenham de decidir pela imputação da responsabilidade e *quantum* indenizatório em relação à parte autora do ato ilícito. Não se trata de uma demanda específica dos casos pluriconectados envolvendo a Internet. Entretanto, a multiplicidade das conexões proporcionadas pela ubiquidade, virtualidade e caráter multiterritorial dos atos praticados naquele ambiente fazem da grande rede mundial de computadores autêntico laboratório para questões de lei aplicável aos ilícitos cibernéticos."

Para Dario Moura Vicente, em demandas envolvendo privacidade e proteção de dados pessoais, é preciso levar em conta o local onde está estabelecido o agente econômico responsável pelo seu tratamento, considerado a origem da informação. A seu ver, trata-se do elemento de conexão fundamental a ser observado em tal matéria para reputar uma lei como aplicável, na hipótese de estabelecimento localizado na União Europeia, revelando a chamada "conexão principal". Nos demais casos, o autor aponta como aplicável a lei do local onde for realizado o tratamento dos dados, tratando-se da conexão subsidiária[562].

Em caso de empresa com estabelecimento fora do território da União, ainda que a ação possa ser ajuizada no país da residência habitual da vítima do dano, a lei aplicável é a do local de tratamento dos dados que, por sua vez, poderia ser distinto de ambos os países de autor e réu da ação. Importante ressaltar, contudo, as hipóteses nas quais reputa-se o RGPD como aplicável, constantes no art. 2º[563], que determina o âmbito de aplicação material da norma[564].

No caso brasileiro, a atual Lei de Introdução às Normas do Direito Brasileiro (LINDB) sucedeu a Introdução ao Código Civil de 1916, que previa a adoção do critério da nacionalidade como regra de conexão para reger o estatuto pessoal – diferentemente dos

[562] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, p. 143 e ss.

[563] UNIÃO EUROPEIA. *Regulamento 2016/679*. Regulamento Geral sobre a Proteção de Dados. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:T OC. Acesso em: 08 mar. 2020. "Art. 2º. Âmbito de aplicação material. 1. O presente regulamento aplica-se ao 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. 2. O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. 3. O Regulamento (CE) n. 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n. 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no art. 98. 4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus arts. 12 a 15."

[564] PINHEIRO, Alexandre Sousa *et al*. (Coords.). Op. cit., 2018, p. 101 e ss. "O propósito existente consiste em assegurar a aplicação da RGPD respeitando o princípio da neutralidade tecnológica, o que significa que as suas suposições devem aplicar-se a tratamentos de dados automatizados ou manuais [...]. O n.º 2 da disposição sob comentário estabelece as delimitações negativas do âmbito material de aplicação do RGPD. Na alínea a) estão as atividades não sujeitas à aplicação do direito da União, que tem como exemplo as atividades de defesa nacional [...]. Ou seja, segundo esta doutrina, a regra geral será a da não aplicação do RGPD na utilização das redes sociais. A boa leitura do considerando leva, no entanto, a concluir que nos casos de natureza comercial ou profissional, por não se tratar de matéria exclusivamente pessoal ou doméstica, verificar-se-á a aplicação do RGPD, nomeadamente do complexo de direitos envolvidos. Tal significa que a rede social deve garantir aos utilizadores formulares de proteção da privacidade que permitam limitar o acesso à informação, escolhendo-se destinatários exclusivos ou permitindo a criação de grupos fechados [...]."

demais países da América Latina[565]. Assim, desde 1942, a Lei do Domicílio é aquela que rege, no Brasil, a personalidade, a capacidade, o nome e os direitos de família[566].

As regras que determinam a lei aplicável a cada caso, e como será a sua prova em caso de lei estrangeira, podem ser encontradas atualmente na LINDB (especialmente nos arts, 9º a 16), assim como no Regimento Interno do Supremo Tribunal Federal (art. 115, inc. I[567], e art. 116[568]) e no Código de Processo Civil (art. 376[569]). Por serem regras de conflito, as normas da LINDB não oferecem a solução material para os conflitos, mas tão somente indicam a lei aplicável para tal fim – se a lei estrangeira ou a lei do foro[570].

Os critérios de conexão adotados podem sofrer exceções, de modo que há princípios que permitem um determinado ordenamento jurídico rejeitar os elementos que

---

[565] MONACO, Gustavo Ferraz de Campos. Direito Internacional Privado da Família: influências da História e da Geografia do Brasil. *In*: MONACO, Gustavo Ferraz de Campos; FULCHIRON, Hugues (Orgs.). *Famílias internacionais:* seus direitos, seus deveres. São Paulo: Intelecto, 2016, v. 1, pp. 3-28, p. 18. "Nacionalidade e domicílio despontam, assim, como conceitos jurídicos apegados a valores socialmente presentes desde os tempos coloniais e podem, assim, dar pistas acerca das escolhas que, em termos de direito internacional privado das famílias, se haverá de fazer no Brasil e nos estados soberanos provenientes da reorganização das antigas colônias espanholas. Daí porque, e essa é a hipótese aqui defendida, tenham os brasileiros optado por manter-se vinculados ao critério da nacionalidade [...] ao passo que nossos vizinhos tenham cedo se rendido ao domicílio como critério de conexão apto a levar as leis dos Estados independentes a serem mais constantemente aplicadas em matéria de personalidade, capacidade e direitos de família. [...] Assim, nas colônias espanholas eram, via de regra, aplicados os próprios direitos nacionais, [...]. No entanto, no Brasil, as questões [...] tanto podiam ser resolvidas com a aplicação da lei brasileira, quanto de uma lei estrangeira qualquer, pois o critério determinante no Império era o da nacionalidade do chefe de família."

[566] Id., ibid., p. 26. "Assim é que, aproveitando-se da encomenda política para a elaboração de uma Lei de Introdução ao Código Civil que revogasse a Introdução ao Código Civil de 1916 [...], modificaram a conexão para as questões pessoais, fazendo incidir, a partir da edição do Decreto-lei n.º 4.567, de 1942, a lei do domicílio para reger a personalidade, a capacidade, o nome e os direitos de família."

[567] STF. Supremo Tribunal Federal. *Regimento Interno*. 2019. Disponível em: https://www.stf.jus.br/arquivo/cms/legislacaoRegimentoInterno/anexo/RISTF.pdf. Acesso em: 17 abr. 2020. "Art. 115. Nos recursos interpostos em instância inferior, não se admitirá juntada de documentos desde que recebidos os autos no Tribunal, salvo: I – para comprovação de textos legais ou de precedentes judiciais, desde que estes últimos não se destinem a suprir, tardiamente, pressuposto recursal não observado; [...]."

[568] Id., ibid. "Art. 116. Em caso de impugnação, as partes comprovarão a fidelidade da transcrição de textos de leis e demais atos do poder público, bem como a vigência e o teor de normas pertinentes à causa, quando emanarem de Estado estrangeiro, de organismo internacional ou, no Brasil, de Estado e Municípios."

[569] BRASIL. *Lei n.º 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 17 abr. 2020. "Art. 376. A parte que alegar direito municipal, estadual, estrangeiro ou consuetudinário provar-lhe-á o teor e a vigência, se assim o juiz determinar."

[570] ARAUJO, Nadia de. Op. cit., 2016. "O método conflitual tradicional, ainda utilizado pelo Direito Internacional Privado dos países da Europa e da América Latina, com as modificações que a seguir serão comentadas, tem como particularidade a existência de uma regra de DIPr – a regra de conflito, que dá a solução de uma questão de direito contendo um conflito de leis através da designação da lei aplicável pela utilização da norma indireta. Não compete ao DIPr fornecer a norma material aplicável ao caso concreto, mas unicamente designar o ordenamento jurídico ao qual a norma aplicável deverá ser buscada. Para a concepção clássica do DIPr, é através de normas de conflitos que o DIPr cumpre a sua missão de prover a regulamentação da vida jurídica internacional. [...] Outra maneira de enfrentar essas diferenças entre as regras conflituais, pela sua diversidade de país a país, foi a criação de normas conflituais internacionalmente uniformes. Para Dolinger, esse seria um DIPr uniformizado, em oposição àquele já existente quando se trata de uma determinada área de direito substantivo, resultante do esforço comum de cooperação de dois ou mais Estados."

se chocam com suas concepções. Neste ponto, Luiz Olavo Baptista trata do princípio da ordem pública, da fraude à lei, da reciprocidade e, por fim, do interesse nacional lesado[571].

Há entendimento, conforme expõe Fabrício Bertini Pasquot Polido, no sentido de possibilitar a adoção de outros critérios de conexão pelo julgador em situações que envolvem atos de violação transfronteiriça de direitos de personalidade (inclusive aqueles relativos à violação da privacidade). Assim, revisitados "tanto o método clássico do Direito Internacional Privado como problemas apresentados pela Internet, seria possível identificar uma pluralidade de elementos de conexão relacionados à lei aplicável aos ilícitos pluriconectados"[572].

Necessária, contudo, a seguinte ressalva: considerando que a justificativa legal é imprescindível para fundamentar decisões judiciais, havendo que se apontar a norma com base na qual a lide foi decidida, o mesmo se aplica aos critérios de conexão: em caso de adoção de critérios distintos daqueles dispostos expressamente no texto da lei, faz-se imprescindível justificativa, também com base legal.

Depreende-se, portanto, que a aplicação de critérios alternativos de conexão se faria possível tão somente em duas hipóteses: em caso de previsão expressa (por meio de uma "cláusula de exceção") ou em caso de lacuna, diante da qual o juiz não pode se abster de

---

[571] BAPTISTA, Luiz Olavo. Aplicação do direito estrangeiro pelo juiz brasileiro. *Revista de Informação Legislativa*. Brasília, abr./jun. 1999, ano 36, n.º 142, p. 271. "Pode também ocorrer a impossibilidade de se empregar um ponto de localização, uma circunstância de conexão: é o caso de nacionalidade em relação aos apátridas, ou a pessoas cuja lei nacional seja indeterminável. A impossibilidade de se estabelecer uma circunstância de conexão ou a inexistência da figura jurídica definida pela lei estrangeira tem conseqüências jurídicas diferentes dos casos de ordem pública e fraude à lei: não há a ineficácia, mas sim a impossibilidade jurídica de se abranger a situação da forma indicada pela regra de conflitos, a ensejar a aplicação da lei nacional. Assim, a regra de conflitos, como toda a regra, comporta exceções: exceções à aplicação do direito por ela indicado, ou a sua própria aplicação. Essa é uma outra maneira pela qual o problema poderia ser abordado. Essas exceções vêm, com desculpas pelo chavão, confirmar a regra de aplicabilidades do direito estrangeiro. Servem-lhe de elemento moderador, reforçando a validade do sistema multissecular que busca antes de tudo a justiça, a certeza do direito e a estabilidade das relações jurídicas internacionais. A balança da justiça aí coloca em seus pratos, de um lado, a autoridade, visando assegurar a justiça nas relações interpessoais, e, de outro, a vontade dos indivíduos, procurando tirar o melhor partido de sua liberdade. E é o equilíbrio dessa balança que todos nós buscamos."

[572] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, p. 138 e ss. Neste contexto, Fabrício Bertini Pasquot Polido propõe outros critérios que podem ser utilizados para fins de determinação da lei aplicável, além daqueles já expostos [anteriormente]: a) Critérios tradicionalmente utilizados: (i) local no qual o ato ilícito foi praticado; (ii) local do domicílio, residência habitual e nacionalidade de uma das partes ou da vítima; (iii) local em que a vítima tenha sentido com maior intensidade os efeitos dos danos; (iv) local de registro ou classificação do bem cujo manuseio tenha resultado em ato ilícito; (v) a conexão e convergência entre competência jurisdicional e a aplicação da *lex fori*; b) Outros critérios passíveis de utilização/aplicação: (vi) local em que os prejuízos são efetivamente sentidos/experimentados pela vítima, coincidente ou não com a lei do local de seu domicílio ou residência habitual; (vii) local no qual os direitos, alvos de violação, sejam economicamente explorados pelo titular; (viii) local em que o servidor ou o provedor de conteúdo esteja localizado; (ix) domicílio do usuário de internet, seja enquanto vítima ou enquanto autor do ato delitual.

dirimir o conflito que a ele foi submetido, abrindo-se espaço para analogias e outros recursos com o propósito de preenchimento da lacuna em questão[573].

No contexto do Ordenamento Jurídico brasileiro, o recurso ao princípio da proximidade, por exemplo, dependeria de autorização expressa da lei (colocando-o na condição de cláusula de exceção, como o faz a lei suíça)[574], ou, ainda, da necessidade de preenchimento de lacuna pelo Judiciário, com base no fato de que o juiz não pode recusar-se à prestação jurisdicional quando chamado a decidir determinado conflito em relação ao qual é competente[575].

Importante lembrar, por fim, que em 2020 passará a vigorar a Lei Geral de Proteção de Dados, a qual contém previsão, no art. 3º, de aplicabilidade "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"[576].

A LGPD afasta os critérios da sede da empresa ou da localização dos dados sempre que o seu tratamento ocorrer em território brasileiro, ou tiver por objetivo oferecer ou

---

[573] DOLINGER, Jacob; TIBURCIO, Carmen. Op. cit., 2020. No art. 4º da LINDB é possível encontrar a base legal para preenchimento de lacunas, mediante o recurso aos usos e costumes: "Segundo o art. 4º da Lei de Introdução, os usos e costumes fazem parte do sistema jurídico, eis que suprem as lacunas da lei. O costume terá idêntico valor no plano do Direito Internacional Privado, desde que no direito estrangeiro aplicável se lhe atribua o valor de fonte de direito. Conclui-se que a prova dos usos e costumes comerciais de Estados estrangeiros se submete aos mesmos meios de prova do direito estrangeiro em geral."

[574] DOLINGER, Jacob. Op. cit., jan./mar. 2004, pp. 139-146, p. 140. Exemplo de adoção expressa do princípio da proximidade em texto normativo pode ser encontrado no ordenamento suíço (diferentemente do ordenamento brasileiro), analisado por Jacob Dolinger: "Neste sentido, há que se reconhecer que as clássicas regras de conexão representam uma armadura pesada, apertada, uma camisa de força um tanto inconfortável, da qual é válido querer se desvencilhar um pouco. [...] A solução foi encontrada. [...] Refiro-me ao art. 15 da lei federal de 18 de dezembro de 1987, que leio em uma das três línguas oficiais em que os suíços promulgam suas leis: "O direito designado pela presente lei excepcionalmente não é aplicável se, tendo-se em conta o conjunto das circunstâncias, é manifesto que a causa não possui relação próxima com tal direito, e que ela se encontra em uma relação muito mais estreita com outro direito. Esta disposição não é aplicável em caso de escolha de lei." (Tradução livre). '*Le droit designé par la présente loi n'est exceptionnellement pas applicable si, au regard de l'ensemble des circonstances, il est manifeste que la cause n'a qu'un lien très lâche avec ce droit et qu'elle se trouve dans une relation beaucoup plus étroite avec un autre droit. Cette disposition n'est pas applicable en cas d'élection de droit*.' Isto quer dizer o seguinte: para todas relações jurídicas temos no direito internacional privado as setas – regras de conexão – indicadoras da lei aplicável, mas, se em determinada hipótese, estivermos diante de uma situação jurídica em que notamos que a lei indicada não é realmente relevante, que a ligação entre o fato e a norma é tênue, fraco, distante, e que há um outro direito, outro sistema jurídico que fica muito mais próximo à situação ou relação jurídica, este será o direito a aplicar e não aquele indicado pela regra de conexão. Esta regra foi denominada "cláusula de exceção", porque afasta a regra de conexão."

[575] BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao compilado.htm. Acesso em: 17 abr. 2020. Art. 5º, inc. XXXV: "[...] a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito; [...]".

[576] O referido artigo impõe condições para a sua aplicação. Assim, poderá ser aplicada a LGPD às hipóteses contidas no *caput*, 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 (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

fornecer bens e serviços no território nacional, ou, ainda, sempre que os dados forem coletados em território nacional. Trata-se, portanto, de ampla aplicação, cuja hermenêutica poderá ser mais bem avaliada após o início da vigência da Lei em agosto de 2020.

Neste momento, constatada a amplitude do âmbito de aplicação material da LGPD, cumpre questionar se o art. 3º constitui norma de aplicação imediata[577], bem como se as hipóteses ali previstas revelam caso de jurisdição universal[578].

Depreende-se, então, que o artigo em questão não poderia implicar sua jurisdição universal, posto que, embora o direito à privacidade possa ser encontrado no texto constitucional, ainda não há consenso expresso sobre a natureza e gravidade de violações quanto à proteção de dados no meio digital, nos termos já aqui expostos. Não foram distinguidos elementos, na LGPD, que levem a concluir pela jurisdição universal de seus dispositivos, o que revelaria, em última análise, interpretação além do texto da lei.

Quanto à condição de norma de aplicação imediata, cumpre retomar o conceito exposto por Cláudia Lima Marques e Daniela Corrêa Jacques, segundo o qual tais normas seriam aptas a solucionar diretamente os conflitos[579]. Isto significa que, ao considerar normas de aplicação imediata, é possível afastar o método de Direito Internacional Privado, conduzindo à aplicação direta da norma em questão[580]. As referidas normas

---

[577] MARQUES, Cláudia Lima; JACQUES, Daniela Corrêa. Normas de Aplicação Imediata como um método para o Direito Internacional Privado de proteção do consumidor no Brasil. *Cadernos de Pós-Graduação em Direito da UFRGS*, n. 1, 2004, p. 65-96. Ao analisarem as relações de consumo sob a ótica do Direito Internacional Privado, as autoras definem as normas de aplicação imediata da seguinte maneira: "São as chamadas "leis de aplicação imediata", leis básicas de segurança do mercado ou sociedade ("sauvegarde de l'organisation politique, social e/ou économique du pays"), leis para nacionais e estrangeiros e para todas as relações privadas, sem necessidade de antes passarem pelo método clássico do Direito Internacional Privado, da indicação de uma lei aplicável. Esta própria lei "de aplicação imediata" ou lei de "polícia" tem pretensões de aplicação genérica e extraterritorial sempre, não importando se são leis de direito privado, uma vez que positivam fortes interesses de organização da sociedade nacional. Como a chamada lei de aplicação imediata é direta ou resolve o conflito diretamente, sua aceitação e identificação hierárquica dentro do DIP é uma técnica (por sinal cada vez mais usada) de "materialização" das novas regras de conflitos de leis."

[578] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 106. "À luz do princípio da jurisdição universal, todo Estado é considerado competente para julgar e punir os indivíduos que cometeram crimes considerados particularmente ofensivos por toda a comunidade internacional. Assim, aqueles que foram acusados desses crimes de máxima gravidade podem ser julgados por qualquer Estado, independentemente do local de cometimento do crime ou de qualquer vínculo de nacionalidade. São exemplos desses crimes, a pirataria, o genocídio, os crimes de guerra e os crimes contra a humanidade."

[579] MARQUES, Cláudia Lima; JACQUES, Daniela Corrêa. Normas de aplicação imediata como um método para o Direito Internacional Privado de proteção do consumidor no Brasil. *Cadernos de Pós-Graduação em Direito da UFRGS*, 2004, n. 1, pp. 65-96.

[580] MONACO, Gustavo Ferraz de Campos. *Conflitos de leis no espaço e lacunas (inter)sistêmicas).* São Paulo: Quartier Latin, 2019, p. 69. "O modo de atuação contemporânea das normas de aplicação imediata nos diversos sistemas nacionais de Direito Internacional Privado tem variado conforme os objetivos que se visa atingir, mas, de uma maneira geral, é sempre possível perceber que o mecanismo presta-se, essencialmente, para a vinculação material ou substancial de determinada questão a determinado sistema jurídico, grandemente o do foro. E tal modo de proceder justifica-se, normalmente, por razões de salvaguarda dos valores ali vigentes."

também possuem o condão de afastar a ocorrência de fraudes à lei, garantindo a autonomia da vontade das partes em relações contratuais.

As obrigações ora analisadas podem ter natureza relacionada a um dever de caráter contratual ou extracontratual[581] (no âmbito da responsabilidade civil, relacionadas à prática de atos ilícitos, bem como abarcar atos omissivos ligados à inobservância de texto legal).

Quanto à responsabilidade extracontratual[582], é útil diferenciar hipóteses nas quais há efetivamente a prática de um ato ilícito, provocando danos e resultando na obrigação de sua reparação, além de hipóteses nas quais há meramente inobservância de dever estabelecido legalmente, com caráter omissivo (tratando-se de ilícito, contudo, não de um ato).

Destaca-se, a título exemplificativo, o art. 8º, § 5º da LGPD, que prevê obrigatoriedade na remoção de conteúdo ou de dados mediante solicitação do titular (revogação do consentimento)[583]. Nestas hipóteses, conclui-se pela aplicabilidade imediata da norma contida no art. 3º da LGPD. Em se tratando de dever legal inobservado, e ocorrendo uma das hipóteses previstas no art. 3º, parece que tal norma tem o condão de afastar o método de Direito Internacional Privado, sendo o juiz brasileiro competente e a lei nacional aplicável.

Aparenta, ademais, distinto caso de responsabilidade civil extracontratual em decorrência de prática de ato ilícito[584]. Não havendo contrato que regule a relação entre as

---

[581] PEREIRA, Caio Mário da Silva. *Responsabilidade civil*. Rio de Janeiro: Forense, 1990, p. 77. "O ponto de partida é a violação de uma norma preexistente. Haverá sempre uma norma de conduta (legal ou contratual). A sua observância é um fator de harmonia social. Quando uma pessoa deixa de a ela obedecer, desequilibra a convivência coletiva. Para que se caracterize a responsabilidade civil é necessário que desse confronto resulte um dano a alguém. A conduta contraveniente pode em termos genéricos, ser voluntária ou involuntária. [...] A voluntariedade pressuposta na culpa é a da ação em si mesma. É a consciência do procedimento que se alia à previsibilidade."

[582] BEVILÁQUA, Clóvis. *Comentários ao Código Civil*. Rio de Janeiro: Francisco Alves, 1949, v. I, p. 449. "Ato ilícito é a violação do dever ou o dano causado a outrem por dolo ou culpa. [...] Na culpa há, sempre, a violação a um dever pré-existente. Se este dever se funda em um contrato, a culpa é contratual; se no princípio geral de Direito que manda respeitar a pessoa e os bens alheios, a culpa é extracontratual ou aquiliana".

[583] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/ L13709.htm. Acesso em: 17 abr. 2020. Art. 8º. "§ 5º. O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei."

[584] TUNC, André. *La responsabilité civile*. Paris: Econômica, 1981, p. 32. "A distinção entre as responsabilidades delitual e contratual é tão fundamental, porém tão delicada, quanto a distinção entre delito e segurança social. [...] O objetivo da responsabilidade civil é obrigar uma pessoa a compensar os danos que causou ilicitamente a outra pessoa fora de qualquer relação contratual. Na maioria das vezes, o autor do dano e sua vítima são estranhos um ao outro. Como já foi dito, a lei da responsabilidade civil torturante garante a coexistência de cidadãos livres e a harmonização de sua liberdade. O direito contratual, por outro lado, rege os direitos e obrigações de pessoas cujo pelo menos um prometeu ao outro fazer ou dar algo ou abster-se de

partes, nem se tratando de responsabilidade legal, são válidas as disposições do CPC e do CDC abordadas anteriormente, cabendo analisar não apenas o local da sede (ou filial) da empresa, mas também o local onde ocorreram os danos.

Tratando-se de ato ilícito praticado no exterior por empresa com representação exclusivamente no estrangeiro, como uma fraude eventualmente realizada em outro país a partir de roubo de dados, dificilmente o Judiciário brasileiro será competente, uma vez que a ação foge do escopo das normas do CPC, as quais dispõem sobre os limites da jurisdição nacional, e por não se enquadrarem nas hipóteses de competência trazidas pelo CDC.

Não se tratando das hipóteses ali previstas, não haverá competência do Judiciário brasileiro, tampouco aplicação de qualquer lei material – *lex fori* ou *lex causae* – pelo juiz nacional. Como resultado, não seria possível designar o art. 3º da LGPD como norma de aplicação imediata, mas se trataria, diferentemente, de hipótese de competência concorrente ou internacional.

Diante disto, o art. 3º da LGPD pode ser considerado norma de aplicação imediata, exclusivamente nas três hipóteses ali previstas[585] (tratamento realizado no território nacional; bens ou dados de indivíduos localizados no território nacional; e dados coletados em território nacional). Ademais, somente poderá ser considerado de aplicação imediata e conduzir ao afastamento do método de Direito Internacional Privado, quando se tratar: a) de obrigação **legal** inobservada (como ocorre no caso de remoção de conteúdo solicitada pelo titular); ou b) de obrigação **contratual**, na qual não há eleição de foro diverso ou de outra lei como aplicável.

Não é possível sob a ótica aqui proposta, contudo, considerar o art. 3º como de aplicação imediata em hipóteses nas quais as partes exerceram sua **autonomia** contratual, elegendo outro foro como competente, ou dispondo diferentemente sobre a lei aplicável.

O referido artigo também não constitui norma de aplicação imediata em situações de responsabilidade civil **extracontratual** nas quais o dano não tenha ocorrido em

---

fazer algo. As partes são relacionadas entre si e concordaram em se vincular." (Tradução livre). "*La distinction entre les responsabilités civiles délictuelle et contractuelle est aussi fondamentale, mais aussi délicate, que la distinction entre la responsabilité civile délictuelle et la sécurité sociale. [...] L'objet de la responsabilité délictuelle est d'obliger une personne à compenser um dommage qu'elle a illégalement causé à une autre em dehors de toute relation contractuelle. La plupart du temps, l'auteur du dommage et sa victime sont étranger l'un à l'autre. Comme on l'a dit, le droit de la repsonsabilité civile délictuelle assure la coexistence de citoyens libres et l'harmonisation de leur liberte. Le droit des contrats, em revanche, régit les droits et les obligations de personnes dont l'uyne au moins a promis à l'autre de faire ou donner quelque chose ou de s'abstenir de faire quelque chose. Les parties sont liées l'une à l'égard de l'autre, et eles ont accepté de se lier."*

[585] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 30. "Por outras palavras, as normas de aplicação imediata que no foro se estabeleçam devem ser antes a exceção que a regra."

território nacional, tampouco possui a empresa sede aqui, fugindo dos limites da jurisdição nacional estabelecidos no CPC, não se tratando, inclusive, de relação de consumo que atrairia a aplicação das disposições do CDC.

No art. 61 a LGPD trata da responsabilidade de empresas estrangeiras, determinando que

> A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Neste ponto, cumpre aguardar a aplicação da LGPD pelo Judiciário brasileiro, já que, conforme restará demonstrado na análise jurisprudencial a seguir, ainda não há neste momento unanimidade a respeito do que se considera efetivamente uma representação da empresa estrangeira no território nacional.

3.3 RECONHECIMENTO DE SENTENÇAS ESTRANGEIRAS

Para que uma decisão (judicial ou não) produza seus efeitos, é necessário que possa ser executada, trazendo relevância à análise do tema da execução de sentenças ou cumprimento de decisões[586]. Tal tarefa pode se mostrar desafiadora nos casos que envolvem empresas estrangeiras, em especial em demandas sobre o meio digital. Em algumas situações, ainda que a decisão tenha sido proferida no território de um país, há interesse de que surta efeito em outra ou outras jurisdições.

A depender do país em que a sentença será executada, isto poderá ocorrer por meio do *exequatur* (adotado, por exemplo, pelo Brasil) ou da *actio judicati* (utilizada no

[586] GRECO FILHO, Vicente. *Homologação de sentença estrangeira*. São Paulo: Saraiva, 1978, pp. 7-8. "As exigências de fato resultantes da convivência internacional, porém, impuseram justificativas para o reconhecimento de julgados estrangeiros em certas condições, não mais, é claro, sob o fundamento da unidade do Direito Romano comum, mas, segundo uma nova concepção, em virtude da *comitas gentium*. Segundo os autores que a sustentaram, como discorre Marnoco e Souza, a legislação estrangeira deveria ser repelida, visto o poder legislativo dum Estado acabar nas suas fronteiras. Mas como daí resultariam inúmeros inconvenientes, visto todos os Direitos ficarem inteiramente dependentes do acaso da deslocação, os Estados deveriam permitir a aplicação do Direito estrangeiro por mera condescendência e cortesia, a fim de obterem vantagens recíprocas. [...] A doutrina da *comitas gentium*, como é evidente, tem apenas valor histórico e não poderia resistir por muito tempo como fundamentadora da aplicação extraterritorial de leis ou sentenças de outros países. A noção de cortesia internacional, além de vaga, variável e incerta, como afirma Marnoco e Souza, não é conceito jurídico ou filosófico que possa sustentar um sistema."

common law)[587]. No capítulo anterior foram mencionadas, ainda, sentenças arbitrais e a possibilidade de resoluções alternativas de conflito pelas *Online Dispute Resolution* (ODR)[588]. Em todos esses casos, a forma como a decisão será cumprida é importante para avaliar a sua efetividade, consideradas a diversidade cultural e a multiplicidade de formas de jurisdição.

Se as sentenças estrangeiras representam exercício da jurisdição de um Estado, expressando sua soberania, as mudanças trazidas pela Sociedade da Informação suscitam reflexões acerca dos seus fundamentos[589]. Tal reconhecimento reflete respeito à soberania do Estado estrangeiro, assim como demonstra a relevância que o sistema interno confere à sentença que lhe foi submetida[590].

Precisamente por tal motivo há situações nas quais questões de ordem pública impedem o reconhecimento de sentenças estrangeiras, e outras nas quais é possível o reconhecimento da jurisdição em casos de ordens que não foram emanadas por Estados. A homologação de uma sentença estrangeira faz com que os seus efeitos se tornem semelhantes aos de uma sentença proferida em território nacional[591].

No Brasil, a competência para homologar sentenças estrangeiras foi, originariamente, atribuída ao Supremo Tribunal Federal, tendo passado, após a Emenda

---

[587] CAMARGO, Solano de. Op. cit., 2015, p. 40. "Dois são os sistemas de atribuir eficácia e dar execução às sentenças estrangeiras: a *actio judicati* e o *exequatur*. O primeiro é utilizado no *common law*, onde a sentença opera inovação, ou seja, substitui a sentença estrangeira primitiva por um direito à condenação, não havendo processo de *exequatur*, e sim *actio iudicati*: para a obtenção do título executivo, a parte interessada deve propor uma nova ação, fundada em seu direito à condenação; em algumas jurisdições, a sentença estrangeira seria um meio de prova, havendo necessidade de uma nova sentença de mérito. Alguns ordenamentos incluem ainda, como critério de recepção da sentença estrangeira, a *reciprocidade* [...]."

[588] CAMARGO, Solano de. O reconhecimento e a execução de sentenças cibernéticas no Direito Internacional Privado. *In*: MALHEIROS, Clara; MONTE, Mário Ferreira; PEREIRA, Maria Assunção; GONÇALVES, Anabela (Orgs.). *Direito na Lusofonia.* Direito e novas tecnologias. Braga: Escola de Direito da Universidade do Minho, 2018, v. 1, pp. 477-484.

[589] MOURA VICENTE, Dário Manuel Lentz de. Op. cit., 2005, pp. 111-112. Cumpre concordar com o autor, no que tange às normas de aplicação imediata e princípio da ordem pública, especialmente quanto ao seguinte trecho: "É, de todo o modo, ao Estado do foro que pertence, no exercício da sua soberania, definir os pressupostos e limites a que se subordina a aplicação na ordem interna de Direito estrangeiro. A lei desse Estado é, por isso, a ordem jurídica de referência no juízo acerca da tolerabilidade do resultado da aplicação da lei designada pelas regras de conflitos. Não pode, por outro lado, negar-se a importância que contemporaneamente assume o primado das normas internacionalmente imperativas do Estado do foro sobre as da *lex causae* – [...] –, porquanto numa economia "globalizada" essas normas são indispensáveis à implementação das políticas econômicas de cada Estado e dos regimes locais sobre concorrência. Uma rigorosa igualdade entre a *lex fori* e o Direito estrangeiro aplicável às situações da vida privada internacional não se afigura, vistas as coisas sob este ângulo, desejável ou sequer viável."

[590] CAMARGO, Solano de. Op. cit., 2018, v. 1, pp. 477-484.

[591] MONACO, Gustavo Ferraz de Campos. Op. cit., 2017, pp. 381-382. "Ao determinar que a competência é da jurisdição brasileira, com exclusão de qualquer outra, o legislador brasileiro dirige-se não ao legislador estrangeiro, mas ao STJ, enquanto autoridade competente para homologar decisões estrangeiras, determinando à alta Corte federal que se abstenha de homologar decisões estrangeiras que determinem, por exemplo, a partilha *mortis causa* de bens situados no Brasil. Essa exegese é corroborada e complementada pelo disposto no art. 964, *caput*, do CPC/2015."

Constitucional n.º 45, de 2004, para a instância do Superior Tribunal de Justiça. Embora o processo de homologação envolva apenas requisitos formais e não reapreciação do mérito da sentença[592], o julgador avalia possível violação da ordem pública, de modo que, havendo tal violação, não será permitida a homologação.

Conforme art. 17 da LINDB[593], "as leis, atos e sentenças de outro país, bem como quaisquer declarações de vontade, não terão eficácia no Brasil quando ofenderem a soberania nacional, a ordem pública e os bons costumes"[594]. Há, portanto, ao menos três hipóteses nas quais não ocorrerá a homologação[595].

Anteriormente, quando abordadas as sentenças cibernéticas proferidas por programas de Inteligência Artificial, como aquele desenvolvido atualmente pela Estônia, foi mencionado o posicionamento de Solano de Camargo sobre a impossibilidade de homologação das decisões[596]. Precisamente por ofenderem a ordem pública nacional e os princípios do devido processo legal e ampla defesa, decisões que não foram proferidas por seres humanos não poderiam ser homologadas em território brasileiro.

---

[592] STJ. Superior Tribunal de Justiça. *Regimento Interno – RISTJ*. Disponível em: https://ww2.stj.jus.br/publicacaoinstitucional/index.php/Regimento/issue/view/1/showToc Acesso em: 17 abr. 2020. A decisão deverá ter sido proferida por juiz competente, com regular citação das partes ou verificação de revelia, cumprimento das formalidades necessárias para execução onde proferida, tradução juramentada (ou apostilamento) e, por fim, homologada pelo STJ (art. 216-B do Regimento Interno do Superior Tribunal de Justiça – RISTJ). Após o trânsito em julgado da homologação, cumpre ao interessado requerer, independente de petição, a extração da "Carta de Sentença" (art. 216-N do Regimento Interno do Superior Tribunal de Justiça), documento expedido pela Coordenadoria de Execução Judicial mediante o qual poderá ser iniciada execução da sentença estrangeira na Justiça Federal competente.

[593] Além dos dispositivos da LINDB, regulam a homologação de sentenças estrangeiras em matéria civil no Brasil: (i) art. 105, alínea "i", da Constituição Federal; (ii) Código de Processo Civil, arts. 483 e 484; (iii) Regimento Interno do Superior Tribunal de Justiça; e (iv) Tratados: (a) Mercosul; (b) Interamericanas (Código de Bustamente e Eficácia); (c) Haia (Sequestro e Adoção); (d) ONU (Nova Iorque – Alimentos); (e) Tratados bilaterais: Argentina, Espanha, França, Itália e Uruguai.

[594] BATALHA, Wilson de Souza Campos. *Tratado de Direito Internacional Privado*. São Paulo: RT, 1997, v. I, p. 266. "Bons costumes são, em geral, os princípios de conduta impostos pela moralidade média do povo. É no meio social que se apuram tais princípios e não de acordo com certa religião ou filosofia. E tem-se em vista a moralidade média do povo, considerada indispensável para a manutenção da ordem social e para harmonia nas relações humanas. As leis concernentes aos bons costumes têm as mesmas características que as leis de ordem pública e seguem os mesmos princípios."

[595] CAMARGO, Solano de. *Homologação de sentenças estrangeiras:* Ordem Pública Processual e Jurisdições Anômalas. São Paulo: Quartier Latin, 2019, pp. 62-63. "A homologação de sentença estrangeira no Brasil é uma ação de competência originária do STJ, de acordo com o artigo 105, I, "i", da Constituição Federal, sendo que o artigo 961 do CPC determina o reconhecimento dos efeitos da decisão estrangeira após a efetiva homologação, cujos requisitos encontram-se no artigo 963 do CP e nos artigos 216-C e 216-D do RISTJ, introduzidos pela Emenda Regimental nº 18. O procedimento de homologação está disciplinado nos artigos 216-A a 216-X do RISTJ. Na atualidade, não há dúvidas de que se trata de uma ação de conhecimento, cujo escopo é a obtenção de sentença constitutiva. A homologação da sentença estrangeira cria, modifica ou extingue relações jurídicas, de sorte que a questão não será reapreciada no Brasil, após o trânsito em julgado. No Brasil, adota-se o chamado juízo de delibação, verificando o juiz nacional se a sentença se encontra regular quanto à forma, à autenticidade, à competência do órgão prolator estrangeiro, adentrando na substância da sentença para verificar se, face ao direito nacional, não houve ofensa à ordem pública e aos bons costumes."

[596] Id., ibid., pp. 477-484.

Nas demandas indenizatórias ora abordadas, há diversas outras possibilidades de se recusar a homologação de uma determinada decisão estrangeira – seja pelo não reconhecimento da competência da autoridade que emanou a decisão, outras questões formais, ou questões de ordem pública, conforme aventado anteriormente[597]. Existe, também, a possibilidade de a parte encontrar dificuldade em fazer cumprir, em país estrangeiro, uma decisão proferida pelo Judiciário brasileiro, impedindo que surta efeito, podendo, inclusive, se tratar de dificuldades de ordem técnica[598].

Uma vez que a legislação interna de cada Estado determina a forma como uma decisão judicial ou sentença estrangeira é reconhecida ou homologada, alguns programas e aplicativos intencionalmente estabelecem sede em jurisdições que lhes são favoráveis, sendo possível citar, como exemplo, casos envolvendo endereços para apostas *online* ou oferta de conteúdo ilícito[599].

---

[597] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, p. 272. "Seria também de se questionar, nessas condições, os problemas decorrentes de uma homologação, pelo País "A", da sentença estrangeira proveniente de "B", rejeitando a ação de indenização pelos atos de violação da patente, sustentando que esta, então registrada em "B", era de fato nula? [...]. As soluções para muitas dessas questões parecem ainda estar nos limites estritos da doutrina do *act-of-state* e do princípio da territorialidade. O juiz nacional não poderia declarar a nulidade de uma patente estrangeira, já que essa questão é afeta à competência territorial daquele país onde fora registrada (aqui a territorialidade). Por outro lado, poderia reconhecer a sentença estrangeira que, no curso do processo, veio decretar a nulidade, pois, nesse caso, seria justamente admitir o reconhecimento de um ato soberano de um Estado, cujos tribunais se manifestaram sobre a validade da patente atacada com base no exercício de sua competência territorial. Trata-se de autêntica resposta pela teoria da separabilidade ou cindibilidade das pretensões: de um lado, a pretensão do titular de obter indenização pelos atos de violação detectados em determinado país e praticados por terceiros; de outro, a pretensão do demandado, alegado infrator, de obter a declaração de nulidade da patente que teria sido violada."

[598] TJ/SP. Tribunal de Justiça do Estado de São Paulo. 11ª Câmara de Direito Criminal. Mandado de Segurança n.º 2271462-77.2015.8.26.0000. Rel. Des. Xavier de Souza. Julgado em 17 dez. 2015; TJ/SE. Tribunal de Justiça do Estado de Sergipe. *Mandado de Segurança n.º 201600110899*. Des. Rel. Ricardo Múcio Santana de Abreu Lima. Julgado em 03 maio 2016. Tais mandados de segurança tiveram grande repercussão nacional quando determinado, em duas ocasiões distintas, o bloqueio do aplicativo *WhatsApp* em território nacional, relacionado à recusa em fornecimento de informações com a finalidade de investigação criminal – o qual, contudo, apresenta dificuldades técnicas pela criptografia, dupla verificação e outros dispositivos de segurança utilizados.

[599] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 121. Em 2007, o site de download de *torrents "Pirate Bay"* iniciou campanha de arrecadação com o objetivo de adquirir ilha situada fora de qualquer jurisdição estatal, a fim de alocar seus servidores. A intenção era escapar das diversas ações judiciais em face da empresa, em múltiplas jurisdições, por conta da facilitação de compartilhamento de conteúdo protegido por direitos autorais. Evidentemente, o site não logrou sucesso em sua empreitada, ignorando disposições de Direito Internacional Público relevantes. De todo modo, trata-se de exemplo interessante para se pensar a questão do reconhecimento de decisões e sentenças estrangeiras, destacando-se as seguintes reflexões sobre o tema: "Fator adicional que contribui para o surgimento e fortalecimento desses paraísos é a dificuldade de execução de decisões proferidas na jurisdição do domicílio ou residência habitual de um possível demandante. Em diversos casos, tribunais locais afirmaram sua jurisdição sobre atos e condutas originados no estrangeiro, mas encontraram sérias dificuldades para fazer cumprir suas decisões. Em certos litígios privados transfronteiriços foram utilizados mecanismos que permitiram a devida execução de sentenças por meio da responsabilização de subsidiários ou outros tipos de ativos na jurisdição do tribunal em questão. Todavia, casos que configuram uma situação de paraíso jurisdicional não oferecem opções semelhantes. [...] Embora os operadores do *Pirate Bay* não

3.4 ANÁLISE JURISPRUDENCIAL: ASPECTOS DE DIREITO INTERNACIONAL PRIVADO BRASILEIRO

Expostos os aspectos teóricos do Direito Internacional Privado, bem como a maneira como a privacidade e a proteção de dados vêm sendo tratadas pelos legisladores e tribunais brasileiros e estrangeiros, resta analisar a forma como o Judiciário brasileiro vem decidindo questões relativas à qualificação, competência internacional e lei aplicável em demandas que envolvem a Internet. Igualmente, importa saber se tais decisões são efetivamente cumpridas, quando necessária a sua eficácia em jurisdição estrangeira.

No âmbito estadual, inicialmente merece destaque o Incidente de Uniformização de Jurisprudência, suscitado perante o Tribunal de Justiça do Distrito Federal, que versa sobre produtos de consumo adquiridos em países estrangeiros, de modo que o elemento de estraneidade está justamente no local de aquisição do bem ou produto.

> INCIDENTE DE UNIFORMIZAÇÃO DE JURISPRUDÊNCIA – IUJ. CONSUMIDOR – PRODUTO DE CONSUMO ADQUIRIDO EM PAÍS ESTRANGEIRO – CÓDIGO DE DEFESA DO CONSUMIDOR – APLICAÇÃO AFASTADA. COBERTURA DE GARANTIA CONTRATUAL – RECONHECIDA A COMPETÊNCIA DO JUIZ BRASILEIRO. INCIDENTE DE UNIFORMIZAÇÃO DE JURISPRUDÊNCIA ADMITIDO. FIXADAS TESES JURÍDICAS. [...] 3. No exame do mérito, a Turma de Uniformização de Jurisprudência fixou as seguintes teses jurídicas: 1. **Os produtos de consumo adquiridos em país estrangeiro não gozam da mesma proteção jurídica outorgada pelas normas brasileiras de proteção e defesa do consumidor**, destinadas aos negócios celebrados em território nacional. 2. **É competente o juiz brasileiro para o processo e julgamento da causa em que o consumidor, baseado na norma estrangeira ou na garantia contratual, busca proteção jurídica a produto adquirido no estrangeiro, contra pessoa jurídica domiciliada no Brasil**, assim definida no parágrafo único do art. 21 do CPC. [...][600]. (grifamos).

Na decisão supracitada, proferida no âmbito do TJ/DF, há dois pontos relevantes a destacar, relativos a cada uma das teses jurídicas fixadas. Primeiramente, é levado em consideração o critério do local de celebração do contrato para fins de designação da lei brasileira como aplicável (embora a aplicação do CDC tenha sido afastada). Sob este aspecto, é importante a conceituação clara do local de celebração em caso de contratos eletrônicos.

Em segundo lugar, o domicílio da pessoa jurídica é admitido como critério para fixar a competência do juiz brasileiro, inclusive para produtos adquiridos no exterior, de

---

tenham logrado sucesso, o caso demonstra o quão fácil pode ser escapar de uma jurisdição estatal por meio da realocação de atividades para paraísos jurisdicionais."

[600] TJ/DF. Tribunal de Justiça do Distrito Federal. *Incidente de Uniformização de Jurisprudência n.º 003150-90.2018.8.07.0000.* Rel. Asiel Henrique de Souza, julgado em 18 out. 2018.

modo que se o domicílio da empresa demandada for localizado no Brasil, o Judiciário brasileiro é considerado competente. Esta tese, contudo, não se aplica às inúmeras situações nas quais o domicílio da empresa demandada se situa no exterior, por fugir ao escopo do art. 21, inc. I, do CPC, bem como das demais hipóteses de competência ali elencadas.

Ainda no âmbito estadual, no julgado a seguir, proferido nos autos de Apelação Cível que tramitou no Tribunal de Justiça de São Paulo, há exemplo de demanda na qual o Judiciário brasileiro declarou-se incompetente, precisamente por se tratar de hipótese de pessoa jurídica sediada no exterior. Considerou-se que, embora o contrato tenha sido celebrado eletronicamente, isto ocorreu no exterior, levando à extinção do feito.

Os aspectos efetivamente analisados pelo julgador foram: o **domicílio da autora** na época dos fatos (Portugal); a aplicação de **legislação alienígena** (aplicável por ser a ré empresa estrangeira); a **legitimidade passiva** da Paypal do Brasil (ilegítima por não ter sido a empresa que celebrou o contrato); e a **autonomia** da ré para liberar conta se o bloqueio tiver sido efetivado por outra pessoa jurídica (impossibilidade de cumprimento da obrigação de fazer).

> AÇÃO DE OBRIGAÇÃO DE FAZER C.C. REPARAÇÃO DE DANOS. Contrato de prestação de serviços de processamento para pagamentos eletrônicos "Paypal" celebrado no âmbito da internet. Contrato celebrado no exterior. Ilegitimidade da apelada para figurar no polo passivo da demanda por não ter sido a empresa contratada. Contrato celebrado com Paypal Europe. Incompetência da Justiça brasileira. Recurso improvido. [...] **A discussão desses autos envolve as seguintes questões: domicílio da autora ao tempo dos fatos; eleição de foro; aplicação de legislação alienígena; legitimidade passiva da Paypal do Brasil; autonomia da ré para liberar conta no exterior e mesmo no Brasil se o bloqueio foi efetivado por outra pessoa jurídica**. Com efeito, a ré apelada não é parte legítima para figurar no polo passivo da demanda, na medida em que o contrato que se pretende discutir não foi celebrado com a empresa brasileira, mas com sua sede no exterior, a Paypal Europe, sediada em Luxemburgo. Assim, não poderia cumprir a obrigação de fazer constante do pedido da ação. **A verdade é que o contrato, celebrado virtualmente no exterior, é regido por lei estrangeira motivo pelo qual a ação não poderia nem mesmo ter sido ajuizada no Brasil. Por tal razão, correta a extinção do feito, sem resolução de mérito, quer seja em face da ilegitimidade passiva da apelada, quer seja pela incompetência do MM. Juízo *a quo***. [...] Com efeito, a pessoa jurídica ré, Paypal do Brasil, não pode ser considerada agência, filial ou sucursal. Como esclarecido pela ré em sua defesa, a ré e a contratada têm personalidades jurídicas distintas, de modo que **aplicável ao caso a legislação alienígena**. De acordo com o **artigo 9º da LICC**, "Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem. **Conforme se pode vislumbrar dos autos, as obrigações foram constituídas em Portugal; tanto é verdade que o domínio da loja virtual é ".pt" e o valor que lhe foi bloqueado está em euros, sendo indiscutível que a obrigação foi contraída fora do Brasil, e ali deveria se cumprir, razão pela qual a discussão acerca de eventual ato ilícito há de se realizar naquele país, sob a égide das normas estrangeiras**. [...] No caso em apreço, **a autora tinha domicílio em Portugal**

> **quando da celebração do contrato de prestação de serviços, sendo evidente que toda a negociação se deu no exterior, local onde houve acesso ao sítio eletrônico por parte da autora**. De se assinalar que não se aplica o CDC ao caso concreto, primeiro por se tratar de relação estabelecida para fomentar a atividade comercial da autora, de intermediação de pagamentos, sendo certo que não se trata de consumidora, e em segundo lugar porque **inaplicável toda a legislação brasileira à hipótese**. Sendo assim, de todos os ângulos que se tome a questão, evidente é a conclusão de que a Autoridade Judiciária brasileira não é competente para o julgamento da demanda, **não se enquadrando em nenhuma das hipóteses dos artigos 21 e 22 do NCPC, justamente porque a ré não é parte legítima para o polo passivo, e sim a empresa europeia, de personalidade jurídica diversa, cuja competência será da autoridade judiciária portuguesa**. Pelo exposto, pelo meu voto, é negado provimento ao recurso[601]. (grifamos).

No caso, são analisados tanto o art. 9º da LINDB (embora o acórdão ainda se refira à Introdução ao Código Civil) quanto os arts. 21 e 22 do CPC de 2015, a fim de fundamentar a incompetência do Judiciário brasileiro, uma vez que a empresa demandada possui sede europeia, atraindo para Portugal a competência para dirimir conflitos decorrentes de falhas na prestação do serviço pela empresa. O art. 9º da LINDB, no entanto, é utilizado como base legal para fins de determinação da lei aplicável – quando, conforme apontado anteriormente, relaciona-se à qualificação do objeto da lide.

Entendeu-se na ocasião que o contrato celebrado virtualmente no exterior é regido por lei estrangeira – segundo consta no art. 9º – o que impediria o ajuizamento da ação no Brasil, quando, em verdade, o dispositivo invocado não trata de competência internacional, mas de qualificação e lei aplicável.

A aplicabilidade da lei estrangeira e o reconhecimento da incompetência do Judiciário brasileiro foram justificados sob o argumento de que a empresa contratada possui sede no exterior (Luxemburgo), e que a contratação se deu em Portugal, em euros. Optou-se, portanto, pela inaplicabilidade da legislação brasileira e pela incompetência do juiz nacional – ao final, invocando os dispositivos do CPC que tratam da competência internacional.

A qualificação pela lei brasileira ou pela lei portuguesa é questão autônoma diante da competência internacional, relacionada aos arts. 21 e 22 do Código de Processo Civil, cujos dispositivos também são invocados no acórdão. Neste ponto, assiste razão ao julgador que fundamenta a sua incompetência em tais artigos, pois a ré não estava domiciliada no Brasil (art. 21, inc. I, CPC), tampouco deveria ser aqui cumprida a

---

[601] TJ/SP. Tribunal de Justiça de São Paulo. *Apelação Cível n.º 1001507-77.2016.8.26.0079*. 21ª Câmara de Direito Privado. Des. Rel. Silveira Paulilo. Julgado em 17 jan. 2018.

obrigação (art. 21, inc. II, CPC) já que o ato ou fato sequer foi praticado no Brasil (art. 21, inc. III, CPC).

Por não ter sido considerada relação de consumo, já que a autora fazia uso do Paypal para fomentar a sua atividade comercial, tampouco haver cláusula de eleição do foro brasileiro, não se considerou aplicável o art. 22 para determinação da competência brasileira. Igualmente foram inaplicáveis as hipóteses de competência exclusiva enumeradas no art. 23 do mesmo Código, as quais não foram mencionadas ao longo do acórdão.

O fato é que, ao se aplicar o art. 9º da LINDB, a qualificação ocorreu a partir da lei do local onde havia sido celebrada a obrigação – apontado como sendo Portugal. Supondo coincidência entre a conceituação e a classificação feitas nos ordenamentos brasileiro e português[602], tratou-se de demanda envolvendo responsabilidade decorrente de obrigações contratuais, oriundas de contrato eletrônico, celebrado em Portugal, quando a autora residia naquele país. Ao aplicar-se o critério da *lex domicilii*, da *lex loci executionis* ou da *lex destionationis*, de qualquer forma a competência é portuguesa, assim como a lei materialmente aplicável[603].

---

[602] MONACO, Gustavo Ferraz de Campos. Op. cit., 2019, pp. 83-84. "Por outro lado, quando se estiver diante de uma situação da vida à qual se tenha determinado a aplicação da lei material de um Estado estrangeiro qualquer, que não seja, portanto, o do foro (E≠1), hipótese em que a *lex causae* será E≠1, será o Direito Material deste ordenamento quem assumirá a situação fática em tela para dar-lhe enquadramento classificatório adequado e interpretação segundo os ditames deste mesmo sistema, procedendo-se à devida subsunção. Nesse caso, pode ocorrer de o sistema material da *lex causae* atribuir àquela relação jurídica [...] uma estrutura idêntica à imaginada pelo legislador do foro, [...]. De outro lado, havendo divergências jurídico-estruturais no modo de se encarar aquela situação da vida, pode sempre ocorrer de o sistema jurídico material da *lex causae* atribuir à relação juridicamente relevante um enquadramento diverso daquele de que se partiu. [...] Perceba-se que não se trata de alteração do *nomen iuris*, como já se afirmou. Há verdadeira divergência estrutural, mudando-se a tipologia jurídica de que o intérprete partiu e de que se valem as normas de conflito para designar a conexão adequada. [...] Ambas as hipóteses forçariam o intérprete a proceder a uma readequação de sua estrutura de pensamento (consequentemente da subsunção dos fatos às normas materiais estrangeiras aplicáveis) na medida em que no sistema que deverá aplicar para o deslinde da questão, por força de as regras de conflito terem-no indicado como o sistema jurídico competente, a valoração for diversa daquela de que partiu e com a qual estava acostumado. Passa-se, assim, a proceder a uma espécie de requalificação da situação da vida à luz dos jurídicos conceitos da *lex causae*."

[603] "I - A **determinação do tribunal internacionalmente competente** precede a questão de saber qual a lei material aplicável, pois que será ao sistema de regras de conflito do Estado do foro – depois de afirmada a sua competência internacional – que há que recorrer para a resolver; II – Segundo o critério da al b) do nº 1 do art 65º CPC, na versão aplicável aos autos, a competência internacional dos tribunais portugueses depende de dever a acção ser proposta em Portugal, segundo as regras da competência territorial estabelecidas nas leis portuguesas; III – Porque **na acção está em causa o incumprimento de um contrato, haverá que recorrer à norma do art 74º/1 CPC, e proceder à qualificação dos elementos técnico jurídicos a que a mesma recorre - "domicílio do réu" e "lugar de cumprimento da obrigação**". IV – Há quem entenda que esses conceitos devem ser **qualificados** pela *lex fori*, isto é, pela lei do Estado em que a acção está pendente, e há quem entenda que devem ser qualificados pela lex causae, ou seja, por uma lei que é determinada pelas normas de conflitos do foro; V – Neste último entendimento, seria pelo recurso às normas dos arts 41º e 42º CC, referentes à lei reguladora das obrigações provenientes de negócios jurídicos, que se acabaria por determinar o conteúdo material daqueles conceitos; VI – [...]. Ainda que assim não se entendesse**, não sendo**

Embora o raciocínio feito pelo julgador não tenha ficado totalmente claro no que tange ao método do Direito Internacional Privado, a conclusão a que se chegou é correta, pois de fato o Judiciário brasileiro é incompetente para solucionar lide que guarda pouca ou nenhuma relação com o país, enquanto a lei estrangeira é inaplicável pelo julgador brasileiro[604].

Fosse o juiz nacional competente de acordo com o disposto no ordenamento brasileiro, a lei estrangeira seria por ele aplicável, já que conforme apontado anteriormente, tal lei é determinada pelo local onde é constituída a obrigação – o que, na hipótese, ocorreu fora do território nacional. Conforme apontado, ao aplicar-se o critério da *lex domicilii*, da *lex loci executionis* ou da *lex destionationis*, a lei materialmente aplicável ao caso seria a portuguesa.

Em 2008 houve grande polêmica acerca de decisão proferida nos autos de ação ajuizada pela atriz e modelo Daniella Cicarelli Lemos, com o objetivo de obrigar a

---

comum a residência habitual das partes e estando em causa contrato não gratuito, sempre a lei aplicável ao mesmo se haveria de entender ser a da República da África do Sul, por ser **a lei do lugar da celebração do contrato**, [...]; VII – No momento processual em que se encontram os autos, não se tem este tribunal suficientemente habilitado a respeito do direito sul africano no que concerne ao conteúdo que nele é dado ao lugar do cumprimento da obrigação no que se refere à situação dos autos; VIII **– Havendo os referidos conceitos técnico-jurídicos da norma do art. 76/1 CPC de ser qualificados pela *lex fori*, recorrer-se-ia aos arts 772 a 776 CC**; **IX – Foi fixado como forma e lugar do cumprimento**, o depósito em conta bancária da 1ª A. no banco "Q", com sede no **Luxemburgo**. Tendo a R. encerrado essa conta, sem autorização da A., sua titular, colocou-se em mora. Se pretendesse pôr fim a esta e não obtivesse o consenso das AA. para a (re)abertura da (nova) conta, só o poderia fazer **no domicílio destas, como decorre do art. 774 CC**; **X – O conceito de domicílio estabelece-se com base no Direito do Estado do foro**; XI – [...]; XII – Na versão aplicável aos autos, resulta da al d) do nº 1 do art 65 CPC que **os tribunais portugueses serão internacionalmente competentes em função da circunstância de** "**ter sido praticado em território português o facto que serve de causa de pedir na acção, ou algum dos factos que a integram**". XIII - [...] XVI – Estando em causa naquela actividade e neste efeito décadas de factos ocorridos em Portugal, **não é sustentável**, mesmo que se pudessem configurar os factos alegados a este respeito como complementares, **que a competência internacional que desencadeiam para os tribunais portugueses se possa configurar como exorbitante** (Sumário elaborado pela Relatora)." PORTUGAL. Tribunal da Relação de Lisboa. *Processo 7438/08.4TVLSB.L1-2*. Julgado em 08 nov. 2012. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/d2f8a5f750a0c95380257b240053c2c0?OpenDocument&Highlight=0,Regulamento,44%2F2001 Acesso em: 22 dez. 2019. (grifamos).

[604] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, pp. 127-128. "Tradicionalmente, segundo o método clássico conflitual no Direito Internacional Privado, a determinação do Direito Material aplicável aos casos envolvendo obrigações extracontratuais dependeria fundamentalmente da localização do ato delitual no espaço, em dado território. A conexão objetiva ou pertinência do local de ocorrência do delito é justificada ao menos por dois critérios: primeiro, pela ausência de autonomia da vontade constitutiva da relação entre as partes envolvidas – sujeito ativo (pessoa que comete o ilícito) e passivo (pessoa que sofre o dano); segundo, pelo fato de ato delitual ocorrer em qualquer Estado, por onde quer que a atividade infrativa seja observada. Daí porque, segundo o método clássico (ainda de inspiração savigniana), o local de ocorrência dos atos e fatos delituais, dos quais emergem as obrigações (extracontratuais), seria decisivo para a determinação da lei que regula seus efeitos. Essa constatação aponta para uma das justificativas para a regra clássica de conexão *lex loci delicti*. [...] Do ponto de vista metodológico, a doutrina jusprivatista internacional reconhece como problemática a aplicação da lei do local do ilícito para aqueles casos em que o indivíduo prejudicado pelos efeitos do dano sequer tenha relação com o direito do local em que o delito se aperfeiçoa."

remoção de conteúdo não autorizado nas redes[605]. O vídeo divulgado sem sua autorização, no entanto, foi amplamente compartilhado em diversas plataformas, utilizando-se inúmeros provedores e programas distintos, de modo que faltou compreensão, por parte dos julgadores, quanto às impossibilidades técnicas relacionadas a transmissões de vídeos por demanda, técnicas de geolocalização de usuários, distinção entre serviços de provimento de acesso à Internet e acesso universal a plataformas de compartilhamento.

O acórdão em questão não chega a mencionar questões transnacionais, muito embora as empresas demandadas (*Internet Group do Brasil Ltda*., Organizações Globo de Comunicação e Youtube Inc.) possuam servidores e sedes no exterior, assim como o próprio material objeto da divulgação foi registrado na Espanha.

Assim, apesar de não haver incorrido hipótese de incompetência do juiz nacional, ou mesmo de aplicação de lei estrangeira, houve dificuldade substancial em fazer cumprir a decisão, pela própria natureza da Internet e pela forma e velocidade como conteúdos são compartilhados. Ainda hoje é possível ter acesso ao conteúdo que supostamente deveria ter sido removido, assim como em diversos outros casos nos quais foram ajuizadas demandas com pedidos semelhantes.

Já no âmbito do Superior Tribunal de Justiça, as decisões vêm sendo, em grande parte, no sentido da proteção dos dados e informações dos indivíduos em face dos sites de busca e provedores de Internet, mesmo quando suscitadas questões relativas à competência internacional ou aplicabilidade da lei estrangeira.

Nesse sentido, a decisão proferida pelo STJ em demanda que envolve o site de buscas Google expressa que se a Justiça brasileira for acionada para solucionar conflito decorrente de prática ilícita na Internet, ela será competente se a parte autora tiver domicílio no país, e se for este o local de acesso ao site onde foi veiculada a informação. Ou seja: o STJ adota o critério do domicílio do autor, bem como do local de acesso à informação (ou seu destino)[606].

---

[605] TJ/SP. Tribunal de Justiça de São Paulo. 4ª Câmara de Direito Privado. *Agravo de Instrumento nº 472.738-4*. Des. Rel. Ênio Santarelli Zuliani. Julgado em 17 jul. 2008. "Pedido de antecipação de sentença por violação do direito à imagem, privacidade, intimidade e honra de pessoas fotografadas e filmadas em posições amorosas em areia e mar espanhóis – Tutela inibitória que se revela adequada para fazer cessar a exposição dos filmes e fotografias em websites, por ser verossímil a presunção de falta de consentimento para a publicação [art. 273, do CPC] – Interpretação do art. 461, do CPC e 12 e 21, do CC – Provimento, com cominação de multa diária de R$ 250.000,00, para inibir transgressão ao comando de abstenção."

[606] TIBURCIO, Carmen. Op. cit., 2006, p. 64. "Vale dizer, portanto, que para as lesões a direitos ocorridos no âmbito do território brasileiro, em linha de princípio, a autoridade judiciária nacional detém competência para processar e julgar o litígio. Não sendo assim, poder-se-ia colher a sensação incômoda de que a Internet é um refúgio, uma zona franca, por meio da qual tudo seria permitido sem que daqueles atos adviessem responsabilidades. Desse modo, ordinariamente, a autoridade judiciária brasileira será competente na esfera

> [...] O tema a respeito do limite da responsabilidade dos provedores de internet tem suscitado grandes debates, na medida em que, rotineiramente, as informações veiculadas violam a intimidade, a vida privada de pessoas, causando danos substancialmente danosos em razão da natureza disseminadora da rede mundial de computadores. Nesse contexto, verifica-se um considerável número de demandas submetidas à Justiça brasileira, buscando a reparação civil por danos sofridos em razão de **divulgações ilícitas, não obstante possam advir de sítios eletrônicos hospedados no exterior**. A propósito, a Quarta Turma já se manifestou no sentido de que, **caso acionada para dirimir o conflito oriundo de atividade ilícita praticada pela internet, a Justiça brasileira é competente se a parte autora tem domicílio no Brasil e este é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada**, interpretando-se como ato praticado no Brasil e aplicando-se, à hipótese, o disposto no artigo 88, III, do CPC/73. [...] A ordem judicial já foi prolatada, quebrando o sigilo telemático, mas a medida ainda não foi cumprida pela Google Brasil, **sob o pálido argumento de que é a empresa controladora Google Inc., sediada em território americano, que armazena os dados de e-mail, os quais estariam inacessíveis física e juridicamente para a subsidiária brasileira, ressaltando que essas informações estariam sob proteção da legislação americana**. [...]. **A sede-matriz (empresa controladora) em território americano se faz representar aqui pela Google Brasil**. Ora, o que se pretende é a **entrega de mensagens remetidas e recebidas por brasileiros em território brasileiro, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira**. Nesse cenário, é irrecusável que **o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro**, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados. **Trata-se, evidentemente, de elemento de prova produzido, transmitido e recebido em território brasileiro**, repito. **Nada tem a ver com terras alienígenas, a não ser pelo fato de, por questões estratégico-empresariais, estarem armazenadas nos Estados Unidos**. [...] Vale ressaltar que a **referida empresa foi constituída em conformidade com as leis brasileiras e, evidentemente, deve se submeter à legislação pátria**, não podendo se esquivar do cumprimento de requisição judicial **invocando leis americanas, pelo todo exposto, inaplicáveis ao caso**. Não se pode admitir que uma empresa se estabeleça no país, explore o lucrativo serviço de troca de mensagens por meio da internet – o que lhe é absolutamente lícito –, mas se esquive de cumprir as leis locais. [...] deve-se compreender que a determinação deve alcançar a remoção das indexações também do sítio Google.com e variações, não podendo a recorrida eximir-se da obrigação ao argumento de impossibilidade técnica ou jurídica para cumprimento da ordem. Diante do exposto, nos termos do art. 255, § 4º, III, do RISTJ, dou provimento ao recurso especial, a fim de determinar a remoção das URLs indicadas na inicial, não apenas do site www.google.com.br, mas também do site www.google.com e variações[607]. (grifamos).

Há diferenças relevantes entre o acórdão do TJ/SP, tratado anteriormente, e o julgado do STJ supracitado. Naquela oportunidade, considerou-se incompetente a Justiça brasileira sob o argumento de que seria inviável pretender que empresa estrangeira, pessoa jurídica diversa daquela que fora demandada, viesse a cumprir decisão do Judiciário

---

cível para processar e julgar litígios internacionais relacionados à Internet em, pelo menos, duas hipóteses no contexto de ilícitos. Em primeiro lugar, quando o réu for domiciliado no Brasil – critério tradicional de fixação da competência internacional. Além disso, o Judiciário brasileiro também será competente quando houver dano produzido no Brasil."

[607] STJ. Superior Tribunal de Justiça. *Recurso Especial n.º 1354484*. Rel. Min. Lázaro Guimarães. Julgado em 19 jun. 2018.

brasileiro. Já no caso ora analisado, considerou-se a competência da Justiça brasileira também em relação à responsabilidade da empresa estadunidense, independentemente de sua localização.

No caso anteriormente analisado, a autora, na época dos fatos, residia em Portugal, o que não ocorreu na demanda apreciada pelo STJ. Naquela oportunidade, o site havia sido acessado no exterior, também em Portugal, de modo que, adotando-se os critérios do local da execução da obrigação, ou do local de acesso, chega-se à competência portuguesa.

Neste ponto, é necessária uma ressalva quanto à abordagem do STJ, já que, pelos mesmos fundamentos apresentados no acórdão do TJ/SP, não é viável obrigar pessoa jurídica diversa, com sede em país distinto, a cumprir decisão proferida em face de empresa brasileira. Há de se considerar, em cada caso, se de fato constitui uma filial, subsidiária ou representante, como considerado pelo STJ[608], ou se inexiste relação entre as empresas, como avaliado pelo TJ/SP.

Em caso de site acessado no Brasil, resta competente o Judiciário brasileiro para dirimir conflitos oriundos da Internet, já que o art. 21 do CPC prevê que cabe à autoridade judiciária brasileira processar e julgar as ações cujo fundamento seja fato ocorrido ou ato praticado no Brasil. É possível, contudo, que haja obstáculos ao efetivo cumprimento das decisões judiciais nas hipóteses em que uma das partes envolvidas, mesmo que não diretamente demandada, esteja situada em território de país estrangeiro.

No caso do Recurso Especial referido anteriormente, determinou-se, ao final, a remoção da URL indicada não apenas do site brasileiro do Google (www.google.com.br), como, também, do site internacional (www.google.com) e, ainda, de suas variações. Ou seja: pressupõe-se que o Google no Brasil possui controle sobre todas as filiais e representantes da empresa, em todo e qualquer país do mundo, subentendendo-se que disporia da capacidade técnica para realizar a remoção do conteúdo em todas as diferentes jurisdições. Resta clara, portanto, a dificuldade em fazer cumprir integralmente a decisão.

A seguir, passa-se a analisar, individualmente alguns dos precedentes citados na referida decisão. No Recurso Especial, o ponto mais relevante é o fato de que se considera competente a Justiça brasileira, sob o argumento de que "para as lesões a direitos ocorridos no âmbito do território brasileiro, em linha de princípio, a autoridade judiciária nacional possui competência para processar e julgar o litígio". Ou seja: há adoção do critério do

[608] STJ. Superior Tribunal de Justiça. *Ag 748.056/RJ*. Rel. Min. Humberto Gomes de Barros. Publicado em 05 maio 2006. Nesta ocasião, em episódio que ficou conhecido como "caso Panasonic", houve o reconhecimento da responsabilidade da subsidiária pelos atos realizados pela sua controladora.

local de ocorrência do dano para fixação da competência, relacionado ao art. 21, inc. III, do CPC.

> DIREITO PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR UTILIZAÇÃO INDEVIDA DE IMAGEM EM SÍTIO ELETRÔNICO. PRESTAÇÃO DE SERVIÇO PARA EMPRESA ESPANHOLA. CONTRATO COM CLÁUSULA DE ELEIÇÃO DE FORO NO EXTERIOR. 1. A evolução dos sistemas relacionados à informática proporciona a internacionalização das relações humanas, relativiza as distâncias geográficas e enseja múltiplas e instantâneas interações entre indivíduos. 2. **Entretanto, a intangibilidade e mobilidade das informações armazenadas e transmitidas na rede mundial de computadores, a fugacidade e instantaneidade com que as conexões são estabelecidas e encerradas, a possibilidade de não exposição física do usuário, o alcance global da rede, constituem-se em algumas peculiaridades inerentes a esta nova tecnologia, abrindo ensejo à prática de possíveis condutas indevidas**. 3. O caso em julgamento traz à baila a controvertida situação do impacto da internet sobre o direito e as relações jurídico-sociais, em um ambiente até o momento desprovido de regulamentação estatal. A origem da internet, além de seu posterior desenvolvimento, ocorre em um ambiente com características de autorregulação, pois os padrões e as regras do sistema não emanam, necessariamente, de órgãos estatais, mas de entidades e usuários que assumem o desafio de expandir a rede globalmente. 4. A questão principal relaciona-se à **possibilidade de pessoa física, com domicílio no Brasil, invocar a jurisdição brasileira, em caso envolvendo contrato de prestação de serviço contendo cláusula de foro na Espanha**. A autora, percebendo que sua imagem está sendo utilizada indevidamente por intermédio de sítio eletrônico veiculado no exterior, mas acessível pela rede mundial de computadores, ajuíza ação pleiteando ressarcimento por danos material e moral. 5. **Os artigos 100, inciso IV, alíneas "b" e "c" c/c art. 12, incisos VII e VIII, ambos do CPC, devem receber interpretação extensiva, pois quando a legislação menciona a perspectiva de citação de pessoa jurídica estabelecida por meio de agência, filial ou sucursal, está se referindo à existência de estabelecimento de pessoa jurídica estrangeira no Brasil, qualquer que seja o nome e a situação jurídica desse estabelecimento**. 6. Aplica-se a **teoria da aparência** para reconhecer a validade de citação via postal com "aviso de recebimento-AR", efetivada no endereço do estabelecimento e recebida por pessoa que, ainda que sem poderes expressos, assina o documento sem fazer qualquer objeção imediata. Precedentes. 7. **O exercício da jurisdição, função estatal que busca composição de conflitos de interesse, deve observar certos princípios**, decorrentes da própria organização do Estado moderno, que se constituem em elementos essenciais para a concretude do exercício jurisdicional, sendo que dentre eles avultam: **inevitabilidade, investidura, indelegabilidade, inércia, unicidade, inafastabilidade e aderência**. No tocante ao princípio da aderência, especificamente, este pressupõe que, **para que a jurisdição seja exercida, deve haver correlação com um território. Assim, para as lesões a direitos ocorridos no âmbito do território brasileiro, em linha de princípio, a autoridade judiciária nacional detém competência para processar e julgar o litígio**. 8. O art. 88 do CPC, mitigando o princípio da aderência, cuida das hipóteses de jurisdição concorrente (cumulativa), sendo que **a jurisdição do Poder Judiciário brasileiro não exclui a de outro Estado, competente a justiça brasileira apenas por razões de viabilidade e efetividade da prestação jurisdicional, estas corroboradas pelo princípio da inafastabilidade da jurisdição**, que imprime ao Estado a obrigação de solucionar as lides que lhe são apresentadas, com vistas à consecução da paz social. 9. A comunicação global via computadores pulverizou as fronteiras territoriais e criou um novo mecanismo de comunicação humana, porém **não subverteu a possibilidade e a credibilidade da aplicação da lei baseada nas fronteiras geográficas, motivo pelo qual a inexistência de legislação internacional que regulamente a jurisdição no ciberespaço abre a**

> **possibilidade de admissão da jurisdição do domicílio dos usuários da internet para a análise e processamento de demandas envolvendo eventuais condutas indevidas realizadas no espaço virtual**. 10. Com o desenvolvimento da tecnologia, passa a existir um novo conceito de **privacidade**, sendo o **consentimento** do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem. 11. É reiterado o entendimento da preponderância da regra específica do art. 100, inciso V, alínea "a", do CPC sobre as normas genéricas dos arts. 94 e 100, inciso IV, alínea "a" do CPC, **permitindo que a ação indenizatória por danos morais e materiais seja promovida no foro do local onde ocorreu o ato ou fato, ainda que a ré seja pessoa jurídica, com sede em outro lugar, pois é na localidade em que reside e trabalha a pessoa prejudicada que o evento negativo terá maior repercussão**. Precedentes. 12. **A cláusula de eleição de foro existente em contrato de prestação de serviços no exterior, portanto, não afasta a jurisdição brasileira**. 13. Ademais, a imputação de utilização indevida da imagem da autora é um "*posterius"* em relação ao contato de prestação de serviço, ou seja, o direito de resguardo à imagem e à intimidade é autônomo em relação ao pacto firmado, não sendo dele decorrente. **A ação de indenização movida pela autora não é baseada, portanto, no contrato em si, mas em fotografias e imagens utilizadas pela ré, sem seu consentimento, razão pela qual não há se falar em foro de eleição contratual**. 14. **Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil**, aplicando-se à hipótese o disposto no artigo 88, III, do CPC. 15. Recurso especial a que se nega provimento[609]. (grifamos).

No que dispõe acerca da competência concorrente, nos termos do Código de Processo Civil, reconhece-se que o fato de a Justiça brasileira ser competente não impede que o Judiciário de outro Estado também o seja. É aceita a competência brasileira, ainda, por se tratar de local do domicílio do usuário demandante. Do referido *decisium*, portanto, é considerado o critério da lei do domicílio do autor – embora inexista previsão legal expressa nesse sentido no ordenamento brasileiro, conforme análise feita anteriormente acerca dos limites da jurisdição brasileira.

Ao final, consta, ainda, o critério do local onde os danos produziram seus efeitos, ou, em outras palavras, "na localidade em que reside e trabalha a pessoa prejudicada que o evento negativo terá maior repercussão", mesmo se houver cláusula de eleição de foro dispondo em sentido diverso (no caso, designando a Justiça espanhola como competente).

Apesar de haver relação contratual entre autora e réu, o STJ considerou tratar-se de hipótese de responsabilidade extracontratual, pois relativa à divulgação indevida de fotografias e imagens sem consentimento, resultando na competência brasileira para ações

[609] STJ. Superior Tribunal de Justiça. *Resp. 1168546/RJ*. Rel. Ministro Luis Felipe Salomão. Quarta Turma, julgado em 11 maio 2010, DJE em 07 fev. 2011.

que envolvem atividades ilícitas do gênero, independentemente do foro eleito contratualmente.

Os critérios utilizados para embasar a competência do Judiciário brasileiro foram aplicados, portanto, cumulativamente: considerou-se o local de acesso ao site, sendo este interpretado como o local de prática do ato e, também, de ocorrência do dano, o qual produziu maiores efeitos negativos[610] – cujos locais coincidem com o domicílio da vítima (autora).

É trazida à tona a teoria da aparência para justificar a citação de empresa brasileira e não da matriz estrangeira – de modo que é inarredável concluir pela semelhança entre as empresas, já que o Aviso de Recebimento foi aceito sem objeções. Assiste, portanto, razão ao STJ ao declarar a Justiça brasileira competente, independentemente da cláusula de eleição de foro na Espanha, ou de haver matriz ou representante estrangeira, entendendo pela aplicabilidade do princípio da inafastabilidade da jurisdição.

Há outros casos nos quais se considerou que a origem estrangeira da empresa não implicaria impossibilidade de cumprimento de ordem emanada pelo Judiciário brasileiro. Observa-se, contudo, que no julgado destacado a seguir, proferido também no âmbito do STJ, a fundamentação não reside em normas de Direito Internacional Privado propriamente dito, mas, sim, na teoria da aparência e na teoria do risco, de modo que se entendeu pela assunção de riscos pela empresa estrangeira quando esta aufere benefícios e se apresenta como empresa semelhante no mercado brasileiro.

> RECURSO ESPECIAL. RESPONSABILIDADE CIVIL. ANTECIPAÇÃO DE TUTELA. RETIRADA DE PÁGINA DA REDE MUNDIAL DE COMPUTADORES. CONTEÚDO OFENSIVO À HONRA E À IMAGEM. **ALEGADA RESPONSABILIDADE DA SOCIEDADE CONTROLADO-**

[610] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, pp. 102-103. "Desde o início dos anos 2000, a prática jurisprudencial brasileira em torno de litígios da Internet, especialmente envolvendo usuários e redes de relacionamento social, revela as vicissitudes da definição dos limites jurisdicionais do Estado, vale dizer a partir da competência internacional dos tribunais domésticos. Alguns critérios foram sendo sedimentados nesse sentido e permitem afinar as bases de jurisdição concorrente ou relativa para solução de demandas com conexão internacional: (i) o domicilio ou residência habitual, no território brasileiro, de vítimas ou titulares de direitos violados; (ii) o local de aperfeiçoamento de ilícitos cibernéticos (*cybertorts*); (iii) a extensão dos danos decorrentes da atividade ilícita sobre a esfera de direitos de usuários sediados no território nacional; (iv) contatos sistemáticos entre o sítio de internet, empresa de provimento de acesso e o foro acionado; (v) sede de atividades da empresa ofertante de serviços de internet, dentre os quais redes de relacionamento social, plataformas de compartilhamento e vídeos e intercâmbio de mensagens. Em geral, dois recortes temporais podem ser estabelecidos para análise dos casos de Internet envolvendo questões jurisdicionais em litígios cibernéticos no Brasil (e.g. violação de direitos da personalidade, remoção de conteúdos, bloqueio de plataformas de comunicação, suspensão de acesso a websites): o primeiro compreendido entre 2002 e 2015; e o segundo, de 2015 até o presente, em especial delimitado a partir da entrada em vigor do Marco Civil da Internet, que altera substancialmente o Direito Material aplicável à responsabilidade civil de provedores de Internet (acesso e conteúdo)."

> **RA, DE ORIGEM ESTRANGEIRA. POSSIBILIDADE DA ORDEM SER CUMPRIDA PELA EMPRESA NACIONAL**. [...]. 2. Se empresa brasileira aufere diversos benefícios quando se apresenta ao mercado de forma tão semelhante à sua controladora americana, deve também, responder pelos riscos de tal conduta. 3. Recurso especial não conhecido[611]. (grifamos).

Cumpre questionar, contudo, a forma como tais decisões serão efetivamente executadas[612]. O fato de uma empresa estrangeira auferir benefícios a partir de uma sucursal, filial ou representante não implica necessariamente o controle efetivo de uma sobre a outra, levando, por vezes, à impossibilidade técnica de cumprir decisões.

De fato, pela teoria da aparência associada à teoria do risco, não parece haver óbice para que a empresa estrangeira assuma a responsabilidade decorrente das atividades da representante, no sentido de realizar o pagamento de indenizações, havendo a possibilidade de ajuizar ação de execução específica. Quando a condenação, contudo, determinar obrigações, como a remoção de conteúdo, há de se avaliar as questões práticas e técnicas envolvidas a fim de possibilitar o cumprimento da decisão.

No âmbito penal, especificamente, há previsão de mecanismos de cooperação internacional tanto na legislação brasileira quanto de acordos ou tratados internacionais, como anteriormente já foi mencionado. Assim, há outras formas de garantir a execução ou cumprimento das decisões, bem como normas aplicáveis distintas, diferenciando-se da esfera cível[613].

---

[611] STJ. Superior Tribunal de Justiça. *REsp 1021987/RN*. Rel. Ministro Fernando Gonçalves, Quarta Turma. Julgado em 07 out. 2008, DJe 09 fev. 2009.

[612] CAMARGO, Solano de. Op. cit., 2015, p. 39. "De mais a mais, corolário das ordens jurídicas estatais e da consequente relatividade dos valores jurídicos é que a decisão judicial tem eficácia limitada à jurisdição onde foi proferida. Para o *foro*, no dizer de Amilcar de Castro, as sentenças estrangeiras não passam de fatos relevantes, mas destituídos de obrigatoriedade. Nenhum Estado pode pretender que as suas sentenças judiciais tenham eficácia executiva *de per se*, em outras jurisdições. Porém, mediante procedimentos próprios (na maioria dos casos pelo *exequatur* ou pelo procedimento de homologação), se reconhecem as sentenças estrangeiras."

[613] STJ. Superior Tribunal de Justiça. *Inq. 784/DF*. Rel. Ministra Laurita Vaz. Corte Especial, julgado em 17 abr. 2013. DJe 28 ago. 2013. "QUESTÃO DE ORDEM. DECISÃO DA MINISTRA RELATORA QUE DETERMINOU A QUEBRA DE SIGILO TELEMÁTICO (GMAIL) DE INVESTIGADOS EM INQUÉRITO EM TRÂMITE NESTE STJ. **GOOGLE BRASIL INTERNET LTDA. DESCUMPRIMENTO. ALEGADA IMPOSSIBILIDADE. INVERDADE. GOOGLE INTERNATIONAL LLC E GOOGLE INC. CONTROLADORA AMERICANA. IRRELEVÂNCIA. EMPRESA INSTITUÍDA E EM ATUAÇÃO NO PAÍS. OBRIGATORIEDADE DE SUBMISSÃO ÀS LEIS BRASILEIRAS, ONDE OPERA EM RELEVANTE E ESTRATÉGICO SEGMENTO DE TELECOMUNICAÇÃO. TROCA DE MENSAGENS, VIA E-MAIL, ENTRE BRASILEIROS, EM TERRITÓRIO NACIONAL, COM SUSPEITA DE ENVOLVIMENTO EM CRIMES COMETIDOS NO BRASIL. INEQUÍVOCA JURISDIÇÃO BRASILEIRA**. DADOS QUE CONSTITUEM ELEMENTOS DE PROVA QUE NÃO PODEM SE SUJEITAR À POLÍTICA DE ESTADO OU EMPRESA ESTRANGEIRA. AFRONTA À SOBERANIA NACIONAL. IMPOSIÇÃO DE MULTA DIÁRIA PELO DESCUMPRIMENTO." (grifamos). STJ. Superior Tribunal de Justiça. Terceira Sessão. *RJ 2006/0161102-7*. Min. Rel. Og Fernandes. Julgado em 16 fev. 2009. "CONFLITO DE COMPETÊNCIA. PROCESSUAL PENAL. RACISMO PRATICADO ATRAVÉS DE PUBLICAÇÃO DE MENSAGENS RACISTAS EM SÍTIO DE

Interessante, de todo modo, analisar um último acórdão proferido pelo Superior Tribunal de Justiça acerca da competência internacional. E, embora verse sobre matéria de Processo Penal, aprecia a jurisdição brasileira, pois considera que o delito decorrente da divulgação de pornografia infantil se consuma no momento da publicação das imagens, sendo o local considerado para fins de fixação da competência[614]. Neste caso, pouco importa a localização da sede do provedor responsável pelo acesso ao conteúdo ilícito.

> CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSO PENAL. VEICULAÇÃO NA INTERNET DE **IMAGENS PORNOGRÁFICAS ENVOLVENDO CRIANÇAS E ADOLESCENTES**. **COMPETÊNCIA QUE SE FIRMA PELO LOCAL DA PUBLICAÇÃO ILÍCITA**. 1. Conforme entendimento desta Corte, **o delito previsto no art. 241 da Lei 8.069/90 consuma-se no momento da publicação das imagens**, ou seja, aquele em que ocorre o lançamento na Internet das fotografias de conteúdo pornográfico. **É irrelevante, para fins de fixação da competência, o local em que se encontra sediado o responsável pelo provedor de acesso ao ambiente virtual**. 2. Conflito conhecido para determinar competente o suscitado, Juízo Federal da 1ª Vara Criminal, do Júri e das Execuções Penais da Seção Judiciária do Estado de São Paulo[615]. (grifamos).

Constata-se, ao final desta análise jurisprudencial, a utilização de critérios diversos pelo Judiciário brasileiro para fixar a sua competência e determinar a lei aplicável a demandas que envolvem o meio digital. Deste modo, os critérios adotados pelo CPC, LINDB, CDC, ou outras normas potencialmente aplicáveis, ainda são pouco uniformes e interpretados de maneira escassa quanto ao método do Direito Internacional Privado. Por vezes, o domicílio da parte autora é citado como critério relevante para fins de determinação da lei aplicável, por exemplo, sem que exista disposição expressa a respeito no texto da lei. Assim, o espaço para o desenvolvimento jurisprudencial do tema ainda é bastante amplo, e deve ser motivado pela vigência da LGPD, a partir de agosto de 2020.

RELACIONAMENTO. INTERNET. IDENTIFICAÇÃO DOS AUTORES. NECESSIDADE. LOCAL DO CRIME. LUGAR DE ONDE FORAM ENVIADOS OS TEXTOS OFENSIVOS. AUSÊNCIA DE DADOS APTOS A PROVAR A ORIGEM DAS OFENSAS. CONTINUIDADE DO PROCEDIMENTO INVESTIGATÓRIO. PREVENÇÃO. COMPETÊNCIA DAQUELE JUÍZO QUE PRIMEIRO CONHECEU DA INVESTIGAÇÃO. 1. A competência para processar e julgar os crimes praticados pela internet, dentre os quais se incluem aqueles provenientes de publicação de textos de cunho racista em sites de relacionamento, é do local de onde são enviadas as mensagens discriminatórias. 2. Na espécie, mesmo após recebidas as informações da empresa proprietária do sítio, não houve como identificar, por enquanto, os autores das ofensas, o que impõe, obviamente, a manutenção do feito no âmbito daquele juízo que primeiro tomou conhecimento da investigação. 3. Conflito conhecido para declarar a competência do JUÍZO FEDERAL DA 4ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DO ESTADO DO RIO DE JANEIRO, o suscitado."

[614] Cumpre destacar que, diferentemente dos demais julgados pesquisados, o referido recurso versa sobre matéria de Direito Penal, havendo de se considerar, em lugar das normas de competência do CPC, aquelas que constam no CPP, especialmente nos arts. 88 e seguintes do referido Código.

[615] STJ. Superior Tribunal de Justiça. Terceira Sessão. *RS 2009/0183264-2*. Rel. Min. Ministro Jorge Mussi. Julgado em 27 out. 2010.

3.5 CONCLUSÕES PARCIAIS

Neste capítulo, finalmente, foram abordadas as questões de Direito Internacional Privado, delineadas nos tópicos anteriores: diante de questões controversas e novos conflitos, permeados pela fluidez e descentralização das relações no contexto da sociedade digital, torna-se necessária a revisão dos conceitos e critérios fundamentais que orientam a qualificação, a fixação da competência internacional, a lei aplicável aos litígios e o cumprimento de decisões estrangeiras[616].

Conclui-se, quanto à qualificação, que o mundo digital trouxe novos desafios quanto à definição da natureza das relações jurídicas formadas por meio da Internet, especialmente entre pessoas (físicas ou jurídicas) situadas em países diferentes. Os desafios podem ser ainda maiores quando se trata de definir a jurisdição internacionalmente competente para dirimir conflitos, já que diversos elementos de conexão estão presentes, e somente mediante uma análise caso a caso será possível definir o julgador mais próximo da lide[617].

O mesmo vale para a lei aplicável: mesmo em casos nos quais há eleição de foro pelas partes, a lei escolhida por contrato poderá ser eventualmente afastada, por exemplo, em demandas que envolvem o direito do consumidor e nas quais há uma parte hipossuficiente.

A multiplicidade de jurisdições potencialmente competentes e de leis igualmente aplicáveis gera, consequentemente, inúmeras possibilidades quanto ao local de ajuizamento de uma ação indenizatória relacionada à privacidade ou à proteção de dados no meio digital, possibilitando às partes que expressem a autonomia de sua vontade[618]. Por

---

[616] RIBEIRO, Marilda Rosado de Sá; ALMEIDA, Bruno. Op. cit, 2011, (s.p.). "Conforme se pôde constatar, o direito contemporâneo é marcado pelo dinamismo das instituições, incrementado pelo aumento da circulação das construções jurídicas carreadas nos variados fluxos das atividades cotidianas que extravasam as fronteiras dos Estados soberanos. Reafirma-se, nesse contexto, o Direito Internacional Privado como importante ferramenta para compreensão da realidade jurídica contemporânea em visão convergente, entre o público e o privado, em vertente inspirada em um direito cosmopolita.

[617] POLIDO, Fabrício Bertini Pasquot. Op. cit., 2018, p. 113. "No cenário pós-Marco Civil, casos recentes ainda deixam de explorar questões possíveis de interface com jurisdição e direito internacional privado no Brasil, ainda que considerem critérios de conexão relevantes, tais como localização de servidores, sede de empresas de processamento e guarda de dados no estrangeiro e país de registro do nome de domínio. Boa parte do silêncio se deve à orientação persistente de muitas decisões de primeira instância, entre tribunais brasileiros, que unilateralizam soluções genuinamente afetas ao processo civil transnacional."

[618] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, p. 121. "A preocupação com o *forum shopping* e os paraísos jurisdicionais vai muito além das dificuldades geradas para casos individuais. A complexidade envolvida em se definir a jurisdição competente para julgar e executar decisões judiciais em qualquer situação também pode se revelar um grande entrave para qualquer tentativa de criação de mecanismos normativos internacionais para solução de conflitos de jurisdição. Mesmo que, por exemplo, algum nível de harmonização legislativa procedimental fosse

outro lado, é inquestionável que também provoque o surgimento de novas oportunidades de fraude à lei, ou de *forum shopping* que envolva paraísos jurisdicionais.

Dentre os pontos centrais desta terceira parte do estudo parece ser especialmente relevante a discussão sobre o caráter de norma de aplicação imediata em relação ao art. 3º da LGPD. Conclui-se que tal norma somente poderá ser aplicada de forma direta em determinadas situações, afastando-se, por exemplo, as hipóteses em que for exercida a autonomia contratual pelas partes, ressaltando-se o posicionamento defendido por Gustavo Ferraz de Campos Monaco, com o qual se concorda, pois enxerga tais normas como exceção no ordenamento e não como uma regra.

Igualmente relevante a discussão acerca dos critérios de conexão atualmente existentes na lei e efetivamente adotados na solução de controvérsias com elementos transnacionais, pois questionam os limites da flexibilização de tais normas. Por mais que o princípio da proximidade possa ser encontrado, inclusive como fundamento de normas de conflitos existentes no Ordenamento brasileiro, é importante ressaltar que inexiste autorização expressa para a sua aplicação como critério subsidiário, ficando restrito ao preenchimento de eventuais lacunas.

Os resultados obtidos ao longo da pesquisa, no entanto, parecem apontar para a suficiência dos critérios de conexão já existentes, restringindo ainda mais uma eventual aplicação do princípio da proximidade.

Por fim, na análise jurisprudencial realizada, observou-se a adoção de critérios de conexão diversos, tanto para a fixação da competência quanto para a determinação da lei aplicável. Somente em uma ocasião dentre as aqui pesquisadas foram mencionados, pelo julgador, os artigos da LINDB relativos à qualificação no Direito Internacional Privado.

Há, contudo, espaço para amplo desenvolvimento jurisprudencial e doutrinário do tema, que, por ser recente, apresenta novos e constantes desafios, da mesma forma como crescem as demandas envolvendo Direito e Internet. Espera-se que a partir da vigência da Lei Geral de Proteção de Dados no Brasil, em 2020, tais aspectos passem a ser abordados com mais frequência e profundidade, garantindo a harmonia das decisões e a segurança jurídica das partes.

---

convencionada por um grande número de Estados, como nas iniciativas levadas a cabo pela Conferência da Haia de Direito Internacional Privado, ou Organização Mundial da Propriedade Intelectual, bastariam alguns poucos Estados discordantes para que todo o propósito de um tratado daquela natureza fosse severamente prejudicado. Diferentemente de outros tipos de iniciativas de harmonização normativa envolvendo o mundo físico comum, nas quais a adesão por um número maior de Estados seria diretamente proporcional à eficácia no combate do problema em questão. Na Internet essa regra não existe sem que sejam usados mecanismos de filtragem e fragmentação da rede."

Espera-se, ainda, que o caráter eminentemente transnacional das temáticas aqui tratadas torne o Direito Internacional Privado um recurso constante nos julgados proferidos internamente, agregando cada vez maior relevância ao estudo da área.

CONCLUSÕES E PERSPECTIVAS

Na primeira parte deste estudo foi apresentada a forma como se desenvolveu a Sociedade da Informação nas últimas décadas, bem como a influência exercida sobre os legisladores em diferentes locais do mundo. Diversos países – Brasil, inclusive – vêm aprovando normas específicas para regular o ambiente digital e, em especial, para solucionar os conflitos advindos da Internet.

As mudanças no meio digital são mais rápidas do que as adaptações legislativas, ensejando um estudo contínuo sobre o tema, bem como a reavaliação de conceitos tradicionalmente utilizados[619]. No caso do Direito Internacional Privado, merecem revisão não apenas os conceitos de fronteira e soberania, mas, também, os critérios de qualificação utilizados para enquadrar os objetos das lides, determinar a competência jurisdicional e apontar a lei aplicável[620].

Embora seja necessária uma nova interpretação de tais critérios, adaptada à realidade pós-moderna, conclui-se pela suficiência das normas já existentes no

---

[619] RIBEIRO, Marilda Rosado de Sá; ALMEIDA, Bruno. A cinemática jurídica global: conteúdo do Direito Internacional Privado contemporâneo. *Revista da Faculdade de Direito da UERJ*, 2011, v.1, n. 20, ISSN 22363475. Disponível em: file:///C:/Users/anadi/Downloads/1516-8697-2-PB.pdf. Acesso em: 17 abr. 2020. Para confirmar tais mudanças, os autores apresentam o entendimento de COTTERRELL, Roger. Is it so bad to be different? *In*: ÖRÜCÜ, Esin; NELKEN, David (Eds.). *Comparative law*: a handbook. Portland: Hart Publish, 2007, e de DOLINGER Jacob. *Direito Internacional Privado* – Parte Geral. 9. ed. Rio de Janeiro: Renovar, 2008: "Muito embora as distâncias geográficas e de comunicação tenham sido minimizadas pela revolução dos transportes e da telecomunicação com amplas possibilidades em tempo real, persistem barreiras de todas ordens com repercussão no mundo jurídico. Militar em prol da diversidade e da pluralidade parece ser a tônica do Terceiro Milênio (COTTERRELL, 2007, p. 133). Assim, tendo em vista que o Direito Internacional Privado é, por excelência, o direito da tolerância (DOLINGER, 2008, p. 23), é preciso sempre atentar para as lições do passado para que a boa compreensão dessa disciplina auxilie na superação dos desafios hodiernos."

[620] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. *Governança global da internet, conflito de leis e jurisdição*. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), 2018, p. 171 e ss. "A erosão dos princípios e regras clássicos em virtude de processos da globalização e da informatização da comunicação levanta questionamentos quanto à própria viabilidade e adequação da aplicação dessas normas nesse novo cenário. Questiona-se se a internet possibilita que seus usuários realizem atividades novas, ou se ela apenas permite que pessoas façam atividades tradicionais de novas formas e em quantidades maiores. [...] Ao se debruçar sobre este questionamento, Jack Goldsmith afirma que as atividades conduzidas na internet não são diferentes daquelas realizados no mundo não digital. Segundo ele, transações *online* utilizam a internet como meio, mas não deixam de ser transações entre duas ou mais pessoas reais, localizadas em jurisdições diferentes. Transações digitais são funcionalmente idênticas às atividades transfronteiriças realizadas por outros meios, como por correio ou telefone. [...]. Contrariando Goldsmith, David G. Post afirma que a internet é essencialmente excepcional. Conforme defendido por ele, as questões advindas das relações travadas na internet são diferentes e mais intrincadas do que aquelas que surgem a partir das interações no mundo real. Assim, os conflitos de jurisdição nos litígios de internet não podem ser adequadamente resolvidos por meio da aplicação de princípios e regras tradicionais, que foram desenvolvidos para lidar com conflitos jurisdicionais referentes ao mundo real. Um dos argumentos apresentados por Post se assenta na grande quantidade de produtos que são comercializados mundialmente *online*. Ele alega que, apesar de o comércio transnacional ter existido antes da internet, ele não ocorria com a escala de hoje. As circunstâncias mudaram de tal forma que aplicar regras clássicas de jurisdição aos litígios *online* prejudicaria a prestação jurisdicional às partes interessadas."

Ordenamento para solucionar a quase totalidade dos conflitos. Não parece, contudo, ao menos no que se refere ao Direito Internacional Privado, ser necessária a edição de novo diploma normativo, trazendo normas específicas para o contexto digital.

De fato, as normas de conflito encontradas no CPC, LINDB ou CDC, por exemplo, não restam prejudicadas pelo MCI ou pela LGPD: ao contrário, a hermenêutica conjunta dos diplomas não é apenas possível, mas necessária para conferir à norma a aplicação dos princípios e valores que o legislador buscou proteger.

Nesse contexto, surgem novas questões de ordem pública que devem ser levadas em conta por ocasião do reconhecimento de sentenças estrangeiras. Por outro lado, faz-se necessário apreciar a efetividade e a possibilidade de cumprimento das decisões emanadas em território nacional decorrentes de conflitos plurilocalizados.

Na segunda parte da pesquisa foram apresentadas algumas questões relevantes e controvertidas, bem como normas materiais a elas aplicáveis, igualmente inseridas no contexto digital. Objetivou-se, com isso, trabalhar o aspecto da qualificação em demandas que envolvem a proteção de dados, privacidade e danos transnacionais. Conforme exposto em sede de conclusão preliminar, destaca-se a importância da correta qualificação, relembrando o fato de que esta poderá produzir resultados materiais distintos, a depender da *lex fori* ou da *lex causae*.

Ao longo desses capítulos buscou-se expor a problemática estudada, bem como oferecer elementos necessários à análise da competência e da lei aplicável na terceira e última parte. Há, ainda, aspectos que podem ser trabalhados posteriormente, tais como a cooperação internacional[621], somente tangenciada nesta dissertação. Efetivamente, os temas aqui abordados abrem inúmeras oportunidades em termos acadêmicos, pois trazem novos problemas e suscitam a necessidade de distintas soluções.

Cumpre questionar, contudo, se diante desta exposição, os critérios de conexão atualmente utilizados se mostram adequados e suficientes para lides que envolvem a

[621] RIBEIRO, Marilda Rosado de Sá. Cooperação Internacional. *Revista da Faculdade de Direito da UERJ*, 2005, v. 13-14, pp. 185-203, p. 188. "Vários aspectos da cooperação tecnológica foram objeto das convenções assinadas durante a Reunião Rio 1992, tais como: acesso à tecnologia, sistemas de informação, desenvolvimento de recursos humanos e mecanismos financeiros. Além desses, foram reiterados princípios internacionais consagrados pelo Programa de Ação votado em Viena em 1979, tanto que, na Declaração do Rio, estão relacionados em seus arts. 5º, 7º e 9º, princípios relacionados à mobilização para o desenvolvimento e à questão da transferência de tecnologia. Esses princípios internacionais foram, ainda, ratificados pela Assembleia Geral das Nações Unidas também em 1992. Entretanto, apesar do aparente consenso e desse reconhecimento internacional, enquanto países menos desenvolvidos e ONGs buscam facilitar o acesso à tecnologia, verifica-se a fortificação das barreiras protecionistas, de propriedade intelectual, dos países desenvolvidos, mantendo o conflito e a dualidade de interesses constantes das negociações das convenções e acordos internacionais."

Internet. Uma revisão da interpretação dos critérios e princípios já utilizados, tendo como pano de fundo a Sociedade da Informação, parece ser suficiente para garantir tal adequação, de modo que não parece necessária nem viável a criação de um "Direito Internacional da Internet" com pretensões universalistas, ao menos no presente momento[622].

Válido, ainda, levar em consideração a tolerância e o respeito à diversidade cultural e jurídica[623]. É importante, contudo, que as regras que norteiam o julgador sejam claras, de modo a garantir não apenas a harmonia das decisões judiciais, como, também, a segurança das partes quanto aos locais em que podem demandar uma à outra, bem como quanto à lei aplicável aos conflitos surgidos e aos contratos celebrados[624].

---

[622] Id., ibid., pp. 122-124. "Com tantas complexidades e dificuldades envolvendo a aplicação de regras e princípios tradicionais na resolução de conflitos de jurisdição na internet, é natural que alternativas começassem a ser propostas para superá-las. A maioria dessas soluções reconheceram a difícil aplicação dos princípios tradicionais ou também consideram indesejável a adaptação das novas tecnologias a estes princípios. [...] A ideia de um Direito Internacional da internet existe desde o princípio da própria internet, quando David Johnson e David Post argumentaram que o ciberespaço seria um local radicalmente diferente do mundo *offline* e que, por isto, deveria ser regido pelo seu próprio Direito, como se possuísse sua própria soberania. A ideia foi considerada ingênua e simplista e já na época em que os primeiros trabalhos a respeito foram lançados, mas foi de importância seminal para que teorias mais consistentes fossem desenvolvidas na década seguinte. [...] Com a popularização e expansão do acesso à internet, questões envolvendo direitos humanos, propriedade intelectual, comércio eletrônico e outros tópicos até então não trabalhados por essas organizações, passaram a exigir uma atenção maior dos atores interessados, na medida em que cresceram em sua relevância para a sociedade moderna. [...] Entretanto, a própria autora admite que o desenvolvimento de um marco regulatório internacional para a internet depende, em grande medida, do consenso e cooperação entre diversos Estados. Nos atuais fóruns de debate multissetorial, já se reconheceu a dificuldade de alcançar um consenso entre países com valores culturas e interesses soberanos tão distintos, como aqueles que possuem os maiores números de usuários de internet. Os próprios instrumentos legislativos de *hard law* são esparsamente ratificados pelos Estados, não tendo signatários influentes, como Brasil e Rússia. Sequer há consenso a respeito de um ponto tão crucial como o modelo multissetorial: tradicionalmente, países como China e Rússia favoreceram o modelo multilateral e intergovernamental, que se baseia na primazia de organizações internacionais (como as Nações Unidas, a União Internacional de Telecomunicações, a Organização Mundial da Propriedade Intelectual e Organização Mundial do Comércio) na regulação transnacional da rede, sem intervenção de outros setores. Existem, ainda, os já citados problemas relacionados a paraísos jurisdicionais. O desenvolvimento de um Direito Internacional da internet ainda tem, portanto, diversos e complexos desafios a enfrentar antes de atingir um patamar de aceitação universalmente satisfatória. [...] Enfrentar questões relativas à jurisdição na internet envolverá uma ressignificação de conceitos antes pacíficos, como os de comunidade, território, soberania, fronteira e estatalidade. Embora esses elementos continuem existindo na sociedade da informação, eles sofrem mitigações. O Direito deve renunciar a uma posição de negligência e acompanhar essas mudanças; com isso, tem condições de compreender os conceitos e narrativas de forma social e politicamente contextualizadas."

[623] MONACO, Gustavo Ferraz de Campos. *Controle de constitucionalidade da lei estrangeira*. São Paulo: Quartier Latin, 2013, p. 25. "O império de diferentes leis, ditadas para diferentes realidades sociais, por diferentes soberanias, e o entrecruzamento que decorre desse cenário são produtos da tolerância política, religiosa, étnica, econômica. E, se tais formas de tolerância tornaram possíveis as diferenças quanto à razão do governo jurídico dos diferentes conglomerados humanos dotados de soberania, gerando diferentes leis, a mesma tolerância mostra-se um imperativo para a manutenção e o pacífico convívio entre tais diferentes aspectos da realidade social."

[624] POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. Op. cit., 2018, pp. 171 e ss. "Naturalmente, não seria possível negar que a internet trouxe elementos novos para a compreensão dos conflitos de jurisdição. Um site pode permitir que qualquer pessoa do Globo com acesso à internet adquira produtos nele disponíveis. Precisamente porque ele é acessado em escala global, o seu

De fato, embora conste na LGPD dispositivo delimitando o seu âmbito de aplicação material (art. 3º), bem como dispositivo que expressa a obrigação da filial, representante ou sucursal de empresa estrangeira no Brasil (art. 61), as questões relativas ao Direito Internacional Privado poderiam ter sido trabalhadas de forma mais aprofundada pelo legislador nacional, levando em conta o aumento significativo de demandas relativas à privacidade e à proteção de dados na rede[625], bem como a possibilidade de surgimento de conflitos de qualificação.

A LGPD poderia, por exemplo, ter disposto, de forma clara, a natureza dos dados, mediante uma conceituação mais detalhada do que a constante no art. 5º, e esclarecer, também, se os direitos a eles relacionados são de natureza fundamental ou contratual.

Cabe aguardar e analisar a forma como tais normas serão aplicadas pelo Judiciário brasileiro a partir de agosto de 2020, cujo fim será o de tutelar o direito à privacidade e à proteção de dados em um contexto notadamente transnacional e plurilocalizado. Não obstante, a pesquisa demonstra que já existem normas no Ordenamento Jurídico nacional que designam critérios de qualificação e de conexão aplicáveis mesmo a demandas que

---

proprietário também pode ser eventualmente processado por um consumidor em qualquer local do planeta. O risco de possíveis ações e a conformidade (o compliance) com a lei local têm consequências sobre a viabilidade do negócio. Da mesma forma, um jornal de notícias *online* pode sofrer uma ação em seu desfavor em qualquer jurisdição, ainda que, segundo a lei interna do local da sede da companhia que administra este site, o conteúdo das notícias não possui qualquer irregularidade. Essa variedade identificada nos ordenamentos jurídicos dos Estados enseja uma multiplicidade de prioridades dos Estados ao estabelecer ou negar a sua jurisdição. Certos países podem considerar a proteção dos consumidores como mais importante do que a promoção do comércio eletrônico, de forma a adotar uma política agressiva de afirmação da sua jurisdição para proteger os consumidores locais (foro do domicílio do autor/consumidor). Outros Estados podem enfatizar a promoção da intimidade de seus nacionais, afirmando a sua jurisdição para resolução de litígios envolvendo violação da privacidade. Além disso, a aplicação de regras tradicionais no espaço digital pode resultar em denegação de justiça. Se, por exemplo, o foro do domicílio do autor do ato lesivo é admitido como critério absoluto para a fixação da competência de um tribunal estatal, muitas pessoas ficarão, inevitavelmente, fadadas a não receber qualquer prestação jurisdicional, pois o juiz competente para processar e julgar a demanda pode estar localizado, muitas vezes, em outro continente. Em termos práticos, o acesso à justiça restaria negado em sua essência. Portanto, a autoridade julgadora deve refletir sobre as regras e princípios clássicos, com o objetivo de redefini-los para lidar com os conflitos transnacionais de jurisdição no espaço digital."

[625] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, SC, jul./dez. 2011, v. 12, n. 2, pp. 91-108, p. 103. "No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, mas da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada. [...] Parece existir no Direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais."

envolvem danos transnacionais e Internet, diante de todas as suas particularidades, com ênfase na deslocalização.

Isto não significa, contudo, que tais normas dispensam reflexão: pelo contrário, é necessário avaliar a forma como os diplomas normativos mais recentes influenciam a interpretação dos critérios que já vigoravam anteriormente. Tal reflexão, ao apontar novos desafios e possíveis soluções, constituiu o centro desta pesquisa, na qual se buscou fomentar discussões sob aspectos ainda pouco explorados e extremamente atuais.

REFERÊNCIAS

ABRAHAM, Marcus; RICARDO CATARINO, João. O uso da inteligência artificial na aplicação do direito público: o caso especial da cobrança dos créditos tributários – um estudo objetivado nos casos brasileiro e português. e-Pública: *Revista Eletrônica de Direito Público*, 2019, v. 6, n. 2, pp. 188-219.

ABREU, Jacqueline de Souza. O compartilhamento de dados pessoais no Decreto n.º 8.789/16: um Frankenstein de dados brasileiro? *Uol,* 08 jul. 2016. Disponível em: http://jota.uol.com.br/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro. Acesso em: 20 jul. 2016.

ABREU, Jacqueline de Souza; SMANIO, Gianluca Martins. Compatibilizando o uso de tecnologia em investigações com direitos fundamentais: o caso das interceptações ambientais. *Revista Brasileira de Direito Processual Penal*, 2019, v. 5, n. 3, pp. 1449-1481.

ABRUSIO, Juliana. O direito ao esquecimento na Internet e a (im)possibilidade de recomeçar. *CESA - Anuário*, 2013, v. 1, pp. 17-26.

ABRUSIO, Juliana. Com certo atraso, Brasil finalmente é inserido no rol de países com marco legal em proteção de dados. *Informativo Migalhas*, 2018, v. 1. Disponível em: https://www.migalhas.com.br/depeso/286385/com-certo-atraso-brasil-finalmente-e-inserido-no-rol-de-paises-com-marco-legal-em-protecao-de-dados. Acesso em: 18 abr. 2020.

ABRUSIO, Juliana. O uso do link patrocinado como prática de conduta desleal no comércio da internet. *Pensamento Jurídico*, 2018, v. 12, pp. 291-311.

ACCIOLY, Dante. Comissão aprova MP que cria órgão para proteção de dados. *Agência Senado*, 07 maio 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/05/07/comissao-aprova-mp-que-cria-orgao-para-protecao-de-dados. Acesso em: 14 out. 2019.

ADORNO JÚNIOR, Helcio Luiz; SOARES, Marcele Carine dos Praseres. Processo judicial eletrônico, acesso à justiça e inclusão digital: os desafios do uso da tecnologia na prestação jurisdicional. *Revista Universitas.* Ano 2, jul./dez. 2013, n.º 11, pp. 65-86.

ÁFRICA DO SUL. *Protection of Personal Information Act (PROPIA*), 2013. Disponível em: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of 2013protec tionof persona linforcorrect.pdf. Acesso em: 08 mar. 2020.

AGU. Advocacia Geral da União. *Advocacia-Geral aposta em inteligência artificial e automação de processos para agilizar trabalhos jurídicos*, 26 fev. 2013. Disponível em: http://www.agu.gov.br/page/content/detail/id_conteudo/230719. Acesso em: 15 dez. 2019.

ALEMANHA. *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie*, 2006/24/EG.

ALEMANHA. *Strafprozessordnung* – StPO.

ALEMANHA. *Telekommunikationsgesetz* – TKG.

ALEMANHA. *Tribunal Constitucional Federal Alemão*. BvR 256/08, julgado em 02 mar. 2010. Disponível em: http://www.bverfg.de/e/rs20100302_1bvr025608en.html. Acesso em: 05 mar. 2020.

ALVES, Hugo Ramos. Smart contracts: entre a tradição e a inovação. *In*: CORDEIRO, António Menezes *et al*. *FinTech II:* novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019.

AMORIM, Ana. O direito à privacidade e a evolução tecnológica: a propósito da publicidade com recurso ao reconhecimento facial. *In*: ANJOS, M. R.; AZEVEDO, P. A.; GONÇALVES, R. M.; VEIGA, F. S. (Eds.). *Atualidades na Ciência Jurídica:* Intercâmbio Ibero-Americano. Maia, Portugal: Ed. Ismai, 2018, pp. 269-276. Disponível em: http://hdl.handle.net/11328/ 2836. Acesso em: 05 mar. 2020.

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. *Revista Brasileira de Políticas Públicas UniCEUB*, dez. 2017, v. 7, n. 3, pp. 44-59.

ANGOLA. *Lei n.º 7, de 16 de fevereiro de 2017*. Lei de Proteção das Redes e Sistemas Informáticos. Disponível em: https://animalexdominis.files.wordpress.com/2018/03/ protecc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf. Acesso em: 08 mar. 2020.

ANTUNES, Júlia Caiuby de Azevedo. A previsibilidade nas condenações por danos morais: uma reflexão a partir das decisões do STJ sobre relações de consumo bancárias. *Revista Direito GV*. São Paulo, jun. 2009, v. 5, n. 1, pp. 169-184. Disponível em: http://www.scielo. br/scielo.php?script=sci_arttext&pid=S1808-24322009000100009&lng =en&nrm=iso. Acesso em: 09 mar. 2020.

ARAÚJO, Nadia de. *Direito Internacional Privado:* teoria e prática brasileira. 6. ed. Porto Alegre: Revolução eBook, 2016.

ARBIX, Glauco. Inteligência artificial ainda sofre com algoritmos enviesados. *Jornal da USP*, 18 nov. 2019. Disponível em: https://jornal.usp.br/radio-usp/colunistas/inteligencia-artificial-ainda-sofre-com-algorit mos-enviesados/. Acesso em: 15 dez. 2019.

ARBULU, Rafael. Novo sistema de vigilância chinês identifica pessoas pelo jeito de andar. *Canaltech*, 07 nov. 2018. Disponível em: https://canaltech.com.br/seguranca/novo-sistema-de-vigilancia-chines-identifica-pessoas-pelo-jeito-de-andar-126421/. Acesso em: 06 jan. 2020.

ARGENTINA. *Ley Nacional de Protección de Datos Personales nº 25.326, de 30 de outubro de 2000*. Disponível em: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf. Acesso em: 06 jan. 2020.

ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. O que está em jogo no debate sobre dados pessoais no Brasil? *Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o anteprojeto de Lei de Proteção de Dados pessoais.* São Paulo, 2016. Disponível em: http://www.internetlab.org.br/wp-content/ uploads/ 2016/05/reporta_apl_dados_pessoais_final.pdf. Acesso em: 17 abr. 2016.

ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. *O que são dados pessoais?* [especial]. São Paulo, 2016. Disponível em: http://www.internetlab.org.br/ pt/opiniao/especial-o-que-sao-dados-pessoais/. Acesso em: 17 abr. 2020.

AUDIT, Bernard. Qualification et droit international privé. *Droits*, 1993, n. 18.

AUSLOOS, Jef; KINDT, Els; LIEVENS, Eva; VALCKE, Peggy; DUMORTIER, Jos. Guidelines for Privacy-Friendly Default Settings, Feb. 18, 2013. *ICRI Research Paper n. 12/2013*. Disponível em: https://ssrn.com/abstract=2220454. Acesso em: 08 mar. 2020.

BAHL, Aman; BHARSAKLE, Sarthak. The Privacy Jungle – Comparative Study of the Indian Personal Data Protection Act, 2018, with EU GDPR and California Privacy Law. *Indian Journal of Law and Public Policy (IJLPP),* dez. 2019. Disponível em: https://ijlpp.com/the-privacy-jungle-comparative-study-of-the-indian-personal-data-protection-act-2018-with-eu-gdpr-and-california-privacy-law/. Acesso em: 06 jan. 2020.

BAPTISTA, Luiz Olavo. Aplicação do direito estrangeiro pelo juiz brasileiro. *Revista de Informação Legislativa*. Brasília, abr./jun. 1999, ano 36, n.º 142.

BARBAGALO, Érica Brandini; DE MATTIA, Fábio Maria. *Contratos eletrônicos*: contratos formados por meio de redes de computadores peculiaridades jurídicas da formação do vínculo. São Paulo: Universidade de São Paulo, 2000.

BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel da. A coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral de Proteção de Dados. *RJLB*, ano 5, 2019, nº 6, pp. 473-514.

BASILIEN-GAINCHE, Marie-Laure. Les frontières européennes – Quand le migrant incarne la limite. *Revue de l'Union Européene,* jun./2017, n.º 609.

BATALHA, Wilson de Souza Campos. *Tratado de Direito Internacional Privado*. São Paulo: RT, 1997, v. I.

BERGÉ, Jean-Sylvestre; GRUMBACH, Stéphane. The datasphere and the law: new space, new territories. *Revista Brasileira de Políticas Públicas (Brazilian Journal of Public Policy).* Direito e o Mundo Digital, dez. 2017, v. 7, n.º 8.

BEVILÁQUA, Clóvis. *Comentários ao Código Civil*. Rio de Janeiro: Francisco Alves, 1949, v. I.

BIONI, Bruno Ricardo. *Proteção de dados pessoais.* A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIOY, Xavier. Le libre développement de la personnalité en droit constitutionnel, essai de comparaison (Allemagne, Espagne, France, Italie, Suisse). *Revue Internationale de Droit Comparé*, 2003, v. 55, n.º 1, pp. 123-147.

BITTAR, Carlos Alberto. *Responsabilidade civil* – Teoria e prática. 5. ed. Rio de Janeiro: Forense Universitária, 2005.

BOYLE, James. Foucault in Cyberspace: Surveillance, Sovereignty and Hardwwired Censors. *University of Cincinnati Law Review,* 1997, n.º 66.

BRANDÃO, André Martins. Interpretação jurídica e direito à privacidade na Era da Informação: uma abordagem da hermenêutica filosófica. *Revista Paradigma*. Ribeirão Preto, SP, ano XVIII, jan./dez. 2013, n.º 22, pp. 232-257.

BRASIL (Constituição, 1988). *Constituição da República Federativa do Brasil de 198*8. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao compilado.htm. Acesso em: 19 out. 2019.

BRASIL. *Decreto-Lei n.º 4.657 de 04 de setembro de 1942*. Lei de Introdução às Normas do Direito Brasileiro (LINDB). Disponível em: http://www.planalto.gov.br/ccivil_03/ decreto-lei/del4657.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 5.534, de 14 de novembro de 1968*. Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências. Disponível em: http://www.planalto. gov.br/ccivil_03/LEIS/L5534.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: http://www.planalto.gov.br/ ccivil_03/ leis/l8069.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ ccivil_03/leis/l8078.htm. Acesso em: 17 abr. 2020.

BRASIL. *Decreto n.º 99.710, de 21 de novembro de 1990*. Promulga a Convenção sobre os Direitos da Criança. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D99710.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/ LEIS/L9296.htm. Acesso em: 17 abr. 2020.

BRASIL. *Decreto n.º 1.979, de 09 de agosto de 1996*. Promulga a Convenção Interamericana sobre Normas Gerais de Direito Internacional Privado, concluída em Montevidéu, Uruguai, em 8 de maio de 1979. Disponível em: http://www.planalto.gov.br/ ccivil_03/decreto/1996/ D1979.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 9.472, de 16 de julho de 1997*. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos

institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/ LEIS/L9472.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n. 9.613, de 3 de março de 1998*. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras (COAF), e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/ leis/l9613.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 17 abr. 2020.

BRASIL. *Resolução CNS n.º 340, de 08 de julho de 2004*. Incorpora todas as disposições contidas na Resolução CNS n.º 196/96, do Conselho Nacional de Saúde, sobre Diretrizes e Normas Regulamentadoras de Pesquisas Envolvendo Seres Humanos, da qual é parte complementar da área temática específica, e incorpora também, no que couber, as disposições constantes das Resoluções CNS n.º 251/97, 292/99, 303/2000 e 304/2000. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/cns/2004/res0340_08_07_2004. html. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_ 03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 12.527, de 18 de novembro de 2011.* Regula o acesso a informações previsto no inc. XXXIII do art. 5º, no inc. II do § 3º do art. 37, e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 13.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato 2011-2014/2012/lei/l12737.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 12.850, de 02 de agosto de 2013.* Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2014/lei/ l12965.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 17 abr. 2020.

BRASIL. *Decreto n.º 8.506, de 24 de agosto de 2015*. Promulga o Acordo entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América para melhoria da observância tributária internacional e implementação do FATCA. Disponível em: http://www. planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/D8506.htm. Acesso em: 17 abr. 2020.

BRASIL. *Decreto n.º 8.789, de 29 de junho de 2016*. Disponível em: http://www.planalto. gov.br/ccivil_ 03/_Ato2015-2018/2016/Decreto/D8789.htm. Acesso em: 17 abr. 2020.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/ L13709.htm. Acesso em: 17 abr. 2020.

BRASIL. *Decreto n.º 9.663/2019, de 1º de janeiro de 2019*. Aprova o Estatuto do Conselho de Controle de Atividades Financeiras (Coaf). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/ 2019/Decreto/D9663.htm. Acesso em: 17 abr. 2020.

BRASIL. Câmara dos Deputados. *PL 3.420/2019.* Altera o a Lei nº 13.709, de 14 de agosto de 2018, a fim de alterar o critério da multa aplicada às entidades de direito privado em caso de vazamento de dados pessoais. Autoria de Heitor Freire (PSL/CE), apresentado em 11 jun. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramita cao?id Proposicao=2207337. Acesso em: 09 mar. 2020.

BRASIL. Ministério Público do Distrito Federal e Território (MPDFT). *Vazamento de dados leva MPDFT a ajuizar ação contra grupo que explora criptomoedas*, 26 abr. 2019. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/107 94-vazamento-de-dados-leva-mpdft-a-ajuizar-acao-contra-grupo-que-explora-criptomoedas. Acesso em: 21 dez. 2019.

BRASIL. *Projeto de Lei n. 5.762/2019*. Altera a Lei n. 13.709 de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Disponível em: https://www.camara.leg.br/propostas-legislativas/2227704. Acesso em: 17 abr. 2020.

BRASIL. Câmara dos Deputados. *Projeto de Lei n.º 1.179/2020*. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Disponível em: https://www.camara.leg. br/proposicoesWeb/fichadetramitacao?idProposicao=2247564. Acesso em: 17 abr. 2020.

BRASIL. Ministério Público Federal. *Nota Técnica Conjunta – PFDC & Câmara Criminal – Epidemia Covid-19 e PLS (Substitutivo) 1.179/20:* Manutenção do prazo de entrada em vigor da LGPD (ressalvadas as sanções administrativas). PLS (Substitutivo)1179/20, trata do Regime Jurídico Emergencial e transitório das relações jurídicas de Direito Privado no período da pandemia da doença do coronavírus-19 (COVID-19). Art. 25 do PLS ajustado, que adia a *vacatio legis* da LGPD – Lei Geral de

Proteção de Dados até 1º de janeiro de 2021, com a ressalva de que os artigos relativos às sanções só entrarão em vigor em agosto de 2021. Disponível em: https://www.conjur.com.br/dl/nota-tecnica-lgpd.pdf. Acesso em: 18 abr. 2020.

BUSINESS GHANA. *We are working on a cyber security law* – Ursula meets the press [online]. 14 dez. 2018. Disponível em: https://www.businessghana.com/site/news/General/178337/We-are-working-on-a-cyber-security-law-Ursula-meets-the-press-(full-address). Acesso em: 06 jan. 2020.

CAMARA, Dennys Eduardo Gonsales; LAZZARINI, Giuseppe Mateus Boselli; GHERINI, Pamela Michelena de Marchi. *E-sports:* visão geral e desafios jurídicos. Disponível em: https://baptistaluz.com.br/ wp-content/uploads/2018/10/artigo-baptista-luz-pt-E-sports.pdf. Acesso em: 15 dez. 2019.

CAMARGO, Solano de. *Forum shopping:* modo lícito de escolha de jurisdição? Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de São Paulo. Orientador: Prof. Dr. Gustavo Ferraz de Campos Monaco. São Paulo, 2015.

CAMARGO, Solano de. O reconhecimento e a execução de sentenças cibernéticas no Direito Internacional Privado. *In*: MALHEIROS, Clara; MONTE, Mário Ferreira; PEREIRA, Maria Assunção; GONÇALVES, Anabela (Orgs.). *Direito na Lusofonia.* Direito e novas tecnologias. Braga: Escola de Direito da Universidade do Minho, 2018, v. 1, pp. 477-484.

CAMARGO, Solano de. As sanções da LGPD e o Inferno de Dante. *Revista do Advogado,* nov. 2019, v. 1, n.º 144, pp. 220-232.

CAMARGO, Solano de. *Homologação de sentenças estrangeiras:* Ordem Pública Processual e Jurisdições Anômalas. São Paulo: Quartier Latin, 2019.

CAMARGO, Solano de. LGPD restringe inovações na saúde. *Valor Econômico.* São Paulo, 24 jun. 2019. Disponível em: https://valor.globo.com/legislacao/noticia/2019/06/24/lgpd-restringe-inovacoes-na-saude.html. Acesso em: 05 mar. 2020.

CARVALHO, Marcelo Sávio Revoredo Menezes de. *A trajetória da Internet no Brasil:* do surgimento das redes de computadores à instituição dos mecanismos de governança. 239 p. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro. Rio de Janeiro: COPPE, 2006.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999, v. I.

CASTRO, Emília Lana de Freitas; WINTER, Patrícia Pereira. O conflito de jurisdições em caso de violação de direitos da personalidade por publicação na internet. *Revista de Estudos Jurídicos – Unesp,* 2014, v. 18.

CAVALIERI FILHO, Sergio. *Programa de responsabilidade civil*. 7. ed. São Paulo: Atlas, 2007

CEDH. Convenção Europeia dos Direitos do Homem. Roma, 4 nov. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 09 jan. 2020.

CEJAS, Eileen Berenice; GONZÁLEZ, Carlos César. Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales. *SID 2015 – 15º Simposio Argentino de Informática y Derecho.* Disponível em: http://sedici.unlp.edu.ar/bitstream/handle/10915/55549/Documento_ completo.pdf?sequence=1. Acesso em: 06 jan. 2020.

CELLI JÚNIOR, Umberto. Solução de conflitos na União Europeia: lições para o Mercosul? *Revista da Faculdade de Direito. Universidade de São Paulo.* São Paulo, 2002, v. 97, pp. 415-434.

CEYHAN, Ayse. Technologization of Security: management of uncertainty and risk in the age of biometrics. *Surveillance & Society,* 2008, v. 2, n.º 5, pp. 102-123.

CHING, Ke Wan; SINGH, Manmeet Mahinderjit. Wearable technology devices security and privacy vulnerability analysys. *International Journal of Network Security & Its Applications (IJNSA),* maio 2016, v. 8, n. 3. Disponível em: https://pdfs.semanticscholar.org/ed59/579757 a718715ef61c 3346a667257464d312.pdf. Acesso em: 17 abr. 2020.

CHRISTENSEN, Katie. The California Consumer Privacy Act of 2018: are your interests at stake? *Golden Gate University School of Law – GGU Law Review Blog*. 10 jan 2018. Disponível em: https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1055&context=ggu_law_review_blog. Acesso em: 06 jan. 2020.

CISCO. Relatório Cisco VNI Mobile. Disponível em: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~mobile-forecast. Acesso em: 02 nov. 2019.

CITTADINO, Gisele. *Pluralismo, Direito e Justiça Distributiva:* elementos da filosofia constitucional contemporânea. 4. ed. Rio de Janeiro: Lumen Juris, 2009.

CNJ. Conselho Nacional de Justiça. *Inovações em Inteligência Artificial para o PJe são apresentadas no CNJ*, 22 maio 2019. Disponível em: https://www.cnj.jus.br/inovacoes-em-inteligencia-artificial-para-o-pje-sao-apresentadas-no-cnj/. Acesso em: 15 dez. 2019.

COAF. Conselho de Controle de Atividades Financeiras. *Relatório de Atividades 2018*. Disponível em: http://www.fazenda.gov.br/centrais-de-conteudos/publicacoes/relatorio-de-atividades/arquivos/relatorio-de-atividades-coaf-2018.pdf. Acesso em: 02 nov. 2019.

COLOMBIA. *Ley Estatutaria n. 1.266, de 2008*. Parcialmente Regulamentada por el Decreto n. 1.081, de 2015. Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488. Acesso em: 17 abr. 2020.

COLOMBIA. *Ley Estatutaria n. 1.581, de 2012*. Reglamentada parcialmente por el Decreto Nacional n. 1.377, de 2013. Disponível em: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf. Acesso em: 17 abr. 2020.

COLOMÉ, Jordi Pérez. Facebook lança Libra, uma moeda própria para "reinventar o dinheiro". *El País,* 18 jun. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/06/18/tecnologia/1560851467_183722.html. Acesso em: 07 jan. 2020.

COMISSÃO DA UNIÃO AFRICANA (UA); INTERNET SOCIETY (ISOC). Directrizes relativas à Protecção de Dados Pessoais para África, 09 maio 2018.

CONSELHO DE JUSTIÇA FEDERAL. III Jornada de Direito Civil. *Enunciado n.º 173 ao Código Civil.* 2004. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/311. Acesso em: 17 abr. 2020.

CORDEIRO, Antonio Barreto Menezes. O consentimento do titular dos dados no RGPD. *In*: CORDEIRO, Antonio Barreto Menezes *et al. FinTech II:* novos estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019.

CORRÊA, Adriana Espíndola; LOUREIRO, Maria Fernanda Battaglin. Novo regulamento europeu é reforço na proteção dos dados pessoais? (Parte 1). *CONJUR*, 2018. Disponível em: https://www.conjur.com.br/2018-jul-09/direito-civil-atual-regulamento-europeu-ereforco-protecao-dados-pessoais. Acesso em: 13 out. 2019.

CORREIA, António Ferrer. *Lições de Direito Internacional Privado*. Coimbra: Almedina, 2000.

CORREIA, Emanuella Chagas Jaguar. O efeito vinculante do reenvio prejudicial na União Europeia: um caminho para desenvolver o direito comunitário. *Revista de la Secretaría del Tribunal Permanente de Revisión*, 2014, año 2, n.° 4, pp. 65-82.

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. *Direito, Estado e Sociedade,* jul/dez. 2013, n.º 43, pp. 135-161.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. *Comunicado de Imprensa nº 117/15*. Luxemburgo, 6 out. 2015. Disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150 117en.pdf. Acesso em: 24 jul. 2016.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. *Julgamento do Caso C-362/14*. Maximillian Schrems *v.* Data Protection Commissioner. Luxemburgo, 6 out. 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=920501. Acesso em: 08 mar. 2020.

COSTA, José Augusto Fontoura; MINIUCI, Geraldo. Não adianta nem tentar esquecer: um estudo sobre o direito ao esquecimento. *Revista Brasileira de Políticas Públicas (Brazilian Journal of Public Policy).* Direito e Mundo Digital, dez./2017, v. 7, n.º 3.

COSTA, José Augusto Fontoura; SANTOS, Ramon Alberto dos. Contratos internacionais e a eleição do foro estrangeiro no Novo Código de Processo Civil. *Revista de Processo*, mar. 2016, v. 253.

COSTA, José Augusto Fontoura; SOLA, Fernanda. Desenvolvimento e direito de autor na sociedade da informação. *Revista de Direito Econômico e Socioambiental.* Curitiba, jul./dez. 2010, v. 1, n. 2, pp. 285-301.

COSTA, José Augusto Fontoura; SOLA, Fernanda. Direito das tecnologias de comunicação e informação: uma primeira abordagem do Marco Civil da Internet. *PIDCC.* Aracaju, fev. 2015, ano IV, ed. n.º 08/2015, pp. 336-351.

COSTA, José Augusto Fontoura; WACHOWICZ, Marcos. Cláusulas contratuais nulas no Marco Civil da Internet. *Revista da Faculdade de Direito da UFMG.* Belo Horizonte, jan./jun. 2016, n. 68, pp. 477-496.

COSTA, Ligia Maura. *Direito Internacional Eletrônico.* Manual das Transações *On-Line*. São Paulo: Quartier Latin, 2008.

COTTERRELL, Roger. Is it so bad to be different? *In*: ÖRÜCÜ, Esin; NELKEN, David (Eds.). *Comparative law*: a handbook. Portland: Hart Publish, 2007.

CROSBY, Michael; NACHIAPPAN; PATTANAYAK, Pradan; VERMA, Sanjeev; KALYANARAMAN, Vignesh. *Block Chain Technology*: Beyond Bitcoin. Applied Innovation Review, jun./2016, n. 2. Disponível em: https://j2-capital.com/wp-content/uploads/ 2017/11/AIR-2016-Blockchain.pdf. Acesso em: 08 mar. 2020.

CUNHA JÚNIOR, Eurípedes Brito. Os contratos eletrônicos e o Novo Código Civil. *Revista CEJ.* Brasília, out./dez. 2002, n. 19, pp. 62-77.

DHDH. Declaração Universal dos Direitos Humanos. Genebra, Suíça, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 09 jan. 2020.

DÍAZ REVORIO, Francisco Javier. *Valores superiores e interpretación constitucional*. Madrid: Centro de Estudios Políticos y Constitucionales, 1997.

DINHEIRO DIGITAL. *Atlas não quis acordo, agora é com o Ministério Público.* Petição inicial. Disponível em: https://www.mpdft.mp.br/portal/pdf/A%c3%a7%c3%a3o_civil_ por_ danos_ coletivos_Atlas. pdf. Acesso em: 21 dez. 2019.

DINIZ, Maria Helena. Uma visão constitucional e civil do novo paradigma da privacidade: o direito a ser esquecido. *Revista Brasileira de Direito.* Passo Fundo, RS, maio/ago. 2017, v. 13, n.º 2, pp. 7-25. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/ article/ view/1670/1205. Acesso em: 8 mar. 2020.

DLA PIPER. *Data Protection Laws of the World.* Russia, March 2020. Disponível em: www.dlapiperdata protection.com. Acesso em: 08 mar. 2020.

DLA PIPER. *GDPR Data Breach Survey*: February 2019. Disponível em: https://www. dlapiper.com/~/ media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf. Acesso em: 17 abr. 2020.

DOLINGER, Jacob. Direito Internacional Privado – O princípio da proximidade e o futuro da humanidade. *Revista Brasileira de Direito Administrativo*. Rio de Janeiro, jan./mar. 2004, v. 235, pp. 139-149.

DOLINGER Jacob. *Direito Internacional Privado* – Parte Geral. 9. ed. Rio de Janeiro: Renovar, 2008.

DOLINGER, Jacob. Supreme Court Solutions for conflicts between domestic and International Law: An Exercise in Eclecticism. *Capital University Law Review*, 1993, v. 22, n.º 1041.

DOLINGER, Jacob; TIBURCIO, Carmen. *Direito Internacional Privado*. 15. ed. Rio de Janeiro: Forense, 2020.

DONEDA, Danilo. Os direitos da personalidade no Código Civil. *In:* TEPEDINO, Gustavo (Coord.). *A parte geral do novo Código Civil:* estudos na perspectiva civil-constitucional. 2. ed. Rio de Janeiro: Renovar, 2003.

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

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. Joaçaba, SC, jul./dez. 2011, v. 12, n. 2, pp. 91-108.

DREXL, Josef. Le commerce électronique et la protection des consommateurs. *Revue Internationale de Droit Économique*, 2002/2 (t. XVI), doi 10.3917/ride.162.0405. Disponível em: http://www.cairn.info/revue-internationale-de-droit-economique-2002-2-page-405.htm Acesso em: 17 abr. 2020.

EEA-Lex. Disponível em: https://www.efta.int/eea-lex. Acesso em: 05 mar. 2020.

EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. O direito à privacidade na sociedade da informação. *In*: LIMA, Alberto Jorge de Barros; NETTO, Antonio Alves Pereira; SOTTO-MAYOR, Lorena Carla Santos Vasconcelos; LIMA NETO, Manoel Cavalcante de (Orgs.). *I Encontro de Pesquisas Judiciárias da Escola Superior da Magistratura do Estado de Alagoas – ENPEJUD:* Poder Judiciário: estrutura, desafios e concretização dos direitos. Maceió: Fundesmal, 2016. Disponível em: http://enpejud.tjal.jus.br/ index.php/exmpteste01/article/view/63/44. Acesso em: 04 jan. 2020.

EQUIVANT. Disponível em: https://www.equivant. com/northpointe-suite/. Acesso em: 15 dez. 2019.

ESPANHA. *Constituição Federal. 27 de dezembro de 1978*. Disponível em: https://www.boe.es/legisla cion/documentos/ConstitucionCASTELLANO.pdf. Acesso em: 09 jan. 2020.

ESTADOS UNIDOS. Amendment IV. Disponível em: https://constitution.congress.gov/ constitution/amendment-4/. Acesso em: 17 abr. 2020.

ESTADOS UNIDOS. *Consumer Online Privacy Rights Act (Copra) of 2019*. Disponível em: https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf. Acesso em: 06 jan. 2020.

ESTADOS UNIDOS. *The California Consumer Privacy Act (CCPA).* AB375. 2018. Disponível em: https://www.isipp.com/resources/full-text-of-the-california-consumer-privacy-act-of-2018-ccpa/. Acesso em: 07 jan. 2020.

ESTADOS UNIDOS. *USA x Ross William Ulbricht*. Case 1:14-cr-00068-KBF, 02 maio 2015. Disponível em: https://www.docketalarm.com/cases/New_York_Southern_ District_Court/1--14-cr-00068/USA_v.Ulbri cht/183/. Acesso em: 21 dez. 2019.

ESTADOS UNIDOS. *Illinois – Biometric Information Privacy Act (BIPA).* (740 ILCS 14/). Disponível em: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004& ChapterID=57. Acesso em: 18 abr. 2020.

EU-US. European Data Protection Supervisor (EDPS). Press Release EDPS/2016/11. *Privacy Shield:* more robust and sustainable solution needed. Brussels, 30 May 2016. Disponível em: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/ Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf. Acesso em: 08 mar. 2020.

EU-US. *Privacy Shield Framework.* Principles Issued by the U.S. Department of Commerce. Disponível em: https://www.privacyshield.gov/servlet/servlet.FileDownload? file=015t00000004qAg. Acesso em: 08 mar. 2020.

EVANGELISTA, Rafael de Almeida; SOARES, Tiago; SCHIMIDT, Sarah Costa; LAVIGNATTI, Felipe. DIO: um jogo em dispositivos móveis para mapear câmeras de vigilância. *Liind em Revista*. Privacidade e vigilância nos meios digitais. Rio de Janeiro, nov. 2016, v. 12, n. 2, pp. 322-333.

FARELL, Henry; NEWMAN, Abraham. The transatlantic data war. *Foreign Affairs,* jan./fev. 2016. Disponível em: https://www.foreignaffairs.com/articles/united-states/2015-12-14/ transatlantic-data-war. Acesso em: 13 out. 2019.

FARQUHAR, Peter. An FOI request has revealed ‘anonymous’ browser Tor is funded by US government agencies. *Business Insider Australia,* 02 mar. 2018. Disponível em: https://www. businessinsider. com.au/claims-tor-funded-by-us-government-agencies-2018-3. Acesso em: 17 abr. 2020.

FEBRABAN. Federação Brasileira de Bancos. *Pesquisa FEBRABAN de Tecnologia Bancária*, 2019. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/ PDF/Pesquisa-FEBRABAN-Tecnolo gia-Bancaria-2019.pdf. Acesso em: 13 out. 2019.

FERNÁNDEZ, Dora García. El derecho a la intimidad. *Dereito.* México, 2010, v. 19, n.º 2, pp. 269-284.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da USP*, 1993.

FIUZA, César. Para uma releitura da teoria geral da responsabilidade civil. *Revista da Faculdade Mineira de Direito (PUCMG)*, 2006, v. 7, n. 13, pp. 9-15.

FLAHERTY, David H. On the utility of constitutional rights to privacy and data protection. *Case Western Reserve Law Review,* 1990-1991, v. 41, pp. 831-855

FRANÇA. *Lei de Reforma da Justiça* (Réforme de la justice et renforcement de l'organisation des juridictions), 25 de março de 2019. Disponível em: http://www.senat.fr/ espace_presse/ actualites/ 201810/reforme_de_la_justice.html. Acesso em: 15 dez. 2019.

FRANÇA. *Loi n. 1978-17, 6 Janvier 1978.* Relative à l'informatique, aux fichiers et aux libertés modifiée – Loi Informatique et Libertés (Lei n. 1978-17, relativa à informática, aos arquivos e às liberdades – Lei para Informática e Liberdades, LIL). Paris: Journal Officiel de la République Française (Jornal Oficial da República Francesa), 7 jan. 1978, pp. 227-231. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cid Texte=JORFTEXT 000000 8864 60. Acesso em: 17 abr. 2020.

FRANÇA. *Loi n. 2004-801, 6 Août 2004*. Relative à la protection des personnes physiques à l'égard des traitments de données à caractère personnel (Lei n. 2004-801, de 6 ago. 2004, relativa à proteção das pessoas físicas em caso de tratamento de dados pessoais). Paris: Journal Official de la République Française (Jornal Oficial da República Francesa), 2004. Disponível em: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORF TEXT000000441676. Acesso em: 13 out. 2019.

FRANÇA. *Loi n. 2016-1.321, 7 Octobre 2016.* Loi pour une république numérique (Lei para uma República digital, LRD). Paris: Journal Officiel de la République Française (Jornal Oficial da República Francesa), 8 out. 2016. Disponível em: https://www.legi france.gouv.fr/ affichTexte.do?cidTexte=JORFTEXT0000332027 46&categorieLien=id. Acesso em: 17 abr. 2020.

FRANÇA. *Loi n. 70-643, 17 juillet 1970*. Tendant à renforcer la garantie des droits individuels des citoyens. Disponible en: https://www.legifrance.gouv.fr/affichTexte Article.do?idArticle=LEGIARTI000006529714&cidTexte=LEGITEXT000006068385&da teTexte=29990101. Accès à: 17 abr. 2020.

G1. *Documentos da NSA apontam Dilma Rousseff como alvo de espionagem*. Publicado em 01 set. 2013. Disponível em: http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acesso em: 02 nov. 2019.

G29. *Déclaration du G29 relative à la décision de la Commission européenne concernant le Privacy Shield* (bouclier de protection des données UE-États-Unis). 29 juillet 2016. Disponível em: https://www.cnil.fr/fr/declaration-du-g29-relative-la-decision-de-la-commis sion-europeenne-concernant-le-privacy-shield. Acesso em: 08 mar. 2020.

GANA. *Data Protection Act*, 2012. Disponível em: http://media.mofo.com/files/Privacy Library/3981/GHANAbill.pdf. Acesso em: 08 mar. 2020.

GANA. *Electronic Transactions Act*, 2008. Disponível em: https://www.researchictafrica. net/countries/ ghana/Electronic_Transactions_Act_no_772:2008.pdf. Acesso em: 08 mar. 2020.

GARCÍA, María de los Angeles Guzmán. *El derecho fundamental a la protección de datos personales en México:* análisis desde la influencia del orenamiento jurídico espanhol. Tese

(Doutorado) – Universidad Complutense de Madrid, Facultad de Derecho, sob orientação do Prof. Dr. Ildefonso Soriano López, 2013.

GIACOMOLLI, Nereu José; SANTOS, Laura Rodrigues dos. Cooperação Jurídica Internacional em matéria criminal: autoridades centrais, das rogatórias ao auxílio direto. *Revista de Estudos Criminais*, jul./set. 2012, n. 46.

GIBBS, Samuel. What is "safe harbor" and why did the EUCJ just declare it invalid? *The Guardian*, 06 out. 2016. Disponível em: https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection. Acesso em: 20 jun. 2016.

GIBBS, Samuel. Your phone number is all a hacker needs to read texts, listen to calls and track you – Weaknesses within mobile phone network interconnection system allows criminals or governments to remotely snoop on anyone with a phone. *The Guardian*, 18 abr. 2016. Disponível em: https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you. Acesso em: 17 abr. 2020.

GOMES, Helton Simões. Google recebe maior multa já aplicada por violar dados pessoais na Europa. *Uol*, 21 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/21/google-e-multado -na-franca-por-violar-de-dados-pessoais.htm. Acesso em: 06 jan. 2020.

GOMES, Helton Simões. Reconhecimento facial usado na China é testado no Brasil: saiba como opera. *Uol*, 18 jan. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/01/18/reconhecimento-facial-usado-na-china-e-testado-no-brasil-saiba-como-opera.htm. Acesso em: 06 jan. 2020.

GOMES, Rodrigo Dias de Pinho. *Desafios à privacidade:* Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais. Disponível em: https://its rio. org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf. Acesso em: 04 jan. 2020.

GONÇALVES, Anabela Susana de Sousa. O caso *Bolagsupplysningen* e o lugar da ocorrência do facto danoso *online* na violação transfronteiriça de direitos de personalidade. *Direito na Lusofonia.* Direitos e novas tecnologias. Minho, Portugal: Escola de Direito da Universidade do Minho, 2018.

GONÇALVES, Pedro Vilela Resende; CAMARGOS, Rafael Coutinho. Blockchain, Smart Contracts e "Judge as a Service" no Direito Brasileiro. II Seminário Governança das Redes e o Marco Civil da Internet: globalização, tecnologias e conectividade. *Anais*... Belo Horizonte: Instituto de Referência em Internet e Sociedade-IRIS, 2017, pp. 207-212.

GRECO FILHO, Vicente. *Homologação de sentença estrangeira*. São Paulo: Saraiva, 1978.

GREENLEAF, Graham. Global data privacy laws: 89 countries and accelerating. *Privacy Laws & Business International Report*, 2012, n. 115.

GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, 06 jun. 2013. Disponível em: https://www.theguardian.com/world/ 2013/ jun/06/nsa-phone-records-verizon-court-order. Acesso em: 05 jul. 2016.

GREENWALD, Glenn. *The Intercept*. Disponível em: https://theintercept.com/. Acesso em: 05 jul. 2016.

GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, 07 jun. 2013. Disponível em: https://www.the guardian. com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 05 jul. 2016.

GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. *Revista de Direito Administrativo*, 1997, n. 207.

GUEDES, Anielle. Inteligência artificial no tribunal: da análise de dados ao algoritmo juiz. *Uol*, 21 nov 2019. Disponível em: https://anielleguedes.blogosfera.uol.com.br/2019/11/21/ inteligencia-artificial-no-tribunal-da-analise-de-dados-ao-algoritmo-juiz/. Acesso em: 15 dez. 2019.

GUERRA, Sidney. Direito fundamental à intimidade, vida privada, honra e imagem. *In*: XV Encontro Preparatório para o Congresso Nacional do Conpedi. *Anais...* Florianópolis: Fundação Boiteux, 2006. Disponível em: http://conpedi.org.br/manaus/arquivos/anais/ recife/direitos_fundam_sidney_guerra.p. Acesso em: 05 mar. 2020.

HARTZOG, Woodrow. There is no such thing as "public" data – and it's not Ok for researchers to scrape information from websites like OkCupid. *Slate,* 19 maio 2016. Disponível em: http://www.slate.com/articles/technology/futuretense/2016/05/okcupids dataleakshowstheresnosuchthingaspublic_data.html. Acesso em: 17 abr. 2020.

HENRIKSSON, Emil Albihn. Data protection challenges for virtual reality applications. *Interactive Entertainment Law Review.* Jun. 2018. Disponível em: https://www.elgaron line.com/abstract/journals/ielr/1-1/ielr.2018.01.05.xml. Acesso em: 17 abr. 2020.

IBGE. Instituto Brasileiro de Geografia e Estatística. Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento. *Pesquisa Nacional por Amostra de Domicílios Contínua* (PNAD Contínua), 2017.

IBM Watson. *Coloque a Inteligência Artificial para trabalhar*. Disponível em: https://www.ibm.com/watson/br-pt/. Acesso em: 15 dez. 2019.

IDEC. Instituto Brasileiro de Defesa do Consumidor. *Ação Civil Pública com Pedido de Tutela de Urgência.* Petição inicial. Disponível em: https://idec.org.br/sites/default/files/ acp_viaquatro.pdf. Acesso em: 21 dez. 2019.

INTERNETLAB. *Especial Apps para crianças*. Disponível em: http://www.internetlab. org.br/pt/projetos/ especial-apps-para-criancas/. Acesso em: 21 dez. 2019.

INTERNETLAB. Pesquisa em Direito e Tecnologia. *Semanário*, 10 dez. 2019. Disponível em: http://www.internetlab.org.br/pt/itens-semanario/dados-pessoais-apresentado-parecer-pela-aprovacao-de-pec-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-fundamentais/. Acesso em: 04 jan. 2020.

INTERNETLAB. Pesquisa em Direito e Tecnologia. *Vigilância das comunicações pelo Estado brasileiro.* São Paulo, 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_ Vigilancia_Entrega_v2-1.pdf. Acesso em: 17 abr. 2020.

IRLANDA. High Court. *Maximillian Schrems v. Data Protection Commissioner*. IEHC 310, 18 June 2014.

ISAAK, Jim; HANNA, Mina J. User Data Privacy: Facebook, Cambridge Analytica and Privacy Protection. *Computer*, 2018, v. 51, n. 8, pp. 56-59.

JAPÃO. *Lei n. 57, de 2003*. Lei de Proteção de Informações Pessoais (APPI). Disponível em: http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf. Acesso em: 13 out. 2019.

JAYME, Erik. Direito Internacional Privado e Cultura pós-moderna. *Cadernos da Pós-Graduação em Direito da UFRGS.* 2. ed. Porto Alegre: PPGDir, 2004, pp. 105-114.

JAYME, Erik. O Direito Internacional Privado do novo milênio: a proteção da pessoa humana face à globalização. *Cadernos do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul – PPGDir/UFRGS*. Porto Alegre, mar. 2003, v. 1, n. 1, pp. 136-146.

JAYME, Erik. O Direito Internacional Privado do novo milênio: a proteção da pessoa humana face à globalização. *In*: ARAÚJO, Nadia de; MARQUES, Cláudia Lima (Orgs.). *O novo Direito Internacional* – estudos em homenagem a Erik Jayme. Rio de Janeiro: Renovar, 2005, pp. 2-15.

JAYME, Erik. Sociedade multicultural e novos desenvolvimentos no Direito Internacional Privado. *Cadernos do Programa de Pós-Graduação em Direito da UFRGS*, mar. 2003, v. 1, n.º 1, pp. 102-103.

JUNQUEIRA, Miriam. *Contratos eletrônicos*. Rio de Janeiro: Mauad, 1997.

KESSEDJIAN, Catherine. Dispute resolution on-line (Symposium on Jurisdiction and the Internet). *The International Lawyer*, 1998, v. 32, n.º 4, pp. 977-990.

KESSEDJIAN, Catherine. *Le temps du droit au XXIe siècle.* Compatibilité avec la codification? Les Cahiers de droit. Faculté de droit de l'Université Laval, 2005, v. 46, n.º 1-2, pp. 547-560

KISS, Jemima. Privacy shield deal lets US tech firms transfer European customer's data again. *The Guardian*, 08 jul. 2016. Disponível em: https://www.theguardian.com/ technology/ 2016/jul/08/privacy-shield-data-transfer-us-european-union. Acesso em: 13 jul. 2016.

LAÉ, Jean-François. L'intimité: une histoire longue de la propriété de soi. *Sociologie et sociétés*, 2003, v. 35, n° 2, pp. 139-147. Disponível em: http://id.erudit.org/iderudit/ 008527ar. Acesso em: 18 jun. 2016.

LAFER, Celso. A reconstrução dos direitos humanos: a contribuição de Hannah Arendt. *Estudos Avançados*. São Paulo, ago. 1997, v. 11, n.º 30, pp. 55-65.

LAFER, Celso. Vazamentos, sigilo, diplomacia: a propósito do significado do WikiLeaks. *Revista Política Externa*, mar./abr./maio 2011, v. 19, n.º 4.

LAPOWSKY, Issie. Bill Could Give Californians Unprecedented Control Over Data. *Wired*, 22 jun. 2018. Disponível em: www.wired.com/story/new-privacy-bill-could-give-californians-unprecedented-control-over-data. Acesso em: 17 abr. 2020.

LESSIG, Lawrence. Internet: the architecture of privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1999, v. 1, pp. 56-101.

LUCA, Cristina de. G20: Japão propõe que governança mundial de dados seja prioridade. *Blog Porta 23* (Uol). Disponível em: https://porta23.blogosfera.uol.com.br/2019/06/29/g20-japao-propoe-que-governanca-mundial-de-dados-seja-prioridade/. Acesso em: 13 out. 2019.

LUIZ, Gabriel. *CPF em troca de desconto:* MP investiga venda de dados de clientes por farmácias, 16 mar. 2018. G1. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 21 dez. 2019.

LYON, David. Surveillance in Cyberspace: the Internet, Personal Data and Social Control. *Queen's Quarterly*, 2002, n.º 109, pp. 345-357.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. Caderno Especial. São Paulo: RT, dez. 2018, v. 998, pp. 99-128.

MACHADO, J. Baptista. *Âmbito de eficácia e âmbito de competência das leis*. Coimbra: Almedina, 1998.

MACHADO, J. Baptista. *Lições de Direito Internacional Privado*. 3. ed. Coimbra: Almedina, 2006.

MAGALHÃES COLLAÇO, Isabel Maria de. *Da qualificação em direito internacional privado*. Lisboa: s/e, 1964.

MAGALHÃES COLLAÇO, Isabel Maria de. *Direito internacional privado*. Lisboa, 1958-1963.

MAKULILO, Alex Boniface. Privacy and data protection in Africa: a state of the art. *International Data Privacy Law*, 2012, v. 2, n. 3, pp. 163-178.

MANN, Drake. The California Consumer Privacy Act of 2018: why it matters to clients in Arkansas. *The Arkansas Lawyer*, 2019, v. 54, n.° 1. Disponível em: https://www.gill-law.com/wp-content/uploads/ 2019/03/Mann-proof-edited-locked.pdf. Acesso em: 06 jan. 2020.

MARANHÃO, Juliano Souza de Albuquerque. A pesquisa em inteligência artificial e Direito no Brasil. *Consultor Jurídico* (Conjur), 09 dez. 2017. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 18 abr. 2020.

MARANHÃO, Juliano Souza de Albuquerque; FERRAZ JÚNIOR, Tércio Sampaio; FINGER, Marcelo. O desafio do Whatsapp ao Leviatã. *Folha de São Paulo, Tendências/Debates*, 16 ago. 2016. Disponível em: https://www1.folha.uol.com.br/ opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml. Acesso em: 18 abr. 2020.

MARKON, Jerry; NAKASHIMA, Ellen; O'KEEFE, Ed. Lawmakers defend and criticize NSA program to collect phone logs. *The Washington Post*, 06 jun. 2013. Disponível em: https://www.washingtonpost.com/ world/national-security/administration-lawmakers-defend-nsa-program-to-collect-phone-records/2013/06/06/2a56d966-ceb9-11e2-8f6b-67f40e176f03_story.html?tid=a_inl. Acesso em: 17 abr. 2016.

MARQUES, Cláudia Lima. A insuficiente proteção do consumidor nas normas de direito internacional privado – da necessidade de uma convenção interamericana (CIDIP) sobre a lei aplicável a contratos e relações de consumo. *Revista dos Tribunais.* São Paulo, 2001, v. 788, pp. 11-56.

MARQUES, Cáudia Lima, Ensaio para uma introdução ao Direito Internacional Privado. *In*: DIREITO, Carlos Alberto Menezes; PEREIRA, Antonio Celso Alves; TRINDADE, Antônio Augusto Cançado. *Novas perspectivas do Direito Internacional Privado Contemporâneo*. Rio de Janeiro: Renovar, 2008, pp. 315-340.

MARQUES, Cláudia Lima; JACQUES, Daniela Corrêa. Normas de aplicação imediata como um método para o Direito Internacional Privado de proteção do consumidor no Brasil. *Cadernos de Pós-Graduação em Direito da UFRGS*, 2004, n. 1, pp. 65-96.

MARTIAL-BRAZ, Nathalie. O direito das pessoas interessadas no tratamento de dados pessoais: anotações da situação na França e na Europa. *Revista de Direito, Estado e Telecomunicações*. Brasília, maio 2018, v. 10, n. 1, pp. 85-108.

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, v. 1.

MELO, Milena Barbosa de; LUCENA, Elis Formina; TEIXEIRA, Ana Luiza Figueiredo Quirino. Contratos eletrônicos internacionais: uma análise sobre a lei aplicável e competência. *Revista Dat@venia*, jan./abr. 2015, v. 7, n. 1, pp. 70-96.

MENDONÇA, Fernanda Graebin. Proteção de dados pessoais na Internet: análises comparativas da situação do direito à autodeterminação informativa no Brasil e em países latino-americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA*, 2016, v. 11, n. 1.

MÉXICO. *Nueva Ley DOF, de 05 de julho de 2010*. Ley Federal de Protección de Datos Personales em Posesión de los Particulares. Disponível em: http://www.diputados.gob.mx/ LeyesBiblio/pdf/LFPDPPP.pdf. Acesso em: 17 abr. 2020.

MIGALHAS. *MP/RJ acusa Decolar.com de manipular preços para discriminar brasileiros:* ACP requer reparação de R$ 57 milhões por danos morais coletivos. 2018.

Disponível em: https://www.migalhas.com.br/ Quentes/17,MI273955,91041-MPRJ+ acusa+Decolarcom+de+ manipular+precos+para+discriminar+brasilei ros. Acesso em: 21 dez. 2019.

MIRON, Rafael Brum. O sigilo bancário e a atuação do Coaf: análise dos critérios definidos pelo STF no julgamento da ADI2390/DF para a transferência de sigilo de dados. *Revista da AJURIS*. Porto Alegre, jun. 2017, v. 44, n. 142.

MONACO, Gustavo Ferraz de Campos. A globalização entre o passado e o futuro da soberania. *Revista da Faculdade de Direito do Sul de Minas*, v. extra, 2008, pp. 45-53.

MONACO, Gustavo Ferraz de Campos. *Controle de constitucionalidade da lei estrangeira*. São Paulo: Quartier Latin, 2013.

MONACO, Gustavo Ferraz de Campos. Competência internacional (limites à jurisdição nacional) em matéria de ação revisional de prestação alimentícia e partilha de bens. *Revista de Processo*, 2017, v. 266, pp. 365-391.

MONACO, Gustavo Ferraz de Campos. Direito Internacional Privado da Família: influências da História e da Geografia do Brasil. *In*: MONACO, Gustavo Ferraz de Campos; FULCHIRON, Hugues (Orgs.). *Famílias internacionais:* seus direitos, seus deveres. São Paulo: Intelecto, 2016, v. 1.

MONACO, Gustavo Ferraz de Campos. Uso indevido de imagem de crianças e o papel da escola básica. *JOTA*. Publicado em 09 fev. 2018. Disponível em: https://www.jota.info/ opiniao-e-analise/artigos/uso-indevido-de-imagem-de-criancas-e-o-papel-da-escola-basica-09022018. Acesso em: 28 jun. 2018.

MONACO, Gustavo Ferraz de Campos. *Conflitos de leis no espaço e lacunas (inter) sistêmicas.* São Paulo: Quartier Latin, 2019.

MONACO, Gustavo Ferraz de Campos; CAMARGO, Solano de; SMITH MARTINS, Amanda Cunha e Mello. Sem sanções, LGPD é inócua. *Valor Econômico,* 13 abr. 2020. Disponível em: https://valor.globo.com/legislacao/noticia/2020/04/13/sem-sancoes-lgpd-e-inocua.ghtml. Acesso em: 18 abr. 2020.

MORASSUTTI, Bruno Schimitt. Uma breve crítica ao *Privacy By Design* e seus "princípios basilares". *In*: SARLET, Ingo Wolfgang (Org.). *Temas atuais e polêmicos de Direitos Fundamentais.* Contribuições do XIV Seminário Internacional de Direitos Fundamentais. Porto Alegre: Fi, 2018.

MOREIRA, André de O. Schenini. Propriedade intelectual e esportes: o premente conflito entre o direito de exclusividade e a liberdade desportiva. *Lei em campo*, 25 nov. 2019. Disponível em: https://leiemcampo.com.br/propriedade-intelectual-e-esports-o-premente-conflito-entre-o-direito-de-exclusiva-e-a-liberdade-desportiva/. Acesso em: 15 dez. 2019.

MOTA, Joana. Proteção de dados desde a concepção e por defeito. Avaliação de impacto e segurança. *In*: CORDEIRO, António Menezes *et al. FinTech II:* novos estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019.

MOURA RAMOS, Rui Manuel Gens de. Introdução ao Direito Internacional Privado da União Europeia: da interação originária do Direito Internacional Privado e do Direito Comunitário à criação de um Direito Internacional Privado da União Europeia. *In*: MOURA RAMOS, Rui Manuel Gens de; MONACO, Gustavo Ferraz de Campos (Coords.). *Aspectos da unificação europeia do Direito Internacional Privado.* São Paulo: Intelecto, 2016.

MOURA RAMOS, Rui Manuel Gens de; MONACO, Gustavo Ferraz de Campos (Coords.). *Aspectos da unificação europeia do Direito Internacional Privado.* São Paulo: Intelecto, 2016.

MOURA VICENTE, Dário Manuel Lentz de. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005.

MOZETIC, Vinícius Almada; BABARESCO, Daniele Vedovatto Gomes da Silva. Lei Geral de Proteção de Dados de Crianças e Adolescentes no Brasil: coleta de dados e o problema da obrigatoriedade do consentimento dos pais. *A Era Digital e os direitos das crianças e adolescentes,* 2020. Disponível em: https://www.academia.edu/42044798/LGPD_E_A_OBRIGATORIEDADE_DO_CONSENTIMENTO_NA_COLETA_DE_DADOS_DE_CRIAN%C3%87AS_E_ADOLESCENTES_NO_BRASIL. Acesso em: 10 out. 2019.

NAKAMOTO, Satoshi. *Bitcoin:* a Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 08 dez. 2019.

NAKASHIMA, Ellen. Verizon providing all call records to U.S. under court order. *The Washington Post*, 06 jun. 2013. Disponível em: https://www.washingtonpost.com/world/national-security/verizon-providing-all-call-records-to-us-under-court-order/2013/06/05/98656606-ce47-11e2-8845-d970ccb04497_story.html. Acesso em: 17 abr. 2020.

NARAYANAN, Arvind; FELTEN, Edward W. *No silver bullet*: de-identification still doesn't work. 2014. Disponível em: https://www.semanticscholar.org/paper/No-silver-bullet-%3A-De-identification-still-doesn-'-Narayanan-Felten/1df5567c45ac8cb9289411268573aea89e74 e542. Acesso em: 20 out. 2018.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. *RIL.* Brasília, jan./mar. 2017, ano 54, n.º 213, pp. 265-288.

NCUBE, Caroline. A comparative analysis of Zimbabwean and South African data protection systems. *Journal of Information, Law & Technology*, 2004, v. 2.

NILLER, Eric. Can al be a fair judge in court? Estonia Thinks so. *Wired*, 25 mar. 2019. Disponível em: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/. Acesso em: 17 abr. 2020.

NOJIRI, Sérgio. O direito à privacidade na era da informática: algumas considerações. *Revista Jur – UNIJUS.* Uberaba, MG, maio/2005, v. 8, n.º 8, pp. 99-106.

OCDE. Organização para a Cooperação e Desenvolvimento Econômicos. *Síntese das Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados*

Pessoais, 1980. Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 17 abr. 2020.

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, 2010, v. 57. University of Colorado Law Legal Studies Research Paper n. 9-12. Disponível em: https://ssrn.com/abstract=1450006. Acesso em: 20 out. 2018, pp. 1735-1746.

OLIVEIRA, Carlos Eduardo Elias de. *Aspectos principais da Lei nº 12.965, de 2014, o Marco Civil da Internet:* subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, abr./2014 (Texto para Discussão nº 148). Disponível em: www.senado.leg.br/estudos. Acesso em: 20 out. 2018.

OLIVEIRA, Elsa Dias. *A proteção dos consumidores nos contratos celebrados através da Internet.* Coimbra: Almedina, 2002.

OLIVEIRA, Elsa Dias. Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em direito internacional privado. *Cuadernos de Derecho Transnacional*, mar./2013, v. 5, n.º 1, pp. 139-162.

ONU. Organização das Nações Unidas. *Declaração Universal dos Direitos Humanos*. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 05 mar. 2020.

ORTEGA, João. Moeda digital oficial da China está pronta para lançamento. *StartSe*, 12 ago. 2019. Disponível em: https://www.startse.com/noticia/ecossistema/criptomoeda-oficial-china. Acesso em: 07 jan. 2020.

PACTO INTERNACIONAL DOS DIREITOS CIVIS E POLÍTICOS. 16 dez. 1966. Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20 sobre%20 Direitos%20Civis%20e%20Pol%C3%ADticos.pdf. Acesso em: 09 jan. 2020.

PAUCHET, Maria. RGPD vs Privacy Shield? *In: Digital we Trust* – Faire le lien entre confiance et simplicité. Disponível em: https://www.indigitalwetrust.fr/2017/11/rgpd-privacy-shield/. Acesso em: 08 mar. 2020.

PELTZ-STEELE, Richard J. The pond betwixt: differences in the US-EU data protection/safe harbor negotiation. *Journal of Internet law* [1094-2904], 2015, v. 19, pp. 20-25.

PEREIRA, Caio Mário da Silva. *Responsabilidade civil*. Rio de Janeiro: Forense, 1990.

PEREIRA, Caio Mário da Silva. *Instituições de Direito Civil*. 11. ed. Rio de Janeiro: Forense, 2004, v. III.

PERES, Bruno; SALES, Robson; POLITO, Rodrigo. Ataque de *hackers* atinge o Brasil; INSS do Rio e TJ-SP são afetados. *Agência O Globo e Folhapress*, 12 maio 2017. Disponível em: https://www.valor. com.br/empresas/4967124/ataque-de-hackers-atinge-o-brasil-inss-do-rio-e-tj-sp-sao-afetados Acesso em: 02 nov. 2019.

PERU. *Ley n.º 29.733*. Ley de Protección de Datos Personales. Disponível em: https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf. Acesso em: 17 abr. 2020.

PINHEIRO, Alexandre Sousa *et al.* (Coords.). *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra: Almedina, 2018.

POLIDO, Fabrício Bertini Pasquot. *Direito internacional privado nas fronteiras do trabalho e tecnologias:* ensaios e narrativas na Era Digital. Rio de Janeiro: Lúmen Juris, 2018.

POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves. *Governança global da internet, conflito de leis e jurisdição*. Belo Horizonte: Instituto de Referência em Internet e Sociedade (IRIS), 2018.

POLIDO, Fabrício Bertini Pasquot; SILVA, Lucas Sávio Oliveira da. Contratos Internacionais eletrônicos e o Direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. *Sequência*. Florianópolis, abr. 2017, n. 75, pp. 157-188. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2177-70552017000100157 &lng= en&nrm=iso. Acesso em: 21 dez. 2019.

PORTUGAL. *Constituição da República Portuguesa*. Disponível em: https://www. parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 17 abr. 2020.

PORTUGAL. *Relatório de Atividades da Comissão Nacional de Proteção de Dados, 2017-2018*. Disponível em: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf. Acesso em: 20 out. 2019.

PORTUGAL. Tribunal da Relação de Lisboa. *Processo 7438/08.4TVLSB.L1-2*. Julgado em 08 nov. 2012. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565 fa00497eec/d2f8a5f750a0c95380257b240053c2c0?OpenDocument&Highlight=0,Regulam ento,44%2F2001. Acesso em: 22 dez. 2019.

RAJPUKAR, Pravan *et al.* CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning. Computer Vision and Pattern Recognition. *Cornell University*. 14 nov. 2017. Disponível em: https://arxiv.org/abs/1711.05225. Acesso em: 15 dez. 2019.

RAMOS, Victor de Moraes. A validade dos contratos celebrados pela internet (contratos eletrônicos). *Revista de Direito UNIFACS – Debate Virtual*, 2009, n. 105, ISSN 1808-4435. Disponível em: https://revistas.unifacs.br/ index.php/redu/article/view/539. Acesso em: 07 jan. 2020.

REINO UNIDO. Information Comissioner's Office (ICO). *Intention to fine British Airways £183.39m under GDPR for data breach*, 08 jul. 2019. Disponível em: https://ico.org.uk/ about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/. Acesso em: 20 out. 2019.

REINO UNIDO. Information Comissioner's Office (ICO). *Statement:* Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 09 jul.

2019. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/. Acesso em: 17 abr. 2020.

REMOLINA-ANGARITA, Nelson. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *Rev. Colomb. Derecho Int. ildi.* Bogotá, Colômbia, jan./jun. 2010, n° 16, pp. 489-524.

RESINA, Fernando *et al. Cloud – a lei e a prática:* guia e perguntas frequentes. Coimbra: Almedina, 2016.

REYNOLDS, Matt. *What is article 13?* The EU's divisive new copyright plan explained. *Wired.* Publicado em: 24 maio 2019. Disponível em: https://www.wired.co.uk/article/what-is-article-13-article-11-european-directive-on-copyright-explained-meme-ban. Acesso em: 17 abr. 2020.

RIBEIRO, Marilda Rosado de Sá; ALMEIDA, Bruno. A cinemática jurídica global: conteúdo do Direito Internacional Privado contemporâneo. *Revista da Faculdade de Direito da UERJ*, 2011, v.1, n. 20, ISSN 22363475. Disponível em: file:///C:/Users/anadi/Downloads/1516-8697-2-PB.pdf. Acesso em: 17 abr. 2020.

RIBEIRO, Marilda Rosado de Sá. Cooperação Internacional. *Revista da Faculdade de Direito da UERJ*, 2005, v. 13/14, pp. 185-203.

ROBERTO, Wilson Furtado. *Dano transnacional e internet:* direito aplicável e competência internacional. Curitiba: Juruá, 2010.

ROTENBERG, Marc. Updating the law of information privacy: the new framework of the European Union. *Harvard Journal of Law and Public Policy* [0193-4872], 2013, v. 36 iss: 2.

SANTOS, João Vieira dos. Desafios jurídicos e regulatórios das *Initial Coin Offerings. In*: CORDEIRO, António Menezes *et al. FinTech II:* novos estudos sobre tecnologia financeira. Coimbra: Almedina, 2019.

SAUNDERS, David; GLOVER, Allison. Insight: a Federal Privacy Bill May be Closer than Once Thought. *Bloomberg Law,* 14 fev. 2020. Disponível em: https://news.bloomberglaw.com/privacy-and-data-security/insight-a-federal-privacy-bill-may-be-closer-than-once-thought. Acesso em: 05 mar. 2020.

SCHREIBER, Anderson. As três correntes do direito ao esquecimento. *Jota,* 18 jun. 2017. Disponível em: https://bit.ly/2QErVqY. Acesso em: 09 jan. 2020.

SHILS, Edward. Privacy. Its constitution and vicissitudes. *In*: *Law and Contemporary Problems*. Durham, Carolina do Norte, EUA: Duke Law University, LCP, 1966, v. 31, n.° 2, pp. 281-306.

SILVA, Matheus Passos. A segurança da democracia e a *blockchain*. *Projeção, Direito e Sociedade*, 2018, v. 9, n. 1, pp. 119-138.

SIMÃO, Rui Jorge Costa. Alinhamento da União Europeia e Japão sobre Proteção de Dados – e "Step in Japan". *República do Direito:* Associação Jurídica de Coimbra, dez. 2018.

SOARES, Pedro Silveira Campos. Legítimo interesse como hipótese para tratamento de dados. *Conjur*, 18 jun. 2019. Disponível em: https://www.conjur.com.br/2019-jun-18/pedro-soares-tratamento-dados-baseado-legitimo-interesse. Acesso em: 07 jan. 2020.

SOLOVE, Daniel J. Access and aggregation: public records, privacy and the Constitution. (Modern Studies in Privacy Law). *Minnesota Law Review* [0026-5535], 2002, v. 86, iss: 6.

SOMERVILLE, Heather. Uber to pay $148 million to settle data breach cover-up with U.S. states. *Reuters*, 26 set. 2018. Disponível em: https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ. Acesso em: 20 out. 2019.

SOPRANA, Paulo. Analistas veem risco à privacidade com tecnologia de reconhecimento facial. *Folha de São Paulo*, 17 jan. 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/01/analistas-veem-risco-a-privacidade-com-tecnologia-de-reconhecimento-facial.shtml. Acesso em: 17 abr. 2019.

SOULIER, Jean-Luc; SLEE, Sandra. La protection des données à caractère personnel et de la vie privée dans le secteur des communications électroniques. Perspective française. *Revue Internationale de Droit Comparé*, abr./jun. 2002, v. 54, n.° 2, pp. 663-676. Disponível em: http://www.persee.fr/doc/ridc_0035-3337_2002_num_54_2_18761 Acesso em: 18 maio 2016.

STF. Supremo Tribunal Federal. *Habeas Corpus 75.261 MG.* Rel. Min. Octávio Gallotti – Julgado em 24/06/1997. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/14700087/habeas-corpus-hc-75261-mg?ref=serp. Acesso em: 17 abr. 2020.

STF. Supremo Tribunal Federal. *HC 81.154*. Rel. Min. Maurício Corrêa, publicado em 19 dez. 2001.

STF. Supremo Tribunal Federal. *Inteligência artificial vai agilizar a tramitação de processos no* STF, 30 maio 2018. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe. asp?idConteudo=380038. Acesso em: 15 dez. 2019.

STF. Supremo Tribunal Federal. *Recurso Extraordinário n.º 1055941*. Rel. Min. Dias Toffoli. Julgado em: 04 dez. 2019.

STF. Supremo Tribunal Federal. *Regimento Interno.* 2019. Disponível em: https://www.stf.jus.br/arquivo/ cms/legislacaoRegimentoInterno/anexo/RISTF.pdf. Acesso em: 10 out. 2019.

STJ. Superior Tribunal de Justiça. *Ag 748.056/RJ*. Rel. Min. Humberto Gomes de Barros. Publicado em 05 maio 2006.

STJ. Superior Tribunal de Justiça. *REsp 1021987/RN*. Rel. Ministro Fernando Gonçalves, Quarta Turma. Julgado em 07 out. 2008, DJe 09 fev. 2009.

STJ. Superior Tribunal de Justiça. Terceira Sessão. *RJ 2006/0161102-7*. Min. Rel. Og Fernandes. Julgado em 16 fev. 2009.

STJ. Superior Tribunal de Justiça. *REsp 1.089.993-SP*. Rel. Ministro Massami Uyeda, julgado em 18 fev. 2010.

STJ. Superior Tribunal de Justiça. Terceira Sessão. *RS 2009/0183264-2*. Rel. Min. Ministro Jorge Mussi. Julgado em 27 out. 2010.

STJ. Superior Tribunal de Justiça. *Resp. 1168546/RJ*. Rel. Ministro Luis Felipe Salomão. Quarta Turma, julgado em 11 maio 2010, DJE em 07 fev. 2011.

STJ. Superior Tribunal de Justiça. I*nformativo n.º 495, de 9 a 20 de abril de 2012*, 3ª Turma, REsp 1.306.066-MT, rel. Min. Sidnei Beneti.

STJ. Superior Tribunal de Justiça. *Recurso Especial n.º 1.192.208-MG*. Rel. Min. Nancy Andrighi, Terceira Turma. Julgado em 12/06/2012, publicado em 02/08/2012.

STJ. Superior Tribunal de Justiça. *Inq. 784/DF*. Rel. Ministra Laurita Vaz. Corte Especial, julgado em 17 abr. 2013. DJe 28 ago. 2013.

STJ. Superior Tribunal de Justiça. *REsp 1306157/SP*. Rel. Ministro Luis Felipe Salomão, Quarta Turma, julgado em 17 dez. 2013, DJe 24 mar. 2014.

STJ. Superior Tribunal de Justiça. *Recurso Especial n.º 1354484*. Rel. Min. Lázaro Guimarães. Julgado em 19 jun. 2018.

STJ. Superior Tribunal de Justiça. *Regimento Interno – RISTJ*. Disponível em: https://ww2.stj.jus.br/publicacaoinstitucional/index.php/Regimento/issue/view/1/showToc Acesso em: 17 abr. 2020.

STRENGER, Irineu. Aspectos da contratação internacional. *Revista da Faculdade de Direito, Universidade de São Paulo.* São Paulo, jan./2001, v. 96, pp. 455-474.

SWINHOE, Dan. Os oito maiores vazamentos de dados de 2018. Hacks e roubos de dados custaram um total de quase US$ 280 milhões para empresas. *Computerworld*. Disponível em: https://computerworld.com.br/2018/10/31/os-8-maiores-vazamentos-de-dados-de-2018/. Acesso em: 20 out. 2019.

TAKAHASHI, Tadao (Org.). *Sociedade da Informação no Brasil – Livro Verde*. Brasília: Ministério da Ciência e Tecnologia, set. 2000.

TERWANGE, Cécile de. Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *IDP. Revista de Internet – Derecho y Política*, 2012, v. 13. Disponível em: https://www.redalyc.org/pdf/788/78824460006.pdf. Acesso em: 09 jan. 2020.

TIBURCIO, Carmen. As regras sobre o exercício da jurisdição brasileira no novo Código de Processo Civil. *Revista Interdisciplinar de Direito.* Faculdade de Direito de Valença, jan./jun. 2018, v. 16, n. 1, pp. 67-90.

TIBURCIO, Carmen. *Extensão e limites da jurisdição brasileira:* competência internacional e imunidade de jurisdição. Salvador: JusPodivm, 2006.

TJ/DF. Tribunal de Justiça do Distrito Federal. *Incidente de Uniformização de Jurisprudência n.º 003150-90.2018.8.07.0000.* Rel. Asiel Henrique de Souza, julgado em 18 out. 2018.

TJ/RJ. Tribunal de Justiça do Rio de Janeiro. *Apelação Cível n.º 0022893-68.2014.8.19.0202*. 26ª Câmara Cível. Consumidor Rel. Des. Natacha Nascimento Gomes Tostes Gonçalves de Oliveira. Julgado em 27 jul. 2017.

TJ/RJ. Tribunal de Justiça do Rio de Janeiro. *Apelação Cível n.º 0031762-47.2012.8.19.0054*. 5ª Câmara Cível. Rel. Des. Heleno Ribeiro Pereira Nunes. Julgado em 10 dez. 2019.

TJ/SE. Tribunal de Justiça do Estado de Sergipe. *Mandado de Segurança n.º 201600110899*. Des. Rel. Ricardo Múcio Santana de Abreu Lima. Julgado em 03 maio 2016.

TJ/SP. Tribunal de Justiça de São Paulo. 4ª Câmara de Direito Privado. *Agravo de Instrumento nº 472.738-4*. Des. Rel. Ênio Santarelli Zuliani. Julgado em 17 jul. 2008.

TJ/SP. Tribunal de Justiça de São Paulo. *Apelação Cível n.º 1001507-77.2016.8.26.0079*. 21ª Câmara de Direito Privado. Des. Rel. Silveira Paulilo. Julgado em 17 jan. 2018.

TJ/SP. Tribunal de Justiça do Estado de São Paulo. 11ª Câmara de Direito Criminal. *Mandado de Segurança n.º 2271462-77.2015.8.26.0000*. Rel. Des. Xavier de Souza. Julgado em 17 dez. 2015.

TOLEDO, Letícia. Como a Inteligência artificial está guiando o mercado financeiro. *InfoMoney*, 17 jan. 2019. Disponível em: https://www.infomoney.com.br/mercados/como-a-inteligencia-artificial-esta-guiando-o-mercado-financeiro/. Acesso em: 15 dez. 2019.

TRAÇA, João Luís; EMBRY, Bernardo. The Angolan Data Protection Act: first impressions. *International Data Privacy Law,* 2012, v. 2, n. 1.

TRF3. Justiça Federal da 3ª Região. 9ª Vara Cível Federal de São Paulo. *Ação Civil Pública n.º 5009507-78.2018.4.03.6100.* Sentença proferida em 27 abr. 2018, por Cristiane Farias Rodrigues dos Santos.

TUNC, André. *La responsabilité civile*. Paris: Econômica, 1981.

UNIÃO EUROPEIA. *Charte des droits fondamentaux de l'Union européenne* (Carta dos Direitos Fundamentais da União Europeia), 2000, C364/01. Journal Officiel des Communautés Européennes. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_fr.pdf. Acesso em: 15 jun. 2016.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *2000/520/EC:* Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy

principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX: 32000D0520&from=EM. Acesso em: 05 mar. 2020.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *Documento de trabalho dos serviços da Comissão sobre a aplicação da Decisão 520/2000/CE da Comissão, 26 jul. 2000.* Disponível em: https://ec.europa.eu/transparency/regdoc/ rep/2/2002/PT/2-2002-196-PT-1-1.Pdf. Acesso em: 05 mar. 2020.

UNIÃO EUROPEIA. *Comissão Europeia (CE).* Disponível em: https://ec.europa.eu/ info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/how-consent-processing-scientific-research-obtained_pt#resposta. Acesso em: 17 abr. 2020.

UNIÃO EUROPEIA. Conference of the Representatives of the Governments of the Member States. *Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community*. 2007/C 306/01, art. 16B, Dec. 13, 2007. Disponível em: https://www.refworld.org/docid/476258d32.html. Acesso em: 17 abr. 2020.

UNIÃO EUROPEIA. Conselho da Europa. *Convenção Europeia de Direitos Humanos.* 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 05 mar. 2020.

UNIÃO EUROPEIA. Conselho da Europa. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Jan. 28, 1981, Eur. T.S. n. 108 [Convention 108].

UNIÃO EUROPEIA. *Directive 95/46/EC.* European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.

UNIÃO EUROPEIA. *Directive 97/66/EC*. European Parliament and the Council concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 15 Dec. 1997.

UNIÃO EUROPEIA. *Regulamento (EU) n.º 1215/2012*. Parlamento Europeu e do Conselho de 12 de dezembro de 2012 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial.

UNIÃO EUROPEIA. *Regulamento 2016/679.* Regulamento Geral sobre a Proteção de Dados. Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/45/CE. Disponível em: http://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=uri serv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:T OC. Acesso em: 08 mar. 2020.

UNIÃO EUROPEIA. TJUE. *Bundesverband der Verbraucherzentralen und Verbraucherverbände* – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH.

Processo C-673/17, 01 out. 2019. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=D5DC4CA415C605B28E70747FD3C5158C?text&docid=218462&pageIndex=0&doclang=PT&mode=req&dir&occ=first&part=1&cid=1458627. Acesso em: 08 mar. 2020.

UNIÃO EUROPEIA. *Tratado sobre o Funcionamento da União Europeia*. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-1aa75ed71a1.0019.01/DOC_3&format= PDF. Acesso em: 08 mar. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Caso C-131/12*. Google Spain SL e Google Inc. vs. Agencia Española de Proteção de Dados, 13 maio 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT. Acesso em: 17 abr. 2020.

VAAS, Lisa. Two schoolkids sue Google for collecting biometrics. *Naked Security*, 07 abr. 2020. Disponível em: https://nakedsecurity.sophos.com/2020/04/07/two-schoolkids-sue-google-for-collecting-biometrics/ Acesso em: 18 abr. 2020.

VAINZOF, Rony. Geopricing é ilegal? *JOTA*. Disponível em: //www.jota.info/opiniao-e-analise/colunas/direito-digital/geopricing-e-ilegal-12012017. Acesso em: 01 jul. 2020.

VALENTE, Jonas. Legislação da proteção de dados já é uma realidade em outros países. *Agência Brasil*, 2018. Disponível em: http://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 13 out. 2019.

VALENZUELA, Daniel Álvarez. Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridade de control em matéria de protección de datos? *RDUCN – Revista de Derecho*. Coquimbo, jun. 2016, v. 23, n.º 1. Disponível em: https://scielo.conicyt.cl/ scielo.php?pid=S0718-97532016000100003&script =sci_arttext&tlng=em. Acesso em: 06 jan. 2020.

VICENTE, Dário Moura. *Direito Internacional Privado.* Problemática Internacional da Sociedade da Informação. Coimbra: Almedina, 2005.

VILLALTA, Luis Fernando García. *It compliance, privacidad y protección de datos para empresas públicas en el Perú*. Tese (Trabalho de Conclusão de Curso) – Universidad Nacional del Altiplano, Facultad de Ciencias Jurídicas y Políticas, Escuela Professional de Derecho, sob orientação do Prof. Dr. Javier Sócrates Pineda Ancco. Puno, Peru, 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, 1890, n.º 193.

WARZEL, Charlie. Will Congress Actually Pass a Privacy Bill? *The New York Times*. 10 dez. 2019. Disponível em: https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html.Acesso em: 06 jan. 2020.

WORLOCK, Charlotte. European Union: GDPR – The First Complaints. *Mondaq*, 07 jun. 2018. Disponível em: http://www.mondaq.com/uk/x/708562/data+protection/GDPR+The+First+Complaints. Acesso em: 17 abr. 2020.

YAKOWITZ, Jane. Tragedy of the Data Commons. *Harvard Journal of Law & Technology*, 2011, v. 25, n. 1.

ZHANG, Gil; YIN; Kate. More updates on the Chinese data protection regime in 2019. *International Association of Privacy Professionals.* Disponível em: https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/. Acesso em: 08 mar. 2020.

ZIMBABUÉ. *Access to Information and Protection of Privacy Act*, 2003. Disponível em: https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Zimbabwe_ Access%20to%20Information%20Law_2008_en.pdf. Acesso em: 08 mar. 2020.

OBRAS CONSULTADAS

ABRUSIO, Juliana; FLORENCIO FILHO, Marco Aurélio. Reflexões sobre as relações de consumo na sociedade da Informação. In: (Orgs). CARACIOLA, Andrea Boari; ANDREUCCI, Ana Cláusia Pompeu Torezan; FREITAS, Aline da Silva. Código de Defesa do Consumidor – 20 anos. São Paulo: LTr., 2010.

ABRUSIO, Juliana. A recepção de novas tecnologias em relação aos negócios jurídicos e assinatura digital. Revista Fórum CESA, v. 2, p. 61-64, 2007.

ALEXY, Robert. Constitutional Rights and Proportionality. *Revus* [Online], 2014, v. 22, pp. 51-65. Disponível em: http://revus.revues.org/2783. Acesso em: 29 dez. 2019.

ALVIM, Agostinho. *Da inexecução das obrigações e suas consequências*. 5. ed. São Paulo: Saraiva, 1980.

AMARAL, Francisco. Código Civil e interpretação jurídica. *Revista Brasileira de Direito Comparado*, jan./jun. 2013, n. 44/45, pp. 147-167.

ANDRADE, André Gustavo Corrêa de. *Indenização punitiva*. Disponível em: http://www.tjrj.jus.br/c/document_library/get_file?uuid=dd10e43d-25e9-478f-a346-ec511dd4188a. Acesso em: 22 maio 2018.

ARAÚJO, Nadia de. *Contratos internacionais*. Rio de Janeiro: Renovar, 2004.

ARAÚJO, Nadia de (Coord.). *Cooperação jurídica internacional no Superior Tribunal de Justiça*. Rio de Janeiro/São Paulo: Renovar, 2010.

ASOCIACIÓN POR LOS DERECHOS CIVILES (ADC). El Sistema de Protección de Datos Personales en América Latina. Oportunidades y desafios para los derechos humanos. Buenos Aires, 2017, v. I. Disponível em: https://adcdigital.org.ar/portfolio/sistema-proteccion-datos-personales-latam/. Acesso em: 19 jul. 2018.

ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. *O que são dados públicos?* [Especial]. São Paulo, 2016. Disponível em: http://www.internetlab.org.br/pt/opiniao/o-que-sao-dados-publicos/. Acesso em: 20 jul. 2016.

ASSOCIAÇÃO INTERLAB DE PESQUISA EM DIREITO E TECNOLOGIA. Vigilância das comunicações pelo Estado brasileiro. São Paulo, 2015. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf. Acesso em: 03 jul. 2016.

ARENHART, Sérgio Cruz. *A tutela inibitória da vida privada.* São Paulo: Revista dos Tribunais, 2000.

BANSHO, A. Y. O. *Proteção de dados pessoais, privacidade, liberdade e autonomia do sujeito, no direito brasileiro.* Monografia (Graduação em Direito) – Universidade Federal do Paraná, 2010.

BASSO, Maristela. *Curso de Direito Internacional Privado*. 5. ed. São Paulo: Atlas, 2016.

BASSO, Maristela. *Da aplicação do Direito Estrangeiro pelo juiz nacional:* o Direito Internacional privado à luz da jurisprudência. São Paulo: Saraiva, 1988.

BASSO, Maristela. *O Direito Internacional da propriedade intelectual*. Porto Alegre: Livraria do Advogado, 2000.

BAUMAN, Zygmunt. *Vigilância líquida:* diálogos com David Lyon. Rio de Janeiro: Zahar, 2013 [versão Kindle].

BATIFFOL, Henri. Le pluralisme de méthodes en Droit Internacional Privé. *Recueil des Cours.* Paris: Librairie du Recueil Sirey, 1973, v. 139, n. II, pp. 75-148.

BATIFFOL, Henri. Les tendances doctrinales actuelles en droit international privé. *Recueil des Cours*. Paris: Librairie du Recueil Sirey, 1948, v. 72, pp. 1-66.

BOELE-WOELKI, Kathatina; KESSEDJIAN, Catherine (Eds.). Internet. Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique? *Kluwer Law International*. Haia/Londres/Boston, 1998.

BOOTH, Wayne C.; COLOMB, Gregory G.; WILLIAMS, Joseph M. *A arte da pesquisa*. 2. ed. Traduzido por Henrique A. Rego Monteiro. São Paulo: Martins Fontes, 2005.

BORRÁS RODRÍGUEZ, Alegría. Les ordres plurilégislatifs dans le droit international privé actuel. *Recueil des Cours*. Dordrecht/Boston/Lancaster: Martinus Nijhoff Publishers, 1994, v. 249, pp. 145-368.

BORGES, Roxana Cardoso Brasileiro. Direito à privacidade e lixo: abandono de coisa e irrenunciabilidade a direitos de personalidade. *Revista Fórum de Direito Civil – RFDC.* Belo Horizonte, ano 2, maio/ago. 2013, n. 3.

CABRAL FILHO, Adilson Vaz; COUTINHO, Guttemberg. Web 2.0: caminhos e desafios no desenvolvimento da internet. *In*: FRAGOSO, Suely; MALDONADO, Alberto Efenedy. *A internet na América Latina*. São Leopoldo, RS: Unisinos; Porto Alegre: Sulinas, 2009.

CAPELO DE SOUZA, Rabindranath Valentino Aleixo. *O direito geral de personalidade*. Coimbra: Coimbra Ed., 1995.

CASELLA, Paulo Borba; SANCHEZ, Rodrigo E. (Orgs.). *Cooperação judiciária internacional*. Rio de Janeiro: Renovar, 2002.

CASTRO, Luiz Fernando Matins. Proteção de dados pessoais – internacional e brasileiro. *Revista CEJ*. Brasília, out./dez. 2002, n. 19, p. 43.

CHINELLATO, Silmara Juny de Abreu. Tendências da responsabilidade civil no direito contemporâneo: reflexos no Código de 2002. *In*: DELGADO, Mário Luiz; ALVES, Jones Figueiredo (Orgs.). *Novo Código Civil:* questões controvertidas. São Paulo: Método, 2006, v. 5.

CONSULTORIA LEGISLATIVA DA CÂMARA DOS DEPUTADOS. *Privacidade e Internet.* Brasília, mar. 2000. Disponível em: http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/arquivos-pdf/pdf/001854.pdf. Acesso em: 05 jul. 2016.

COSTA, Mário Julio de Almeida. *Direito das Obrigações*. 12. ed. rev. e atual. Coimbra: lmedina, 2016.

DIAS, José de Aguiar. *Da responsabilidade civil*. 10. ed. Rio de Janeiro: Forense, 1995, v. 1.

DOTTI, René Ariel. A liberdade e o direito à intimidade. *Revista de Informação Legislativa.* Brasília, abr./jun. 1980a, n. 66, pp. 125-152.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação:* possibilidades e limites. São Paulo: Revista dos Tribunais, 1980b.

DOTTI, René Ariel. Tutela jurídica da privacidade. *In*: DIAS, Adahyl Lourenço *et al. Estudos em homenagem ao Professor Washington de Barros Monteiro*. São Paulo: Saraiva, 1982.

EHRHARDT JÚNIOR, Marcos; PEIXOTO, Erick Lucena Campos. Os novos paradigmas da responsabilidade civil na Internet. *In*: GODINHO, Adriano Marteleto *et al.* (Orgs.). *Temas de direito civil:* da constitucionalização à humanização. João Pessoa: Ed. da UFPB, 2015.

FARIAS, Cristiano; ROSENVALD, Nelson. *Curso de Direito Civil – Obrigações*. 11. ed. Salvador: Ed Jus Podivm, 2017, v. 2.

FERRER CORREIA, António. Principais interesses a considerar na resolução dos conflitos de leis. *In*: FERRER CORREIA, António. *Direito internacional privado – Estudos Jurídicos III*. Coimbra: Atlântida, 1970, pp. 84-92.

FERRER CORREIA, António. O método conflitual em direito internacional privado e as soluções alternativas. *Revista de Direito Comparado Luso-Brasileiro*. Rio de Janeiro, jul. 1982, n. 1, pp. 1-24.

FERRER CORREIA, António. *Temas de Direito Comercial e Direito Internacional Privado*. Coimbra: Almedina, 1989.

FREZZA FILHO, Ezio. O sigilo de dados e a proteção da intimidade em face do interesse público. *Revista Paradigma*. Ribeirão Preto, 2003, v. 12, n. 15.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 4. Ed. São Paulo: Atlas, 2002.

GODOY, Claudio Luiz Bueno. Responsabilidade Civil pelo Risco da Atividade e Nexo de Imputação da Obrigação de Indenizar: Reflexões para um Colóquio Brasil – Portugal. *In*: SIMÃO, José Fernando; ARAÚJO; Fernando (Orgs.). *Cadernos de Pós-Graduação em Direito:* estudos e documentos de trabalho. Comissão de Pós-Graduação da Faculdade de Direito da USP. São Paulo, 2011, n. 1, pp. 38-48.

GOLDENBERG, Mirian. *A arte de pesquisar.* Como fazer pesquisa qualitativa em Ciências Sociais. 8. ed. Rio de Janeiro: Record, 2004.

GOMES, Orlando. *Responsabilidade civil*. Texto revisado e atualizado por Edvaldo Brito. Rio de Janeiro: Forense, 2011.

GONÇALVES, Carlos Roberto. *Responsabilidade civil*. 15. ed. São Paulo: Saraiva, 2015.

GOODMAN, J. W. The pros and cons of online dispute resolution: na assessment of cyber-mediation websites. *Duke Law & Technology Review*. 2003. Disponível em: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1073&context=dltr. Acesso em: 15 dez. 2019.

GUERRA, Sidney. A internet e os desafios para o direito internacional. *Buscalegis*, 2009. Disponível em: http://biblioteca.versila.com/9347136. Acesso em: 30 jun. 2016.

HIRONAKA, Giselda Maria Fernandes Novaes. *Responsabilidade pressuposta*. Belo Horizonte: Del Rey, 2005.

JAEGER JR, Augusto. *Europeização do Direito Internacional Privado*. Curitiba: Juruá, 2012.

LEITÃO, Luís Manuel Teles de Menezes. *Direito das obrigações.* 8. ed. Coimbra: Almedina, 2009, v. I.

LEVI-STRAUSS, Claude. Raça e História. *In*: LEVI-STRAUSS, Claude. *Antropologia Estrutural II*. 4. ed. Rio de Janeiro: Tempo Brasileiro, 1993, cap. XVIII.

LIMA, Alvino. *Culpa e risco*. 2. ed. São Paulo: RT, 1999.

LINKE, W. R. *Uma análise da conjuntura da proteção de dados pessoais no Brasil à luz do caso Europa v. Facebook.* Florianópolis: Universidade Federal de Santa Catarina, 2015.

LOUREIRO, Francisco Eduardo. *Responsabilidade Civil e sua Repercussão nos Tribunais*. São Paulo: Saraiva, 2009 [Série GVlaw].

LYON, David. Surveillance, Snowden and Big Data: capacities, consequences, critique. *Big Data & Society,* Jul./Dez. 2014, pp. 1-13.

LYON, David; WOOD, David Murakami. Security, Surveillance and Sociological Analysis. *Canadian Review of Sociology,* 2012, v. 49, n. 4, pp. 317-328.

MAIA, Luciano Soares. A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. *In*: CONSELHO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM DIREITO. XVI Congresso Nacional do Conpedi. *Anais...* Florianópolis: Fundação Boiteux, 2007.

MALHEIROS, Pablo. *Responsabilidade por danos:* imputação e nexo de causalidade. Curitiba: Juruá, 2014.

MARANHÃO, Juliano Souza de Albuquerque; CAMPOS, Ricardo Resende. Proteção de Dados de Crédito na Lei Geral de Proteção de Dados. *IDP – Revista de Direito Público*. [S.l.], dez. 2019, v. 16, n. 90. ISSN 2236-1766. Disponível em: https://www.portalde periodicos.idp.edu.br/direitopublico/article/view/3739. Acesso em: 06 jan. 2020.

MARANHÃO, Juliano Souza de Albuquerque. Censura ao anonimato na internet?. Folha de São Paulo, São Paulo-SP, 08 nov. 2017. Disponível em: https://www1.folha.uol.com.br/ opiniao/2017/11/1933620-censura-ao-anonimato-na-internet.shtml?origin=uol Acesso em: 18 abr. 2020.

MARCHI, Eduardo C. Silveira Vita. *Guia de Metodologia Jurídica.* Teses monografias e artigos. 2. ed. São Paulo: Saraiva, 2009.

MARQUES DOS SANTOS, António. Direito Internacional Privado. *In*: MARQUES, Claudia Lima; ARAÚJO, Nádia de. *O novo direito internacional:* estudos em homenagem a Erik Jayme. Rio de Janeiro: Renovar, 2005, pp. 29-55.

MEYER, David. Looks like data will keep flowing from the EU to the U.S. after all. *Fortune.com*. Disponível em: http://fortune.com/2016/02/02/looks-like-data-will-keep-flowing-from-the-eu-to-the-u-s-after-all/. Acesso em: 05 jul. 2016.

MILLER, Arthur. *Assault on privacy*. Ann Arbor: University of Michigan, 1971.

MINISTÉRIO DA JUSTIÇA. *Homologação de Sentenças Estrangeiras em matéria civil.* Disponível em: https://www.justica.gov.br/sua-protecao/cooperacao-internacional/ cooperacao-juridica-internacional-em-materia-civil/orientacao-por-diligencia/ homologacao-de-sentencas-estrangeiras Acesso em: 29/12/2019.

MONACO, Gustavo Ferraz de Campos; RODAS, João Grandino. *A Conferência da Haia de Direito Internacional Privado:* a Participação do Brasil. Brasília: Funag, 2007.

MONTEIRO, Washington de Barros. *Curso de Direito Civil*. 13. ed. São Paulo: Saraiva, 1977, v. 4.

MORATO, Antonio Carlos. Quadro geral dos direitos da personalidade. *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo, jan./dez. 2011, v. 106/107, pp. 121-158.

MOTA PINTO, Paulo. O direito à reserva sobre a intimidade da vida privada. *Boletim da Faculdade de Direito.* Coimbra, 1993, v. 69.

MOURA RAMOS, Rui Manuel Gens de. *A Carta dos Direitos Fundamentais da União Europeia e a Proteccção dos Direitos Fundamentais*. Coimbra: Coimbra, 2000.

MOURA RAMOS, Rui Manuel Gens de. *Direito Internacional Privado e Constituição:* introdução a uma análise das suas relações. Coimbra: Coimbra, 1994.

ORWELL, George. *1984*. São Paulo: Companhia Editora Nacional, 1998.

PARKER, B. Clifton. New Stanford research finds computers are better judges of personality than friends and family. *Stanford News*. Disponível em: http://news.stanford.edu/2015/01/12/personality-computer-knows-011215/ Acesso em: 03 jul. 2016.

PELA, Juliana Krueger. "Inadimplemento Eficiente" (Efficient Breach) nos Contratos Empresariais. *Cadernos do Programa de Pós-Graduação em Direito – PPGDir./UFRGS*, 2016, v. 11, n. 2. Disponível em: https://seer.ufrgs.br/index.php/ppgdir/article/view/69111/39932. Acesso em: 06 jan. 2020.

PARKER, B. Clifton. New Stanford research finds computers are better judges of personality than friends and family. *Stanford News*. Disponível em: http://news.stanford.edu/2015/01/12/personality-computer-knows-011215/. Acesso em: 03 jul. 2016.

PELA, Juliana Krueger. Rembrandt e o Direito Privado. *Revista da Faculdade de Direito da Universidade de São Paulo*, jan./dez. 2015, v. 110, pp. 319-327. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/115495/113077. Acesso em: 06 jan. 2020.

PEREIRA, Alexandre Libório Dias. A Jurisdição na Internet segundo o Regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas). *Boletim da Faculdade de Direito*. Coimbra, 2001, v. LXXVII, pp. 633-687.

PEREIRA, Alexandre Libório Dias. O tribunal competente em casos da Internet segundo o acórdão "eDate Advertising" do Tribunal de Justiça da União Europeia. *Revista Jurídica Portucalense Law Journal*. Porto, 2014, n.º 16.

PEREIRA, Caio Mário da Silva (revisto e atualizado por Tânia da Silva Pereira.). *Instituições de direito civil*: 17. ed. Rio de Janeiro: Forense, 2.009, v. V.

PINHEIRO, Luís de Lima. Um direito internacional privado para o século XXI. *Suplemento da Revista da Faculdade de Direito da Universidade de Lisboa*. Lisboa, 2001.

PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado:* parte geral. Tomo II: Bens e fatos jurídicos. São Paulo: Revista dos Tribunais, 2012.

PONTES DE MIRANDA, Francisco Cavalcanti. *Tratado de Direito Privado*. Parte Especial. Tomos XXII - XXX. Atualizado por Vilson Rodrigues Alves em conformidade com o Código Civil de 2002. Campinas, SP: Bookseller, 2003.

PRINO, C.S.A. *O enquadramento legal do Facebook*. Dissertação (Mestrado em Ciências Sociais e Humanas) – Universidade Nova de Lisboa. Lisboa, 2012.

RECHSTEINER, Beat Walter. *Direito Internacional Privado* – teoria e prática. 15. ed. São Paulo: Saraiva, 2012.

RODAS, João Grandino. *Direito Internacional Privado brasileiro*. São Paulo: RT, 1993.

RODAS, João Grandino. Elementos de conexão do Direito Internacional Privado brasileiro relativamente às obrigações contratuais. *In*: RODAS, João Grandino (Coord.) *Contratos Internacionais*. 3. ed. São Paulo: RT, 2002.

RODOTÀ, Stefano. *A privacidade na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Silvio. *Direito Civil*. São Paulo: Saraiva, 1975, v. 4.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada.* Belo Horizonte: Del Rey, 1998.

SARMENTO E CASTRO, Catarina. *Direito da informática, privacidade e dados pessoais.* Coimbra: Almedina, 2005.

SCHWARTZ, Paul. The EU-U.S. privacy collision: a turn to institutions and procedures. (Privacy Self-Management and the Consent Dilemma). *Harvard Law Review*, 2013, v. 126, iss 7.

SCOTT, Mark. U.S. and Europe in "Safe Harbor" data deal, but legal fight may await. *The New York Times.* Disponível em: http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=0. Acesso em: 20 maio 2016.

SERPA LOPES, Miguel Maria de. *Curso de direito civil:* fontes acontratuais das obrigações. Responsabilidade Civil. 4. ed. Rio de Janeiro: Freitas Bastos, 1995, v. V.

SLOAN, Robert H.; WARNER, Richard. The Harm in Merely Knowing: privacy, complicity, surveillance and the Self. *Journal of Internet law* [1094-2904], 2015, v. 19.

STOCO, Rui. *Tratado de responsabilidade civil*. 7. ed. São Paulo: Ed. RT, 2007.

SWINHOE, Dan. Os 8 maiores vazamentos de dados de 2018. Hacks e roubos de dados custaram um total de quase US$ 280 milhões para empresas. *Computerworld*. Disponível em: https://computerworld.com.br/2018/10/31/os-8-maiores-vazamentos-de-dados-de-2018/. Acesso em: 20 out. 2019.

SYMEONIDES, Symeon C. *American Private International Law.* Alphen aan den Rijn: Kluwer Law International, 2008.

SYMEONIDES, Symeon C.; PERDUE, Wendy Collins; MEHREN, Arthur T. von. *Conflict of laws:* American, comparative, international. Cases and materials. St. Paul, Minn., 1998.

TAKLE, Marianne. The Treaty of Lisbon and the European Border Control Regime. *In*: *Journal of Contemporary European Research*, 2012, v. 8.

TARTUCE, Flávio. *Direito civil:* Direito das Obrigações e Responsabilidade Civil. 11. ed. São Paulo: Grupo GEN, 2015, v. 2.

VICENTE, Dário Moura. A autonomia privada e os seus diferentes significados à luz do Direito Comparado. *Revista de Direito Civil Contemporâneo*. São Paulo: Revista dos Tribunais, ano 3, jul./set. 2016, v. 8, pp. 275-302.

VICENTE, Dário Moura. *Da responsabilidade pré-contratual em direito internacional privado*. Coimbra, 2001.

VEIGA, Luiz Adolfo Olsen da; ROBER, Aires José. Dados e informação na internet: é legítimo o uso de robôs para formação de base de dados de clientes? *In*: ROVER, Aires José (Org.). *Direito e Informática.* São Paulo: Manole, 2004. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/luizvaires-livro_manole_artigo_robos.pdf. Acesso em: 01 jul. 2016.

VENOSA, Sílvio de Salvo. *Direito Civil:* responsabilidade civil. 3. ed. São Paulo: Atlas, 2003.

WEINTRAUB, Russel J. *Commentary on the conflict of laws.* 4. ed. New York, 2001.

WENGLER, Wilhelm. L'Évolution moderne du droit international privé et la previsibilité du droit applicable. *Revue Critique de Droit International Privé*. Paris, 1990, v. 79, n. 4, pp. 657-681.

WESTIN, Alan. *Privacy and Freedom.* Nova Iorque: Atheneum, 1967.

ZANETTI, Cristiano de Souza. A relatividade dos efeitos contratuais e a autonomia da pessoa jurídica. *Revista dos Tribunais*. São Paulo, mar. 2011, v. 100, n. 905, pp. 119-135.