

UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO DE CIÊNCIAS JURÍDICAS  
DEPARTAMENTO DE DIREITO  
CURSO DE DIREITO

Israel Weingartner

**Os Impactos da Aplicação (Extra)territorial do Regulamento Geral de Proteção de  
Dados da União Europeia para as Empresas de Tecnologia da Informação de  
Florianópolis - SC**

Florianópolis

2021

Israel Weingartner

**Os Impactos da Aplicação (Extra)territorial do Regulamento Geral de Proteção de  
Dados da União Europeia para as Empresas de Tecnologia da Informação de  
Florianópolis - SC**

Trabalho Conclusão do Curso de Graduação em Direito  
do Centro de Ciências Jurídicas da Universidade Federal  
de Santa Catarina como requisito para a obtenção do  
título de Bacharel em Direito.  
Orientador: Profa., Dra. Aline Beltrame de Moura.

Florianópolis

2021

Ficha de identificação da obra elaborada pelo autor,  
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Weingartner, Israel

Os impactos da aplicação (extra)territorial do GPDR para as empresas de Tecnologia da Informação e Comunicação de Florianópolis-SC / Israel Weingartner ; orientador, Aline Beltramde de Moura , 2021.

p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2021.

Inclui referências.

1. Direito. 2. Proteção de Dados Pessoais. 3. GDPR. 4. União Europeia . 5. Aplicação extraterritorial. I. , Aline Beltramde de Moura. II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Título.

Israel Weingartner

**Os Impactos da Aplicação (Extra)territorial do Regulamento Geral de Proteção de  
Dados da União Europeia para as Empresas de Tecnologia da Informação de  
Florianópolis - SC**

Este Trabalho Conclusão de Curso foi julgado adequado para obtenção do Título de “Bacharel em Direito” e aprovado em sua forma final pelo Curso de Direito

Florianópolis, 12 de maio de 2021.

---

Prof. Luiz Henrique Cademartori, Dr.  
Coordenador do Curso

**Banca Examinadora:**

---

Profa. Aline Beltrame de Moura, Dra.  
Orientadora  
Universidade Federal de Santa Catarina

---

Prof. Matheus Passos Silva, Msc.  
Universidade de Lisboa

---

Letícia Mulinari Gnoatton  
Universidade Federal de Santa Catarina

---

Carla Lerin  
Universidade Federal de Santa Catarina

## AGRADECIMENTOS

O início da produção deste trabalho coincidiu com um dos momentos mais difíceis que a humanidade já enfrentou na sua história recente, a pandemia de Covid-19. Neste último ano, no qual o distanciamento social foi a regra, percebemos que, ao fim e ao cabo, o que realmente importa na vida são as relações que construímos com as pessoas que nos querem bem e que nos ajudam a evoluir. Não posso deixar de agradecer, portanto, a todas essas pessoas que, ainda que distantes, contribuíram para eu chegasse até aqui.

Primeiramente, aos meus pais, Saulo e Marciana, por sempre acreditarem nos meus sonhos e por nunca medirem esforços para me auxiliar a seguir em frente.

As minhas irmãs, Sarah e Johanna, e aos meus cunhados, Maicon e Marcos, por todo apoio que sempre me deram e por me ensinarem a ver a vida com leveza e alegria.

Aos meus queridos sobrinhos, Davi e Pedro, por me mostrarem que há sempre uma parte de criança em nós, que nunca se esvai.

A minha amada namorada, amiga e companheira, Thais Carolina da Cunha, por sonhar junto comigo e ser meu porto seguro. Não cabem nas margens desta página todo o amor e gratidão que sinto por você.

Aos queridos amigos Paulo Vitor Tambosi e Jaqueline Marlene Cardoso, que muito me auxiliaram na construção deste trabalho e por quem guardo grande carinho e admiração.

A todas as pessoas incríveis com quem tive a alegria de compartilhar todos esses anos de graduação na UFSC, em especial, aos amigos Vinicius, Anderson, Fernando, Izabelly, Leandro B., Leandro C., Bernardo, Marco Antônio, Arthur, Ayra, Juliana O., Henrique C., Henrique S., João e Tiago.

Ao time GEARB-UFSC e, em especial, aos queridos amigos Juliana Blanco, Ana, Tobias, Guilherme e Hamilton, com quem compartilhei uma das melhores experiências que tive na Universidade. Não posso deixar de agradecer também aos coaches do time, prof. Caetano, dr. Lio Bocorny, Bettina e Gustavo Becker.

A minha querida orientadora, professora Aline Beltrame de Moura, por todo o apoio e incentivo que me deu, e por todas as oportunidades que me proporcionou durante a graduação. Seu comprometimento e amor pela docência são exemplo a todos que, assim como eu, tiveram a honra de poder aprender com você.

Ao Instituto Federal de Santa Catarina e à Universidade Federal de Santa Catarina, instituições que, com ensino de altíssima qualidade, transformaram a minha vida.

*Porque a vida, a vida, a vida,  
a vida só é possível  
reinventada.*

(Cecília Meireles, *Vaga Música*, 1942)

## RESUMO

Diante dos desafios que as novas tecnologias impõem para a proteção de dados pessoais, a União Europeia aprovou em 2016 o seu Regulamento Geral de Proteção de Dados (GDPR), cujo escopo territorial permite que até mesmo empresas sem nenhuma presença física nos países do bloco possam se enquadrar dentro do seu escopo de aplicação. Considerando que Florianópolis é, atualmente, um polo de empresas de Tecnologia da Informação e Comunicação (TIC), surge a problemática deste trabalho, que consiste em investigar se a aplicação extraterritorial do GDPR pode alcançar tais empresas e, caso positivo, quais os principais impactos diretos decorrentes desse fenômeno. A hipótese desta pesquisa é de que o GDPR pode ser, de fato, diretamente aplicável a algumas empresas de TIC de Florianópolis-SC, e que tal aplicação extraterritorial já causou impactos diretos para o setor. Com base em abordagem metodológica dedutiva, o presente trabalho utilizou as técnicas de análise bibliográfica bem como a produção de pesquisa empírica realizada com empresas que atuam no setor analisado para chegar ao seu objetivo. Primeiramente, aborda-se a formação histórica e as principais normas da União Europeia bem como a evolução do direito à proteção de dados nesse contexto. Em seguida, analisa-se as bases teóricas que justificam a aplicação extraterritorial do GDPR e a discussão sobre sua legitimidade. Por fim, avalia-se os resultados da pesquisa empírica para verificar se, de fato, o GDPR pode ser aplicável às empresas do setor e, caso positivo, se essa aplicação impacta na perspectiva de custos das organizações. Constatou-se que, devido ao longo histórico de formulação de normas sobre proteção de dados pessoais, a União Europeia é tida como modelo internacional para a temática. Ademais, verificou-se que a maioria da doutrina considera legítima a aplicação extraterritorial do GDPR. Por fim, concluiu-se que o GDPR pode ser aplicável a algumas empresas de TIC de Florianópolis e que tal aplicação extraterritorial já importou em aumento de custos para essas instituições.

**Palavras-chave:** Proteção de Dados Pessoais. União Europeia. GDPR. Aplicação extraterritorial.

## **ABSTRACT**

In light of the challenges imposed by new technologies for the protection of personal data, in 2016 the European Union approved its General Data Protection Regulation (GDPR), whose territorial scope allows even companies with no physical presence in the bloc's countries to fall within its scope of application. Having regard the importance of Florianópolis-SC as a hub of information technology (IT) companies, the problem of this research consists in knowing whether the GDPR can be applicable to such companies and, if so, what are the main direct impacts arising from this phenomenon. The research hypothesis is that the GDPR can indeed be directly applicable to some IT companies based in Florianópolis-SC, which has already brought impacts to this sector in terms of costs. The study has been developed under deductive reasoning, with the use of bibliographic analysis as well as empirical research conducted with IT companies. Firstly, the historical development and the main rules of the European Union are addressed, along with the evolution of Personal Data Protection in the European Law. Subsequently, the theoretical bases of the GDPR's extraterritorial reach are approached, followed by a discussion about its legitimacy. In the sequence, the results of the empirical research are evaluated in order to verify whether the GDPR can be, in fact, applicable to IT companies based in Florianópolis. It was found that, due to its tradition on the personal data protection field, the European Union is currently considered a model for other countries on the subject. Moreover, the analysis of the scholars' opinion led to the conclusion that the extraterritorial applicability of the GDPR is legitimate. Finally, this paper concluded that the GDPR can be applicable to some IT companies based in Florianópolis and such extraterritorial reach has already led to increased costs for such institutions.

**Keywords:** Data Protection. European Union. GDPR. Extraterritorial Applicability

## LISTA DE FIGURAS

|                                                                                          |     |
|------------------------------------------------------------------------------------------|-----|
| Figura 1 –Gráfico das respostas compiladas da pergunta número 3 do questionário.....     | 108 |
| Figura 2 – Evolução das empresas do setor de tecnologia catarinense.....                 | 109 |
| Figura 3 – Gráfico das respostas compiladas da pergunta número 9 do questionário.....    | 110 |
| Figura 4 – Gráfico das respostas compiladas da pergunta número 8 do questionário.....    | 111 |
| Figura 5 – Gráfico das respostas compiladas da pergunta número 10 do questionário.....   | 112 |
| Figura 6 – Gráfico das respostas compiladas da pergunta número 5 do questionário.....    | 113 |
| Figura 7 – Gráfico das respostas compiladas da pergunta número 11 do questionário.....   | 114 |
| Figura 8 – Gráfico das respostas compiladas da pergunta número 13.1 do questionário..... | 116 |
| Figura 9 – Gráfico das respostas compiladas da pergunta número 14.1 do questionário..... | 117 |
| Figura 10 – Gráfico das respostas compiladas da pergunta número 15 do questionário.....  | 118 |
| Figura 11 – Gráfico das respostas compiladas da pergunta número 16 do questionário.....  | 118 |
| Figura 12 – Gráfico dos resultados compilados da pesquisa Serasa Experian.....           | 120 |
| Figura 13 – Proteção de dados ao redor do mundo.....                                     | 121 |

## LISTA DE ABREVIATURAS E SIGLAS

ACATE – Associação Catarinense de Tecnologia  
ANPD – Autoridade Nacional de Proteção de Dados  
CDI – Comissão de Direito Internacional da Organização das Nações Unidas  
CECA – Comunidade Econômica do Carvão e do Aço  
CEE – Comunidade Econômica Europeia  
CEPD – Comitê Europeu de Proteção de Dados  
CNIL – *Commission Nationale de l'Informatique et des Libertés*  
DIP – Direito Internacional Público  
EU – União Europeia  
EUA – Estados Unidos da América  
EURATOM – Comunidade Europeia de Energia Atômica  
FTAIA – *Foreign Trade Antitrust Improvements Act*  
GDPR – Regulamento Geral de Proteção de Dados  
IP – *Internet Protocol Address*  
LGPD – Lei Geral de Proteção de Dados  
OCDE – Organização para a Cooperação e Desenvolvimento Econômico  
ONU – Organização das Nações Unidas  
SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas  
TFUE – Tratado de Funcionamento da União Europeia  
TIC – Tecnologias da Informação e Comunicação  
TJUE – Tribunal de Justiça da União Europeia  
TUE – Tratado da União Europeia

## SUMÁRIO

|                                                                                                          |           |
|----------------------------------------------------------------------------------------------------------|-----------|
| <b>1 INTRODUÇÃO .....</b>                                                                                | <b>15</b> |
| <b>2 A UNIÃO EUROPEIA E O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS.....</b>               | <b>19</b> |
| 2.1. O processo de formação da União Europeia .....                                                      | 19        |
| 2.1.1 As instituições da União Europeia.....                                                             | 24        |
| 2.2 As normas da União Europeia .....                                                                    | 26        |
| 2.3. A evolução do Direito à Proteção de Dados Pessoais na União Europeia .....                          | 30        |
| 2.3.1 Relação entre Direito à Privacidade e Proteção de dados .....                                      | 30        |
| 2.3.2 As primeiras normas sobre proteção de dados pessoais no âmbito europeu .....                       | 32        |
| 2.3.3 A Diretiva 95/46/CE e o direito à proteção de dados pessoais.....                                  | 35        |
| 2.3.4 A caminho do GDPR: a proteção de dados pessoais nas normas primárias da União Europeia.....        | 38        |
| 2.3.5 A construção legislativa do GDPR.....                                                              | 41        |
| <b>3 O ÂMBITO DE APLICAÇÃO EXTRATERRITORIAL DO GDPR.....</b>                                             | <b>45</b> |
| 3.1 Conceitos essenciais do GDPR .....                                                                   | 46        |
| 3.1.1 Dados pessoais.....                                                                                | 46        |
| 3.1.2 O processo de tratamento de dados pessoais .....                                                   | 50        |
| 3.1.3 Controladores e Processadores de dados pessoais segundo o GDPR.....                                | 53        |
| 3.2 Fundamentos teóricos da aplicação extraterritorial do GDPR .....                                     | 55        |
| 3.2.1 Jurisdição .....                                                                                   | 56        |
| 3.2.2 Jurisdição Extraterritorial: perspectiva histórica e definição .....                               | 59        |
| 3.2.3 O caso <i>Lotus</i> e a teoria dos efeitos .....                                                   | 62        |
| 3.3 Análise do escopo territorial e extraterritorial do GDPR .....                                       | 66        |
| 3.3.1 A delimitação do critério do estabelecimento na Diretiva 95/46/CE e na jurisprudência do TJUE..... | 66        |
| 3.3.2 A aplicação extraterritorial do GDPR por meio do critério do estabelecimento (art. 3.1).....       | 71        |

|                                                                                                                                  |            |
|----------------------------------------------------------------------------------------------------------------------------------|------------|
| 3.3.3 O <i>destination approach</i> e a aplicação do GDPR para as empresas estrangeiras (art.3.2).....                           | 75         |
| 3.3.5 A (i)legitimidade da aplicação extraterritorial do GDPR.....                                                               | 82         |
| 3.3.6 A ausência de <i>enforcemnet</i> enquanto limitador da aplicação extraterritorial.....                                     | 87         |
| 3.3.7 Outros impactos extraterritoriais do GDPR: a transferência internacional de dados e o Efeito Bruxelas .....                | 92         |
| <b>4 OS IMPACTOS DA APLICAÇÃO EXTRATERRITORIAL DO GDPR PARA AS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO EM FLORIANÓPOLIS - SC...</b> | <b>99</b>  |
| 4.1 Considerações sobre as hipóteses de aplicação do GDPR às empresas de TIC de Florianópolis.....                               | 100        |
| 4.2 Análise prática da aplicação extraterritorial do GDPR: pesquisa empírica.....                                                | 101        |
| 4.2.1 Metodologia.....                                                                                                           | 102        |
| 4.2.2 Resultados.....                                                                                                            | 103        |
| 4.2.2.1. <i>Perfil das empresas</i> .....                                                                                        | 103        |
| 4.2.2.2. <i>A realização de tratamento de dados pessoais como atividade das empresas entrevistadas</i> .....                     | 105        |
| 4.2.2.3 <i>Presença das empresas na União Europeia</i> .....                                                                     | 106        |
| 4.2.2.4 <i>Conhecimento das empresas sobre o GDPR</i> .....                                                                      | 107        |
| 4.2.2.5 <i>Impactos do GDPR para as empresas a partir da perspectiva do art. 3.2</i> .....                                       | 108        |
| 4.2.2.6 <i>Impactos diretos para as empresas pela perspectiva de incremento de custos</i> .....                                  | 110        |
| 4.2.2.7 <i>Percepção das empresas sobre a LGPD do Brasil</i> .....                                                               | 113        |
| 4.2.3. Conclusões parciais sobre a pesquisa empírica.....                                                                        | 119        |
| <b>5 CONCLUSÃO.....</b>                                                                                                          | <b>120</b> |
| <b>REFERÊNCIAS .....</b>                                                                                                         | <b>123</b> |

## 1 INTRODUÇÃO

Não é de hoje que dados pessoais de indivíduos são coletados e sistematizados para gerar informações, que podem ser úteis a empresas, governos e outras instituições. O primeiro censo geral do Brasil, por exemplo, aconteceu em 1872, ainda no período imperial.<sup>1</sup> Questionários, formulários e cadastros são há muito utilizados em nossa sociedade para identificar atributos pessoais dos indivíduos e são empregados para diferentes finalidades. O que mudou, portanto, nos últimos anos para que algo que antes poderia ter sido considerado como banal viesse a ser compreendido como o “novo petróleo”, fazendo surgir a chamada economia de dados?<sup>2</sup>

A resposta para esse questionamento remonta à concepção de sociedade da informação, termo utilizado para caracterizar o novo estágio da sociedade em que a informação se tornou o elemento estruturante da economia e das próprias interações sociais.<sup>3</sup> Esse novo modelo de conformação da sociedade, que Milton Santos chamou de meio técnico-científico-informacional, teve seu despertar a partir da década de 80 com a rápida evolução das Tecnologias de Informação e Comunicação (TIC's).<sup>4</sup>

O surgimento da internet como o novo paradigma de comunicação, a evolução da capacidade de processamento dos microcomputadores, a utilização de inteligência artificial acoplada a equipamentos eletrônicos, dentre outros exemplos, ao mesmo tempo em que facilitaram a execução de inúmeras atividades cotidianas também tornaram os dados pessoais dos indivíduos cada vez mais expostos às empresas, governos e outros agentes econômicos. Nesse sentido, as novas tecnologias de *Big Data*, que permitem a estruturação e análise de um volume gigantesco de dados,<sup>5</sup> tornaram possível a identificação de características, preferências, localização e gostos singulares de cada pessoa no intuito de influenciá-las em seus padrões de consumo, ou até mesmo opiniões políticas, através das publicidades direcionadas.<sup>6</sup>

---

<sup>1</sup> IBGE. Memória IBGE: Censos Demográficos. Disponível em: <<https://memoria.ibge.gov.br/historia-do-ibge/historico-dos-censos/censos-demograficos.html>>. Acesso em: 10/04/2021.

<sup>2</sup> A frase “*Data is the new oil*” (dados são o novo petróleo, em tradução livre) é atribuída ao matemático inglês Clive Humby.

<sup>3</sup> BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: as funções e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

<sup>4</sup> SANTOS, Milton. **A Natureza do Espaço: Técnica e Tempo, Razão e Emoção**. 4. ed. São Paulo: Editora da Universidade de São Paulo, 2006.

<sup>5</sup> HOLMES, Dawn E. **Big Data: a very short introduction**. 1ª ed. Oxford: Oxford University Press, 2017.

<sup>6</sup> BIONI, Bruno Ricardo. Op. Cit. pág. 39.

Dentro da lógica da sociedade da informação, por conseguinte, os dados pessoais tornaram-se valiosos ativos econômicos.<sup>7</sup> Entretanto, diversos episódios de utilização indevida e vazamentos mostraram que a exploração dessa “economia de dados” sem os devidos regramentos pode acarretar graves danos para a esfera dos direitos da personalidade dos indivíduos.

Sensível à evolução tecnológica e aos desafios dela decorrentes, a União Europeia (UE) desenvolveu, desde o início da década de 90, um conjunto de normas com o objetivo de assegurar um nível elevado de proteção dos dados pessoais dos indivíduos, mas também buscando eliminar os obstáculos à circulação desses “ativos” entre os seus Estados-membros. Com estreita relação com o direito à privacidade e à autodeterminação informativa,<sup>8</sup> o direito à proteção de dados pessoais no âmbito da UE teve sua última normatização feita pelo Regulamento Geral de Proteção de Dados (GDPR, sigla em inglês), que foi aprovado em 2016 e entrou em vigor em 2018.<sup>9</sup>

Apesar de não ser a primeira legislação sobre o tema no âmbito da UE, o GDPR inovou ao consagrar expressamente em seu art. 3º a possibilidade de que empresas sem qualquer presença física dentro dos países do bloco pudessem ser também enquadradas em seu escopo de aplicação territorial. A justificativa estaria no fato de que no ambiente virtual não existem fronteiras físicas e, portanto, a proteção de dados dos indivíduos, que estão na EU, só seria efetiva caso o GDPR também pudesse alcançar as empresas estrangeiras que direcionam suas atividades para o bloco.

Esse fenômeno fez com que diversas empresas ao redor do mundo, principalmente aquelas que atuam no setor de TIC, voltassem suas atenções para o Velho Continente. Isso porque, dentre outras sanções, o GDPR prescreve vultosas multas – que podem chegar a 4% do volume de negócios anual a nível mundial – para as empresas que estejam em desconformidade com seus dispositivos.

---

<sup>7</sup> THE ECONOMIST. The world’s most valuable resource is no longer oil, but data. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10/04/2021.

<sup>8</sup> SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. Tratado de proteção de dados pessoais. 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7.

<sup>9</sup> UNIÃO EUROPEIA. Regulamento nº 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. Acesso em 10 de abril de 2020.

Além da possibilidade da aplicação direta dos dispositivos do GDPR para empresas de fora da UE, o Regulamento também acarretou em impactos indiretos aos demais países do mundo. O mais latente deles diz respeito ao regime de transferência internacional de dados pessoais, que estabeleceu rígidos regramentos para o compartilhamento de dados provenientes dos Estados que compõem o bloco europeu. Dessa forma, considerando a importância econômica e social da UE, diversos países foram influenciados a estabelecer legislações similares para se adequarem aos mesmos padrões do GDPR. Foi o que aconteceu com o Brasil que, em 2018, aprovou a sua Lei Geral de Proteção de Dados, cujos princípios e normas tem clara inspiração no regulamento europeu.<sup>10</sup>

Nesse contexto, o município de Florianópolis, capital do estado de Santa Catarina, tem ganhado notoriedade pela acelerada expansão do seu setor de Tecnologia. Estima-se que, anualmente, o setor movimente cerca de 9 bilhões de reais e empregue mais de 30 mil pessoas na região metropolitana da capital, sendo, portanto, importante engrenagem da economia local.<sup>11</sup>

Dada a importância de Florianópolis como um polo de tecnologia, inclusive com a presença de empresas com atuação internacional,<sup>12</sup> surge o questionamento sobre a possibilidade de o GDPR ser diretamente aplicável a algumas empresas do município, que possam eventualmente se enquadrar no escopo extraterritorial do Regulamento – o que constitui, portanto, o problema desta pesquisa. É a partir dessa indagação que nasce a proposta do presente trabalho, cujo objetivo geral é identificar a existência ou não de impactos diretos da aplicação extraterritorial do GDPR para as empresas de TIC de Florianópolis - SC. A hipótese básica é de que algumas dessas empresas se encontram, de fato, dentro do escopo de aplicação do Regulamento, e que tal fenômeno já implicou em impactos diretos para tais organizações.

Para chegar ao objetivo almejado, a presente monografia foi estruturada em três capítulos. O primeiro deles abordará a formação histórica da União Europeia e o surgimento do direito à proteção de dados no âmbito do bloco. Esse primeiro capítulo servirá para ilustrar qual

---

<sup>10</sup> MOURA, Aline Beltrame de. GNOATTON, Letícia Mulinari; MOURA, Aline Beltrame de. **Os Desafios Da Aplicação Extraterritorial Do Regulamento Geral De Proteção De Dados Pessoais Da União Europeia**. In: GHILARDI, Dóris; SASS, Liz Beatriz (coords.) Temas Atuais De Direito Privado E Sociedade Da Informação: O Direito Na Era Digital. 1ª ed. Florianópolis: Habitus, 2020.

<sup>11</sup> ACATE. **Tech Report 2020**. Disponível em: <<https://www.techreportsc.com/>> Acesso em: 24/03/2021. pág. 23.

<sup>12</sup> A título de mera ilustração, a empresa Neoway, que tem sede em Florianópolis, é tida atualmente como a maior empresa da América Latina em serviços de *Big Data Analytics*.

foi o caminho trilhado pela União Europeia para concretizar a atual sistemática de proteção de dados, que é paradigma para os demais países do mundo.

No segundo capítulo será discutido o arcabouço teórico que fundamenta a aplicação extraterritorial do GDPR, bem como as discussões jurisprudenciais e doutrinárias que circundam o tema. Com tal propósito, serão analisados alguns aspectos fundamentais do escopo material do Regulamento, como o próprio conceito de dados pessoais e tratamento de dados, no intuito de instrumentalizar o leitor com relação aos demais pontos do trabalho.

Por fim, no último capítulo serão apresentados e discutidos os resultados de uma pesquisa empírica realizada com algumas empresas de TIC sediadas no município de Florianópolis. A pesquisa consistiu na aplicação de um questionário sobre os impactos percebidos pelos empresários quanto à aplicação extraterritorial do GDPR. O intuito desse estudo empírico é verificar a hipótese básica deste trabalho descrita anteriormente.

Este trabalho adota abordagem de método dedutivo, implementado por meio da técnica de análise bibliográfica de doutrina e jurisprudência e por meio da técnica de aplicação de questionários e análise de dados.<sup>13</sup>

Ressalta-se que as obras estrangeiras referenciadas ao longo desta pesquisa foram livremente traduzidas para a Língua Portuguesa. Adotam-se, ainda, as normas atualizadas da Associação Brasileira de Normas Técnicas (ABNT), ressalvada a utilização do modelo numérico de citação em conjunto com notas explicativas.

---

<sup>13</sup> OLIVEIRA, Olga Maria Boschi Aguiar de. **Monografia jurídica: orientações metodológicas para o trabalho de conclusão de curso**. 3ª ed. Porto Alegre: Síntese, 2003. Pág. 31.

## 2 A UNIÃO EUROPEIA E O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

No intuito de melhor compreender e instrumentalizar o leitor quanto ao sistema em que o GDPR está inserido, faz-se necessário, preliminarmente, tecer algumas considerações acerca da própria formação da União Europeia, suas principais normas e sua influência na construção do direito à proteção de dados pessoais. Nesse sentido, a primeira parte deste capítulo será dedicada à análise do contexto histórico de desenvolvimento da União Europeia e do seu direito supranacional. Na segunda parte, será abordado o desenrolar da concepção de direito à proteção de dados no contexto europeu, desde os seus primórdios até a redação final do GDPR.

### 2.1. O PROCESSO DE FORMAÇÃO DA UNIÃO EUROPEIA

Para entender o papel da UE como um atual regulador global no campo da proteção de dados pessoais, há que se investigar, primeiramente, como se desenvolveu a complexa e sofisticada estrutura desta organização.<sup>14</sup> Não há como entender a força normativa do GDPR e seus impactos para o restante do mundo sem antes compreender sua própria fonte, a saber, o Direito Europeu. Nesse sentido, nos parágrafos que se seguirão serão abordados os principais eventos e acordos que tornaram a UE a instituição que conhecemos hoje.

Desde a declaração de Robert Schuman, ministro de negócios estrangeiros da França, propondo a criação da Comunidade Europeia do Carvão e do Aço (CECA), em 1950, até o Tratado de Lisboa de 2007 diversas foram as modificações implementadas para construir a atual estrutura organizacional da União Europeia.<sup>15</sup> Conforme ressalta Costa,<sup>16</sup> após a Segunda Guerra Mundial e diante dos seus nefastos efeitos para a economia e a sociedade europeia, surgiu entre alguns Estados do Velho Continente a intenção de criar mecanismos para evitar novos conflitos. Dentro dessa perspectiva, o tratado de criação da CECA<sup>17</sup> ganhou importância

---

<sup>14</sup> BRADFORD, Anu. **The Brussels Effect: How the European Union Rules the World**. Nova Iorque: Oxford University Press, 2020.

<sup>15</sup> UNIÃO EUROPEIA. **A declaração de Schuman**. Disponível em: <[https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration\\_pt](https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_pt)>. Acesso em 24/03/2020.

<sup>16</sup> COSTA, Olivier. **A União Europeia e sua política exterior (história, instituições e processo de tomada de decisão)**. Brasília: FUNAG, 2017. Disponível em <[http://funag.gov.br/biblioteca/download/1189-Uniao\\_europeia\\_e\\_sua\\_politica\\_exterior.pdf](http://funag.gov.br/biblioteca/download/1189-Uniao_europeia_e_sua_politica_exterior.pdf)>. Acesso em: 24/03/2020.

<sup>17</sup> O Tratado de criação da CECA foi assinado em Paris em abril de 1951 e entrou em vigor em julho de 1952. Seus integrantes eram França, Alemanha Ocidental, Bélgica, Itália, Luxemburgo e Holanda.

como um instrumento de confiança mútua entre os países signatários por meio da integração de segmentos industriais, que antes poderiam ser utilizados para fins bélicos, a exemplo da siderurgia.

Em 1955, na esteira dos eufóricos anos dourados do Pós-Segunda Guerra,<sup>18</sup> os países que integravam a CECA iniciaram discussões para transformar a até então integração setorial em uma integração econômica de maneira geral. O passo inicial deu-se com a criação de uma comissão incumbida de formular estudos sobre a viabilidade de um mercado comum, além de formular propostas no campo do controle do uso da energia nuclear. De fato, o assim denominado “Relatório Spaak”, produzido por essa comissão, contribuiu para a formulação, em 1957, dos tratados de Roma, de onde surgiram a Comunidade Econômica Europeia (CEE) e a Comunidade Europeia de Energia Atômica (EURATOM).<sup>19</sup> A CEE tinha como objetivo criar uma união aduaneira com vistas à futura implementação de um mercado comum europeu, possibilitando a implementação dos quatro eixos da integração: livre circulação de bens, serviços, pessoas e capitais.<sup>20</sup> A EURATOM, por sua vez, veio ao encontro das necessidades do contexto do pós-segunda guerra e início da guerra fria em se discutir a temática sensível do uso da energia nuclear para fins pacíficos.

Os Tratados de Roma somados à CECA constituíram, dessa forma, o quadro das Comunidades Europeias, em que cada comunidade possuía personalidade jurídica distinta. Apesar disso, uma pequena estrutura institucional comum às comunidades foi criada, sendo composta pela Comissão, o Conselho, a Assembleia Comum e o Tribunal de Justiça das Comunidades Europeias.<sup>21</sup> Este último seria o precursor do atual Tribunal de Justiça da União Europeia, enquanto a Assembleia Comum é o órgão que antecedeu o Parlamento Europeu.<sup>22</sup>

Em 1965, a integração europeia sofreu uma forte crise protagonizada pela França, então governada pelo general Charles de Gaulle. O líder francês discordava dos contornos federativos que a Comunidade Europeia estava tomando e, por isso, implementou a chamada

---

<sup>18</sup> HOBBSBAWM, Eric J. **Era dos Extremos: o breve século XX**. 2ª edição. São Paulo: Companhia das letras, 2019.

<sup>19</sup> NUNES, Amandino Teixeira Júnior. **A União Europeia e suas instituições**. Revista de Informação Legislativa. 48 n. 192. Senado Federal: Brasília: out./dez. 2011. Disponível em: <[https://www12.senado.leg.br/ril/edicoes/48/192/ril\\_v48\\_n192\\_p21.pdf](https://www12.senado.leg.br/ril/edicoes/48/192/ril_v48_n192_p21.pdf)>. Acesso em: 24/03/2020.

<sup>20</sup> *Ibid.*

<sup>21</sup> CHAIMOVICH, Mariana Midea Cuccovia. **O direito da integração nas constituições dos estados membros da União Europeia**. Dissertação de Mestrado. Faculdade de Direito da USP. São Paulo: USP, 2011. Disponível em: <[https://teses.usp.br/teses/disponiveis/2/2135/tde-15052012-090748/publico/Mariana\\_Midea\\_Cuccovia\\_Chaimovich\\_ME.pdf](https://teses.usp.br/teses/disponiveis/2/2135/tde-15052012-090748/publico/Mariana_Midea_Cuccovia_Chaimovich_ME.pdf)>. Acesso em: 24/03/2020.

<sup>22</sup> UNIÃO EUROPEIA. **The European Parliament: historical background**. Disponível em: <<https://www.europarl.europa.eu/factsheets/en/sheet/11/the-european-parliament-historical-background>>. Acesso em: 24/03/2020.

política de *empty chair*,<sup>23</sup> pela qual impediu a participação de seus ministros no conselho europeu, paralisando as atividades do órgão por cerca de 7 meses.<sup>24</sup> Contudo, a despeito das incertezas iniciais com relação à viabilidade da integração europeia da forma como planejada, algumas ações foram desde cedo implementadas, como por exemplo a Política Agrícola Comum, em 1962, e a concretização da união aduaneira, em 1968, um ano antes do previsto<sup>25</sup>. Tais exemplos demonstravam as potencialidades do projeto integrador, ainda incipiente.

A partir da década de 70, com a adesão da Dinamarca, Irlanda e do Reino Unido, as Comunidades Europeias ganharam novo fôlego.<sup>26</sup> Ademais, o ano de 1979 ficou marcado como o ano da primeira eleição direta para o Parlamento Europeu, dando maior legitimidade democrática ao projeto integracionista e, inclusive, tendo grande relevância para os debates sobre a proteção de dados pessoais, conforme se verá mais adiante neste trabalho.<sup>27</sup>

Já na década de 80, o ingresso de Grécia, Portugal e Espanha somado às cobranças por ações mais pragmáticas das Comunidades Europeias reacenderam o debate sobre a possível implementação do Mercado Comum Europeu, além da possibilidade de ampliação das políticas europeias para outras áreas até então negligenciadas, como o desenvolvimento social e econômico e os Direitos Humanos. Além disso, o fim da Guerra Fria e a dissolução da URSS, deram novo ímpeto à integração europeia, conforme demonstra Vila Maior<sup>28</sup>:

De repente, o processo de integração europeia passava a circular a uma velocidade vertiginosa. Ainda nem sequer estava em funcionamento o mercado interno (o principal desenvolvimento do Ato Único Europeu, a anterior revisão dos tratados) e já era negociado o passo que se seguia - o modelo da união monetária. A integração europeia abandonava as cautelas e a lentidão que marcaram o desenvolvimento anterior. Esta alteração na estratégia de integração econômica tem o selo da mudança proporcionada pela queda do muro de Berlim.

O aumento das negociações regionais nesse período teve como síntese o Ato Único Europeu, que definiu as etapas para a criação progressiva do mercado único das Comunidades Europeias,<sup>29</sup> a concessão de maiores poderes ao Parlamento Europeu e a criação de políticas

<sup>23</sup> DINAN, Dismon. **Europe Recast: A History of European Union**. 2ª Edição. Lynne Rienner: Boulder, 2014.

<sup>24</sup> COSTA, Olivier. *Op. cit.*, pág. 36.

<sup>25</sup> UNIÃO EUROPEIA. **The common agricultural policy at a glance**. Disponível em: <[https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance\\_en](https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance_en)>. Acesso em: 24/06/2020.

<sup>26</sup> PHINNEMORE, David. **The European Union: Establishment and Development**. in BORRAGÁN, Nieves Pérez-Solórzano; CINI, Michelle. *European Union Politics*. 5ª edição. Oxford University Press: Nova Iorque, 2016.

<sup>27</sup> UNIÃO EUROPEIA. **The European Parliament: historical background**. *Op. cit.*

<sup>28</sup> VILA MAIOR, Paulo. **A União Europeia após a queda do muro de Berlim: sucesso e desafios**. Revista da Faculdade de Ciências Humanas e Sociais. Porto: Edições UNiversidade Fernando Pessoa, 2009. Disponível em: <[https://bdigital.ufp.pt/bitstream/10284/1329/1/196-205\\_FCHS06-4.pdf](https://bdigital.ufp.pt/bitstream/10284/1329/1/196-205_FCHS06-4.pdf)>. Acesso em 30/03/2020.

<sup>29</sup> Conforme art. 14º do Ato Único Europeu que alterou o art. 8º-B do Tratado da CEE.

para desenvolvimento social dos países-membros. Mesmo com tal avanço no sentido de aumentar as competências da UE, o Ato Único Europeu não foi resposta suficiente para a crescente demanda por uma integração europeia mais aprofundada – era preciso dar continuidade às tratativas.

O Ato Único Europeu serviria para lançar as bases sob as quais seria posteriormente negociado o Tratado da União Europeia (TUE), também conhecido como Tratado de Maastricht de 1992.<sup>30</sup> O TUE foi visto como um ambicioso avanço, mas ainda não representava um projeto final e acabado, conforme restou expressamente declarado em seu art. A: “O presente Tratado assinala uma nova etapa no processo de criação de uma união cada vez mais estreita entre os povos da Europa, em que as decisões serão tomadas ao nível mais próximo possível dos cidadãos.”

O Tratado de Maastricht alicerçou-se em 3 pilares distintos: nas Comunidades Europeias, na política externa de segurança comum e na cooperação entre os governos da UE nos domínios da justiça e dos assuntos internos.<sup>31</sup> Com relação ao primeiro pilar, destaca-se a manutenção dos três tratados que formavam as comunidades europeias (CEE, CECA e EURATOM), porém atribuindo-lhes uma maior dimensão política. O segundo pilar, por seu turno, teve como principais objetivos: salvaguardar os valores comuns e a independência da UE; desenvolver e consolidar a democracia e o Estado de direito, bem como o respeito pelos direitos humanos e as liberdades fundamentais; e preservar a paz e a segurança internacional. Já o terceiro pilar, dizia respeito à colaboração entre os Estados para o controle de fronteiras, além da cooperação judiciária na luta contra o tráfico e terrorismo.<sup>32</sup>

Nota-se, portanto, que com o alinhamento político que resultou no TUE as instituições do bloco ganharam maior sofisticação e complexidade, o que fez da União Europeia um dos atores emergentes no jogo da geopolítica pós-guerra fria.<sup>33</sup>

Foi também pelo Tratado de Maastricht que se instituiu o conceito de cidadania europeia, onde restou consignada a igualdade de tratamento a todos os cidadãos dos países-membros, independentemente do seu país de origem.<sup>34</sup> Segundo Moura, a cidadania europeia,

---

<sup>30</sup> NUNES, Amandino Teixeira Júnior. *Op. cit.*

<sup>31</sup> UNIÃO EUROPEIA. Tratado da União Europeia. Artigo A.

<sup>32</sup> UNIÃO EUROPEIA. **Síntese do Tratado de Maastricht sobre a União Europeia**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:xy0026&from=PT>>. Acesso em: 30/03/2020.

<sup>33</sup> SOARES, Antonio Goucha. **A União Europeia como potência global?** As alterações do Tratado de Lisboa na política externa e de defesa. *Rev. Bras. Polít. Int.* 54 (1): 87-104. 2011.

<sup>34</sup> MOURA, A. B.. Paradoxos e limites de uma cidadania sem deveres: o caso da cidadania da União Europeia. *Âmbito Jurídico*, v. 90, p. 1-8, 2011.

à primeira vista, pode parecer paradoxal, quando se considera que o conceito de cidadania está estreitamente ligado ao de nacionalidade.<sup>35</sup> Entretanto, para a autora, esse fenômeno justifica-se da seguinte forma:

A cidadania da União surge no momento em que a antiga Comunidade européia assumia novas e relevantes competências legislativas em matérias que interferiam diretamente na vida e nos interesses do homem comum, como a tutela ao meio ambiente, aos consumidores, a proteção à saúde e a política social. Nesse contexto, era imprescindível aproximar, informar e fazer com que o cidadão participasse das decisões adotadas em âmbito supranacional.<sup>36</sup>

Com o crescente número de países solicitando a adesão à União Europeia na década de 90, os países-membros modificaram os tratados fundadores da UE, por meio dos Tratados de Amsterdã, em 1997, e de Nice, em 2001.<sup>37</sup> A ampliação esperada concretizou-se, de fato, em 2004, com a adesão de 10 novos Estados-membros, principalmente vindos da antiga União Soviética. Esse fenômeno fez com que alguns países do bloco, como Alemanha e Itália, demandassem por uma reestruturação da organização no intuito de comportar adequadamente esse novo número de países.<sup>38</sup>

Nasce, portanto, o debate sobre a construção de um ambicioso tratado, que ficaria conhecido como a Constituição da Europa. A proposta dessa Constituição inflamou as discussões sobre qual era e qual deveria ser a natureza política da União Europeia: uma federação ou organização intergovernamental. Depois de intensos debates, a proposta acabou por ser abandonada, após derrotas em plebiscitos na França e Holanda, em 2005.<sup>39</sup> Para contornar a situação criada pela não aprovação da Constituição, os líderes do bloco negociaram, no ano de 2007, em Lisboa, um novo tratado sobre a estrutura e funcionamento da União Europeia, retirando do texto questões polêmicas sobre a sua natureza federativa e constitucional.<sup>40</sup>

O Tratado de Lisboa entrou em vigor em 2009, e pôs fim ao sistema de 3 pilares que até então baseavam a União Europeia. Com este tratado, a Comunidade Europeia passou a

---

<sup>35</sup> *Ibid.*

<sup>36</sup> MOURA, A. B.. Cidadania europeia: uma verdadeira e própria cidadania? *Direito em Debate*, v. 32, p. 09-34, 2009.

<sup>37</sup> UNIÃO EUROPEIA. O tratado de Nice. Disponível em: <<https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/treaty-of-nice>>. Acesso em 30/03/2020.

<sup>38</sup> PINDER, John; USHERWOOD, Simon. *The European Union: a very short introduction*. 3ª edição. Oxford University Press: Oxford, 2013. pág. 52.

<sup>39</sup> *Ibid.* pág. 53.

<sup>40</sup> COSTA, Olivier. *Op. cit.*

integrar a União Europeia, formando uma única entidade com personalidade jurídica própria e com maiores áreas de atuação.<sup>41</sup>

### 2.1.1 As instituições da União Europeia

Conforme demonstrado acima, após um longo processo de crescente institucionalização, a União Europeia é constituída atualmente por 7 órgãos oficiais, quais sejam: o Conselho Europeu, a Comissão Europeia, o Conselho da União Europeia, o Parlamento Europeu, o Tribunal de Justiça da União Europeia, o Tribunal de Contas e o Banco Central Europeu.<sup>42</sup> Algumas dessas instituições têm papel fundamental na sistemática de Proteção de Dados Pessoais. É o caso, por exemplo, da Comissão Europeia, a quem coube a iniciativa de formular tanto a Diretiva 95/46/CE quanto o GPDR e, posteriormente, criar as condições para as suas implementações.<sup>43</sup> Também é da Comissão a responsabilidade pela elaboração das chamadas Decisões de Adequação – tema que será abordado no próximo capítulo – que permitem a transferência internacional de dados pessoais para terceiros países. Para o exercício dessas funções, a Comissão recebe o assessoramento técnico de órgãos especializados como o antigo Grupo de Trabalho do Artigo 29 e o atual Comitê Europeu de Proteção de Dados (CEPD).<sup>44</sup>

De igual modo, não se pode olvidar o importante papel do TJUE na uniformização da aplicação do Direito à Proteção de Dados em todos os países que compõem o bloco. Ainda que a corte tenha reconhecido a autonomia do Direito à Proteção de Dados tardiamente, casos como o *Google Spain* e *Schrems* são internacionalmente reconhecidos como paradigmas no tema.<sup>45</sup> Ademais, cabe, de igual forma, destacar a importância do Conselho da União Europeia e do Parlamento Europeu no debate das questões políticas que giram em torno das normas de Proteção de Dados quando exercem suas funções legislativas e fiscalizatórias.<sup>46</sup>

---

<sup>41</sup> SOARES, Antonio Goucha. A União Europeia como potência global? As alterações do Tratado de Lisboa na política externa e de defesa. Rev. bras. polít. int., Brasília, v. 54, n. 1, p. 87-104, 2011. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0034-73292011000100006&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292011000100006&lng=en&nrm=iso)>. Acesso em: 28/04/2020. <https://doi.org/10.1590/S0034-73292011000100006>.

<sup>42</sup> TUE, Artigo 13.

<sup>43</sup> USTARAN, Eduardo (ed.). **European Data Protection Law and Practice**. New Hampshire: International Association Of Privacy Professionals, 2018.p. 45.

<sup>44</sup> *Ibid.*

<sup>45</sup> *Ibid.* pág. 47.

<sup>46</sup> *Ibid.* págs.41-47.

No intuito de esclarecer o funcionamento dos órgãos que compõem a UE, os parágrafos seguintes serão dedicados a breves apontamentos, de caráter descritivo, sobre tais instituições.

O Conselho Europeu tem a função primordial de definir as diretrizes gerais e as prioridades da União Europeia em termos políticos.<sup>47</sup> Suas reuniões acontecem ordinariamente quatro vezes ao ano, mas o presidente tem a prerrogativa de convocar reuniões extraordinárias de acordo com a necessidade. As políticas definidas pelo Conselho Europeu são decididas, em geral, por consenso, porém, em alguns casos é permitida a votação por maioria qualificada.<sup>48</sup>

A Comissão Europeia, por sua vez, é o órgão executivo da União Europeia, sendo o responsável pela propositura de atos legislativos e pela execução e monitoramento destes uma vez aprovados. Trata-se do órgão de maior importância na perspectiva do Regime de Proteção de Dados da União Europeia, como ressaltado acima. O órgão é formado por 28 membros, sendo um comissário para cada país que compõe o bloco, além do próprio presidente da comissão. O processo de escolha dos membros tem ampla participação do Parlamento Europeu, a quem cabe eleger o presidente da Comissão e aprovar a nomeação de todos os demais membros.<sup>49</sup> Além de um órgão com caráter eminentemente político, a Comissão também exerce diversas funções administrativas dentro da União Europeia.<sup>50</sup> Sendo assim, é o órgão com maior estrutura burocrática e suporte administrativo, contando com cerca de 32 mil funcionários.<sup>51</sup>

O Conselho da União Europeia é formado pelos ministros que representam os governos dos Estados-membros de acordo com cada temática debatida.<sup>52</sup> Como tais ministros têm poderes para assumir compromissos vinculantes aos seus Estados, a atuação do Conselho é de grande relevância no processo decisório das políticas e normas da União Europeia. Dentre as diversas funções deste órgão dentro da EU, destacam-se as seguintes: competência legislativa, que é compartilhada com o Parlamento Europeu; poder de aprovação do orçamento da UE, em conjunto com o Parlamento Europeu; prerrogativa de firmar acordos internacionais,

---

<sup>47</sup>UNIÃO EUROPEIA. **European Council**. Disponível em:<[https://europa.eu/european-union/about-eu/institutions-bodies/european-council\\_en](https://europa.eu/european-union/about-eu/institutions-bodies/european-council_en)> Acesso em: 05/04/2020.

<sup>48</sup> *ibid.*

<sup>49</sup> *ibid.*

<sup>50</sup> COSTA, Olivier. *Op. cit*

<sup>51</sup> UNIÃO EUROPEIA. **EU administration - staff, languages and location**. Disponível em<[https://europa.eu/european-union/about-eu/figures/administration\\_en](https://europa.eu/european-union/about-eu/figures/administration_en)>. Acesso em: 08/04/2020.

<sup>52</sup> UNIÃO EUROPEIA. **Council of the European Union**. Disponível em:<[https://europa.eu/european-union/about-eu/institutions-bodies/council-eu\\_en](https://europa.eu/european-union/about-eu/institutions-bodies/council-eu_en)>. Acesso em: 08/04/2020.

representando a política externa da UE; e funções executivas residuais em relação à Comissão.

53

O Parlamento Europeu é o principal órgão representativo dos cidadãos da União Europeia, desde que, em 1979, foram estabelecidas eleições diretas para sua formação. Ao longo dos anos, suas competências foram ampliadas,<sup>54</sup> mas ainda assim o Parlamento Europeu não exerce todas as funções que os parlamentos nacionais geralmente exercem.<sup>55</sup> O exemplo mais sintomático disto é o fato de que cabe à Comissão Europeia a iniciativa de propor os atos legislativos, enquanto o Parlamento somente aprecia tais propostas, e ainda divide tal poder com o Conselho da União Europeia, por meio do processo de co-decisão. Tal característica gerou discussões doutrinárias acerca da existência ou não do chamado “déficit democrático” no processo decisório da União Europeia.<sup>56</sup> Além disso, o Parlamento Europeu não participa das decisões referentes à defesa e política externa da União Europeia, que se submetem a um regime especial de votação.

## 2.3 AS NORMAS DA UNIÃO EUROPEIA

Muito embora não exista uma Constituição formal em moldes estritamente federativos, pode-se afirmar que o direito da União Europeia assenta-se em diferentes fontes normativas que, para alguns doutrinadores, instituem um sistema jurídico *sui generis*.<sup>57</sup> Dentro da concepção dialética entre federalismo e intergovernamentalismo em que foi estruturado, o direito da União Europeia dialoga com as ordens jurídicas internas dos Estados-membros por

<sup>53</sup> COSTA, Olivier. *Op. cit.*

<sup>54</sup> UNIÃO EUROPEIA. **O PE após o Tratado de Lisboa: um papel reforçado na construção da Europa.** Disponível em: <<https://www.europarl.europa.eu/about-parliament/pt/powers-and-procedures/the-lisbon-treaty>> Acesso em: 28/04/2020.

<sup>55</sup> COSTA, Olivier. *Op. cit.*

<sup>56</sup> MEDEIROS, Marcelo de Almeida; CAMPOS, Cinthia Regina. **União Européia, reformas institucionais e déficit democrático: uma análise a partir do mecanismo de co-decisão.** Rev. bras. polít. int., Brasília, v. 52, n. 1, p. 29-52, June 2009. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0034-73292009000100002&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292009000100002&lng=en&nrm=iso)>. Acesso em: 20/04/2020. Também nesse sentido: MICOLTA PORTOCARRERO, Ma. Catalina. **El proceso legislativo en el Tratado de Lisboa: privilegio de la eficacia en detrimento de la democracia.** Pap.polit., Bogotá, v. 19, n. 1, p. 237-263, June 2014. Disponível em: <[http://www.scielo.org.co/scielo.php?script=sci\\_arttext&pid=S0122-44092014000100012&lng=en&nrm=iso](http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-44092014000100012&lng=en&nrm=iso)>. Acesso em: 20/04/2020.

<sup>57</sup> WALKER, Neil. The Philosophy of European Union. In: ARNULL, Anthony; CHALMERS, Damian (ed.). **The Oxford Handbook of European Union Law.** Oxford: Oxford University Press, 2015. Cap. 1.pág. 24.

meio dos seguintes princípios estruturantes: o princípio da competência por atribuição, o da primazia, o da autonomia e o princípio dos efeitos diretos do direito da União Europeia.<sup>58</sup>

O princípio da competência por atribuição está estabelecido no art. 5º do Tratado da União Europeia que, em abreviada síntese, dispõe que a UE somente pode criar normas dentro dos limites das competências firmadas nos seus próprios Tratados Constitutivos.<sup>59</sup> Nesse sentido, em primeira análise, caso não houvesse previsão nos tratados constitutivos sobre a possibilidade de a União Europeia estabelecer normas sobre proteção de dados pessoais, o GDPR não poderia vir a existir.

No tocante ao princípio da primazia do direito da União Europeia, conforme elucida Moura,<sup>60</sup> deve-se ressaltar que não se trata de um princípio explícito dos textos normativos, mas decorre da própria jurisprudência do Tribunal de Justiça da União Europeia, que vem reiterando seu posicionamento desde 1964.<sup>61</sup> Segundo esse princípio, as normas emanadas da União Europeia, originárias ou derivadas, têm superioridade hierárquica com relação às legislações internas dos países-membros, ainda que se trate de norma constitucional. Conforme o entendimento do TJUE, trata-se de condição de existência para o próprio ordenamento jurídico supranacional, sem o qual os agentes políticos dos países-membros poderiam derogar ou modificar o Direito da UE.<sup>62</sup>

Segundo o princípio da autonomia, as normas do ordenamento jurídico supranacional, ainda que integradas ao direito interno dos países-membros, devem preservar sua eficácia própria e distinta das demais legislações. Nas palavras de Moura, cuida-se de verdadeira “marca congênita” das normas da UE, da qual decorre o dever das cortes nacionais de interpretarem o direito Europeu com base nos entendimentos firmados no âmbito supranacional pelo TJUE.<sup>63</sup> Esse princípio ganha relevância no contexto das normas supranacionais da UE que impõem aos países-membros o dever de legislar sobre determinada matéria, como é o caso das Diretivas.

Por fim, destaca-se que é por meio do princípio dos efeitos diretos que as normas emanadas da UE criam direitos e deveres que podem ser diretamente invocados pelos

<sup>58</sup> CLAES, Monica. The Primacy of EU Law in European and National Law. In: ARNULL, Anthony; CHALMERS, Damian (ed.). **The Oxford Handbook of European Union Law**. Oxford: Oxford University Press, 2015. Cap. 8. pág. 178. Também nesse sentido: PINDER, John; USHERWOOD, Simon. *Op. cit.* pág. 71.

<sup>59</sup> TUE, Art. 5.

<sup>60</sup> MOURA, Aline Beltrame de. **As Bases Principiológicas do Sistema Jurídico da União Europeia**. In: Gustavo Ferraz de Campos Monaco; Maria Rosa Loula; Coordenadores. (Org.). *Direito Internacional e Comparado: Trajetória e Perspectivas*. 1ª ed. São Paulo: Quartier Latin do Brasil, 2021, v. 2, p. 43-58.

<sup>61</sup> UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Caso Flaminio Costa v. Ente Nazionale per l'Energia Elettrica (ENEL) [1964] ECR 585, [1964] CMLR 425.

<sup>62</sup> MOURA, Aline Beltrame de. **As Bases Principiológicas do Sistema Jurídico da União Europeia**. *Op. cit.*

<sup>63</sup> *Ibid.* pág. 48.

particulares nas cortes nacionais. Conforme ressalta Moura, “a atuação do indivíduo como sujeito ativo e passivo em um sistema jurídico criado pelos Estados é um fenômeno historicamente recente e que encontra no ordenamento jurídico da União Europeia o mais atual e avançado desenvolvimento.”<sup>64</sup>

O princípio dos efeitos diretos faz com que as normas supranacionais da UE devam ser dotadas de clareza, precisão e completude, ainda mais quando se considera os diferentes ordenamentos jurídicos dos países que a compõem e os diversos idiomas que os documentos jurídicos devem ser traduzidos. Nesse sentido, ressalta-se a importância do TJUE na uniformização da interpretação do Direito Europeu e das próprias entidades que auxiliam a Comissão Europeia na criação de documentos informativos, como é o caso do Comitê Europeu de Proteção de Dados.

Não se pode confundir, entretanto, o efeito direto com a aplicabilidade direta do Direito da União Europeia. A aplicabilidade direta diz respeito à entrada automática das normas da UE no ordenamento jurídico interno dos países-membros, ou seja, trata-se somente da manifestação do monismo jurídico adotado entre a União e os Estados que a compõem.<sup>65</sup>

Conforme elucida Fairhurst, além dos princípios elencados acima, que norteiam a aplicação do direito supranacional, pode-se identificar sete principais fontes do direito da União Europeia, a saber: (1) os Tratados Constitutivos da União Europeia; (2) as normas derivadas dos tratados (secundárias); (3) os documentos de Soft Law; (4) os tratados relacionados com a UE e firmados entre os Estados-membros; (5) os tratados internacionais firmados pela UE no âmbito da sua competência; (6) as decisões do Tribunal de Justiça da União Europeia; (7) os princípios gerais do Direito nos quais as constituições dos Estados-membros estão embasados.<sup>66</sup>

Todas as fontes listadas acima têm relação com o direito à proteção de dados; entretanto, deve-se ressaltar, desde já, a importância dos Tratados Constitutivos e das normas derivadas. Isso porque, é na Carta de Direitos Fundamentais – considerada parte dos tratados constitutivos após o Tratado de Lisboa – que o direito à proteção de dados é caracterizado como um direito fundamental.<sup>67</sup> Além disso, a instrumentalização desse direito fundamental é feita por meio de normas derivadas, como foi o caso da Diretiva 95/46/CE e do atual GDPR.

---

<sup>64</sup> *Ibid.* pág. 52.

<sup>65</sup> *Ibid.*

<sup>66</sup> FAIRHURST, John. **Law of the European Union**. 11. ed. Harlow: Pearson Education Limited, 2016. pág. 57.

<sup>67</sup> UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. Art. 8º

As normas jurídicas que compõem o ordenamento supranacional podem ainda ser classificadas entre primárias e secundárias.<sup>68</sup> As normas primárias são compostas pelos Tratados Constitutivos da UE, juntamente com seus textos modificativos, protocolos e anexos. Atualmente, portanto, as normas primárias são formadas pelo Tratado da União Europeia, pelo Tratado de Funcionamento da União Europeia e pela Carta de Direitos Fundamentais da União Europeia.<sup>69</sup> Além disso, são também equivalentes às normas primárias os tratados de adesão de Estados-membros.<sup>70</sup> Esses documentos conformam a estrutura jurídica que dá sustentação para todas as demais normas e políticas da UE. São eles que também definem os objetivos, a organização e os métodos de trabalho de todas as instituições da União.<sup>71</sup>

As normas secundárias, por seu turno, são constituídas pelos atos legislativos, atos delegados, atos de implementação e outros instrumentos legais, tais como os acordos intergovernamentais e internacionais. Segundo o art. 288 do Tratado Sobre o Funcionamento da União Europeia os atos legislativos podem ser classificados como: regulamentos, diretivas, decisões, recomendações ou pareceres. O mesmo artigo também elucida a natureza jurídica e a força normativa de cada um destes atos.<sup>72</sup>

Os regulamentos, a exemplo do GDPR, são normas gerais de caráter obrigatório para todos os Estados-membros e são diretamente aplicáveis em todo o território do bloco. Já as diretivas são normas que vinculam os Estados-membros com relação a objetivos a serem alcançados, porém delegam para cada um deles a competência legislativa de decidir sobre a melhor forma de implementar internamente tais comandos. As decisões, por sua vez, são caracterizadas por seu caráter específico que as tornam vinculantes somente para as partes para as quais são direcionadas. Por fim, o artigo 288 estabelece que as recomendações e os pareceres não são vinculantes.<sup>73</sup>

Uma vez ilustrado o contexto histórico de formação da União Europeia e suas principais normas jurídicas, passa-se a análise da evolução do direito à proteção de dados pessoais nesse cenário como um direito autônomo e fundamental.

---

<sup>68</sup> SYRPIS, Phil. **The Relationship Between Primary and Secondary Law in the EU**. Common Market Law Review. Vol. 52. p 461–488. Kluwer Law International: United Kingdom, 2015.

<sup>69</sup> UNIÃO EUROPEIA. EU Law. Disponível em <[https://e-justice.europa.eu/content\\_eu\\_law-3-en.do](https://e-justice.europa.eu/content_eu_law-3-en.do)>. Acesso em 05/04/2020;

<sup>70</sup> *Ibid.*

<sup>71</sup> COSTA, Olivier. *Op. cit.*

<sup>72</sup> UNIÃO EUROPEIA. TRATADO SOBRE FUNCIONAMENTO DA UNIÃO EUROPEIA. Artigo 288. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>>. Acesso em: 05/04/2020.

<sup>73</sup> TFUE, art. 288.

## 2.3. A EVOLUÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA

Embora cada vez mais presente nas discussões acadêmicas e corporativas, o assunto do direito à proteção de dados não é algo novo no contexto dos países da União Europeia. Uma das razões que fazem, atualmente, o GDPR ser referência para outras leis de proteção de dados pessoais que surgem pelo mundo – como a brasileira – é por ser ele o resultado de uma longa evolução normativa e jurisprudencial iniciada há quase meio século. Dessa forma, este subcapítulo será dedicado ao estudo do desenvolvimento desse instituto, desde suas origens até a formulação do GDPR. Antes disso, contudo, é necessário tecer breves considerações sobre a discussão doutrinária existente acerca da relação entre o direito à privacidade e o direito à proteção de dados pessoais.

### 2.3.1 Relação entre Direito à Privacidade e Proteção de dados

Para alguns doutrinadores, a origem do direito à proteção de dados pessoais encontra-se nas primeiras declarações internacionais que mencionavam o direito à privacidade, como a Declaração Universal de Direitos Humanos, de 1948. Em sentido diverso, parte da doutrina advoga pela necessidade de serem distinguidas as origens e o conteúdo de tais direitos, embora reconheçam a estreita relação existente entre eles, conforme será abordado abaixo.

Para Schünemann e Baumann, existe uma relação de hierarquia entre o direito à privacidade e o direito à proteção de dados pessoais – quase como uma relação entre gênero e espécie. A privacidade seria, portanto, o direito que fundamenta a proteção de dados pessoais; e a proteção de dados, por sua vez, corresponderia ao aspecto informacional da privacidade dentro do novo contexto da digitalização das relações humanas – ou seja, um dos instrumentos para a garantia da privacidade.<sup>74</sup>

Na tentativa de apresentar a questão sob uma perspectiva histórica, Ustaran acredita que as raízes do direito à proteção de dados encontram-se dentro das próprias normas que firmaram a proteção à privacidade como um dos direitos humanos.<sup>75</sup> Nesse sentido, o autor pontua a importância dos arts. 12 e 19 da Declaração Universal dos Direitos Humanos e os arts.

---

<sup>74</sup> SCHÜNEMANN, Wolf J.; BAUMANN, Max-Otto (ed.). **Privacy, Data Protection and Cybersecurity in Europe**. Cham: Springer, 2017. pág. 2.

<sup>75</sup> USTARAN, Eduardo. *Op. cit.* pág. 18.

8 e 10 da Convenção Europeia de Direitos Humanos, de 1950, ambos com redações muito similares. Também nesse sentido, Alsenoy concorda que os fundamentos das normativas criadas para a proteção de dados pessoais estão no direito à privacidade, embora reconheça a dificuldade em tentar conceituar o Direito à Privacidade.<sup>76</sup>

Lynskey, por seu turno, ao analisar a discussão doutrinária e jurisprudencial sobre o tema, sistematiza o debate em três vertentes: aqueles que acreditam que tais direitos são distintos, mas complementares; aqueles que defendem que a proteção de dados é uma subespécie da privacidade; e, por fim, aqueles que consideram o direito à privacidade como um direito independente que serve para diferentes funções dentre elas – mas não exclusivamente – à proteção da privacidade. Após discutir minuciosamente cada um dos três posicionamentos, a autora filia-se à terceira corrente, uma vez que, segundo ela, o direito à proteção de dados “oferece aos indivíduos mais direitos sobre mais tipos de informações do que o direito à privacidade, quando aplicada no contexto do processamento de dados pessoais.”<sup>77</sup> Sendo assim, o direito à proteção de dados traz outras nuances que vão além da proteção da privacidade dos indivíduos titulares dos dados.

Não obstante a existência de fértil discussão sobre a temática, conforme brevemente apresentado acima, fato é que, atualmente, a Carta dos Direitos Fundamentais da União Europeia nomeia o direito à privacidade e o direito à proteção de dados de maneira distinta. Para Lynskey, isso é um indicativo da inclinação do legislador europeu à terceira corrente. Ademais, outro elemento que, segundo a autora, justifica a adoção da terceira interpretação é o fato de que os Estados-membros da UE fundamentam de maneira distinta o direito à proteção de dados e o direito à privacidade. Na Alemanha, por exemplo, a proteção de dados pessoais está ligada umbilicalmente ao princípio da dignidade da pessoa humana, enquanto na França tal instituto advém do princípio da Liberdade Individual.<sup>78</sup>

No intuito de facilitar a exposição da temática em análise neste trabalho, no tópico seguinte será apresentada a evolução do Direito à Proteção de Dados Pessoais dentro da União Europeia com foco nas normas que façam menção específica a esse direito.

---

<sup>76</sup> ALSENOY, Brendan Van. **Data Protection in the EU: Roles, responsibilities and liability**. Intersentia Ltd: Cambridge, 2019. pág. 158.

<sup>77</sup> LYNKEY. Orla. **The Foundations of EU Data Protection Law**. Oxford University Press: Oxford, 2015. pág. 90.

<sup>78</sup> *Ibid.* pág. 103-104.

### 2.3.2 As primeiras normas sobre proteção de dados pessoais no âmbito europeu

Para Alsenoy,<sup>79</sup> a evolução do direito à proteção de dados pela perspectiva da União Europeia pode ser dividida em quatro períodos. No primeiro período surgiram as primeiras leis nacionais sobre a temática, ainda nas décadas de 70 e 80. Já no segundo, iniciado a partir da década de 80, ocorre a internacionalização do direito à proteção de dados. No terceiro, vislumbra-se um movimento de internalização no ordenamento jurídico dos países-membros das normas internacionais. E, por fim, o quarto período corresponde à harmonização europeia das normas de proteção de dados pessoais entre 1995 e 2016, com a implementação da Diretiva 95/46/CE e do GDPR.

A primeira lei que se tem registro sobre proteção de dados pessoais foi adotada em 1970, pelo estado de Hesse, na então República Federal da Alemanha, e tinha como principal objetivo controlar o processamento de dados pessoais realizados pelas autoridades públicas. A lei foi criada após a instalação de diversos centros de processamentos de dados pessoais pelo governo local e, dentro desse contexto, instituiu o conceito de *Datenschutz*, que mais tarde seria traduzido para o inglês como *Data Protection* e, em português, Proteção de Dados.<sup>80</sup>

Nos anos seguintes, outros estados alemães adotaram medidas semelhantes, até o ponto em que a própria República Federal da Alemanha estabeleceu sua Lei Federal de Proteção de Dados, em 1977.<sup>81</sup> Essa lei, aplicável tanto a entes públicos quanto privados, estabelecia que o tratamento de dados pessoais só seria permitido nas hipóteses estipuladas na própria lei ou por consenso do titular. Também foram criados pela legislação o Comissariado Federal de Proteção de Dados e a figura do *Data Protection Officer* como obrigatoriedade para determinados entes privados.<sup>82</sup> Já de início, é possível notar, portanto, que alguns dos mecanismos utilizados atualmente pelo GDPR e pela própria LGPD brasileira já estavam presentes nesses primeiros atos normativos sobre proteção de dados pessoais.

Durante a década de 70, outros países europeus como a Suécia, Áustria, Dinamarca, França e Noruega seguiram o exemplo alemão e criaram legislações similares. A despeito de tal expansão normativa, é preciso esclarecer que nem sempre o termo proteção de dados pessoais foi utilizado uniformemente. Na França, por exemplo, a *Loi relative à l'informatique*,

<sup>79</sup> ALSENOY, Brendan Van. *Op. cit.* pág. 151.

<sup>80</sup> FUSTER, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Springer: Bruxelas, 2014. pág. 57.

<sup>81</sup> OSTER, Jan. Data Protection. In **European and International Media Law** (pp. 304-369). Cambridge: Cambridge University Press, 2016. doi:10.1017/9781139208116.009

<sup>82</sup> FUSTER, Gloria González. *Op. cit.* pág. 61

*aux fichiers et aux libertés*, de 1978, considerava os dados pessoais como “informações nominativas”, ou seja, aquelas informações que pudessem identificar um determinado indivíduo após o tratamento por entes públicos ou privados.<sup>83</sup>

Outra experiência relevante para a evolução do reconhecimento do direito à proteção de dados no âmbito europeu foi a promulgação da Constituição da República Portuguesa de 1976, após a Revolução dos Cravos. O artigo 35º da constituição portuguesa, em sua versão original, faz menção ao direito de todo cidadão de ter conhecimento das suas informações constantes em registros mecanográficos e poder pedir a retificação e atualização desses dados, conforme se reproduz abaixo:

ARTIGO 35.º (Utilização da informática)

1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos.<sup>84</sup>

Segundo Fuster, o texto do artigo 35º da Constituição Portuguesa tornou-se popular em diversas partes do mundo e, inclusive, foi inspiração para a instituição do *habeas data* na Constituição Brasileira de 1988.<sup>85</sup>

As crescentes discussões internas dos países europeus sobre a temática de privacidade e proteção de dados pessoais durante a década de 70 transbordam para o âmbito internacional, principalmente no seio da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Preocupados com os efeitos econômicos que uma política protecionista de fluxo de dados poderia ter, os países-membros da OCDE iniciaram tratativas para criarem normas internacionais sobre o tratamento e o fluxo de dados pessoais. Por conseguinte, no ano de 1978 foi constituída uma comissão de experts que ficaria responsável em elaborar um documento contendo diretrizes sobre proteção da privacidade e do fluxo transfronteiriço de dados pessoais.

<sup>86</sup> Após dois anos de debates, foram aprovadas as chamadas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, em tradução livre, Diretrizes sobre Proteção da Privacidade e Fluxo Transfronteiriço de Dados Pessoais.

---

<sup>83</sup> *Ibid.* pág. 63.

<sup>84</sup> PORTUGAL. Constituição (1976). **Constituição da República Portuguesa**, de 02 de abril de 1976. Redação original.

<sup>85</sup> FUSTER, Gloria González. *Op.cit.* pág. 67

<sup>86</sup> *Ibid.* pág. 77

Conforme elucida Fuster, por forte influência dos EUA e em razão da grande diversidade linguística dos então 24 países que compunham a OCDE, as *Guidelines* não mencionam a necessidade de adoção de leis de proteção de dados pessoais pelos países-membros da organização, mas sim de leis de proteção da privacidade ou da vida privada.<sup>87</sup>

Ainda no campo internacional e concomitante aos trabalhos realizados na OCDE, o Conselho da Europa – organização internacional fundada em 1949 e que foi responsável pela elaboração da Convenção Europeia de Direitos Humanos de 1953 – também iniciou suas discussões sobre a proteção dos direitos humanos relacionados à utilização de dados pessoais.

O Conselho da Europa investigou, na época, quais eram os pontos em comum e divergentes nas legislações nacionais sobre proteção de dados pessoais até então aprovadas. Chegou-se à conclusão de que ainda havia algumas divergências que deveriam ser superadas para não prejudicar à proteção dos direitos humanos em nível europeu e, ao mesmo tempo, para facilitar o fluxo de dados entre os países do Velho Continente.<sup>88</sup>

A constatação da necessidade de harmonização do direito à proteção de dados em nível europeu levou o Conselho da Europa, em 1981, a aprovar a Convenção 108, que entrou em vigor em 1985.<sup>89</sup> A Convenção 108 serviu como modelo inicial para as posteriores normas de proteção de dados pessoais que viriam a ser implementadas no âmbito dos países europeus.<sup>90</sup> Além disso, a Convenção foi o primeiro – e até o momento único – instrumento internacional vinculante sobre o tema.<sup>91</sup> Nesse sentido, Falk argumenta que a Convenção pode ser compreendida como um referencial para a construção do modelo europeu supranacional de proteção de dados.<sup>92</sup> Muito embora tenha sido elaborada pelo Conselho da Europa, a adoção à Convenção 108 é aberta para países não-membros, sendo que o primeiro país em tal condição a adotar o documento foi o Uruguai.

Outra importante contribuição da Convenção 108 foi a estipulação de uma série de princípios que passariam a ser reproduzidos nas normas posteriores sobre a temática. Dentre

---

<sup>87</sup> *Ibid.* pág. 78.

<sup>88</sup> *Ibid.* pág. 86.

<sup>89</sup> OSTER, Jan. *Op. cit.*

<sup>90</sup> REICHEL, Jane; LIND, Anna-sara. **Regulating Data Protection within the European Union**. In: DÖRR, Dieter; WEAVER, Russell L.. **Perspectives on Privacy Increasing**. Berlim: de Gruyter, 2014. Cap. 3. p. 22-45.

<sup>91</sup> CONSELHO DA EUROPA. **Handbook on European Data Protection Law**, Bélgica: Council of Europe, 2018. p. 24.

<sup>92</sup> FALK, Matheus. A necessidade de proteção aos dados pessoais no direito brasileiro: tutela jurídica na era da modernidade líquida e da surveillance. 2017. 192 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal do Paraná, Curitiba, 2017. Disponível em: <https://acervodigital.ufpr.br/handle/1884/47787>. Acesso em: 15 jun. 2020

estes princípios encontram-se: o princípio da transparência e limitação do tratamento de dados; da licitude do tratamento; da exatidão; da adequação aos propósitos do tratamento; dentre outros.<sup>93</sup> Por fim, cumpre salientar que em 2018 o texto da Convenção foi modernizado para se adequar ao novo contexto tecnológico da sociedade e ganhou a nomenclatura de Convenção 108+.

### 2.3.3 A Diretiva 95/46/CE e o direito à proteção de dados pessoais

No tocante ao âmbito específico do direito supranacional da União Europeia, pode-se distinguir a evolução do direito à proteção de dados pessoais entre as normas primárias e secundárias. Por mais paradoxal que possa parecer sob o prisma da hierarquia normativa, deve-se ressaltar que a proteção de dados pessoais foi primeiramente reconhecida em uma norma de caráter secundário: a Diretiva 95/46/CE.<sup>94</sup> Como se demonstrará a seguir, isso ocorreu por conta da crescente preocupação da Comissão Europeia, ao longo da década de 80, com a demora de alguns países membros da UE em ratificar a Convenção 108 do Conselho da Europa.<sup>95</sup>

Na década de 70, o Parlamento Europeu já havia discutido a necessidade de implementação de normas comunitárias com relação à proteção dos direitos individuais dos cidadãos europeus em face das novas técnicas de processamento de dados. Chegou-se, inclusive, à fase de elaboração de estudos e à aprovação de três resoluções nos anos de 1975, 1976 e 1979, onde o Parlamento Europeu solicitava à Comissão que elaborasse alguma Diretiva para harmonizar as legislações nacionais sobre proteção de dados pessoais. Contudo, essas solicitações não foram acolhidas pela Comissão, que permaneceu inerte.<sup>96</sup>

Em 1981, após a aprovação da Convenção 108 do Conselho da Europa, a Comissão considerou que este era o instrumento adequado para garantir a proteção de dados no âmbito europeu, sem, portanto, haver a necessidade de elaboração de qualquer Diretiva própria das

<sup>93</sup> CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981.

<sup>94</sup> UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>>. Acesso em: 05/07/2020.

<sup>95</sup> UNIÃO EUROPEIA. Comunicação da Comissão Europeia relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação. Bruxelas: 1990. Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:51990DC0314&from=EN>>. Acesso em: 05/07/2020.

<sup>96</sup> FUSTER, Gloria González. *Op. cit.* pág. 122.

Comunidades Europeias sobre o tema. Desta forma, recomendou-se formalmente que todos os Estados-membros aderissem à Convenção 108 do Conselho da Europa.<sup>97</sup>

Em 1990, entretanto, a perspectiva da Comissão Europeia foi alterada na medida em que ainda existiam muitas diferenças nas legislações internas sobre proteção de dados, e que muitos países do bloco não haviam aderido à Convenção 108. Esse fato poderia prejudicar os objetivos da integração europeia da livre circulação de bens e serviços.<sup>98</sup> Por conseguinte, naquele mesmo ano, a Comissão enviou ao Parlamento Europeu um projeto de Diretiva que, após cinco anos de negociações, que viria a ser a Diretiva 95/46/CE.

Muito embora não houvesse na época nenhuma menção ao direito à proteção de dados pessoais nos textos constitutivos das Comunidades Europeias (normas primárias), para não ferir o princípio da competência por atribuição, a Comissão justificou a necessidade de implementação da Diretiva para proteger o direito à privacidade contido tanto no art. 8º da Convenção Europeia de Direitos Humanos quanto nos próprios princípios dos ordenamentos jurídicos dos países-membros. Ademais, segundo a Comissão, a preservação desse direito fundamental seria necessária para a implementação do Mercado Comum, conforme o art. 100 do Tratado da Comunidade Europeia, uma vez que garantiria o livre fluxo de dados entre os Estados-membros de maneira segura e adequada.<sup>99</sup>

A proposta de Diretiva continha proposições sobre as condições legais para o tratamento de dados pessoais, os direitos dos titulares dos dados, os requisitos de qualidade e adequação do tratamento e, além disso, previa a criação de um órgão consultivo sobre proteção de dados pessoais em nível comunitário, que depois viria a ser chamado de Grupo de Trabalho do art. 29 (*Art. 29 Working Party*).<sup>100</sup>

No decorrer do processo legislativo para a aprovação da Diretiva, criou-se um grupo de países que se opunham a algumas proposições contidas no projeto original, liderados pelo Reino Unido. As principais discordâncias desse grupo eram com relação à diferenciação entre os setores público e privado contida na proposta inicial bem como com relação à abrangência do escopo da norma, que poderia gerar certa ambiguidade.<sup>101</sup> Entretanto, após 5 anos de

---

<sup>97</sup> *Ibid.* pág. 120

<sup>98</sup> UNIÃO EUROPEIA. **Comunicação da Comissão Europeia relativa à proteção das pessoais no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação.** *Op. cit.*

<sup>99</sup> *Ibid.*

<sup>100</sup> FUSTER, Gloria González. *Op. cit.* pág. 126.

<sup>101</sup> *Ibid.* pág. 127.

tramitação, foi finalmente aprovado em 24 de outubro de 1995 um texto que contemplava as opiniões divergentes e que receberia a nomenclatura de Diretiva 95/46/CE.

Conforme ressaltam Ustaran e Lynskey, o objetivo da Diretiva 95/46 tem natureza dúplice: almeja proteger os direitos fundamentais dos indivíduos, em especial, a proteção dos seus dados pessoais, mas ao mesmo tempo procura eliminar as restrições de circulação desses dados entre os Estados-membros, harmonizando as legislações internas.<sup>102</sup> A menção ao direito à proteção de dados pessoais fica implícita no texto da Diretiva e aparece de maneira marginal nos considerandos.

Quanto à sua estrutura, a Diretiva é composta por 72 considerandos e 34 artigos. Os considerandos não têm força cogente, mas são instrumentos que facilitam a interpretação dos dispositivos por meio da conceituação de termos e exposição dos motivos que levaram a sua adoção. Os artigos da Diretiva foram divididos em 7 capítulos: disposições gerais; condições gerais de licitude do tratamento; medidas judiciais, responsabilidade e sanções; transferência de dados pessoais para países terceiros; códigos de conduta; autoridade de controle e grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais; e medidas de implementação comunitária.<sup>103</sup>

Conforme exposto anteriormente, devido à sua função dentro do rol das normas comunitárias, coube à Diretiva a exposição de regras e princípios gerais que deveriam ser incorporados de maneira específica pelas legislações internas dos Estados-membros, de acordo com suas especificidades, permitindo ainda a implementação de protocolos mais restritivos do que os por ela fixados.

De acordo com Alsenoy, a Diretiva baseou-se fundamentalmente nos princípios e definições elencados anteriormente pela Convenção 108, mas inovou na inserção de alguns novos elementos. Uma dessas inovações diz respeito ao âmbito de aplicação material da norma, pois enquanto a Convenção se aplicava somente ao processamento automático de dados pessoais, a Diretiva não fez tal distinção e, portanto, foi mais abrangente neste ponto. Além disso, a Diretiva também inaugurou a conceituação de processador e o mecanismo de controle compartilhado de dados pessoais.<sup>104</sup>

O artigo 6º da Diretiva, com base na Convenção 108, traz uma série de princípios que devem ser levados em consideração pelos controladores e operadores quando do tratamento de

---

<sup>102</sup> LYNSEY. Orla. *Op. cit.* pág. 130; USTARAN, Eduardo. *Op. cit.* pág. 55.

<sup>103</sup> UNIÃO EUROPEIA. Diretiva 95/46/CE.

<sup>104</sup> ALSENOY, Brendan Van. *Op. cit.* pág. 276.

dados pessoais, tais como: utilização para finalidades lícitas, explícitas e legítimas que não podem ser alteradas ao longo do tratamento; adequação e pertinência do tratamento de dados para com os fins propostos; exatidão e atualidade dos dados; e conservação dos dados apenas para o período necessário do tratamento. Ademais, no artigo seguinte, são explicitadas as seis hipóteses de tratamento legítimo de dados pessoais, sendo a primeira delas o consentimento inequívoco do titular dos dados.<sup>105</sup>

Por fim, cumpre salientar que a Diretiva demandou a criação no âmbito dos Estados-membros de órgãos independentes, que seriam responsáveis pela fiscalização e regulamentação das normas de proteção de dados pessoais no âmbito interno. Alguns países já dispunham de entidades estruturadas para esses fins, como a Alemanha, uma vez que já contavam com legislações sobre o tema.<sup>106</sup>

No contexto das instituições da União Europeia, a Diretiva também criou, em seu artigo 29, um Grupo de Trabalho de caráter consultivo e independente que ficaria responsável –dentre diversas atribuições –por analisar e dar pareceres à Comissão sobre a uniformidade da aplicação dos direitos de proteção de dados pessoais nos países do bloco, além de aconselhar a Comissão em quaisquer situações que pudessem ter impactos sobre tais direitos.<sup>107</sup> O grupo de trabalho ficou conhecido por sua denominação em inglês *Article 29 Working Party* e permaneceu ativo até a criação do Comitê Europeu de Proteção de Dados, após o advento do GDPR.

### **2.3.4 A caminho do GDPR: a proteção de dados pessoais nas normas primárias da União Europeia**

No tocante às normas primárias da União Europeia deve-se ressaltar que as primeiras versões dos tratados constitutivos não faziam referência à temática dos direitos humanos, uma vez que tinham caráter eminentemente econômico-comercial. Entretanto, ao longo dos anos, diversos casos foram levados ao Tribunal de Justiça da União Europeia, alegando violações aos direitos humanos em áreas de competência legislativa da União Europeia. Em resposta, a corte

<sup>105</sup> Diretiva 95/46/CE. art. 6 e 7º

<sup>106</sup> FUSTER, Gloria González. *Op. cit.* pág. 139. UNIÃO EUROPEIA. Diretiva 95/46/CE. Art. 28(1).

<sup>107</sup> UNIÃO EUROPEIA. Diretiva 95/46/CE. art. 29.

construiu jurisprudência no sentido de considerar a proteção aos direitos humanos como parte dos princípios gerais da União Europeia.<sup>108</sup>

Fuster demonstra essa evolução jurisprudencial do TJUE e afirma que até a década de 60 a corte recusava-se a analisar questões afeitas aos direitos humanos. Três casos foram fundamentais para reverter essa tendência, conforme explica a autora: o caso *Stauder*, de 1969;<sup>109</sup> caso *Internationale Handelsgesellschaft*, de 1970;<sup>110</sup> e caso *Nold II*, de 1974.<sup>111</sup> Ao julgá-los, a corte firmou o entendimento de que os direitos humanos fariam parte dos princípios gerais do direito comunitário e que a identificação desses direitos deveria se dar de acordo com a tradição constitucional dos países-membros, bem como dos tratados internacionais que estes são signatários, a exemplo da Convenção Europeia de Direitos Humanos.<sup>112</sup>

Em 1999, o Tratado da Comunidade Europeia foi alterado para incluir o art. 286, segundo o qual “os atos comunitários relativos à proteção das pessoas singulares<sup>113</sup> em matéria de tratamento de dados de caráter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.”<sup>114</sup> Essa foi, portanto, a primeira menção à proteção de dados pessoais em uma norma primária da União Europeia.

Não obstante a relevância do artigo 286 do Tratado da Comunidade Europeia, o passo mais importante em direção ao reconhecimento do direito de proteção de dados pessoais no direito supranacional foi dado após a aprovação da Carta de Direitos Fundamentais da União Europeia, no ano de 2000. A Carta sintetiza os diversos direitos fundamentais colhidos das tradições constitucionais dos Estados-membros, separando-os em seis seções distintas: dignidade, liberdades, igualdade, solidariedade, direitos dos cidadãos e justiça. Dentro da seção sobre liberdades, em seu artigo 8º, o documento faz o primeiro reconhecimento direto do Direito à Proteção de Dados em um instrumento supranacional, distinguindo-o do Direito à Privacidade (artigo 7º da Carta).<sup>115</sup>

<sup>108</sup> CONSELHO DA EUROPA; UNIÃO EUROPEIA. **Handbook on European Data Protection Law**. 2018 edition. Disponível em: <<https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition#TabPubRelated>>. Acesso em: 11/12/2020. Também nesse sentido: DAL RI, Arno. **A Cidadania Europeia e a Livre Circulação de Pessoas**. In: DAL RI, Arno; OLIVEIRA, Odete de. (Orgs.) *Cidadania e Nacionalidade: efeitos e perspectivas regionais, nacionais e globais*. Ijuí: Unijuí, 2002.

<sup>109</sup> TJUE, C-29/69, Caso *Stauder*, julgado em 12/11/1969.

<sup>110</sup> TJUE, C-11/70, Caso *Internationale Handelsgesellschaft*, julgado em 17/12/1970

<sup>111</sup> TJUE, C-04/73, Caso *Nold II*, julgado em 14/05/1974

<sup>112</sup> FUSTER, Gloria González. *Op. cit.* pág. 167.

<sup>113</sup> Salienta-se que no direito brasileiro “pessoas singulares” corresponde ao termo “pessoa natural”

<sup>114</sup> UNIÃO EUROPEIA. **Tratado da Comunidade Europeia**. Versão consolidada de 2002. Art. 286 (1).

<sup>115</sup> FUSTER, Gloria González. *Op. cit.* pág. 199.

Conforme verifica-se a seguir, a Carta dá força de Direito Fundamental a alguns dos princípios já listados em outros instrumentos anteriores, como a Convenção 108 e a Diretiva 95/46/CE:

- Artigo 8º - 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.<sup>116</sup>

No momento da sua aprovação a Carta tinha somente o caráter de documento político não-vinculativo. Contudo, após a entrada em vigor do Tratado de Lisboa, em 2009, o instrumento legal passou a fazer parte do rol das normas primárias da União Europeia e, conseqüentemente, ganhou caráter plenamente vinculativo a todos os Estados-membros e instituições do bloco.<sup>117</sup> Esse reconhecimento é de extrema importância, pois reforça a competência da União Europeia para legislar sobre Proteção de Dados Pessoais, uma vez que, de acordo com o princípio da competência por atribuição, a União Europeia só pode legislar sobre matérias contidas nos seus tratados constitutivos.<sup>118</sup>

O Tratado de Lisboa também realizou alterações no Tratado de Funcionamento da União Europeia para inserir em seu próprio texto o reconhecimento do direito à proteção de dados, conforme reproduzido a seguir:

- Artigo 16.º (ex-artigo 286.º TCE)
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.<sup>119</sup>

Outrossim, o segundo parágrafo do artigo supracitado faz expressa referência a uma futura norma a ser elaborada no âmbito da União Europeia com o objetivo de regulamentar o direito recém reconhecido, abrindo caminho para a elaboração do GDPR em substituição à

<sup>116</sup> CARTA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Art. 8º.

<sup>117</sup> CONSELHO DA EUROPA; UNIÃO EUROPEIA. *Op. cit.* pág. 28.

<sup>118</sup> OLIVIER, Costa. *Op. cit.* pág. 153.

<sup>119</sup> TFUE. Art. 16.

Diretiva 95/46. Cabe mencionar, ainda, que a redação do artigo 39 do Tratado da União Europeia passou a determinar que o Conselho da União Europeia adotasse uma decisão para regulamentar a proteção de dados pessoais nas atividades de processamento de dados realizados pelos Estados-membros que guardem relação com a Política Externa e de Segurança Comum.<sup>120</sup>

Com relação à jurisprudência do TJUE, o direito à proteção de dados foi reconhecido explícita e autonomamente pela corte somente em 2008, no caso *Productores de Música de España (Promusicae) v Telefónica de España*.<sup>121</sup> Durante o desenrolar do caso, a Promusicae havia colhido evidências de que alguns usuários da provedora de internet Telefónica haviam infringido normas de direitos autorais; entretanto, para iniciar uma ação civil contra os infratores era necessário saber alguns de seus dados pessoais. Por isso, a produtora entrou com uma ação para forçar que a provedora de internet fornecesse tais dados, baseando-se em três Diretivas da União Europeia: sobre comércio eletrônico, direitos autorais e propriedade intelectual.<sup>122</sup>

A corte, ao analisar o caso, decidiu que, tendo em vista que todas as três diretivas mencionadas pela Promusicae deixam claro que seus dispositivos não devem afetar os direitos estabelecidos na Diretiva 95/46, e considerando a Carta de Direitos Fundamentais, não existe qualquer obrigação dos Estados membros em forçar a entrega de dados pessoais de usuários de provedores de internet.<sup>123</sup>

### 2.3.5 A construção legislativa do GDPR

Conforme demonstra Alsenoy, após sua entrada em vigor, a Diretiva 95/46 foi reavaliada em duas oportunidades pela Comissão Europeia, em 2003 e 2007, e em ambas as ocasiões a conclusão foi de que não era necessário nenhum ajuste ou atualização da norma. Contudo, em 2010, um ano após o início da vigência do Tratado de Lisboa, uma nova avaliação considerou que, em razão da emergência de novas tecnologias de informação e comunicação e em face dos aspectos trazidos pela globalização, era preciso uma atualização da Diretiva, ainda que os seus princípios basilares permanecessem inalterados.<sup>124</sup>

---

<sup>120</sup> TUE, Art. 39.

<sup>121</sup> LYNSEY. Orla. *Op. cit.* pág. 89.

<sup>122</sup> TJUE. C-275/06, Caso *Productores de Música de España (Promusicae) v Telefónica de España*. Julgado em 2008.

<sup>123</sup> *Ibid.*

<sup>124</sup> ALSENOY, Brendan Van. *Op. cit.* pág. 279

O relatório feito pela Comissão Europeia em 2010 foi baseado em uma consulta pública realizada no ano anterior em alguns setores específicos, cujos resultados demonstraram a necessidade de uma maior harmonização das normas de processamento de dados pessoais em todos os Estados-membros, além da necessidade da introdução de novos direitos.<sup>125</sup> Sendo assim, o documento apontou a intenção da Comissão de propor ao Parlamento e ao Conselho novos regulamentos para o tema, baseados no comando do Art. 16(2) do TFUE.<sup>126</sup>

As propostas legislativas surgiram um pouco depois da data prevista, em janeiro de 2012, e consistiram em uma nova estrutura normativa de proteção de dados pessoais baseada em duas legislações distintas: um Regulamento sobre a proteção dos indivíduos com respeito ao processamento de dados pessoais e livre movimentação destes dados – que viria a ser o GDPR; e uma Diretiva sobre proteção de dados pessoais nos processamentos realizados pelas autoridades estatais em investigações criminais. A comunicação enviada pela Comissão Europeia ao Parlamento Europeu veio acompanhada de um documento intitulado “*Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*” (em tradução livre: “Protegendo a Privacidade em um Mundo Conectado - Uma Estrutura de Proteção de Dados Europeia para o Século 21”), que serviu para explicar o objetivo da nova estrutura e a necessidade de suas implementações.<sup>127</sup>

No documento, a Comissão explica como – caso aprovada – a nova estrutura normativa daria maior segurança para o tratamento de dados pessoais e adaptaria as normas vigentes às novas necessidades tecnológicas do mundo globalizado. Dentre as inovações estão a introdução do Direito ao Esquecimento, a notificação automática de vazamento de dados, o direito à portabilidade de dados, a obrigatoriedade de designação pelas empresas com mais de 250 funcionários de um *Data Protection Officer (DPO)* para atuar junto às Autoridades Nacionais de Proteção de Dados, dentre outros novos dispositivos.<sup>128</sup>

Após seu recebimento, a Proposta do GDPR passou por um longo período de análise e negociações políticas no Parlamento Europeu, com contribuições de diversos organismos do bloco. As primeiras contribuições vieram do Grupo de Trabalho do Art. 29, que emitiu dois

<sup>125</sup> FUSTER, Gloria González. Op. cit. pág. 241.

<sup>126</sup> *Ibid.*

<sup>127</sup> UNIÃO EUROPEIA. **Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century**. UE: Bruxelas, 2012. Disponível em <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>>. Acesso em 17/12/2020.

<sup>128</sup> *Ibid.*

pareceres, principalmente centrados no debate sobre a definição de dados pessoais, a noção de consentimento e os mecanismos de notificação de vazamento de dados pessoais.<sup>129</sup>

Em outubro de 2013, a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu, responsável por analisar a proposta legislativa do GDPR vinda da Comissão, aprovou o texto com diversas emendas, como por exemplo no que diz respeito ao tamanho das multas administrativas que poderiam ser impostas por descumprimento da norma, o escopo territorial da norma, e a transferência de dados para países terceiros. A proposta com as emendas foi posteriormente levada ao plenário do Parlamento e aprovada por ampla maioria em março de 2014.<sup>130</sup>

Seguindo o processo legislativo de co-decisão, a proposta foi levada posteriormente à análise do Conselho. O Conselho não aceitou integralmente a versão vinda do Parlamento, sugerindo diversas revisões no texto. As principais divergências eram referentes à conceituação de consentimento do titular de dados para o tratamento de dados, ao limite da multa que poderia ser aplicado aos infratores do Regulamento e à responsabilidade dos controladores e operadores.<sup>131</sup> Além disso, outra divergência entre as propostas analisadas surgiu com relação ao mecanismo de cooperação entre as Autoridades de Dados dos Estados-membros no chamado mecanismo “*one-stop shop*”, ou balcão único, em português, que deveria ser coordenado pelo novo Comitê Europeu de Proteção de Dados, órgão que substituiria o Grupo de Trabalho do Artigo 29.<sup>132</sup>

Em junho de 2015, o órgão chegou a um “*general approach*” - uma espécie de acordo político estabelecendo as bases em que se dariam as negociações entre o Conselho e o Parlamento para alcançar a redação final do Regulamento.<sup>133</sup> O passo seguinte foi a instauração de um tríplice, que consiste na formação de uma comissão com representantes do Parlamento, do Conselho e da Comissão para negociarem e chegarem a um acordo final sobre os textos

---

<sup>129</sup> UNIÃO EUROPEIA. **The History of the General Data Protection Regulation**. Disponível em: <[https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en#](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#)>. Acesso em: 18/12/2020.

<sup>130</sup> WILHELM, Ernst-Oliver. **A brief history of the General Data Protection Regulation**. International Association of Privacy Professionals (IAPP). Disponível em: <<https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>> . Acesso em: 18/12/2020.

<sup>131</sup> UNIÃO EUROPEIA. **Orientação Geral do Conselho da União Europeia sobre a Proteção de Dados**. Disponível em: <<https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pt/pdf>>. Acesso em: 18/12/2020.

<sup>132</sup> *Ibid.*

<sup>133</sup> UNIÃO EUROPEIA. **Proteção de dados: Conselho chega a acordo sobre orientação geral**. Disponível em: <<https://www.consilium.europa.eu/pt/press/press-releases/2015/06/15/jha-data-protection/>>. Acesso em: 18/12/2020.

legislativos, uma vez que foram propostas diferentes versões pelos três órgãos. O tríplice iniciou os trabalhos ainda no mês de junho de 2015, e já no mês de dezembro chegou a um acordo para definir a redação final do GDPR.

Dessa forma, após cerca de quatro anos de negociações, em 27 de abril de 2016 o GDPR foi finalmente aprovado. Na ocasião, também foi aprovada a nova Diretiva sobre tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais, que também fazia parte do pacote legislativo proposto pela Comissão em 2012.<sup>134</sup> Ficou definido no art. 99 do GDPR que haveria uma *vacatio legis* de 2 anos e, portanto, seus dispositivos só seriam plenamente aplicáveis a partir do dia 25/05/2018.<sup>135</sup>

Durante o período de *vacatio legis* muitas foram as dúvidas advindas organizações que deveriam se adequar aos novos padrões estabelecidos pelo GDPR para o processamento de dados pessoais. Tais dúvidas não surgiram apenas dentre as empresas que operavam nos Países-membros da União Europeia, mas também em diversas partes do mundo, em razão do escopo de aplicação territorial e os possíveis impactos extraterritoriais trazidos pela norma, elementos que serão elucidados no capítulo seguinte deste trabalho.

Conforme verificou-se ao longo deste capítulo, o atual quadro normativo de Proteção de Dados Pessoais no âmbito europeu não se resume ao Regulamento Geral de Proteção de Dados. Trata-se, em realidade, do resultado de uma longa construção e reconhecimento do conteúdo da Proteção de Dados Pessoais como um Direito Fundamental dos indivíduos. Nesse sentido, torna-se compreensível a posição vanguardista da União Europeia como uma espécie de farol do mundo com relação à temática.

---

<sup>134</sup>UNIÃO EUROPEIA. DIRETIVA (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

<sup>135</sup>GDPR. Art. 99.

### 3 O ÂMBITO DE APLICAÇÃO EXTRATERRITORIAL DO GDPR

Um dos assuntos que mais atraem a atenção das empresas que atuam no setor de Tecnologia da Informação após a entrada em vigor do GDPR é sobre o seu âmbito de aplicação territorial e, conseqüentemente, seus possíveis impactos extraterritoriais.<sup>136</sup> A inquietação entre as empresas tornou-se ainda mais latente à medida que começaram a surgir as primeiras multas pela não conformidade com os dispositivos do Regulamento, como a implementada pela Autoridade de Proteção de Dados da França, de cerca de US\$57 milhões, contra a empresa Google, em janeiro de 2019.<sup>137</sup>

No centro dessa discussão encontra-se o seguinte questionamento: como poderia uma legislação sobre proteção de dados pessoais de um determinado país ou comunidade de países – como é o caso da União Europeia – ter aplicabilidade em terceiros países, sem a celebração de tratados ou acordos internacionais? A resposta para esse questionamento pode ser encontrada no estudo do polêmico fenômeno jurídico da aplicação extraterritorial das normas jurídicas.

Para alguns juristas e historiadores, o fenômeno da extraterritorialidade tem origem no século XIX, na denominada era dos impérios; enquanto para outros, é possível identificá-lo já na antiguidade, ou seja, muito antes da formação dos estados modernos e do próprio conceito de soberania.<sup>138</sup> Fato é que, independentemente de sua origem, a aplicação extraterritorial de normas jurídicas é pauta de importantes debates acadêmicos e jurisprudenciais na atualidade, principalmente após a emergência das novas tecnologias de informação e comunicação, que tornaram possíveis que atos realizados em determinado local pudessem ter efeitos globais.

No intuito de contribuir para esse debate, o presente capítulo será dividido em duas partes. Na primeira parte serão analisados alguns conceitos fundamentais para a compreensão do escopo material do GDPR, como o conceito de dados pessoais e tratamento de dados. Na segunda, serão apresentadas as hipóteses de aplicação territorial e extraterritorial do GDPR bem como o debate existente sua legitimidade e *enforcement*.

<sup>136</sup> Valor Econômico. Regulamento de proteção de dados europeu é alerta ao Brasil. Disponível em: <<https://valor.globo.com/patrocinado/machado-meyer-advogados/inteligencia-juridica/noticia/2019/06/24/regulamento-de-protecao-de-dados-pessoais-europeu-e-alerta-ao-brasil.ghtml>> Acesso em: 03/03/2020. Exame. GDPR e Lei Brasileira de Proteção de Dados desafiam empresas. Disponível em: <[https://exame.abril.com.br/negocios/dino\\_old/gdpr-e-lei-brasileira-de-protecao-de-dados-desafiam-empresas/](https://exame.abril.com.br/negocios/dino_old/gdpr-e-lei-brasileira-de-protecao-de-dados-desafiam-empresas/)> Acesso em: 03/03/2020.

<sup>137</sup> New York Times. Google Is Fined \$57 Million Under Europe's Data Privacy Law. Disponível em: <<https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>> Acesso em: 03/03/2020.

<sup>138</sup> SVANTENSSON, Dan Jerker. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. Apud KASSAN, Shalom. Extraterritorial Jurisdiction in the Ancient World, 29 AM. J. INT'L L. 237, 239-40 (1935).

### 3.1 CONCEITOS ESSENCIAIS DO GDPR

Antes de saber em quais locais o GDPR pode ser aplicado (escopo territorial), é necessário ter a exata noção do objetivo primário da norma e em quais situações ela é aplicável (escopo material). Segundo o artigo 2.1, o regulamento aplica-se a controladores ou operadores que realizam o tratamento de dados pessoais por meios automatizados ou não.<sup>139</sup> Assim como estabelecia a Diretiva 95/46, o próprio regulamento também define o que são dados pessoais, controladores, operadores, e o que é tratamento de dados pessoais, conforme será abordado a seguir.

#### 3.1.1 Dados pessoais

Dados pessoais, segundo o que determina o GDPR, são quaisquer informações relacionadas a uma pessoa natural já identificada ou que possa ser identificada, por referência a elementos identificadores como nome, número de identificação, dados de localização, elementos específicos da identidade física ou social da pessoa, dentre outros exemplos.<sup>140</sup> Nessa conceituação, o GDPR não difere substancialmente da perspectiva seguida pela Diretiva, somente incluindo novas exemplificações.<sup>141</sup>

Ademais, conforme demonstra Ustaran,<sup>142</sup> continuam presentes no GDPR os quatro elementos textuais que constituem o conceito de dados pessoais desde que as primeiras normas sobre o tema foram elaboradas. São eles: (1) “qualquer informação”; (2) “relacionada com”; (3) “pessoa natural”; (4) “identificada ou identificável”. Da análise do primeiro elemento infere-se que qualquer declaração sobre um indivíduo, seja ela objetiva ou subjetiva, pode ser considerada como um dado pessoal. Nesse sentido, a natureza da informação tida como dado pessoal deve ser considerada em seu sentido mais amplo, englobando, por exemplo, informações profissionais ou familiares que sirvam para identificar o indivíduo.<sup>143</sup>

---

<sup>139</sup> GDPR. Art. 2.1.

<sup>140</sup> *Ibid.*, art. 4.1

<sup>141</sup> Diretiva 95/46/CE. Art. 2.a

<sup>142</sup> USTARAN, Eduardo (ed.). **European Data Protection Law and Practice**. New Hampshire: International Association Of Privacy Professionals, 2018. 394 p.; UNIÃO EUROPEIA. Art. 29 Working Party. **Opinion 4/2007 on the concept of personal data**. 2007.

<sup>143</sup> *Ibid.*

Com relação ao segundo elemento, conforme esclarecido em relatório do Grupo de Trabalho do Art. 29,<sup>144</sup> para avaliar se uma determinada informação está relacionada a um indivíduo é imprescindível que sejam atendidos três critérios, quais sejam: o critério elemento, o critério propósito e o critério resultado. O critério elemento avalia se a informação está notoriamente relacionada a um determinado indivíduo, como por exemplo no caso de uma avaliação clínica com a identificação clara de quem é o paciente. Já o segundo critério diz respeito à intenção que se tem de avaliar, considerar ou analisar de qualquer modo o indivíduo por meio da informação coletada. No mesmo exemplo da avaliação clínica, o propósito dos dados coletados seria obter um panorama do estado de saúde do indivíduo. Por fim, o terceiro critério é atendido quando o processamento da informação tem como resultado qualquer impacto sobre os direitos e interesses do indivíduo.<sup>145</sup>

No tocante ao terceiro elemento (“pessoa natural”), o regulamento deixa para cada legislação nacional definir e aplicar seu próprio conceito de pessoa natural. Entretanto, conforme descrito no Considerando 27 do GDPR, resta claro que dados pessoais de pessoas falecidas ou de pessoas jurídicas não são abrangidos pelo escopo de aplicação material da norma.

Quanto ao quarto elemento (“identificado ou identificável”), há que se considerar identificável um indivíduo que pode ser reconhecido pela análise conjunta dos elementos informativos disponíveis a seu respeito.<sup>146</sup> Um exemplo pelo qual um dado pessoal pode identificar um indivíduo é por meio da utilização do endereço de IP (*Internet Protocol Address*), que pode informar a localização e o comportamento na rede de uma máquina e, por trás dela, de um usuário.

Neste ponto, é importante ressaltar que o GDPR faz uma distinção entre dados pessoais pseudonimizados e dados anonimizados, conforme exposto no seu considerando 26. Os dados pseudonimizados são aqueles que passam por um processo pelo qual as informações identificadoras de uma determinada pessoa, como o nome, são substituídas por códigos ou pseudônimos. Dessa forma, os dados deixam de poder ser atribuídos a um titular específico sem que sejam utilizadas informações suplementares.<sup>147</sup>

<sup>144</sup> UNIÃO EUROPEIA. Art. 29 Working Party. **Opinion 4/2007 on the concept of personal data**. 2007.

<sup>145</sup> *Ibid.*

<sup>146</sup> *Ibid.*

<sup>147</sup> FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. *International Data Privacy Law*. Vol. 10, n.1. Fevereiro de 2020.págs. 11–36. <https://doi.org/10.1093/idpl/ipz026>

De acordo com o GDPR, para que os dados sejam considerados pseudonimizados, é necessário que as chaves de identificação, que são utilizadas para reverter essa operação, sejam mantidas separadamente e sujeitas a medidas técnicas específicas.<sup>148</sup> O processo de pseudonimização é exigido pelo Regulamento a partir do momento em que a identificação do titular dos dados não é mais necessária para os fins que foram autorizados, à luz do princípio da necessidade, previsto no art. 5º, 1, b e art. 32, 1, a, da norma.<sup>149</sup>

Os dados pessoais pseudonimizados continuam sujeitos às regras do GDPR, o que não ocorre com os dados anonimizados.<sup>150</sup> O esclarecimento dessa questão foi um importante avanço do GDPR com relação à Diretiva 95/46, uma vez que a falta de clareza sobre a aplicabilidade ou não dos regramentos aos dados pseudonimizados gerava debates na literatura e, consequentemente, insegurança jurídica.<sup>151</sup>

Segundo o Considerando n. 26 do Regulamento, os dados anonimizados são aqueles que, após procedimentos técnicos específicos, se tornam impossíveis de serem identificados. A impossibilidade de identificação, nesse caso, é tratada em duas perspectivas: quando o processo de reversão da anonimização for, de fato, tecnicamente impossível ou quando for razoavelmente impraticável pelos custos e o tempo necessário para a reversão da anonimização.<sup>152</sup> Também nesse sentido, é o entendimento do TJUE que, no caso *Breyer vs. República Federal da Alemanha* (C-582/14), considerou que o risco de identificação de um indivíduo é insignificante caso seja necessário um esforço desproporcional em termos de tempo, custos e mão de obra.<sup>153</sup>

O caso da empresa dinamarquesa de serviços de táxi “Taxa 4x35” serve para ilustrar uma aplicação prática do debate entre a diferença da pseudonimização e anonimização. Em outubro de 2018, a Agência de Proteção de Dados da Dinamarca identificou que a empresa guardava dados dos seus usuários por 5 anos, após a data que os usuários utilizavam o aplicativo pela última vez, infringindo a determinação do GDPR de utilização de dados somente para os fins e pelo tempo necessário. A empresa acreditava que esse dispositivo da norma não lhe seria aplicável, uma vez que, após 2 anos de armazenamento, ela excluía os nomes dos usuários que

---

<sup>148</sup> GDPR. Art. 4.5

<sup>149</sup> *Ibid*, art. 32º, 1, a.

<sup>150</sup> ELLIOT, Mark; MACKEY, Elaine; MOURBY, Miranda; et al. **Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the UK.** Computer Law & Security Review. Volume 34, nº2. 2018. Pages 222-233. ISSN 0267-3649. <https://doi.org/10.1016/j.clsr.2018.01.002>.

<sup>151</sup> Shabani, M., Borry, P. **Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation.** Eur J Hum Genet 26, 149–156 (2018). <https://doi.org/10.1038/s41431-017-0045-7>

<sup>152</sup> GDRR, Considerando nº 26.

<sup>153</sup> TJUE. C-582/14. *Caso Breyer./Federal Republic of Germany*. Julgado em 19 de outubro de 2016.

estavam relacionados aos dados das viagens. Com isso, acreditava-se estar anonimizando os dados pessoais dos usuários. Contudo, a Agência Dinamarquesa considerou que esse suposto processo de anonimização realizado pela empresa era, na realidade, inadequado, pois matinha outros dados relevantes dos usuários, como seus números de telefone, que poderiam facilmente torná-los identificáveis novamente.<sup>154</sup>

Dessa forma, a partir do exposto, conclui-se que são abrangidos pelo escopo material do GDPR os dados pessoais identificados ou identificáveis; excluindo-se, portanto, os que foram totalmente anonimizados.

Além dos casos de dados anônimos, o Regulamento também lista quatro outras hipóteses em que o tratamento de dados não se sujeita aos seus regramentos. São elas: tratamentos efetuados no exercício de atividades não sujeitas à aplicação do direito da União Europeia; tratamentos efetuados pelos Estados-membros no exercício de atividades abrangidas pelo âmbito de aplicação da política externa e de segurança comum da UE; tratamentos efetuado por uma pessoa no exercício de atividades exclusivamente pessoais ou domésticas; e tratamentos efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.<sup>155</sup>

É importante ressaltar que, como já dispunha a Diretiva 95/46, o Regulamento dá maior proteção a uma categoria especial de dados pessoais, sobre os quais o tratamento é, em regra, proibido, ressalvados alguns casos. Dentre os dados considerados sensíveis estão listados aqueles que dizem respeito à origem racial ou étnica dos indivíduos; às opiniões políticas; às convicções religiosas ou filosóficas; à filiação sindical; a condições de saúde do indivíduo; e à vida ou orientação sexual de uma pessoa. Além disso, é vedado o tratamento de dados genéticos e dados biométricos utilizados para identificar um indivíduo de forma inequívoca.<sup>156</sup>

Os conceitos de dados genéticos, biométricos e dados relativos à saúde não estavam presentes na Diretiva 95/46, sendo uma inovação do regulamento para se adequar às novas tecnologias e meios de tratamentos de dados<sup>157</sup>

<sup>154</sup> UNIÃO EUROPEIA. **Data anonymization and GDPR compliance: the case of Taxa 4x35**. Disponível em: <<https://gdpr.eu/data-anonymization-taxa-4x35/?cn-reloaded=1>> Acesso em: 17/08/2020.

<sup>155</sup> GDPR. Art. 2º.2.

<sup>156</sup> GDPR. Art. 9.1

<sup>157</sup> MARKKULA, Jouni; ROHUNEN, Anna; TIKKINEN-PIRI, Christina. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. **Computer Law & Security Review**, [S.L.], vol. 34, nº. 1, , pág. 134-153, fev. 2018. <https://doi.org/10.1016/j.clsr.2017.05.015>

Alguns autores, como Purtova<sup>158</sup>, criticam o conceito de proteção de dados pessoais estabelecido no GDPR, alegando que o conceito é muito flexível e amplo, podendo levar, no futuro, ao que a autora chama “*the law of everything*”. Após analisar a interpretação dos órgãos de proteção de dados e do próprio Tribunal de Justiça da União Europeia, a autora conclui que, devido à vagueza e abrangência dos termos utilizados, qualquer informação pode vir a se tornar um dado pessoal ao estar relacionada com uma pessoa identificada ou identificável.<sup>159</sup> Tal fenômeno poderia levar, para a autora, a uma falta de efetividade da norma, por sua demasiada abrangência.

Por outro lado, apesar de concordar com a afirmação de que há uma grande expansão do escopo material do GDPR e das normas de proteção de dados em geral, Brkan afirma que tal expansão ainda não representa ameaça a outros direitos e interesses de indivíduos e empresas.<sup>160</sup> Tal discussão é de grande profundidade e ultrapassa os objetivos deste trabalho, razão pela qual passaremos à análise do conceito de tratamento de dados pessoais.

### 3.1.2 O processo de tratamento de dados pessoais

O conceito de tratamento de dados pessoais encontra-se definido no art. 4.2 do GDPR como “uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados.”<sup>161</sup> O mesmo artigo ainda enumera uma série de hipóteses consideradas como tratamento de dados pessoais, como o recolhimento dos dados, o registro, a estruturação, a divulgação etc. Tal definição segue, em linhas gerais, a conceituação já estabelecida na Diretiva 95/46, apesar de conter novos exemplos em razão da evolução da realidade tecnológica da sociedade.

Como se observa, o artigo 4.2 especifica que o tratamento de dados pessoais pode ser feito por meios automatizados ou não. Entretanto, é notório que, em tempos de *Big Data*, a maioria do tratamento de dados, até mesmo das menores companhias, é realizada por meios automatizados, variando somente a complexidade dos sistemas utilizados. Desse modo, ainda que o tratamento de dados pessoais efetuados por determinado controlador ou processador seja

<sup>158</sup> PURTOVA, Nadezhda. **The law of everything. Broad concept of personal data and future of EU data protection law.** Law, Innovation and Technology. Volume 10, n. 1. Londres: 2018.

<sup>159</sup> *Ibid.*

<sup>160</sup> BRKAN, Maja. The Unstoppable Expansion of the EU Fundamental Right to Data Protection. **Maastricht Journal Of European And Comparative Law**, [S.L.], v. 23, n. 5, p. 812-841, out. 2016. SAGE Publications. <http://dx.doi.org/10.1177/1023263x1602300505>.

<sup>161</sup> GDPR, art. 4.2

executado inteiramente sem a intervenção humana – por meio de uma inteligência artificial, por exemplo–, o Regulamento não o isenta da responsabilidade pelo tratamento.<sup>162</sup> A título de ilustração, uma companhia como a *Google Inc* não pode ser isentada de sua responsabilidade por eventual utilização ilegal de dados pessoais por alegar que tal procedimento foi realizado integralmente por alguma tecnologia de Inteligência Artificial, ou seja, sem a ingerência humana.

Uma vez que os dados são classificados como pessoais, segundo o conceito apresentado no tópico anterior, o seu tratamento só será lícito se estiver dentro de uma das situações estabelecidas no art. 6º e, além disso, se estiver de acordo com os princípios do art. 5º.<sup>163</sup> Apesar de não ser o objetivo deste trabalho analisar exaustivamente esses requisitos, cabe tecer algumas considerações para a melhor compreensão do escopo material do Regulamento.

O art. 6º do GDPR apresenta um rol com seis possibilidades pelas quais o tratamento de dados pessoais é considerado legal. Mesmo não existindo qualquer hierarquia entre as bases legais que permitem o tratamento de dados pessoais, algumas dessas hipóteses fomentaram um maior debate doutrinário no que diz respeito à sua exata delimitação conceitual. É o caso, por exemplo, da realização do tratamento de dados pessoais com fundamento no consentimento do titular dos dados.<sup>164</sup>

O Considerando 32 do regulamento explica que o consentimento do titular deve se dar por meio de um ato positivo e claro, e este ato deve ser maneira livre, específica, informada e inequívoca.<sup>165</sup> Portanto, a mera omissão ou inércia do titular dos dados pessoais com relação ao consentimento não implica em uma permissão para o tratamento dos seus dados pessoais.

Para evitar interpretações conflitantes ou expansivas sobre o que pode ser compreendido como consentimento, nos termos do GDPR, o CEPD emitiu uma diretriz sobre o assunto, em maio de 2020. Segundo o documento, o consentimento somente pode ser base para o tratamento de dados de um indivíduo quando a este é oferecido o pleno controle e a opção genuína de aceitar ou não os termos apresentados pelo controlador.<sup>166</sup> Nesse sentido, para cada finalidade que o controlador utilizará os dados do titular é necessário que haja um

<sup>162</sup> SHARMA, Sanjay. **Data Privacy and GDPR Handbook**. Hoboken: John Wiley & Sons, 2020. 496 p.

<sup>163</sup> GDPR, Art. 5º e 6º.

<sup>164</sup> KOTSCHY, Waltraut. Article6. Lawfulness of processing. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation (GDPR): a commentary**. Oxford: Oxford University Press, 2020. p. 329.

<sup>165</sup> *Ibid*, Considerando 32.

<sup>166</sup> UNIÃO EUROPEIA. Guidelines 05/2020 on consent under Regulation 2016/679. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf)>. Acesso em: 20/08/2020.

consentimento. O exemplo trazido pelo CEPD é o caso de uma plataforma de *streaming* que obtém o consentimento de seus clientes para coletar os seus dados pessoais no intuito de oferecer opções de filmes personalizadas. Dessa forma, caso a mesma plataforma decida compartilhar esses dados com terceiros para fins de propaganda, por exemplo, ela deverá obter um novo consentimento dos titulares dos dados pessoais e estes deverão ter a opção de aceitar ou não.<sup>167</sup>

Além do consentimento do titular como fundamento para o tratamento de dados pessoais, existem outras cinco hipóteses legais que permitem tal atividade. São elas: quando o tratamento for necessário para a execução de um contrato ou para diligências pré-contratuais; quando for necessário para o cumprimento de uma obrigação jurídica a qual o responsável pelo tratamento está sujeito; para a proteção de interesses vitais do titular dos dados ou de outra pessoa; para o exercício de funções de interesses público ou de autoridade pública; ou quando o tratamento for necessário para efeito de interesses legítimos do responsável pelo tratamento de dados, exceto quando sobre esses interesses prevaleçam os direitos fundamentais dos titulares dos dados, em especial quando o titular for criança ou adolescente.<sup>168</sup>

De todas as hipóteses mencionadas, o legítimo interesse é apontado como o mais ambíguo.<sup>169</sup> No intuito de facilitar a interpretação desse termo, o legislador europeu consignou nos Considerandos 47 e 48 do GDPR algumas explicações a respeito. Nos termos do Considerando 47, “poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento”.<sup>170</sup> De qualquer forma, o interesse legítimo deve ser analisado em contraponto ao que seria razoavelmente esperado pelo titular dos dados quanto ao tratamento dos seus dados pessoais.<sup>171</sup>

O Grupo de Trabalho do Artigo 29 já havia se posicionado a respeito do conceito de legítimo interesse, ainda na vigência da Diretiva, por meio de uma opinião. Nesse documento, o órgão adverte que o legítimo interesse do responsável pelo tratamento de dados deve ser ponderado frente aos direitos fundamentais do titular da seguinte forma:

---

<sup>167</sup> *Ibid.*

<sup>168</sup> GDPR, Art. 6º.

<sup>169</sup> REINO UNIDO. Information Commissioner's Office. **Legitimate interests**. Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> Acesso em: 21/08/2020.

<sup>170</sup> GDPR, Considerando 47.

<sup>171</sup> *Ibid.*

Os interesses legítimos do controlador, quando menores e pouco convincentes, só podem, em geral, prevalecer sobre os interesses e direitos dos titulares dos dados quando o impacto sobre esses direitos e interesses seja ainda mais trivial. Por outro lado, interesses legítimos importantes e convincentes podem, em alguns casos e sujeitos a salvaguardas e medidas, justificar até mesmo uma intromissão mais significativa na privacidade ou outro direito do indivíduo.<sup>172</sup>

Em conclusão, verifica-se que o amplo conceito de tratamento de dados trazido pelo Regulamento combinado com a alta velocidade e volume com que atualmente os dados são processados faz com que o escopo material do GDPR englobe diversos setores da economia. Dessa forma, os responsáveis pelo tratamento dos dados pessoais devem estar atentos às possibilidades e bases legais pelas quais realizam suas atividades.

### 3.1.3 Controladores e Processadores de dados pessoais segundo o GDPR

O controlador ou responsável pelo tratamento dos dados pessoais é “a pessoa natural ou jurídica, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais”.<sup>173</sup> Trata-se, portanto, daquele que decide, em última análise, para quais propósitos os dados coletados servirão, por quanto tempo serão guardados, para quem serão compartilhados e quando poderão ser excluídos. Embora tal definição seja, fundamentalmente, a mesma da Diretiva 95/46, a aplicação desse conceito tornou-se cada vez mais sinuosa ao longo do tempo, à medida que a existência de conglomerados econômicos se tornou mais recorrente – o que torna mais complexo a identificação do real responsável pelo tratamento dos dados.<sup>174</sup>

Já o conceito de operador está conscrito no art. 4.8 do Regulamento, segundo o qual trata-se de qualquer “pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes”.<sup>175</sup> A tradução do GDPR para o português de Portugal trouxe o termo “subcontrante” para indicar o operador. O termo, por si só, sugere a relação jurídica existente entre o controlador e o operador no tratamento de dados pessoais: enquanto o primeiro é responsável por determinar a forma e

<sup>172</sup> UNIÃO EUROPEIA. **Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)>. Acesso em 22/08/2020. pág. 30.

<sup>173</sup> GDPR. Art. 4 (7).

<sup>174</sup> USTARAN, Eduardo (ed.). **European Data Protection Law and Practice**. New Hampshire: International Association Of Privacy Professionals, 2018. p. 84.

<sup>175</sup> GDPR. Art. 4.8

o propósito do tratamento dos dados, o segundo é subcontratado para realizar a operacionalização técnica daquilo que foi indicado pelo controlador.

A abrangência conceitual do termo “controlador” faz com que tanto o setor público quanto o privado sejam potencialmente afetados pelo Regulamento na consecução de suas atividades – os exemplos podem variar de um pequeno comércio local ou uma escola até uma grande companhia de tecnologia de dados ou organizações governamentais. Além disso, por ter maior poder de decisão sobre a utilização dos dados pessoais, o controlador é aquele que carrega as maiores responsabilidades no cumprimento das regras estabelecidas no GDPR.<sup>176</sup>

Cumprido ressaltar, à luz da interpretação dada pelo Parecer nº 1/2010 do Grupo de Trabalho do art. 29, que no contexto de uma organização, seja ela empresarial ou não, a responsabilidade pelo tratamento de dados pessoais não deve recair sobre um funcionário específico, mas sim sobre a entidade como um todo, muito embora conste no texto do GDPR que o controlador pode ser uma pessoa natural ou jurídica.<sup>177</sup>

De acordo com o art. 4.7, o controlador pode agir tanto individualmente como em conjunto com outras organizações. Nesse último caso, deve haver um acordo que sirva para repartir as obrigações entre os corresponsáveis pelo tratamento de dados, segundo o art. 26 do GDPR. Esse é o caso, por exemplo, de conglomerados que detêm diversas empresas e que podem, eventualmente, compartilhar informações entre elas. Entretanto, cabe ressaltar que o mero compartilhamento de dados pessoais entre diferentes instituições não faz, por si só, com que estas sejam consideradas como co-controladoras; é preciso que haja uma coordenação entre elas para um propósito comum.<sup>178</sup>

Pode-se tomar como exemplo um determinado indivíduo que decide contratar uma agência de turismo para planejar suas férias. Para realizar as reservas necessárias, a agência coleta os dados deste cliente e repassa para a uma companhia aérea, para um hotel e para um parque de diversões. Neste caso, cada uma das diferentes pessoas jurídicas envolvidas terão o mesmo conjunto de dados pessoais, contudo os utilizarão para diferentes propósitos. Dessa forma, não estará caracterizada a corresponsabilidade entre as empresas, mas sim a responsabilidade individual de cada uma pela maneira como utilizam os dados recebidos.<sup>179</sup>

<sup>176</sup> WELFARE, Damien; CAREY, Peter. Territorial Scope and Terminology. In: CAREY, Peter (ed.). **Data Protection: a practical guide to uk and eu law**. 5. ed. Oxford: Oxford University Press, 2018. Cap. 1. p. 1-32.

<sup>177</sup> UNIÃO EUROPEIA. **Parecer nº. 1 de 2010 do Grupo de Trabalho do Artigo 29 sobre o conceito de controlador e processador**. Bruxelas: UE, 2010. pág. 15.

<sup>178</sup> USTARAN, *Op. cit.* pág. 87

<sup>179</sup> *Ibid.*

Apesar de a responsabilidade pelo tratamento de dados recair primariamente ao controlador, o Regulamento também instituiu deveres específicos para os operadores, tais como o de manter o registro de todas as categorias de dados tratados para fins de verificação das autoridades de controle; implementar medidas técnicas e organizacionais específicas para garantir a segurança do processamento; notificar o controlador sobre eventuais vazamentos de dados; dentre outros.<sup>180</sup> Contudo, conforme esclarece o CEPD, mesmo que exista certa margem de discricionariedade na atuação do operador, este deve exercer suas atividades estritamente de acordo com as orientações recebidas pelo controlador, sob pena de se colocar em pé de igualdade com o controlador e, assim, ter que arcar com maiores responsabilidades.<sup>181</sup>

A relação entre o controlador e o operador, de acordo com o que estabelece o art. 28.3 do GDPR, deve ser necessariamente regulada por um contrato escrito, que deve conter informações sobre: o objeto, a duração, a natureza e a finalidade do tratamento; os tipos de dados que serão tratados e a categoria dos titulares dos dados; e os direitos e obrigações de ambas as partes. Antes de firmar o contrato com o operador, entretanto, cumpre ao controlador certificar-se de que a empresa contratada detém todos os meios físicos e operacionais necessários para dar a devida segurança e sigilo ao tratamento de dados, o que pode variar de acordo com a natureza, a extensão e a finalidade dos procedimentos. Tal avaliação se dá por meio da elaboração de um *risk assessment* ou avaliação de risco, em tradução livre.<sup>182</sup>

### 3.2. FUNDAMENTOS TEÓRICOS DA APLICAÇÃO EXTRATERRITORIAL DO GDPR

Conforme apontado anteriormente, o presente trabalho pretende investigar as hipóteses de aplicação territorial e extraterritorial estabelecidas no GDPR. Além disso, pretende-se, sob uma perspectiva crítica, levantar o debate doutrinário existente sobre a legitimidade do fenômeno da extraterritorialidade no caso do GDPR. Para tanto, serão abordados nos próximos subcapítulos os principais fundamentos teóricos que dão suporte à aplicação extraterritorial do Regulamento, iniciando pela jurisdição.

---

<sup>180</sup> UNIÃO EUROPEIA. **Handbook on European data protection law**. Disponível em: <<https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1>>. Acesso em: 27/02/2021. pág. 204.

<sup>181</sup> UNIÃO EUROPEIA. **Diretrizes 07/2020 sobre os conceitos de controlador e processador de dados no GDPR do Comitê Europeu de Proteção de Dados**. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_202007\\_controllerprocessor\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf)>. Acesso em: 27/02/2020. pág. 4.

<sup>182</sup> *Ibid.*

### 3.2.1 Jurisdição

Durante muito tempo, o conceito de jurisdição esteve estreitamente ligado aos conceitos de território e soberania.<sup>183</sup> Entretanto, com avanço da globalização e o surgimento de novas tecnologias da informação e comunicação, o elo entre essa tríade de conceitos tornou-se cada vez mais flexível.<sup>184</sup> Isso porque, dentro do atual contexto da era digital, as fronteiras físicas, que antes simbolizavam a soberania e o poderio dos Estados modernos, perdem espaço<sup>185</sup> e dão lugar a uma resignificação do papel do Estado junto a outros atores globais emergentes.<sup>186</sup>

Seguindo a visão tradicional do direito internacional público, que vincula a jurisdição exclusivamente à soberania estatal, autores brasileiros como Accioly, Casella e Silva afirmam que a jurisdição é um direito dos Estados exercido no seu território e sobre sua população permanente.<sup>187</sup> Também nesse sentido, Rezek reitera que sobre o seu território, o Estado exerce jurisdição geral e exclusiva, ou seja, tem jurisdição legislativa, administrativa e jurisdicional com exclusividade.<sup>188</sup>

A doutrina estrangeira, por sua vez, divide o conceito de jurisdição em três categorias distintas: a jurisdição prescritiva, a jurisdição adjudicativa e a jurisdição executiva.<sup>189</sup> Ryngaert explica que a jurisdição prescritiva diz respeito à capacidade de tornar suas leis, atos administrativos ou regulamentos aplicáveis a todas as atividades e relações jurídicas realizadas em determinado território. Já a jurisdição adjudicativa, por sua vez, pode ser conceituada como a competência do Estado em sujeitar pessoas ou coisas ao julgamento de suas cortes ou

<sup>183</sup> BUXBAUM, Hannah L. Territory, Territoriality, and the Resolution of Jurisdictional Conflict (2009). Articles by Maurer Faculty. 132. pág. 11.

<sup>184</sup> *Ibid.*

<sup>185</sup> JOHNSON, David Reynold; POST, David G. **Law and Borders - the Rise of Law in Cyberspace**. Stanford Law Review. Vol. 48, p. 1367. Stanford: 1996, Disponível em: <<https://ssrn.com/abstract=535> or <http://dx.doi.org/10.2139/ssrn.535>> Acesso em: 27/02/2021.

<sup>186</sup> CZERNIAWSKI, Michal; HERT, Paul de. **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**. *International Data Privacy Law*. Vol. 6, No. 3. Oxford: Oxford University Press, 2016.

<sup>187</sup> ACCIOLY, Hildebrando; CASELLA, Paulo Borba; SILVA, G E. do Nascimento e. **Manual de Direito Internacional Público**. 20ª edição. São Paulo: Saraiva, 2012. pág. 343.

<sup>188</sup> REZEK, Francisco. **Direito Internacional Público: curso elementar**. 13ª edição. São Paulo: Saraiva, 2011. pág. 193.

<sup>189</sup> MENTHE, Darrel C. **Jurisdiction in Cyberspace: A Theory of International Spaces**. 4 Mich. Telecomm. & Tech. L. Rev. 69. (1998). Disponível em: <<http://repository.law.umich.edu/mttlr/vol4/iss1/3/>>. Acesso em: 27/02/2021. Também nesse sentido: ALSENOY, Brendan Van. **Reconciling the (extra)territorial reach of the GDPR with public international law**. Gert VERMEULEN & Eva LIEVENS (eds.). Transatlantic tensions, EU surveillance, and big data. Maklu: 2017. pág. 77.

tribunais, sejam judiciais ou administrativos. Por fim, a jurisdição executiva relaciona-se com a competência do Estado para compelir o cumprimento ou punir o descumprimento de suas leis, atos administrativos ou decisões judiciais.<sup>190</sup>

Tendo em vista que o presente trabalho tem como objetivo investigar a aplicação extraterritorial do GDPR, será dado enfoque à categoria de jurisdição prescritiva, ou seja, somente ao alcance geográfico das leis dos Estados.<sup>191</sup> Ademais, seguindo a mesma redução metodológica adotada por Taylor,<sup>192</sup> no presente trabalho as ações da União Europeia serão igualadas a ações estatais, até mesmo porque, conforme argumenta a autora, a União Europeia deve seguir o costume internacional no que se refere à jurisdição da mesma forma que os demais Estados.<sup>193</sup>

No que tange à jurisdição prescritiva, são seis os critérios de conexão mais citados pela doutrina que servem para dar embasamento jurídico ao exercício da jurisdição de um Estado: o critério da territorialidade subjetiva, da territorialidade objetiva, da nacionalidade (ativa e passiva), da proteção, e da universalidade.<sup>194</sup> A territorialidade subjetiva é o critério mais utilizado pelas legislações nacionais e se refere ao poder dos estados de regulamentar as atividades ocorridas dentro do seu próprio território. Para alguns autores, reafirma-se, esse é o único critério legítimo do exercício da jurisdição estatal.<sup>195</sup>

A territorialidade objetiva, por seu turno, está relacionada às ações ocorridas fora do território do Estado em análise, mas cujos efeitos são sentidos internamente.<sup>196</sup> Menthe exemplifica a territorialidade objetiva com o caso hipotético de um atirador localizado na parte canadense de Niagara Falls que acerta uma pessoa localizada no outro lado da fronteira com os Estados Unidos. Nesse caso, o ato ocorreu no Canadá, mas os efeitos foram sentidos nos EUA e, portanto, segundo esse critério, os EUA teriam jurisdição para legislar sobre tais atos.<sup>197</sup> É

<sup>190</sup> RYNGAERT, Cedric. **Jurisdiction in International Law**. 2ª edição. Oxford University Press: Oxford, 2015. p. 9-10

<sup>191</sup> RYNGAERT, Cedric. *Op. cit.* pág. 10

<sup>192</sup> TAYLOR, Mistale. **Permissions and Prohibitions In Data Protection Jurisdiction**. Brussels Privacy Hub Working Paper. Vol. 2, nº6. Maio de 2016. pág. 5

<sup>193</sup> TJUE. C-366/10. Caso *Air Transport Association of America and Others v. Secretary of State for Energy and Climate Change*. Julgado em 2010. Parágrafos 101 e 123.

<sup>194</sup> MENTHE, Darrel C. *op. cit.* pág. 71. TAYLOR, Mistale. *Op. cit.* pág. 3. BELETSKY, Roman. **Critical assessment of the extraterritoriality of the EU General Data Protection Regulation**. University of Helsinki: Helsinki, 2019. pág. 12.

<sup>195</sup> MENTHE, Darrel C. *Op. cit.* pág. 72.

<sup>196</sup> LEE, Sang Woo. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing**. Tese de Doutorado. China University of Political Science and Law: Pequim, 2018. pág. 181.

<sup>197</sup> MENTHE, Darrel C. *Op. cit.* pág. 72.

com base nesse critério que foi elaborada a chamada teoria dos efeitos, que será melhor elucidada adiante neste trabalho por ter fortes implicações para o GDPR.

Com relação ao critério da nacionalidade, deve-se pontuar que, segundo elucida Moura, esse fenômeno encontra suas raízes no pensamento de Pasquale Stanislao Mancini, um dos grandes teóricos do direito internacional privado no século XIX. Mancini desenvolveu seus estudos no contexto do período do *risorgimento* em que, pautados em elementos identitários comuns, tentava-se criar um ideal de nacionalidade que servisse à união dos povos italianos, então divididos em pequenos reinos.<sup>198</sup>

Nesse sentido, Mancini advoga “que a Nação é a que deveria ocupar o papel de interlocutor no direito internacional, pois esta seria o verdadeiro sujeito do ordenamento internacional, ente real e permanente, criado pela história e não pela política como seria o Estado.”<sup>199</sup> A centralidade do critério da nacionalidade para o pensamento de Mancini também o faz concluir que “direito civil privado é pessoal e nacional e, como tal, protege e acompanha a pessoa também fora da sua pátria.”<sup>200</sup>

Dentro de uma perspectiva analítica, o critério da nacionalidade divide-se entre passiva e ativa. A primeira diz respeito ao exercício de jurisdição de um Estado sobre seus nacionais, mesmo quando estejam fora do seu território.<sup>201</sup> Esse tipo de critério é amplamente utilizado nas legislações penais para determinar a lei aplicável aos crimes ocorridos no exterior.<sup>202</sup> Já a nacionalidade passiva baseia-se na nacionalidade da própria vítima para determinar a jurisdição aplicável. Trata-se de uma vertente do princípio da nacionalidade que é amplamente rejeitada doutrina e jurisprudência por ser vista como uma das bases mais agressivas de jurisdição extraterritorial.<sup>203</sup>

No mesmo norte, o princípio da proteção é um dos critérios mais controversos para o embasamento da jurisdição dos Estados. Segundo esse princípio, um Estado está autorizado a legislar sobre atos que podem ferir seus interesses vitais, mesmo que cometidos externamente.<sup>204</sup> Historicamente, é utilizado por países como os Estados Unidos para

---

<sup>198</sup> MOURA, Aline Beltrame de. **O Direito Internacional Privado entre a Nacionalidade de Mancini e a Cidadania da União Europeia**. Revista Eletrônica Direito e Política, v. 7, pág. 1058-1084, 2012.

<sup>199</sup> MOURA, Aline Beltrame de. **O critério de conexão da nacionalidade na doutrina e na legislação de direito internacional privado brasileiro (1863-1973)**. SEQUÊNCIA (UFSC), v. 39, 2018. pág. 198.

<sup>200</sup> *Ibid.* pág. 200.

<sup>201</sup> RYNGAERT, Cedric. *Op. cit.* pág. 104.

<sup>202</sup> *Ibid.*

<sup>203</sup> *Ibid.* pág. 110.

<sup>204</sup> MENTHE, Darrel C. *Op. cit.* pág. 74.

implementar embargos a nações estrangeiras e, dessa forma, enseja amplo debate na comunidade internacional.<sup>205</sup>

Por fim, o critério da universalidade está umbilicalmente ligado à proteção das normas de *Jus Cogens* que, segundo o art. 53 da Convenção de Viena sobre o Direito dos Tratados, são conceituadas como “uma norma imperativa de Direito Internacional geral aceita e reconhecida pela comunidade internacional dos Estados como um todo, como norma da qual nenhuma derrogação é permitida e que só pode ser modificada por norma ulterior de Direito Internacional geral da mesma natureza.”<sup>206</sup> A universalidade permite que um Estado possa ter jurisdição extraterritorial sobre atos que atentem contra o *Jus Cogens*, sem haver qualquer conexão com o território onde o fato ocorreu.<sup>207</sup>

Com exceção da territorialidade subjetiva, todos os demais critérios apresentados acima são aventados pela doutrina como formas de justificar ou dar legitimidade à aplicação extraterritorial de normas jurídicas.<sup>208</sup> Entretanto, o tema ainda é polêmico e torna-se ainda mais complexo quando mais de um Estado alega ter jurisdição sobre determinada matéria, principalmente se tal matéria tem caráter internacional, como é o caso das atividades exercidas online. A doutrina estrangeira denomina tal fenômeno como *jurisdictional overlap*<sup>209</sup>, em tradução livre, sobreposição de jurisdições. Esse fenômeno pode dar causa não só a conflitos de ordem jurídica como também econômica e, até mesmo, política.

### 3.2.2 Jurisdição Extraterritorial: perspectiva histórica e definição

Tema central para este trabalho e imprescindível para a análise da aplicação extraterritorial do GDPR é o estudo do fenômeno da jurisdição extraterritorial ou da extraterritorialidade, como preferem alguns doutrinadores. A discussão sobre a extraterritorialidade ganha força na medida em que, a partir do século XX, a hegemonia do

<sup>205</sup> LOHMANN, Sacha. **Extraterritorial U.S. Sanctions**. SWP Comment. nº 5. Fev. 2019. Disponível em: <<https://www.swp-berlin.org/10.18449/2019C05/>> Acesso em: 27/02/2021.

<sup>206</sup> BRASIL. DECRETO Nº 7.030, DE 14 DE DEZEMBRO DE 2009. Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66.

<sup>207</sup> MENTHE, Darrel C. *Op. cit.* pág. 72

<sup>208</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. **A EXTRATERRITORIALIDADE DO REGIME GERAL DE PROTEÇÃO DE DADOS PESSOAIS DA UNIÃO EUROPEIA: MANIFESTAÇÕES E LIMITES**. 2018. 356 f. Tese (Doutorado) - Curso de Direito, Universidade Nova de Lisboa, Lisboa, 2018.

<sup>209</sup> HARTLEY, Trevor. **Overlapping jurisdiction in EC law**. In International Commercial Litigation: Text, Cases and Materials on Private International Law (pp. 237-264). Cambridge: Cambridge University Press, 2009. doi:10.1017/CBO9780511808739.011

território como definidor da soberania e extensão da aplicação do direito dos Estados começa a ser relativizada, dando espaço para “novos territórios”, cujos limites físicos são desconsiderados.<sup>210</sup> A propósito, é ilustrativa a citação de Dobner referenciado no texto de Acunha sobre a ressignificação do território:

“Dobner chega a destacar que estaria em curso não apenas uma crise no território, pela perda de relevância das fronteiras nacionais para fins de incidência das normas jurídicas, como também uma crise do território, não mais visto unicamente em sua dimensão físico-espacial, em virtude da emergência de novos espaços “não geográficos”, como o ambiente virtual digital da Internet.”<sup>211</sup>

Conforme comentado na introdução deste capítulo, não é possível identificar com exatidão o desenvolvimento histórico do conceito de extraterritorialidade, na medida em que alguns autores defendem o surgimento do termo no século XIX e outros encontram referências mais longínquas, na antiguidade.<sup>212</sup> Leopoldino faz um cotejo de aspectos relacionados à extraterritorialidade já no Direito Romano, passando pelas escolas estatutárias dos estados Italianos, da França e da Holanda durante a renascença e chegando até as teorias de Savigny, Gierke e Westlake, já nos séculos XIX e XX.<sup>213</sup>

Para Fonseca, nunca vigorou plenamente uma regra estrita de territorialidade para a aferição da extensão da jurisdição estatal, e com a intensificação das relações entre indivíduos no mundo globalizado fez-se necessário a adaptação da territorialidade ao novo contexto tecnológico para que o Estado pudesse exercer suas funções de proteção dos direitos individuais dos cidadãos.<sup>214</sup>

Já em um panorama moderno, os primeiros debates sobre a aplicação extraterritorial de normas deram-se no âmbito da legislação antitruste, devido à crescente internacionalização das empresas na virada do século XIX para o século XX, principalmente nos EUA.<sup>215</sup> Dessa forma, conforme aponta Casella, o caso *United States v. Alcoa*, julgado pela Suprema Corte dos

<sup>210</sup> ACUNHA, Fernando José Gonçalves. Democracia e transconstitucionalismo: “direito ao esquecimento”, extraterritorialidade e conflito entre ordens jurídicos. **Revista Direito Gv**, São Paulo, v. 12, n. 3, p. 748-775, set. 2016. Quadrimestral.

<sup>211</sup> *Ibid.* pág. 753.

<sup>212</sup> SVANTENSSON, Dan Jerker. Extraterritoriality and targeting in EU data privacy law. *Op. cit.*

<sup>213</sup> LEOPOLDINO, Juliana. **REGIME JURÍDICO DAS SOCIEDADES TRANSNACIONAIS E EFEITOS EXTRATERRITORIAIS DAS LEIS**. 2008. 88 f. Dissertação (Mestrado) - Curso de Direito, Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

<sup>214</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 11.

<sup>215</sup> CASELLA, P. B. **Extraterritorialidade e proteção da livre-concorrência**. Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.], v. 96, p. 501-519, 2001. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67514>. Acesso em: 28/02/2021.

EUA em 1945, foi um marco para a criação de algumas teorias que orbitam o debate da extraterritorialidade, como a teoria dos efeitos.<sup>216</sup>

Mas afinal, qual é o conceito de extraterritorialidade? A resposta para esse questionamento é multifacetada e, por vezes, polêmica. Na doutrina portuguesa, os conceitos mais citados são os desenvolvidos por Dulce Lopes e Fernando Loureiro Bastos. Para a primeira autora, extraterritorialidade é o “conjunto de situações em que o Estado está habilitado, usualmente por via unilateral, a dizer o direito aplicável a situações internacionais.”<sup>217</sup> Já para Bastos, em uma vertente mais voltada para as consequências da aplicação extraterritorial, a “extraterritorialidade determina que as normas de uma determinada ordem jurídica possa vir a produzir efeitos no espaço geográfico de uma ordem jurídica distinta”.<sup>218</sup>

Svantesson baseia-se em uma abordagem mais extensiva do conceito de extraterritorialidade e afirma que, em resumo, trata-se de um “esforço do Estado em tentar controlar atividades de uma pessoa – física ou jurídica – localizada fora de suas fronteiras.”<sup>219</sup> Em uma visão oposta, Ryngaert entende que o termo extraterritorialidade é quase sempre utilizado de maneira tecnicamente incorreta. Isso porque, para o autor, uma jurisdição só seria de fato extraterritorial quando se referisse a uma asserção de jurisdição sobre pessoas, bens ou atividades com nenhuma relação ou fator de conexão com o Estado regulador. Entretanto, o que se verifica na maioria dos casos, conforme o autor, é que as legislações ditas extraterritoriais ainda guardam – de alguma forma e ainda que não exclusivamente – fatores de conexão com o território do Estado.<sup>220</sup>

Além disso, segundo o autor, o termo adquiriu certa conotação negativa ao longo dos anos, uma vez que foi por vezes associada ao intervencionismo dos EUA em outros países da comunidade internacional. Ainda assim, por reconhecer ser um termo utilizado corriqueiramente na doutrina e jurisprudência, Ryngaert prefere empregar em sua obra o termo jurisdição extraterritorial para denotar “a jurisdição sobre situações que surgem no exterior, causando tipicamente efeitos econômicos adversos dentro do Estado que afirma a jurisdição”.<sup>221</sup>

---

<sup>216</sup> *Ibid.*

<sup>217</sup> LOPES, Dulce apud FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. Cit. pág. 5.

<sup>218</sup> BASTOS, Fernando Loureiro apud FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da.

**As Implicações em Países Terceiros Do Regime Geral de Proteção de Dados Pessoais da União Europeia: a sua Extraterritorialidade.** Direito Comparado. RFD, vol. 1 n° 1. Lisboa, 2018. pág. 631.

<sup>219</sup> SVANTESSON, Dan Jerker B. **Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation.** International Data Privacy Law. Vol. 5, No. 2015, pág. 226.

<sup>220</sup> RYNGAERT, Cedric. Op. cit. pág. 8.

<sup>221</sup> *Ibid.*

No intuito de tentar uniformizar as diversas concepções encontradas na doutrina sobre o que é o fenômeno da extraterritorialidade, a Comissão de Direito Internacional da ONU (CDI) emitiu um relatório em 2006, onde indica a necessidade de codificação do tema – haja vista a emergência de novas tecnologias e do avanço da globalização – e conceitua a extraterritorialidade como “uma tentativa de um Estado de regular, através de atos legislativos, judiciais ou executivos, a conduta de pessoas, bens ou atos, além das suas fronteiras, que afetam os seus interesses na ausência de regulação pelo DIP.”<sup>222</sup> Esse conceito, portanto, com o objetivo de uniformizar, acabou abarcando os três aspectos da jurisdição: prescritivo, adjudicativo e executivo.

Apesar da contribuição da CDI e de seu apelo pela codificação da matéria, não há ainda no direito internacional alguma definição de jurisdição extraterritorial fixada em tratados. Entretanto, ao longo dos anos, existiram outras manifestações desse fenômeno advindas da jurisprudência. O exemplo mais emblemático nesse sentido foi o caso *Lotus*,<sup>223</sup> julgado pela Corte Permanente de Justiça Internacional em 1927, que será analisado abaixo.

### 3.2.3 O caso *Lotus* e a teoria dos efeitos

Em 1926 um navio do serviço de correios da França denominado *Lotus* colidiu com um navio carvoeiro da Turquia, matando 8 indivíduos turcos. Ao aportar em Constantinopla, as autoridades turcas iniciaram as investigações no *Lotus* e acabaram prendendo um oficial francês e o sentenciando, já no mês seguinte, a 80 dias de reclusão. As autoridades francesas protestaram o ocorrido e alegaram que, ao manter sob custódia o oficial francês, a Turquia estaria violando normas de Direito Internacional.<sup>224</sup>

As negociações entre os dois países levaram o caso até a Corte Permanente de Justiça Internacional, que decidiu em favor da Turquia, assentando o entendimento de que, em se tratando de jurisdição prescritiva, cada Estado tem discricionariedade para exercer a jurisdição nos termos que considerar mais adequados, salvo expressa norma de direito internacional em contrário.<sup>225</sup> Segundo a corte, contudo, um Estado não pode exercer poder coercitivo dentro do

<sup>222</sup>CDI. “**Report on the Work of its Fifty-Eight Session**”, 1 May-9 June and 3 July-11 August 2006. Doc. A/61/10. Annex E, n.º 2. Disponível em: <[http://legal.un.org/ilc/documentation/english/reports/a\\_61\\_10.pdf](http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf)> Acesso em: 01/03/2021.”

<sup>223</sup> Corte Permanente de Justiça Internacional. (ser. A) No. 10 (1927).

<sup>224</sup>RYNGAERT, Cedric. *Op. cit.* pág. 31.

<sup>225</sup> CORTE PERMANENTE DE JUSTIÇA INTERNACIONAL. Caso *Lotus* (França v Turquia), Julgamento nº 9 de 7 Setembro 1927. P.C.I.J. Reports 1928. Series A. No. 10. pág.18-19

território de outro Estado para fazer cumprir suas leis e, portanto, a jurisdição executiva é fundamentalmente territorial.<sup>226</sup> Dessa forma, aplicando o entendimento ao caso concreto, a corte decidiu que: "Uma vez que é admitido que os efeitos da ofensa se produziram no navio turco, toma-se impossível sustentar que existe uma regra de Direito Internacional que proíbe a Turquia de processar o tenente Demons pelo fato de que o autor da ofensa estava a bordo de navio francês".<sup>227</sup>

O Caso *Lotus*, segundo aponta o relatório da CDI, foi a base para a evolução dos estudos sobre o critério da territorialidade objetiva, elucidada no subitem 3.2.1 deste trabalho, e da teoria dos efeitos. Conforme aponta Fonseca, há ainda na doutrina uma divergência sobre a autonomia da teoria dos efeitos em relação à territorialidade objetiva.<sup>228</sup> Para autores como Ryngaert<sup>229</sup>, não há tal distinção entre os dois fenômenos; para outros, como Taylor, a teoria dos efeitos é um desdobramento do critério da territorialidade objetiva;<sup>230</sup> e segundo o relatório da CDI há de fato uma distinção entre os dois fenômenos.<sup>231</sup>

De acordo com a CDI, a teoria dos efeitos pode ser entendida como o exercício de jurisdição sobre a conduta de um estrangeiro realizada fora de um determinado Estado, mas que cause efeitos substanciais dentro deste território.<sup>232</sup> Contudo, para a Comissão, a distinção existente entre o conceito apresentado acima e o critério da territorialidade objetiva está no fato de que, para este, é necessário que algum elemento da conduta ocorra dentro do território do Estado que pretende exercer a jurisdição, ainda que de forma mínima<sup>233</sup>.

Em se tratando da teoria dos efeitos, é inegável a contribuição do direito norte americano, principalmente sob a perspectiva do direito da concorrência. Em 1890, o Congresso dos EUA aprovou o chamado *Sherman Act*, segundo o qual qualquer combinação ou conspiração para restringir os negócios e o comércio entre os estados (dos EUA) ou com as nações estrangeiras seria declarado ilegal. Nessa época, conforme explica Ryngaert, os EUA ainda não haviam se firmado como a principal potência econômica mundial e, por isso, em 1909, quando primeiramente defrontada com a possibilidade da aplicação extraterritorial do *Sherman Act*, a Suprema Corte dos Estados Unidos fez uma interpretação restrita do princípio

---

<sup>226</sup> *Ibid.*

<sup>227</sup> *Ibid.*

<sup>228</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 33.

<sup>229</sup> RYNGAERT, Cedric. *Op. cit.* pág. 114..

<sup>230</sup> TAYLOR, Mistale. *Op. cit.* pág. 3.

<sup>231</sup> CDI. *Op. cit.* pág. 521-522.

<sup>232</sup> *Ibid.*

<sup>233</sup> *Ibid.*

da territorialidade e assentou que cabe a cada Estado determinar o que é legal dentro do seu próprio território.<sup>234</sup>

Com o fim da Segunda Guerra Mundial e a afirmação dos EUA como a grande potência internacional, a Suprema Corte dos EUA mudou seu posicionamento e, no caso *United States v. Alcoa*, em 1945, firmou o entendimento de que “um Estado pode impor obrigações até mesmo a pessoas não submetidas à autoridade deste Estado, por conduta praticada fora destas fronteiras, que tenham consequências dentro das fronteiras do Estado, condutas estas que o Estado reprova, ao menos na medida em que estes efeitos foram intencionalmente causados.”<sup>235</sup> Desde então, a teoria dos efeitos tem sido reconhecida na jurisprudência da Suprema Corte como fundamento para legitimar a aplicação da jurisdição americana para fatos ocorridos fora do território do país, principalmente nos casos de legislação antitruste.<sup>236</sup>

Até a década de 80, a aplicação da teoria dos efeitos foi amplamente criticada pelos demais parceiros comerciais dos EUA, principalmente Canadá, Japão e os países europeus. Até mesmo as diversas cortes espalhadas pelo país eram céticas quanto à aplicação extraterritorial do *Sherman Act*.<sup>237</sup> Nesse sentido, o Congresso dos EUA buscou delinear melhor as hipóteses em que a referida legislação poderia ser aplicada extraterritorialmente com a aprovação do chamado *Foreign Trade Antitrust Improvements Act* (FTAIA), em 1982. Segundo o FTAIA, o *Sherman Act* somente poderia ser aplicável extraterritorialmente para as condutas que tivessem efeitos diretos, substanciais e razoavelmente previsíveis no comércio dos EUA.<sup>238</sup> Agindo assim, o congresso dos EUA tentou dar contornos mais restritos à aplicação da teoria dos efeitos pelas cortes do país, ainda que tenha deixado considerável margem de discricionariedade para a interpretação do que poderiam ser considerados “efeitos substanciais” ou “razoavelmente previsíveis”.

No âmbito da União Europeia, a aplicação extraterritorial das normas do direito da concorrência migrou por duas bases teóricas até finalmente chegar na aplicação da teoria dos efeitos, já na década de 90. A primeira delas, era denominada doutrina da entidade econômica única, segundo a qual as subsidiárias de uma empresa da União Europeia que estivessem

<sup>234</sup> RYNGAERT, Cedric. *Op. cit.* pág. 68.

<sup>235</sup> Suprema Corte dos Estados Unidos. *Alcoa S. S. Co. v. United States*, 338 U. S. 421 (1949).

<sup>236</sup> BEDERMAN, David J. **Globalization and International Law**. Palgrave Macmillan: Nova Iorque, 2008. pág. 163.

<sup>237</sup> KAVA, Samuel. **The Extraterritorial Application of the Sherman Anti-Trust Act in the Age of Globalization: The Need to Amend the Foreign Trade Antitrust Improvements Act (FTAIA) & Vigorously Apply International Comity**. *Journal of Business and Technology Law*. V. 15, nº 1. 135. 2019. Disponível em: <<https://digitalcommons.law.umaryland.edu/jbtl/vol15/iss1/5>>. Acesso em 01/03/2021.

<sup>238</sup> *Ibid.* pág. 137.

localizadas nos países estrangeiros deveriam ser consideradas como uma mesma entidade para fins de aplicação das normas da UE, caso houvesse uma forte conexão ou relação de controle entre elas.<sup>239</sup>

A segunda teoria, chamada de doutrina da implementação, foi adotada primeiramente no caso *WoodPulp*, que tratava sobre a combinação de preços feita por uma associação estrangeira de produtores de celulose.<sup>240</sup> A Comissão Europeia aplicou multa às empresas que compunham a associação por sua prática anticoncorrencial, e estas, por sua vez, apelaram ao TJUE, alegando que a Comissão não teria competência para analisar o caso, uma vez que nenhuma das empresas tinha presença física na União Europeia. Apesar do parecer do Procurador-Geral do TJUE, que defendia explicitamente a aplicação da teoria dos efeitos, o Tribunal entendeu no caso em questão o que deveria ser levado em conta era o fato de que a combinação de preços praticada pelos reclamantes teria a intenção de ser implementada dentro do território da UE e, sendo assim, os regulamentos da UE poderiam ser aplicados.<sup>241</sup>

Foi somente em 1996, no caso *Gencor*, que o TJUE passou a utilizar a teoria dos efeitos para o caso de aplicação extraterritorial dos regulamentos sobre direito da concorrência.<sup>242</sup> O caso referia-se a uma fusão de uma empresa da África do Sul com outra da Inglaterra, ambas do setor de mineração. A autoridade de defesa da concorrência da África do Sul autorizou a transação, mas a Comissão Europeia não fez o mesmo, pois verificou que a transação resultaria em uma oligopolização do mercado, com consequente aumento de preços para os consumidores europeus.<sup>243</sup> Nesse caso, o então Tribunal de Primeira Instância das Comunidades Europeias adotou a teoria dos efeitos ao considerar que, não obstante a operação de fusão ser realizada na África do Sul, os efeitos seriam sentidos dentro do território da União Europeia e, portanto, a transação estava sujeita à aprovação da Comissão.<sup>244</sup> O Tribunal aplicou no caso os critérios também elencados FTAIA dos EUA, ou seja, considerou que os efeitos da transação analisada eram imediatos, substanciais e previsíveis.<sup>245</sup>

---

<sup>239</sup>XIA, Yue. **Assessing Extraterritorial Application of EU Competition Law**. Ghent University: Gentet, 2017. ág. 8. Ver também: TJEU. Caso C-48/69. *Imperial Chemical Industries Limited v. Commission* [1972] E.C.R. 619.

<sup>240</sup>*Ibid.*

<sup>241</sup>*Ibid.*

<sup>242</sup>TJUE. C-102. Caso *Gencor Ltd v. Commission*. Julgado em 1996.

<sup>243</sup>*Ibid.*

<sup>244</sup>XIA, Yue. Op. cit. pág. 11.

<sup>245</sup>OIZUMI, Monica Yumi Shida. **Conflito de Jurisdição no Direito Concorrencial no Âmbito Internacional**. 2017. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2017. pág. 80.

Apesar de suas origens no direito da concorrência, a teoria dos efeitos também encontrou abrigo em outros campos do direito da União Europeia, como na Proteção de Dados Pessoais, que é pano de fundo deste trabalho. Dessa forma, uma vez delineados os principais aspectos descritivos dos conceitos de Jurisdição e Extraterritorialidade, o próximo subcapítulo servirá para analisar como esses fenômenos interagem com o Regulamento Geral de Proteção de Dados, fazendo cotejo com a evolução histórica dos institutos e com a crítica doutrinária.

### 3.3 ANÁLISE DO ESCOPO TERRITORIAL E EXTRATERRITORIAL DO GDPR

O art. 3º elenca em seus três parágrafos todos os elementos que guiam a aplicação territorial e extraterritorial do GDPR. Para dar uma interpretação mais precisa deste dispositivo, este subcapítulo será desenvolvido da seguinte forma: primeiramente, serão trazidos a comento os dispositivos que tratavam sobre o âmbito de aplicação territorial na Diretiva 95/46/CE, precursora do GDPR, bem como a evolução jurisprudencial do TJUE construída sobre tais artigos. Em seguida, serão examinados em separado cada parágrafo do art. 3º do GDPR, em cotejo com as discussões doutrinárias e jurisprudenciais a eles relacionados. Por fim, serão debatidos os aspectos da legitimidade e do *enforcement* do fenômeno da extraterritorialidade do Regulamento.

#### 3.3.1 A DELIMITAÇÃO DO CRITÉRIO DO ESTABELECIMENTO NA DIRETIVA 95/46/CE E NA JURISPRUDÊNCIA DO TJUE

O parágrafo primeiro do art. 3º do GDPR foi amplamente baseado no art. 4.1.a, da Diretiva 95/46/CE. Além disso, a maior parte da jurisprudência do TJUE que interpreta a aplicação extraterritorial do GDPR foi desenvolvida ainda na vigência da Diretiva (até maio de 2018). Portanto, a análise da Diretiva, neste ponto específico, é um prelúdio para o fiel entendimento da sua norma sucessora, o GDPR.

O texto do art. 4.1.a da Diretiva estava descrito da seguinte maneira:

- 4.1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando:
- a) O tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses

estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;<sup>246</sup>

Como se depreende da análise do artigo transcrito, as normas contidas na Diretiva seriam aplicáveis aos tratamentos de dados realizados no contexto das atividades de algum estabelecimento dentro do território da União Europeia. A vista disso, a primeira interpretação que surgiu deste artigo foi a de que ele estava fundamentalmente enraizado no princípio da territorialidade subjetiva e somente seria aplicável aos casos de empresas ou instituições com instalações físicas na UE.<sup>247</sup> No entanto, à medida que as situações práticas começaram a surgir perante os tribunais, verificou-se que a conceituação do termo “estabelecimento” e, por conseguinte, das “atividades realizadas no contexto de um estabelecimento” não era tão certa como parecia.<sup>248</sup>

Na busca por extrair a melhor interpretação do que seria um estabelecimento, a primeira fonte que deveria ser consultada era o próprio Considerando 19 da Diretiva, que definia que a caracterização de um estabelecimento dentro do território da UE deveria pressupor o “exercício efetivo e real de uma atividade mediante uma instalação estável,”<sup>249</sup> independentemente desta instalação constituir uma filial ou somente uma sucursal de uma empresa estrangeira. Mesmo com o auxílio interpretativo prestado pelo Considerando 19, segundo aponta Alsenoy, o conceito de estabelecimento não era algo uniforme dentro do direito da União Europeia, uma vez que o TJUE já havia, em outros contextos, entendido que um estabelecimento deveria pressupor não só recursos técnicos como também humanos, que deveriam estar permanentemente disponíveis.<sup>250</sup> Era preciso, portanto, harmonizar a interpretação da norma em questão.

Dentro dessa perspectiva, em 2010, o Grupo de Trabalho do Art. 29 buscou esclarecer as dúvidas que permeavam o conceito de estabelecimento por meio da publicação da Opinião nº 8.<sup>251</sup> No documento são enumerados alguns exemplos do que poderia e do que não poderia ser classificado como um exercício efetivo e real de uma atividade por uma instalação estável.

---

<sup>246</sup> Diretiva 95/46/CE. Art. 4.1.

<sup>247</sup> BELETSK, Roman.Op. cit. 33.

<sup>248</sup> *Ibid.*

<sup>249</sup> Diretiva 95/46/CE. Considerando 19.

<sup>250</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial reach of the GDPR with public international law. In: VERMEULEN, Gert; LIEVENS, Eva. **Data Protection and Privacy under Pressure**. Maklu: Portland, 2017. pág. 80.

<sup>251</sup> UNIÃO EUROPEIA. **Opinião nº8/2010 do Grupo de Trabalho do Art. 29 (versão original)**. Disponível em:<[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf)>. Acesso em: 01/03/2021.

Um desses exemplos é o caso de um escritório composto por somente uma pessoa. Nesse caso, segundo documento, o escritório somente poderia ser enquadrado como um estabelecimento, caso participasse no processamento de dados pessoais e não somente realizasse a representação de uma empresa localizada no exterior.<sup>252</sup> Outro exemplo é o caso de um simples servidor de computador de uma empresa localizada no território da UE. Nessa situação, como o aparelho é um mero instrumento para o processamento de dados, ele não pode, por si só, ser caracterizado como um estabelecimento.<sup>253</sup>

Não obstante os esclarecimentos feitos na Opinião nº 8, ainda pairavam dúvidas sobre a aplicação da Diretiva para os controladores que realizassem o tratamento de dados pessoais fora da União Europeia, mas com dados provenientes do território do bloco por meio de suas filiais.<sup>254</sup> Não foi preciso muito tempo para notar que, com os avanços tecnológicos, caso a Diretiva fosse somente aplicada aos estabelecimentos com sede na UE ela poderia ser facilmente evitada pelas empresas transnacionais por meio do chamado *Forum Shopping* – fenômeno pelo qual as empresas procuram estabelecer suas sedes em Estados cujas legislações lhes sejam mais favoráveis.<sup>255</sup>

Esse cenário de insegurança jurídica foi alterado quando, em 2014, o TJUE julgou o caso *Google Spain*,<sup>256</sup> uma das mais notórias decisões em se tratando da interface entre direito e internet.<sup>257</sup> Em apertada síntese, os fatos do caso dizem respeito à tentativa de Mario Costeja González, um cidadão espanhol, de excluir alguns dados tidos como irrelevantes e relacionados a sua pessoa, que poderiam ser facilmente encontrados por meio do mecanismo de busca da empresa *Google Spain*, uma filial da *Google Inc*. Em última análise, portanto, o requerente pleiteava o reconhecimento do direito ao esquecimento pela Corte de Luxemburgo.<sup>258</sup> Todavia, antes de analisar o mérito da questão, o Tribunal defrontou-se com a questão preliminar do âmbito de aplicação territorial da Diretiva.

A *Google Inc*, responsável pelo gerenciamento do mecanismo de buscas, alegava que a Diretiva não lhe poderia ser aplicável segundo o art. 4.1, uma vez que suas atividades não eram exercidas no mesmo contexto que a sua subsidiária na Espanha. O papel da *Google Spain*

---

<sup>252</sup> Ibid.

<sup>253</sup> Ibid.

<sup>254</sup> AZZI, Adèle. **The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation**. JIPITEC. 126 para 126. (2018). pág. 128.

<sup>255</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. Cit. pág. 218.

<sup>256</sup> TJUE. C-131/12. Caso *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González*. julgado em 2014.

<sup>257</sup> SVANTESSON, Dan Jerker B. **Solving The Internet Jurisdiction Puzzle**. Oxford University Press: Oxford, 2017. pág. 174.

<sup>258</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial. Op. cit. pág. 81.

era realizar a representação comercial da *Google Inc* no país ibérico, além de promover a venda de propagandas online. Portanto, segundo o argumento da empresa-mãe, a subsidiária espanhola não participaria do processamento de dados dos clientes.<sup>259</sup> Entretanto, após ponderar os argumentos das partes em cotejo com o texto da Diretiva, a Corte chegou à seguinte conclusão:

Tendo em conta este objetivo da Diretiva 95/46 e a redação do seu artigo 4.º, n.º 1, alínea a), há que considerar que o tratamento de dados pessoais, realizado com vista às necessidades do serviço de um motor de busca como o Google Search, que é explorado por uma empresa sediada num Estado terceiro, mas que dispõe de um estabelecimento num Estado-Membro, é efetuado «no contexto das atividades» desse estabelecimento, se este se destinar a assegurar, nesse Estado-Membro, a promoção e a venda dos espaços publicitários propostos por esse motor de busca, que servem para rentabilizar o serviço prestado por esse motor. Com efeito, nestas circunstâncias, as atividades do operador do motor de busca e as do seu estabelecimento situado no Estado-Membro em causa estão indissociavelmente ligadas, uma vez que as atividades relativas aos espaços publicitários constituem o meio para tornar o motor de busca em causa economicamente rentável e que esse motor é, ao mesmo tempo, o meio que permite realizar essas atividades.<sup>260</sup>

Analisando o trecho em comento, verifica-se que o TJUE considerou que o exercício das atividades econômicas desenvolvidas pela *Google Inc* somente se tornou rentável dentro da Espanha devido à atuação da sua subsidiária. Sendo assim, a forte simbiose – ou “conexão indissociável” – existente entre as duas empresas faz com que o tratamento de dados pessoais colhidos na Espanha, mas realizado pela *Google Inc* nos EUA, seja considerado como ocorrido dentro do contexto de um estabelecimento localizado na União Europeia. Com efeito, tais operações de tratamento de dados pessoais deveriam ser executadas de acordo com os parâmetros estabelecidos pela Diretiva, o que importaria, consequentemente, na garantia de todos os direitos dos titulares dos dados.<sup>261</sup>

A Corte fundamentou o seu entendimento no caso *Google Spain* no propósito da Diretiva de garantir uma efetiva e completa proteção aos direitos fundamentais daqueles que se encontram na União Europeia, prevenindo as eventuais tentativas de contornar a aplicação da norma pelas empresas estrangeiras.<sup>262</sup> Logo, a partir desse caso, o art. 4.1 da Diretiva, que antes era majoritariamente interpretado como mera decorrência do critério da territorialidade subjetiva, ganhou contornos extraterritoriais, na medida em que, agora, restava claro que qualquer tratamento de dados pessoais realizados no contexto de um estabelecimento na UE,

---

<sup>259</sup> *Ibid.*

<sup>260</sup> *Google Spain. Op. cit.* Parágrafos 55 e 56.

<sup>261</sup> *Ibid.*

<sup>262</sup> *Ibid.* Parágrafos 53 e 54.

mesmo que o tratamento em si fosse realizado fora das fronteiras do bloco, deveria estar sujeito ao regime de proteção de dados do bloco.<sup>263</sup>

Para Fonseca, ao julgar o caso *Google Spain*, o TJUE valeu-se da teoria da unidade econômica, pela qual a *Google Inc* e sua subsidiária espanhola foram consideradas como um único agente econômico, abstraindo-se sua personalidade jurídica distinta em prol da proteção efetiva dos direitos fundamentais.<sup>264</sup> Nesse sentido, a autora avalia que o raciocínio consequencialista da Corte buscou dar efeito útil à Diretiva por meio de uma “suavização” do critério da territorialidade.<sup>265</sup>

Fazendo uso das categorias de jurisdição apresentadas anteriormente neste trabalho, pode-se inferir que a Corte de Luxemburgo interpretou o art. 4.1 da Diretiva sob o viés da territorialidade objetiva, na acepção CDI, cujo elemento de conexão é o estabelecimento da empresa subsidiária em solo da União Europeia. Entretanto, conforme referido anteriormente, há ampla discussão sobre as distinções entre a territorialidade objetiva e a teoria dos efeitos, o que também se reflete na interpretação do art. 4.1 da Diretiva. Isso porque, autores como Alsenoy e Koekkoek, afirmam que o referido artigo é baseado na teoria dos efeitos, principalmente por causa da redação do acórdão do TJUE, que cita, por diversas vezes, o objetivo de dar efetividade ao texto da norma.<sup>266</sup>

Outro importante caso julgado pelo TJUE para a interpretação do art. 4.1 da Diretiva foi o caso *Weltimmo*. Julgado em 2015, a controvérsia dizia respeito a um site de anúncio de imóveis, cujo nome era *Weltimmo*, com sede na Eslováquia, mas com atuação na Hungria. O site recebeu diversos pedidos de exclusão de dados por parte dos anunciantes húngaros, mas não respondeu às solicitações. Por causa disso, a Autoridade de Proteção de Dados da Hungria aplicou uma multa ao site que, inconformado, levou o caso ao TJUE. A *Weltimmo* alegava que, por não ter um estabelecimento na Hungria, a Autoridade de Dados húngara não teria competência para lhe aplicar a multa.<sup>267</sup>

No julgamento, a Corte levou em consideração os diversos elementos que demonstravam a forte conexão que a empresa requerente tinha com a Hungria, como, por

---

<sup>263</sup> CAREY, Peter. **Data Protection: A Practical Guide to UK and EU Law**. 5ª Ed. Oxford: Oxford University Press, 2018. pág. 7.

<sup>264</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. Cit. pág. 125.

<sup>265</sup> *Ibid.* pág. 127

<sup>266</sup> ALSENOY, B. Van; KOEKKOEK, Mariek. **Internet and Jurisdiction after Google Spain: the Extraterritorial Reach of the Right to be Delisted**. International Data Privacy Law Review. Vol. 5. 2015. pág.105 – 120.

<sup>267</sup> TJUE. C-230/14. Caso *Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság*. Julgado em 2015.

exemplo, o fato de ter uma conta bancária no país, representantes comerciais, site na língua local, além de ter a maioria dos seus clientes nesse país. Assim como no caso *Google Spain*, a Corte entendeu que o art. 4.1 deve ser interpretado extensivamente e, por consequência, o conceito de estabelecimento deveria ser flexibilizado para dar maior efetividade à Diretiva. Dessa forma, o Tribunal assentou o entendimento de que o estabelecimento abrange qualquer atividade econômica real, efetiva e estável, ainda que mínima. Em decorrência disto, a *Weltimmo* deveria estar submetida a Autoridade de Proteção de Dados húngara.<sup>268</sup>

Além dos casos até aqui mencionados, o TJUE confirmou o mesmo entendimento sobre o conceito de estabelecimento em outros dois casos, julgados ainda antes da entrada em vigor do GDPR: no caso *Verein für Konsumenteninformation*<sup>269</sup> e no caso *Wirtschaftsakademie*.<sup>270</sup> Em ambas as situações foi sedimentada a concepção de que qualquer atividade real e efetiva exercida por arranjos estáveis, ainda que mínima, pode constituir um estabelecimento.<sup>271</sup>

É importante ressaltar, neste ponto, que o projeto de regulamento do GDPR já estava em tramitação desde 2012 no Parlamento Europeu e, portanto, os legisladores europeus puderam acompanhar a evolução da jurisprudência e da doutrina sobre o tema. Isso refletiu nas alterações realizadas no art. 4.1 da Diretiva que se tornaria o art. 3º.1 do GDPR. Além disso, como somente em novembro de 2018 o CEPD emitiu diretrizes sobre a aplicação do art. 3º do GDPR, o entendimento já estabelecido no período de vigência da Diretiva teve grande importância para auxiliar os controladores e operadores na adequação de suas atividades ao novo regulamento.<sup>272</sup>

### 3.3.2 A APLICAÇÃO EXTRATERRITORIAL DO GDPR POR MEIO DO CRITÉRIO DO ESTABELECIMENTO (ART. 3.1)

Uma vez delineadas as nuances interpretativas do art. 4.1 da Diretiva, o presente subcapítulo passará a analisar especificamente o art. 3.1 do GDPR e sua aplicação extraterritorial.

---

<sup>268</sup> Ibid.

<sup>269</sup> TJUE. C-272/18. Caso *Verein für Konsumenteninformation*. Julgado em 2019.

<sup>270</sup> TJUE. C-210/16. Caso *Wirtschaftsakademie*. Julgado em 2018.

<sup>271</sup> BELETSK, Roman. Op. cit. pág. 37.

<sup>272</sup> SVANTESSON, Dan Jerker B.. Article 3. Territorial scope. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation (GDPR): a commentary**. Oxford: Oxford University Press, 2020. p. 82.

O art.3.1 tem a seguinte redação:

o presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um controlador ou de um operador situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.<sup>273</sup>

A primeira conclusão que salta aos olhos a partir da comparação do artigo 3.1 do GDPR com o art. 4.1 da Diretiva é que o entendimento do TJUE no caso *Google Spain* foi incorporado ao texto legislativo.<sup>274</sup> Isso porque, com a redação do art. 3.1, não restam dúvidas de que o local onde o tratamento de dados é realizado é irrelevante para a análise do âmbito de aplicação do Regulamento, desde que o tratamento desses dados tenha estreita relação com a atividade de um estabelecimento localizado dentro do território do bloco.<sup>275</sup>

Uma segunda observação latente na comparação dos dois textos legislativos é que o Regulamento inclui como elemento de conexão não somente o estabelecimento de um controlador, mas também de um operador situado na União Europeia.<sup>276</sup> Esse fato aponta para um alargamento da vocação extraterritorial do art. 3.1, conforme se verá a seguir.

As Diretrizes emitidas pelo CEPD em 2018 sobre o art. 3º do GDPR são de grande valia para a interpretação desse dispositivo, haja vista que, até o momento, a jurisprudência do TJUE sobre a aplicação extraterritorial das normas de Proteção de Dados foi majoritariamente construída sob a vigência da Diretiva 95/46/CE.<sup>277</sup> Essas diretrizes apontam para uma abordagem tríplice que deve ser empregada para verificar se determinada atividade de um controlador ou processador de dados pessoais está sujeita ao GDPR.<sup>278</sup>

O primeiro passo dessa abordagem é identificar se o controlador ou o operador tem algum estabelecimento dentro da UE. O Considerando 22 do GDPR – idêntico ao Considerando 19 da Diretiva – esclarece algumas noções sobre o que poderia ser visto como um estabelecimento, mas não descreve a definição em si desse termo. Para o Comitê, portanto, essa definição ainda deve ser procurada no entendimento construído pelo TJUE nos acórdãos *Google Spain* e *Weltimmo*, que foram analisados anteriormente.<sup>279</sup> Por conseguinte, continua

<sup>273</sup> GDPR, Art. 3.1.

<sup>274</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op.cit.* pág. 142.

<sup>275</sup> ALSENOY, Brendan Van. *Data Protection Law in the UE: Roles, Responsibilities and Liability*. Intersentia: Cambridge, 2019. pág. 29.

<sup>276</sup> *Ibid.*

<sup>277</sup> SVANTESSON, Dan Jerker B.. **Article 3. Territorial scope**. *Op. cit.* p. 79.

<sup>278</sup> UNIÃO EUROPEIA. Diretrizes 3/2018 sobre o âmbito de aplicação territorial do GDPR (Art.3º) do Comitê Europeu de Proteção de Dados. Disponível em:<[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_pt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf)> Acesso em: 01/03/2021. pág. 5.

<sup>279</sup> *Ibid.* pág. 6

prevalecendo a conceituação de estabelecimento como “qualquer atividade real e efetiva – ainda que mínima – exercida através de uma instalação estável”.<sup>280</sup>

Dentro da perspectiva da extraterritorialidade, para identificar se uma entidade estrangeira tem algum estabelecimento dentro do bloco é necessário uma avaliação casuística, levando em consideração o grau de estabilidade das instalações, as especificidades das atividades econômicas desenvolvidas pela entidade e o exercício efetivo dessas atividades dentro do território da UE.<sup>281</sup> A CEPD também ressalta que para os serviços oferecidos *online* os requisitos para a aferição de uma “instalação estável” podem ser baixos, inclusive com a possibilidade de a simples presença de um representante ser considerada para fins de caracterização de um estabelecimento.<sup>282</sup> Entretanto, o próprio Comitê esclarece que o simples fato de um site ser acessível na UE não cria, por si só, um estabelecimento nesse território.<sup>283</sup>

Uma vez identificado que determinada entidade tem um estabelecimento na UE, passa-se a segunda etapa de análise, qual seja, a verificação da existência de atividades de tratamento de dados ocorrendo no contexto deste estabelecimento. O comitê recomenda que essa análise seja feita considerando se há uma relação intrínseca entre o operador ou o controlador situado fora da UE com sua subsidiária local. Essa relação pode ser comprovada, por exemplo, pela geração de receitas da subsidiária local para a empresa-mãe.<sup>284</sup>

Nesse sentido, o CEPD dá o exemplo de uma loja virtual com sede na China, que realiza o tratamento de dados de seus clientes localizados na UE. A empresa decidiu abrir um escritório em algum Estado-membro do bloco europeu para facilitar seus negócios. Sendo assim, como as atividades do escritório tem íntima relação com a atividade de tratamento de dados realizada pela sede chinesa, o escritório é considerado um estabelecimento e, por conseguinte, a empresa deverá estar em conformidade com o GDPR.<sup>285</sup>

Por fim, a terceira etapa diz respeito ao alcance do termo “independentemente de o tratamento ocorrer dentro ou fora da União” do art. 3.1. Na perspectiva do CEPD, o fato de um controlador estrangeiro contratar um operador de dentro da UE não faz com que esse controlador contratante tenha automaticamente um estabelecimento no território do bloco para fins do art. 3.1. Portanto, o controlador não precisará se adequar ao GDPR. No entanto, o

---

<sup>280</sup> UNIÃO EUROPEIA. Caso Weltimmo. *Op. cit.* parágrafo.º 31.

<sup>281</sup> UNIÃO EUROPEIA. Diretrizes 3/2018 do CEPD, pág. 7.

<sup>282</sup> *Ibid.*

<sup>283</sup> *Ibid.*

<sup>284</sup> *Ibid.*, pág. 9.

<sup>285</sup> *Ibid.*

operador contratado deverá sim exercer suas atividades respeitando as normas do Regulamento no que concerne aos deveres específicos dos operadores. Não fosse assim, haveria uma clara desvantagem competitiva para os operadores da UE, uma vez que as empresas evitaram contratá-los para não atrair a aplicação do GDPR para si.<sup>286</sup>

Conclui-se, portanto, desta análise do artigo 3.1, que qualquer entidade que tenha algum estabelecimento no território da União Europeia e que realize, no contexto deste estabelecimento, o tratamento de dados pessoais está sujeita aos regramentos do GDPR. Na perspectiva da aplicação extraterritorial desse dispositivo, infere-se que as empresas estrangeiras mais afetadas são aquelas de perfil transnacional, que atuem por meios estáveis em ao menos um dos 27 Estados da União Europeia e nos demais países onde o GDPR também é aplicável.

Aliás, cabe ressaltar que o GDPR é de igual modo aplicável na Noruega, Liechtenstein e Islândia, por força do tratado do Espaço Econômico Europeu.<sup>287</sup> Já com relação ao Reino Unido – que deixou a União Europeia em 31 de janeiro de 2020 e ficou em um período de transição até 31 de dezembro do mesmo ano –, houve a importação do GDPR da UE como GDPR do Reino Unido, por meio do chamado “*withdraw act*”.<sup>288</sup> Como resultado, foram feitas algumas pequenas adequações técnicas, mas as regras e princípios permaneceram os mesmos.<sup>289</sup> Ademais, está em análise no âmbito da Comissão Europeia a concessão de uma Decisão de Adequação para o Reino Unido, reconhecendo-o como possuidor de um nível adequado de proteção de dados pessoais para fins de transferências internacionais de dados, nos termos dos artigos 44 a 50 do GDPR. Durante o período de análise da referida Decisão, o fluxo de dados pessoais entre a UE e o Reino Unido continua sendo possível graças ao Acordo de Comércio e Cooperação, aprovado em 2020.<sup>290</sup>

---

<sup>286</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 153.

<sup>287</sup> SVANTESSON, Dan Jerker B.. **Article 3. Territorial scope.** *Op. cit.* p. 83.

<sup>288</sup> REINO UNIDO. Information Commissioner’s Office. Data Protection and the EU-UK Trade Deal. Disponível em: <<https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-uk-trade-deal/>>. Acesso em: 01/03/2021.

<sup>289</sup> *Ibid.*

<sup>290</sup> REINO UNIDO. Information Commissioner’s Office. ICO statement in response to the publication of a draft adequacy decision from the European Commission. Disponível em: <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/02/ico-statement-in-response-to-the-publication-of-a-draft-adequacy-decision-from-the-european-commission/>> Acesso em: 01/03/2021.

### 3.3.3 O *DESTINATION APPROACH* E A APLICAÇÃO DO GDPR PARA AS EMPRESAS ESTRANGEIRAS (ART.3.2)

O art. 3.2 é o que atrai maior atenção da doutrina no que tange à discussão sobre a aplicação extraterritorial do GDPR.<sup>291</sup> Esse polêmico dispositivo é também o de maior interesse para o presente trabalho, haja vista que é dele que provém o maior potencial de aplicação do GDPR para as empresas de Tecnologia da Informação de Florianópolis.

Nas palavras de Beletsk, “o parágrafo segundo é a mais explícita e clara manifestação da extraterritorialidade dentro da sistemática do Direito de Proteção de Dados da UE”.<sup>292</sup> Para Kuner, trata-se de uma verdadeira revolução copernicana no contexto do direito de proteção de dados.<sup>293</sup> Nesse sentido, com o objetivo de investigar as diversas facetas desse dispositivo tão controverso, nos parágrafos que se seguirão, o art. 3.2 será examinado à luz de uma perspectiva descritiva e, posteriormente, crítica.

A redação do art. 3.2 é a seguinte:

3.2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável por um controlador ou operador 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 controle do seu comportamento, desde que esse comportamento tenha lugar na União.<sup>294</sup>

O primeiro ponto que deve ser ressaltado com relação ao art. 3.2 do GDPR é sobre a correta interpretação da palavra “residentes”. Segundo explica Fonseca, a tradução para a língua portuguesa e espanhola do GDPR criou uma dupla interpretação do escopo de aplicação do Regulamento.<sup>295</sup> Isso porque, essas versões do texto levam o leitor a crer que somente importa para o Regulamento o tratamento de dados pessoais de indivíduos que residem na União

<sup>291</sup> HERT, Paul de; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*. Volume 6. Número 3. Agosto de 2016. Pág. 238. <https://doi.org/10.1093/idpl/ipw008>; SVANTESSON, Dan J. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*. Volume 5. 2015. pág. 226;

<sup>292</sup> BELETSK, Roman. *Op. cit.* pág. 38.

<sup>293</sup> KUNER, Christopher. The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*. 2012. pág. 1–15.

<sup>294</sup> GDPR. Art. 3.2.

<sup>295</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do GDPR. *UNIO - EU Law Journal*. Vol. 4, No. 2, Julho 2018, pág. 119-131.

Europeia. O termo “residência”, tanto no direito português, espanhol ou até mesmo no direito brasileiro tem uma aceção jurídica clara, a saber: o lugar onde o indivíduo se estabelece com ânimo definitivo.<sup>296</sup>

Esse não foi, contudo, o intuito do legislador europeu. Durante o processo legislativo do GDPR, de fato, houve uma proposta de restringir o âmbito de proteção da norma a somente aqueles que tivessem residência na União Europeia; contudo, tal proposta foi expressamente rejeitada pelo Parlamento Europeu.<sup>297</sup> Além disso, resta claro pela leitura dos Considerandos n. 2 e 14 do Regulamento que os seus dispositivos são aplicáveis a todos os indivíduos que se encontram no território da União Europeia, independentemente de sua nacionalidade ou local de residência.<sup>298</sup>

Ciente dos problemas interpretativos que as diferentes traduções poderiam causar, o Conselho da Europa emitiu uma errata, onde esclarece que o art. 3.2 deve ser lido da seguinte forma em português:

3.2 O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um controlador ou operador 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 controle do seu comportamento, desde que esse comportamento tenha lugar na União.<sup>299</sup>

Infere-se, portanto, que o primeiro requisito para atrair a aplicação do GDPR por força do art. 3.2 é a realização de tratamento de dados pessoais de indivíduos que se encontram na União Europeia por parte de controladores ou operadores estrangeiros, sem presença física no território do bloco.<sup>300</sup> Note-se que, em contraste com o art. 3.1 do Regulamento, o elemento de conexão aqui deixa de ser a atividade relacionada a um estabelecimento na UE e passa a ser a atividade direcionada a um indivíduo localizado no território do bloco.<sup>301</sup> Esse fenômeno é caracterizado pela doutrina como *targeting criterion* ou *destination approach*, ou critério da destinação, em tradução livre. É por meio dele que o legislador europeu pretendeu regulamentar o tratamento de dados pessoais realizados por controladores ou operadores que não têm

<sup>296</sup> BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, art. 70.

<sup>297</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Finalmente: coerência. *Op. cit.* pág. 129.

<sup>298</sup> GDPR. Considerandos 2 e 14.

<sup>299</sup> UNIÃO EUROPEIA. Corrigendum do Conselho da Europa sobre o Regulamento 2016/679. Documento nº8088/2018. Disponível em: <<https://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf>> . Acesso em 02/03/2021.

<sup>300</sup> UNIÃO EUROPEIA. Diretrizes 3/2018 do CEPD. pág. 16.

<sup>301</sup> *Ibid.*

qualquer presença física na UE, mas que intentam alcançar o mercado europeu por meio da oferta dos seus bens ou serviços.<sup>302</sup> Nesse sentido, a frase de Hert e Czerniawski resume bem a intenção do legislador europeu com a redação deste parágrafo: “*you might be targeted by EU law only if you target*”.<sup>303</sup>

Cabe salientar, entretanto, que não é qualquer tratamento de dados pessoais que é relevante para o art. 3.2. e, por conseguinte, deve-se passar a análise do segundo requisito, a saber, que o tratamento de dados pessoais seja relacionado com (1) a oferta de bens e serviços direcionados para pessoas que estejam na UE ou (2) com o monitoramento do comportamento dessas pessoas.<sup>304</sup>

A partir do que foi até aqui exposto, é fácil perceber a razão pela qual o art. 3.2 atraiu a atenção de diversos agentes econômicos, principalmente daqueles que atuam por meio da Internet. Em razão do cenário ainda nebuloso sobre a interpretação do dispositivo, do possível aumento de custos com *compliance* e das altas penalidades que poderiam estar sujeitas, muitas empresas detentoras de sites ou aplicativos resolveram remover o acesso a usuários da União Europeia tão logo o GDPR entrou em vigor.<sup>305</sup> Era necessário, portanto, a divulgação de esclarecimentos sobre a aplicação do dispositivo, fato que só ocorreria no final de 2018, com a Diretriz 8/2018 da CEPD.<sup>306</sup>

Tendo em vista que o art. 3.2 do GDPR não encontra paralelo em nenhum artigo antecessor na Diretiva 95/46/CE, a sua interpretação baseia-se, majoritariamente, nos Considerandos 23 e 24 do próprio Regulamento, na Diretriz 8/2018 do CEPD e no entendimento doutrinário sobre o tema. Apesar disso, alguns autores como Alsenoy e Beletsk defendem que a jurisprudência do TJUE estabelecida nos casos *Google Spain* e *Weltimmo* podem ser de igual forma utilizada como instrumento interpretativo desse dispositivo, uma vez que o critério do *targeting* esteve implícito nas razões de decidir do TJUE nesses casos.<sup>307</sup>

---

<sup>302</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial... *Op. cit.* pág. 89.; HERT, Paul de; CZERNIAWSKI, Michal. *Op. cit.* pág. 238. SVANTESSON, Dan. J. European Union Claims of Jurisdiction over the Internet An Analysis of Three Recent Key Developments. 9 (2018) JIPITEC.

<sup>303</sup> HERT, Paul de; CZERNIAWSKI, Michal. *Op. cit.* pág. 238.

<sup>304</sup> Diretrizes 3/2018 do CEPD. pág. 18.

<sup>305</sup> THE WALL STREET JOURNAL. U.S. **Websites Go Dark in Europe as GDPR Data Rules Kick In.** Disponível em: <<https://www.wsj.com/articles/u-s-websites-go-dark-in-europe-as-gdpr-data-rules-kick-in-1527242038>>. Acesso em: 02/03/2021. THE GUARDIAN. **Sites block users, shut down activities and flood inboxes as GDPR rules loom.** Disponível em: <<https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect>>. Acesso em: 02/03/2021.

<sup>306</sup> SVANTESSON, Dan Jerker B.. **Article 3. Territorial scope...** *Op. cit.* p. 82.

<sup>307</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial... *Op. cit.* pág. 89. BELETISK, Roman. *Op. Cit.* pág. 39.

Com relação ao requisito da oferta de bens e serviços direcionados para pessoas que estejam na UE, o CEPD esclarece que o mero tratamento de dados pessoais de indivíduos que se encontram no território da União Europeia não é suficiente para atrair a aplicação do GDPR, sem que haja também a real intenção dos controladores ou operadores em direcionar suas atividades para o território da UE.<sup>308</sup> Ilustrativamente, caso um brasileiro instale em seu dispositivo celular um aplicativo, que foi desenvolvido para o público brasileiro, e venha a utilizar esse mesmo aplicativo em uma viagem para algum país da União Europeia, os dados coletados pelo aplicativo durante essa viagem não estarão sujeitas às normas do GDPR, haja vista que o direcionamento, nesse caso, era para o público no Brasil e não na UE.

Nesse sentido, o mero fato de um site ou aplicativo ser acessível a partir de alguma localidade dentro do território da UE não faz, por si só, com que os dispositivos do GDPR sejam aplicáveis aos controladores ou operadores que gerenciam essas plataformas virtuais.<sup>309</sup> Além disso, a CEPD pontua que o tratamento de dados de cidadãos europeus no momento em que estes encontram-se fora da União Europeia da mesma forma não desencadeia a aplicação do GDPR, uma vez que, como visto anteriormente, a cidadania não é um fator de conexão para o Regulamento.<sup>310</sup>

A necessidade de que o tratamento de dados pessoais tenha relação com a oferta de bens ou serviços direcionados para o mercado europeu implica, consequentemente, que outras atividades que usualmente demandam o tratamento de dados pessoais, como o registro feito pelos setores de recursos humanos de empresas estrangeiras que tenham empregados na UE, não estejam sujeitas ao GDPR.<sup>311</sup> Destarte, resta saber como identificar quando uma determinada empresa tem a intenção de direcionar suas atividades para o mercado europeu.

O Considerando 23 do GDPR elenca indicativos concretos que podem ser levados em consideração para identificar se uma empresa está direcionando seus serviços e bens para o mercado europeu, tais como: a possibilidade de compra em moeda de algum país-membro; a disponibilização de informações nos idiomas da UE; e a indicação de outros clientes da UE.<sup>312</sup>

Ainda nesse sentido, o CEPD, fundamentando-se no entendimento utilizado pelo TJUE no caso *Pammer & Hotel Alpenhof*,<sup>313</sup> considera que existem outros elementos para além daqueles constantes no Considerando 23, que também podem ser levados em conta neste

---

<sup>308</sup> Diretrizes 3/2018 do CEPD, pág. 18.

<sup>309</sup> GDPR. Considerando 23.

<sup>310</sup> Diretrizes 3/2018 do CEPD, pág. 18

<sup>311</sup> *Ibid*, pág. 21.

<sup>312</sup> GDPR. Considerando 23.

<sup>313</sup> TJUE. C-585/08. Caso *Pammer and Hotel Alpenhof*. Julgado em 2010.

processo de identificação.<sup>314</sup> Nesse norte, o comitê apresenta uma listagem não exaustiva de características que podem ser utilizadas na avaliação, tais como: a natureza internacional da atividade econômica; a utilização de um domínio de primeiro nível; a possibilidade de entrega em um Estado-membro da UE; a possibilidade de pagamento em moeda de algum Estado-membro da UE, que não seja a moeda corrente do local do operador ou controlador; dentre outros.<sup>315</sup>

Hert e Czerniawsk criticam o art. 3.2 no que tange a sua alta carga de subjetividade para a caracterização do que é ou não considerado um direcionamento de uma atividade para a UE. Os autores dão o exemplo de um indivíduo na UE que reserva um hotel na Califórnia - EUA por meio de um site dos EUA. Nessa hipótese, segundo os autores, caso fosse somente considerada a natureza internacional de um hotel, o GDPR deveria ser aplicado aos dados coletados pelo hotel quando da realização da reserva pelo indivíduo na UE.<sup>316</sup> Esse fenômeno, conforme o entendimento dos autores, desconsidera o poder de escolha de mercado que cada indivíduo deveria ter.<sup>317</sup> Em resposta a essa preocupação, o CEDP afirma que todos os casos devem ser analisados em concreto, pois a análise isolada dos elementos listados acima pode levar a conclusões imprecisas.<sup>318</sup>

Para Svantesson, os indicativos elencados tanto no Considerando 23 quanto na Diretriz 8/2018 são insuficientes para identificar a intenção das empresas em alguns casos práticos, como por exemplo, nas hipóteses de oferta de serviços gratuitos na internet que estejam disponíveis no mundo todo. Para o autor, as cortes enfrentarão dificuldades práticas para determinar se em tais casos as empresas tinham claro objetivo de destinar seus serviços para cada país do mundo ou para nenhum em específico.<sup>319</sup>

Já no que se refere ao art. 3.2.b, que trata sobre o monitoramento do comportamento de indivíduos localizados na UE, deve-se levar em consideração a orientação interpretativa dada pelo Considerando 24 do GDPR, segundo o qual:

A fim de determinar se uma atividade de tratamento pode ser considerada «controle do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

<sup>314</sup> Diretrizes 3/2018 do CEPD. pág. 20.

<sup>315</sup> *Ibid.*

<sup>316</sup> HERT, Paul de; CZERNIAWSKI, Michal. *Op. cit.* pág. 239.

<sup>317</sup> *Ibid.*

<sup>318</sup> Diretrizes 3/2018 do CEPD. pág. 20.

<sup>319</sup> SVANTESSON, Dan Jerker B.. **Article 3. Territorial scope...** *Op. cit.* p. 90.

Conforme esclarece Fonseca, a doutrina comumente relaciona o art. 3.2.b à noção de *profiling*, *online tracking* ou, em português, definição de perfis.<sup>320</sup> Para a autora, esse fenômeno “implica no monitoramento permanente dos internautas e a criação de perfis que, por exemplo, são mais tarde utilizados para lhes apresentar anúncios baseados nos seus interesses.”<sup>321</sup> Castelluccia, por sua vez, sintetiza a noção de *profiling* como a atividade de “transformar dados em conhecimento” que servirá para a criação de propaganda direcionada para cada indivíduo, segundo o seu padrão de consumo.<sup>322</sup> Esse processo, segundo o autor, envolve tanto a coleta dos dados, por meio do uso de algoritmos de mineração de dados, como a identificação de padrões do comportamento dos consumidores.<sup>323</sup>

Existem diversos dados que podem ser coletados para formar o perfil de um indivíduo, tais como: a idade, gênero, o local de acesso à internet, o tempo gasto em cada site, os termos procurados em mecanismos de busca, dentre outros.<sup>324</sup> Contudo, essas atividades são complexas e envolvem, ao menos, três figuras: (1) o anunciante – que é a entidade que pretende divulgar seus produtos e serviços online; (2) a página que veicula o anúncio – como, por exemplo, páginas de jornais ou aplicativos; e (3) a rede de publicidade – que é a entidade intermediadora do processo, isto é, que utiliza os mecanismos de *tracking* e *profiling* para divulgar os anúncios em determinados sites, conforme o perfil de cada indivíduo.<sup>325</sup>

A propósito, o próprio GDPR aborda o conceito de definição de perfis em seu art.4.4, conforme reproduz-se a seguir:

«Definição de perfis» qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;<sup>326</sup>

Por conseguinte, na visão de Ustaran, as empresas de comércio eletrônico bem como aquelas que fazem parte da rede de publicidade devem ser as mais afetadas pela alínea “b” do

<sup>320</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 148.

<sup>321</sup> *Ibid.*

<sup>322</sup> CASTELLUCCIA, Claude. Behavioural Tracking on the Internet: A Technical Perspective. In: GUTWITH, Serge et al. (eds.) **European Data Protection: In Good Health?** Springer: Londres, 2012. pág. 21.

<sup>323</sup> *Ibid.*

<sup>324</sup> MONDSCHIEIN, Christopher. **The Regulation of Targeted Behavioural Advertising in the European Union.** MCEL Master Working Paper 2017/2. Maastricht Centre for European Law: Maastricht, 2017. pág. 11. Disponível em: <[https://www.maastrichtuniversity.nl/sites/default/files/mcel\\_master\\_working\\_paper\\_20172\\_mondschein\\_2.pdf](https://www.maastrichtuniversity.nl/sites/default/files/mcel_master_working_paper_20172_mondschein_2.pdf)> Acesso em: 03/03/2021.

<sup>325</sup> CASTELLUCCIA, Claude. *Op. cit.* pág. 22.

<sup>326</sup> GDPR. Art. 4.4.

art. 3.2 do GDPR.<sup>327</sup> No entanto, assim como ocorre nos casos de oferta de bens e serviços para indivíduos na UE, o CEPD também afirma que é necessário que haja uma clara finalidade do controlador ou operador em controlar o comportamento dos indivíduos para posterior utilização desses dados na análise comportamental ou definição de perfis.<sup>328</sup> Nesse sentido, o Comitê aponta alguns elementos que podem ser considerados para analisar tal intenção: a publicidade comportamental; uso de geolocalização para direcionamento de propagandas; coleta de dados por meio do uso de cookies; monitoramento do estado de saúde de um indivíduo; dentre outros.<sup>329</sup>

O CEPD utiliza o exemplo hipotético de uma empresa de consultoria dos EUA que é contratada por um shopping center na França para realizar a atualização do layout do shopping conforme a movimentação dos consumidores. Para realizar tal tarefa a empresa coleta os dados de geolocalização dos consumidores que utilizam a rede Wifi do shopping para analisar o seu comportamento. Dessa forma, nesse caso, a empresa dos EUA é uma controladora que está realizando o controle do comportamento de indivíduos na União Europeia e, portanto, deve se enquadrar no disposto no art. 3.2. b.<sup>330</sup>

Não obstante o esforço do CEPD em esclarecer alguns pontos controversos do art. 3.2.b, Alsenoy indica que ainda persistem alguns questionamentos principalmente com relação à alocação de responsabilidade entre os anunciantes, os sites que veiculam os anúncios e a rede de publicidade.<sup>331</sup> Seriam todos responsáveis pelo monitoramento do comportamento dos indivíduos na UE ou somente aqueles que, de fato, operacionalizam as atividades de *tracking* e *profiling*? Neste tipo de situação, o autor sugere que seja realizada uma análise caso a caso, levando em consideração a teoria dos efeitos, explicada anteriormente.<sup>332</sup>

Por fim, ainda no que diz respeito ao art. 3.2, cabe comentar o caso dos operadores localizados fora da UE que prestam serviços para controladores que direcionam suas atividades ao mercado europeu. Para ilustrar, a CEPD descreve o exemplo de uma empresa brasileira de alimentos que oferta seus produtos a pessoas que estão na União Europeia por meio do seu site. Para melhorar suas vendas, a empresa, que nesse caso é uma controladora, contrata um operador também brasileiro para desenvolver ofertas especiais para determinados clientes com base no

---

<sup>327</sup> USTARAN, Eduardo (ed.). *Op. cit.* pág. 102.

<sup>328</sup> Diretrizes 3/2018 do CEPD. pág. 22.

<sup>329</sup> *Ibid.* pág. 23.

<sup>330</sup> *Ibid.*

<sup>331</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial... *Op. cit.* pág. 96

<sup>332</sup> *Ibid.*

histórico de compras deles e em seus dados pessoais colhidos anteriormente. Nesse sentido, tanto o controlador quanto o operador devem seguir as normas do GDPR ao realizar o tratamento dos dados dos clientes.<sup>333</sup>

O terceiro e último parágrafo do art. 3º refere-se a extensão da aplicação do GDPR para os locais onde o direito de um dos Estados-membros seja aplicável por força de disposições do Direito Internacional Público.<sup>334</sup> Nesse sentido, em linha com o Considerando 25 do GDPR, o CEPD entende que o Regulamento é aplicável para tratamento de dados pessoais realizados por embaixadas e consulados de Estados-membros da UE situados fora do bloco.<sup>335</sup>

Para Svantesson, tanto o art. 3.3 quanto o seu correspondente na Diretiva 95/46/CE partem de premissas equivocadas.<sup>336</sup> Segundo o autor, é certo que as representações diplomáticas gozam de uma série de proteções e imunidades nos termos da Convenção de Viena Sobre Relações Diplomáticas, mas isso não significa que elas tenham que automaticamente aplicar o direito do seu país de origem por força do Direito Internacional Público.<sup>337</sup> Inclusive, conforme ressalta o autor, o art. 41 da supracitada convenção prevê que aqueles que gozam de imunidades diplomáticas também devem cumprir as leis locais dos países acreditantes.<sup>338</sup>

Como essa discussão não está compreendida no objetivo do presente trabalho, não serão elaboradas maiores análises sobre o tema.

### 3.3.5 A (I)LEGITIMIDADE DA APLICAÇÃO EXTRATERRITORIAL DO GDPR

Conforme apresentado acima, apesar de o art. 3º do GDPR trazer o título “âmbito de aplicação territorial”, tanto o primeiro quanto o segundo parágrafo desse dispositivo apresentam clara vocação extraterritorial.<sup>339</sup> Até aqui foram delineadas as hipóteses em que o GDPR pode ser diretamente aplicável às entidades que não estejam localizadas dentro do território da União Europeia. Resta, contudo, a analisar mais detidamente os argumentos que outorgam ou não legitimidade a essa aplicação extraterritorial.

Para Alsenoy, o art. 3.1 do GDPR justifica-se tanto no princípio da territorialidade, que é o mais utilizado nas legislações pelo mundo, quanto na teoria dos efeitos, de acordo com

---

<sup>333</sup> Diretrizes 3/2018 do CEPD, pág. 24.

<sup>334</sup> GDPR, Art. 3.3.

<sup>335</sup> Diretrizes 3/2018 do CEPD, pág. 25.

<sup>336</sup> SVANTESSON, Dan Jerker B.. **Article 3. Territorial scope...** *Op. cit.* p. 92.

<sup>337</sup> *Ibid.*

<sup>338</sup> *Ibid.*

<sup>339</sup> *Ibid.* pág. 76.

os contornos dados pelo caso *Google Spain*.<sup>340</sup> O autor reconhece que a teoria dos efeitos encontra diversas críticas no contexto da Internet, principalmente quando interpretada em um viés expansivo. Entretanto, para o autor, a medida é necessária com vistas a dar efetividade ao direito à proteção de dados pessoais, que na União Europeia é reconhecido como um direito fundamental.<sup>341</sup> O autor também ressalta a necessidade de harmonização dos princípios da efetividade com o da não-intervenção através do uso da razoabilidade.<sup>342</sup>

Com relação ao art. 3.2, o autor afirma que o critério de destinação (*targeting criterion* ou *destination approach*) – utilizado para fundamentar o dispositivo – é amplamente reconhecido pela doutrina e jurisprudência.<sup>343</sup> Dessa forma, o considera legítimo, desde que se possa verificar que uma entidade externa está deliberadamente direcionando suas atividades para o Estado regulador.<sup>344</sup> Além disso, para o doutrinador, não há maiores impactos para os Estados estrangeiros na medida em que o uso do critério da destinação na jurisdição prescritiva intenta somente proteger os indivíduos do território interno.<sup>345</sup>

Tene e Wolf, por sua vez, consideram que a regra prevista no art. 3.1 é legítima quando interpretada restritivamente, uma vez que decorre do princípio da territorialidade.<sup>346</sup> Por outro lado, com relação ao art. 3.2, os autores fazem uso do direito comparado para afirmar que os requisitos de oferta de bens e serviços e monitoramento de comportamento deveriam ser substituídos por um teste de destinação (*targeting criterion*) melhor definido, em linha com a jurisprudência do TJUE, das cortes dos EUA e com outras legislações internacionais.<sup>347</sup> Para os autores, a aplicação extraterritorial do GDPR poderia levar a uma extensão de jurisdição para toda a Internet e, nesse caso, ferir princípios consagrados do direito internacional, como o da não-intervenção.<sup>348</sup>

Ainda durante a vigência da Diretiva 95/46/CE, Svantesson argumentava que a aplicação extraterritorial das normas de proteção de dados pessoais são, ao mesmo tempo,

---

<sup>340</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial... *Op. cit.* pág. 92-93.

<sup>341</sup> *Ibid.*

<sup>342</sup> *Ibid.*

<sup>343</sup> *Ibid.*

<sup>344</sup> *Ibid.* pág. 95-96.

<sup>345</sup> *Ibid.*

<sup>346</sup> TENE, Omer; WOLF, Christopher. **Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation.** *Future of Law Privacy Forum*. 2013. Disponível em: <<https://fpf.org/wp-content/uploads/2013/01/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-201311.pdf>> Acesso em: 04/03/2021.

<sup>347</sup> *Ibid.*

<sup>348</sup> *Ibid.*

razoáveis e irrazoáveis.<sup>349</sup> São razoáveis porque, no contexto do mundo globalizado e interligado pelas novas Tecnologias de Informação e Comunicação, um Estado não poderia dar efetividade ao direito à proteção de dados sem que tomasse medidas contra ações externas com efeitos internos.<sup>350</sup> Contudo, também são irrazoáveis na medida em que tornam extremamente oneroso o trabalho das entidades que atuam pela Internet, que acabam tendo que se adequar a diversas legislações pelo mundo.<sup>351</sup>

Dentro dessa perspectiva, em um artigo publicado em 2015, o autor propôs uma abordagem em camadas (*layered approach*) da aplicação extraterritorial das normas de proteção de dados pessoais.<sup>352</sup> Para Svantesson, a complexidade do assunto demanda que saíamos de uma perspectiva dicotômica para uma abordagem multifacetada do assunto.<sup>353</sup> Sendo assim, em apertada síntese, o autor propõe a criação de três camadas de aplicação extraterritorial das normas de proteção de dados: a primeira diria respeito ao âmbito de aplicação extraterritorial das normas de prevenção de abusos; a segunda, seria a camada dos direitos dos titulares dos dados; e, por fim, a terceira estaria relacionada com a aplicação extraterritorial das medidas administrativas.<sup>354</sup> Para cada uma delas, o autor sugere um critério de jurisdição que possa ser adotado e, inclusive, expõe como poderia ser a redação das normas que viessem a utilizar essa abordagem.<sup>355</sup>

No entendimento de Lee, a aplicação extraterritorial do GDPR está baseada numa verdadeira mistura dos princípios da territorialidade subjetiva (art. 3.1), territorialidade objetiva e teoria dos efeitos (art. 3.2.a) e nacionalidade passiva (art. 3.2.b).<sup>356</sup> Segundo o autor, entretanto, a legitimidade dessa aplicação deve ser analisada em cada caso, levando-se em consideração a real conexão dos controladores e operadores com a jurisdição prescritiva da União Europeia e o eventual conflito de jurisdições com outros Estados.<sup>357</sup>

O critério da destinação (*targeting approach*), utilizado no art. 3.2 do GDPR, foi defendido por Schultz como sendo o fundamento mais razoável e, portanto, legítimo, para o

---

<sup>349</sup> SVANTESSON, Dan Jerker. **Extraterritoriality in the context of Data Privacy Regulation**. Masaryk University Journal of Law and Technology. Vol. 7, .1. 2012.

<sup>350</sup> *Ibid.*

<sup>351</sup> *Ibid.*

<sup>352</sup> SVANTESSON, Dan Jerker. A “**layered approach**” to the extraterritoriality of data privacy laws. **International Data Privacy Law**. Vol. 3, n. 4. 2013.

<sup>353</sup> *Ibid.*

<sup>354</sup> *Ibid.*

<sup>355</sup> *Ibid.*

<sup>356</sup> LEE, Sang Woo. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing**. Tese de Doutorado. China University of Political Science and Law: Pequim, 2018. pág.209

<sup>357</sup> *Ibid.*

exercício da extraterritorialidade no contexto da Internet.<sup>358</sup> Nas palavras do autor, o critério da destinação é o meio termo entre a aplicação pura da teoria dos efeitos e a territorialidade subjetiva.<sup>359</sup> Para ele, isso ocorre porque, pelo critério da destinação, não basta que os efeitos sejam sentidos dentro de um país, mas que o controlador ou operador tenha a real intenção de direcionar suas atividades para esse país, restringindo, portanto, a teoria dos efeitos. Ao mesmo tempo, é mais abrangente do que o princípio da territorialidade subjetiva, na medida em que torna ineficaz o denominado *Forum Shopping*, explicado anteriormente neste trabalho.<sup>360</sup>

Fonseca, por seu turno, após cotejar os argumentos de grande parte da doutrina, extrai dois interesses subjacentes ao art. 3º do GDPR, que legitimam seu caráter extraterritorial.<sup>361</sup> O primeiro deles é garantir a efetiva tutela do direito fundamental à proteção de dados pessoais dos indivíduos localizados na União Europeia, tendo em vista a inexistência de fronteiras no campo da internet e a ausência de normas internacionais sobre o tema com grande adesão.<sup>362</sup> O segundo, de cunho eminentemente econômico, é evitar que o peso regulatório recaia somente sobre as empresas da União Europeia, deixando livres aquelas que não têm presença física no Velho Continente, mas que lá exercem atuação efetiva – o que poderia gerar uma desvantagem concorrencial.<sup>363</sup> Nesse norte, a autora afirma que o critério que legitima o art. 3.1 é o da territorialidade subjetiva – com alguns reflexos da teoria dos efeitos – e, com relação ao art. 3.2, o critério justificador é o da teoria dos efeitos.<sup>364</sup>

Com uma visão um pouco distinta, Azzi busca analisar a legitimidade da extraterritorialidade do art. 3º do GDPR à luz das fontes do Direito Internacional elencadas no art. 38 do estatuto da Corte Internacional de Justiça.<sup>365</sup> Como não há, ainda, tratados internacionais com grande adesão sobre o tema, a autora parte para a análise do costume internacional e, posteriormente, para os princípios gerais de Direito reconhecidos pelas nações civilizadas.<sup>366</sup>

A autora afirma que o princípio da territorialidade satisfaz os requisitos de uniformidade e reiteração por parte da prática dos Estados para ser reconhecido como um

---

<sup>358</sup> SCHULTZ, Thomas. **Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface**. The European Journal of International Law Vol. 19 no.4. 2008. pág. 817.

<sup>359</sup> Ibid.

<sup>360</sup> Ibid.

<sup>361</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. cit. pág. 150.

<sup>362</sup> Ibid. pág. 151.

<sup>363</sup> Ibid.

<sup>364</sup> Ibid. pág. 155.

<sup>365</sup> AZZI, Adèle. Op. cit. pág. 2

<sup>366</sup> Ibid.

costume internacional.<sup>367</sup> Entretanto, o mesmo não ocorre com a teoria dos efeitos que, para ela, é um dos critérios de jurisdição extraterritorial mais controverso, principalmente quando interpretado em uma perspectiva extensiva, já que na economia globalizada “tudo tem um efeito em tudo”.<sup>368</sup> Partindo para a análise da aplicação extraterritorial do GDPR sob o viés dos princípios de direito reconhecido pelas nações, a autora afirma que diversos são os países que têm seguido os padrões da União Europeia e adotado leis de proteção de dados pessoais com aplicação extraterritorial, a exemplo da Austrália e Singapura, o que leva a perceber uma tendência cada vez maior na utilização desse critério.<sup>369</sup>

O Brasil também adotou uma abordagem muito similar na sua Lei Geral de Proteção de Dados (LGPD) quanto ao seu escopo de aplicação territorial, embora com algumas peculiaridades.<sup>370</sup> A redação final do art. 3º da LGPD, aprovada em 2018, é a seguinte:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I - a operação de tratamento seja realizada no território nacional;
- II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei..<sup>371</sup>

A primeira diferença que se verifica entre o artigo da lei brasileira e o art. 3º do GDPR é que, enquanto este último apresenta somente aspectos territoriais no dispositivo, o artigo da LGPD mescla tanto aspectos do escopo material quanto territorial.<sup>372</sup>

Quando desprezadas as diferenças de técnica de redação legislativa de ambas as normas, verifica-se que o inciso I do art. 3º da LGPD segue o mesmo princípio da territorialidade estabelecido no art. 3.1 do GDPR. Para Vainzof, o dispositivo da lei brasileira é ainda mais abrangente, uma vez que não limita sua aplicação às atividades de tratamento de

<sup>367</sup> *Ibid.*

<sup>368</sup> *Ibid.*

<sup>369</sup> *Ibid.* pág. 3.

<sup>370</sup> VAINZOF, Rony. Capítulo I - Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.) **LGPD: Lei Geral de Proteção de dados comentada**. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-85-5321-925-4. pág. 54.

<sup>371</sup> BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de dados Pessoais. Diário Oficial da União, Brasília, DF, n. 157, publicado em 15/08/2018. Seção 1, página 59. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)> Acesso em: 13/03/2021.

<sup>372</sup> VAINZOF, Rony. Op. cit.

dados relacionados a um estabelecimento, como o faz o GDPR. Com relação aos incisos II e III, pode-se inferir que o critério da destinação (*targeting criterion*) também está presente<sup>373</sup>, o que é um indicativo do aumento do uso desse tipo de disposição nas legislações de proteção de dados pelo mundo e, conseqüentemente, de sua legitimidade.

Conforme visto até aqui, a aplicação extraterritorial de leis não é nova e, no contexto das emergentes Tecnologias da Informação e Telecomunicação, é provável que se multipliquem.<sup>374</sup> Dessa forma, uma vez cotejados os argumentos doutrinários, conclui-se que a aplicação extraterritorial art. 3º do GDPR é legítima tanto pelo ponto de vista do critério da territorialidade quanto do critério da destinação. Não fosse assim, os Estados e agentes reguladores em geral não teriam instrumentos para efetivar a proteção aos direitos fundamentais dos indivíduos no âmbito digital.<sup>375</sup>

### 3.3.6 A AUSÊNCIA DE *ENFORCEMENT* ENQUANTO LIMITADOR DA APLICAÇÃO EXTRATERRITORIAL

Ainda que considerada legítima, isso não significa que a aplicação extraterritorial do GDPR é, na prática, seguida pelas empresas que se encontram abarcadas por ela. Nesse sentido, a impossibilidade dos órgãos administrativos e judiciais da União Europeia de executar suas decisões (*enforcement*) ou exercer sua jurisdição executiva em território estrangeiro torna-se um dilema para os resultados práticos da extraterritorialidade do Regulamento.<sup>376</sup>

O art. 58.2 do GDPR concede às autoridades de dados dos Estados-membros diversos poderes para garantir a execução dos seus dispositivos, tais como: impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição; impor multas, nos parâmetros estabelecidos pelo art. 83; ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais; dentre outros.<sup>377</sup> Entretanto, considerando que essas medidas não têm coercitividade para fora das fronteiras da UE, a doutrina discute como o Regulamento pode efetivamente garantir a proteção de dados aos

---

<sup>373</sup> *Ibid.*

<sup>374</sup> GREZE, Benjamin. **The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives.** International Data Privacy Law., Vol. 9, No. 2. 2019. pág. 110.

<sup>375</sup> ALSENOY, Brendan Van. Reconciling the (extra)territorial... Op. cit. pág. 92-93; LEE, Sang Woo. Op. Cit.pág. pág.209; SCHULTZ, Thomas. Op. Cit. pág. 817. FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. cit. pág. 150. GREZE, Benjamin. Op. cit. pág. 110.

<sup>376</sup> BELETSK, Roman. Op. cit. pág. 69.

<sup>377</sup> GDPR. Art. 58.2.

indivíduos que estejam na UE nas ocasiões em que esses dados são tratados por empresas estrangeiras sem presença física no bloco.

A esse respeito, Svantesson é enfático ao afirmar que o Regulamento “*bites off more than it can chew*” (morde mais do que pode mastigar, em tradução livre).<sup>378</sup> Isso significa que, para o autor, o GDPR estabelece um âmbito de aplicação extraterritorial amplo, mas que, na prática, torna difícil para as autoridades de dados dos Estados-membros fiscalizar e, se necessário, aplicar sanções às entidades que não tenham presença física na União Europeia.<sup>379</sup> Esse fator, conforme salienta o autor em outro texto, pode levar à própria deslegitimação internacional do Regulamento, na medida em que a falta de recursos para investigar e punir todos os ilícitos poderá ocasionar em punições mais seletivas e, até mesmo, subjetivas.<sup>380</sup>

Para Greze, por outro lado, não é necessário que as autoridades de dados punam cada caso de infração à norma para que ela seja de fato respeitada.<sup>381</sup> Para o autor, o que é necessário, de fato, é que as entidades destinatárias do Regulamento saibam que existem meios para sancioná-las, em caso de desconformidade.<sup>382</sup> Nesse sentido, o autor lista diversas alternativas que as autoridades regulatórias podem tomar para garantir o cumprimento da norma externamente.

Um desses meios é o poder do constrangimento (*power of embarrassment*), que tem maior efetividades para as empresas de grande porte, uma vez que uma multa aplicada pelas autoridades de dados pode causar maiores impactos para a reputação dessas organizações e, eventualmente, até mesmo resultar na queda de seu valor de mercado.<sup>383</sup> Foi o que ocorreu em julho de 2018, por exemplo, quando a empresa Facebook perdeu mais de 100 bilhões de dólares em valor de mercado, em razão dos escândalos de vazamento de dados envolvendo a empresa *Cambridge Analytica* e também devido a então recente entrada em vigor do GDPR – que ocorreu em maio do mesmo ano.<sup>384</sup>

Outro meio que deve ser empregado para dar efetividade à execução extraterritorial do GDPR, segundo o autor, é a cooperação internacional tanto das entidades de cunho administrativo quanto judicial. Entretanto, o autor admite que, atualmente, a cooperação é ainda

---

<sup>378</sup> SVANTESSON, Dan Jerker. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. *International Data Privacy Law*. Vol. 5, No. 4. 2015. pág. 232.

<sup>379</sup> *Ibid.*

<sup>380</sup> SVANTESSON, Dan Jerker B.. Article 3. Territorial scope... *Op. cit.* p. 95.

<sup>381</sup> GREZE, Benjamin. *Op. cit.* pág. 112.

<sup>382</sup> *Ibid.*

<sup>383</sup> *Ibid.*

<sup>384</sup> THE WASHINGTON POST. **How years of privacy controversies finally caught up with Facebook.** Disponível em: <<https://www.washingtonpost.com/technology/2018/07/26/how-years-privacy-controversies-finally-caught-up-with-facebook/>>. Acesso em: 10/03/2021.

pouco utilizada e encontra diversas barreiras burocráticas, até mesmo entre os próprios países europeus dentro do mecanismo de balcão único.<sup>385</sup>

A obrigatoriedade de indicação de um representante na UE para entidades que não tenham presença física nos países do bloco também é citada por Greze e por Fonseca como uma alternativa para forçar o cumprimento da norma.<sup>386</sup> O art. 27.1 do GDPR determina que “se for aplicável o artigo 3.º, nº 2, o controlador ou o operador devem designar por escrito um representante seu na União.”<sup>387</sup> Esse representante, que pode ser uma pessoa natural ou jurídica, serve como ponto de contato entre as autoridades de proteção de dados e os controladores ou operadores estrangeiros.<sup>388</sup> O Considerando 80 do GDPR, ao explicar o art. 27, elucida que a designação de tal representante não afeta as responsabilidades dos controladores ou operadores; entretanto, ainda assim, estes representantes deverão estar sujeitos aos procedimentos de execução em caso de descumprimento dos dispositivos da norma pelos controladores e operadores que representam.<sup>389</sup> Cabe ressaltar, contudo, que o Considerando 80 não tem força normativa cogente e, além disso, o art. 58 não delega expressamente poder às autoridades de dados para punir com multas ou outras sanções o representante.<sup>390</sup> Como consequência, a utilização deste meio de coerção é questionável, segundo a doutrina.<sup>391</sup>

Dois pontos são ressaltados por Fonseca ao analisar a responsabilização do representante como forma de coibir as empresas estrangeiras a se adequarem ao GDPR. O primeiro deles é o fato de que as relações obrigacionais entre representante e representados variam de acordo com as definições dadas por cada direito interno dos Estados-membros da UE e, portanto, enquanto para alguns países a aplicação de multas e outras sanções podem ser direcionadas diretamente para o representante, para outros não.<sup>392</sup> O segundo está relacionado às hipóteses em que o controlador ou operador externo sequer indicou um representante na União Europeia, como já ocorreu em um caso envolvendo a empresa *Whatsapp*.<sup>393</sup>

Para além das medidas até aqui descritas, algumas alternativas, que não estão expressamente previstas no Regulamento, são defendidas por parte da doutrina. Svantesson

---

<sup>385</sup> *Ibid.* pág. 117.

<sup>386</sup> *Ibid.* pág. 123; FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 215.

<sup>387</sup> GDPR. Art. 27.1.

<sup>388</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 215.

<sup>389</sup> GDPR. Considerando 80.

<sup>390</sup> BELETSK, Roman. *Op. cit.* pág. 72.

<sup>391</sup> *Ibid.*

<sup>392</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 218.

<sup>393</sup> *Ibid.*

intitula essas ações como “ações de destruição de mercado.”<sup>394</sup> O autor sugere que, em determinadas situações, após a devida ponderação dos princípios envolvidos, os Estados possam lançar mão de ações mais extremas como: proibir que o controlador ou operador infrator exerça suas atividades dentro de suas fronteiras; congelar ativos dos infratores; e proibir que outras empresas locais façam negócios com o agente infrator.<sup>395</sup>

Para exemplificar o funcionamento dessas medidas na prática, o autor menciona o caso brasileiro julgado pela 1ª Vara Cível da Comarca de Pinheiros -SP, em que o juiz determinou, em sede de tutela de urgência, que a empresa Facebook retirasse do ar *posts* ofensivos feitos por uma modelo e apresentadora contra seu vizinho. No caso, o juiz deu prazo de 48h para que a empresa cumprisse a decisão sob pena de ter suas atividades suspensas no território nacional.<sup>396</sup> Segundo o autor, apesar de desproporcional, a medida demonstra como um Estado pode encontrar maneiras de agir territorialmente para coibir práticas ilegais cometidas por agentes externos.<sup>397</sup>

Para Fonseca e Greze, considerando os enormes impactos que podem ter para a sociedade, a adoção legislativa ou jurisprudencial das medidas sugeridas por Svantesson devem ser sempre analisadas à luz da razoabilidade e proporcionalidade, e devem incluir a análise do tipo de infração cometida, o tipo de dados tratados, bem como outras especificidades do caso concreto.<sup>398</sup>

Ademais, em se tratando da implementação do GDPR fora das fronteiras da UE, não se pode olvidar o recente entendimento firmado pelo TJUE no caso conhecido como *Google Spain II*.<sup>399</sup> Nesse caso, a *Commission Nationale de l’informatique et de Libertés*, autoridade responsável pela proteção de dados na França, aplicou uma multa de 100 mil euros à *Google LLC* por não ter a empresa implementado a decisão do caso *Google Spain* globalmente, ou seja, por ter limitado a implementação da decisão do TJUE aos domínios dos Estados-membros da UE.<sup>400</sup>

---

<sup>394</sup> SVANTESSON, Dan Jerker B. **Solving The Internet Jurisdiction Puzzle...** *Op. cit.* pág. 142.

<sup>395</sup> *Ibid.* pág. 142-143.

<sup>396</sup> *Ibid.* pág. 148. BRASIL. Tribunal de Justiça de São Paulo. Ação. nº 0005243-38.2013.8.26.0011. Luizeani Altenhofen. Eudes Gondim Junior. Pinheiros, SC, 04 de abril de 2013. Diário de Justiça do Tribunal de Justiça de São Paulo. São Paulo.

<sup>397</sup> SVANTESSON, Dan Jerker B. **Solving The Internet Jurisdiction Puzzle...** *Op. cit.* pág. 148.

<sup>398</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 218; GREZE, Benjamin. *Op. cit.* pág. 126.

<sup>399</sup> TJUE. C-507/17. Caso *Google LLC v. Commission Nationale de l’Informatique et de Libertés*. Julgado em: 24/09/2019.

<sup>400</sup> *Ibid.*

Ao julgar o caso, a corte faz referência à teoria dos efeitos, reconhecendo que a natureza “ubiquitária” da Internet pode possibilitar que eventual tratamento de dados realizados fora da UE tenha efeitos internos aos países do bloco.<sup>401</sup> Entretanto, os julgadores também advertem que o direito à proteção de dados não é absoluto e deve ser sopesado em contraste com outros direitos, como o direito à liberdade de informação dos internautas.<sup>402</sup> Além disso, levou-se em consideração que nem todos os países do mundo reconhecem o direito ao esquecimento, objeto do primeiro caso *Google Spain*.<sup>403</sup> Sendo assim, ao final, o Tribunal entendeu que a empresa *Google LLC* não teria o dever de implementar a decisão do caso *Google Spain* para além dos domínios do seu mecanismo de busca que sejam referentes aos Estados-membros da União Europeia.<sup>404</sup> A decisão demonstra, portanto, uma inclinação do TJUE em aplicar o *enforcement* do GDPR de maneira restritiva.

Conforme mencionado anteriormente, o que chama a atenção no texto do GDPR, além de sua aplicação extraterritorial, é a gravidade das multas que podem ser aplicadas às entidades infratoras, podendo chegar a 4% do lucro líquido anual internacional das empresas.<sup>405</sup> Após quase 3 anos de vigência do GDPR, já foram aplicadas quase 600 multas por descumprimento do Regulamento<sup>406</sup> que, juntas, somam aproximadamente 270 milhões de euros.<sup>407</sup>

Ainda assim, dados revelados pelo jornal *The New York Times* em abril de 2020 demonstraram que os recursos financeiros e de pessoal das autoridades de dados dos Países-membros são insuficientes para a demanda de denúncias que surgem.<sup>408</sup> Na mesma publicação, a presidente da Autoridade de Proteção de Dados da Alemanha, entidade com o maior orçamento dentre seus pares, reconhece que existe “*a lack of enforcement*” (uma falta de aplicação da lei, em tradução livre).<sup>409</sup> Essa percepção é também corroborada por um relatório divulgado pelo CEPD em fevereiro de 2020, que aponta que 21 das 30 autoridades de proteção

---

<sup>401</sup> *Ibid.* parágrafo 57.

<sup>402</sup> *Ibid.* parágrafo 60.

<sup>403</sup> A propósito, em fevereiro de 2021, o Supremo Tribunal Federal do Brasil julgou que o Direito ao Esquecimento é incompatível com a Ordem Constitucional Brasileira, negando seguimento ao Recurso Extraordinário (RE) 1010606, com repercussão geral reconhecida.

<sup>404</sup> TJUE. C-507/17. Caso *Google LLC v. Commission Nationale de l’Informatique et de Libertés*. Julgado em: 24/09/2019. parágrafo 73.

<sup>405</sup> GDPR. Art. 83.5.

<sup>406</sup> GDPR Enforcement Tracker. Disponível em: <<https://www.enforcementtracker.com/?insights>>. Acesso em: 20/03/2021.

<sup>407</sup> *Ibid.*

<sup>408</sup> THE NEW YORK TIMES. **Europe’s Privacy Law Hasn’t Shown Its Teeth, Frustrating Advocates.** Disponível em: <<https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html?searchResultPosition=6>>. Acesso em: 20/03/2021.

<sup>409</sup> *Ibid.*

de dados que aplicam o GDPR alegam não ter os recursos financeiros e de pessoal adequados para o cumprimento de suas funções.<sup>410</sup>

Ante o exposto, pode-se inferir que a execução direta dos dispositivos do GDPR ainda não é adequada, segundo a doutrina. Todavia, existem também outros impactos extraterritoriais indiretos trazidos pelo GDPR, que também devem ser levados em consideração, conforme será brevemente exposto no subitem seguinte.

### 3.3.7 OUTROS IMPACTOS EXTRATERRITORIAIS DO GDPR: A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS E O EFEITO BRUXELAS

Muito se discute na doutrina sobre a diferença entre a aplicação extraterritorial do GDPR em contraste com os seus impactos extraterritoriais.<sup>411</sup> Enquanto para Poulet, por exemplo, existe uma clara distinção entre esses dois conceitos,<sup>412</sup> Kuner afirma que, na prática, essa diferenciação não tem importância significativa.<sup>413</sup> Sem entrar no mérito da discussão, registra-se que, para fins de simplificação metodológica, o presente trabalho tem como foco analisar como o GDPR pode ser diretamente aplicável às entidades estrangeiras; mesmo assim, não se ignoram as demais formas pelas quais o Regulamento alcança efeitos para além da União Europeia. Nesse sentido, deve-se mencionar uma das manifestações mais evidentes dessa influência global do GDPR: o regime de transferência internacional de dados pessoais.<sup>414</sup>

De acordo com os dispositivos do capítulo 5 do GDPR, a transferência de dados pessoais da União Europeia para terceiros países ou organizações internacionais somente poderá ser realizada caso seja verificado nesses locais um nível adequado de proteção de dados pessoais, segundo os padrões estabelecidos pela própria União Europeia.<sup>415</sup> Esse nível proteção adequado deve ser examinado levando-se em conta diversos fatores, tais como: a legislação local do terceiro país; a existência ou não de uma autoridade de proteção de dados independente; as possibilidades de acesso à justiça para a tutela do direito de proteção de dados pessoais; os

<sup>410</sup> CEPD. Contribution of the EDPB to the evaluation of the GDPR under Article 97. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_contributiongdprevaluation\\_20200218.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf)>. Acesso em: 20/03/2021. pág. 30.

<sup>411</sup> KUNER, Christopher. **Extraterritoriality and regulation of international data transfers in EU data protection law**, International Data Privacy Law. Vol 5, n. 4. Novembro de 2015. páginas 235–245. DOI: <https://doi.org/10.1093/idpl/ipv019>.

<sup>412</sup> POULLET, Yves. **Transborder Data Flows and Extraterritoriality: the European Position**. Journal of International Commercial Law and Technology, vol. 2, no. 3, 2007, páginas. 141-153.

<sup>413</sup> KUNER, Christopher. **Extraterritoriality**... Op. cit. pág. 2.

<sup>414</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. Op. cit. pág. 218

<sup>415</sup> GDPR. Art. 45, caput.

compromissos internacionais do país com relação à proteção de dados pessoais; dentre vários outros requisitos.<sup>416</sup>

É por meio das chamadas decisões de adequação que a Comissão Europeia certifica que um determinado país ou organização internacional garante um nível adequado de proteção de dados e, dessa forma, permite que se estabeleça um fluxo de dados entre esses locais e a União Europeia, sem a necessidade de outras autorizações ou garantias.<sup>417</sup> Até o momento, a Comissão já concedeu 12 decisões de adequação para países e territórios, dentre eles, dois países do Mercosul: Argentina e Uruguai.<sup>418</sup> Destaca-se, entretanto, que a maioria dessas decisões foi concedida ainda sob a égide da Diretiva 95/46/CE, de modo que mesmo os países que já se encontravam sob a tutela de tais mecanismos precisaram se atualizar com relação aos novos dispositivos trazidos pelo GDPR. É o caso, por exemplo, da própria Argentina, que desde 2016 discute a criação de uma nova lei de proteção de dados pessoais.<sup>419</sup>

Os Estados Unidos, maior potência econômica global<sup>420</sup> e sede das maiores empresas de Tecnologia da Informação do mundo, têm um histórico conturbado com a UE no que diz respeito à transferência internacional de dados pessoais.<sup>421</sup> No ano de 2000, a União Europeia e os Estados Unidos firmaram um acordo denominado *Safe Harbour* (porto seguro, em tradução livre), por meio do qual foram estabelecidos princípios e regras para o fluxo de dados entre as duas entidades.<sup>422</sup> Pelo acordo, as autoridades americanas deveriam criar uma listagem de empresas que ganhariam um certificado de conformidade e que, portanto, poderiam receber os

---

<sup>416</sup> GDPR. Art. 45.2.

<sup>417</sup> CEPD. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_recommendations\\_202001\\_supplementarymeasures\\_transfer\\_tools\\_pt.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasures_transfer_tools_pt.pdf)>. Acesso em 22/03/2021. pág. 11.

<sup>418</sup> Comissão Europeia. Adequacy decisions. Disponível em: <[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea)>. Acesso em 22/03/2021.

<sup>419</sup> ARGENTINA. Proyecto de Ley de Protección de Datos Personales. Disponível em: <<https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales>>. Acesso em: 20/04/2021.

<sup>420</sup> BANCO MUNDIAL. World Development Indicators. Disponível em: <<https://databank.worldbank.org/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=>>>. Acesso em: 23/03/2021.

<sup>421</sup> KLOSA, Dariusz; SVANTESSON, Dan Jerker (eds.). **Trans-atlantic Data Privacy Relations as a Challenge for Democracy**. European Integration and Democracy Series. Volume 4. Cambridge: Intersentia, 2017.

<sup>422</sup> UNIÃO EUROPEIA. Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção 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://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520>>. Acesso em: 23/03/2021.

dados transferidos do bloco europeu.<sup>423</sup> Nesse contexto, a Comissão Europeia deu uma decisão de adequação para os EUA limitada às empresas participantes do programa *Safe Harbour*.<sup>424</sup>

As transferências de dados entre a UE e os EUA passaram a ocorrer normalmente por meio desse mecanismo até que, em 2013, os escândalos de espionagem perpetrados pela *National Security Agency* dos EUA e revelados por Edward Snowden colocaram em dúvida a efetividade da proteção dos dados transferidos por meio do acordo.<sup>425</sup> Dois anos depois, o caso *Schrems I* colocou o referido acordo sob análise do TJUE.<sup>426</sup> Ao final do processo, a Corte de Luxemburgo decidiu pela invalidade da decisão de adequação concedida pela Comissão, uma vez que, segundo a Corte, não havia nos EUA leis que protegessem os dados pessoais transferidos contra interferências das autoridades e nem mesmo recursos judiciais adequados para tutelar esses direitos.<sup>427</sup>

A decisão acendeu o alerta para as autoridades dos EUA e da União Europeia, haja vista que cerca de quatro mil empresas americanas utilizavam o *Safe Harbour* como meio para receber dados da UE. Rapidamente, as autoridades dos dois lados do Atlântico trataram de reformular os termos do antigo acordo e criar um novo enquadramento para o fluxo de dados pessoais.<sup>428</sup> As autoridades americanas firmaram alguns compromissos com relação aos casos de coleta de dados pelas autoridades públicas e também com relação à melhorias na capacidade fiscalizatória das empresas.<sup>429</sup> Esse esforço resultou, já em 2016, em um novo acordo e uma nova decisão de adequação pela Comissão Europeia, que recebeu o nome de *Privacy Shield*.<sup>430</sup>

Apesar de aprovado por todos os países do bloco, o *Privacy Shield* foi criticado por membros do Parlamento Europeu e pelo próprio CEPD pela existência de lacunas e ambiguidades, que poderiam acarretar insegurança jurídica e eventuais infrações aos regimentos de proteção de dados da UE.<sup>431</sup> Assim como ocorreu como o *Safe Harbour*, em

---

<sup>423</sup> *Ibid.*

<sup>424</sup> *Ibid.*

<sup>425</sup> KLOSA, Dariusz; SVANTESSON, Dan Jerker (eds.). *Op. cit.* pág 11.

<sup>426</sup> TJUE. C-362/14. Caso *Schrems*. Julgado em 2015.

<sup>427</sup> MONTELEONE, Shara; PUCCIO, Laura. **From Safe Harbour to Privacy Shield Advances and shortcomings of the new EU-US data transfer rules**. Bruxelas: União Europeia, 2017. pág. 1. Disponível em: <[https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS\\_IDA\(2017\)595892\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf)>. Acesso em 23/03/2021.

<sup>428</sup> *Ibid.*

<sup>429</sup> *Ibid.* pág. 27.

<sup>430</sup> UNIÃO EUROPEIA. Decisão de Adequação da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: <[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.207.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG)>. Acesso em: 23/03/2021.

<sup>431</sup> MONTELEONE, Shara; PUCCIO, Laura. *Op. cit.* págs 32-33.

2020, a nova decisão de adequação que embasou as transferências pelo *Privacy Shield* foi levada ao TJUE, no caso que ficou conhecido como *Schrems II*.<sup>432</sup>

Novamente, a Corte se posicionou pela invalidade da decisão de adequação, pois considerou que ainda existiam riscos para os dados pessoais de indivíduos da UE transferidos para os EUA.<sup>433</sup> Isso porque, segundo a Corte, alguns programas de vigilância utilizados pelas autoridades públicas dos EUA ainda permitiam acesso indiscriminado aos dados pessoais advindos da UE e, além disso, as empresas eram legalmente obrigadas a repassar esses dados. Ademais, para os julgadores, a autoridade responsável pela fiscalização do cumprimento do acordo (ombudsman) não tinha a independência necessária para executar suas funções.<sup>434</sup>

No julgamento do caso *Schrems II* o TJUE sedimentou o entendimento de que não é necessário que as normas de proteção de dados pessoais dos terceiros países sejam iguais às da UE, mas ao menos deve haver uma equivalência entre os níveis de proteção de dados – o que não foi constatado no caso dos EUA.<sup>435</sup>

Diversas reações foram manifestadas por autoridades dos EUA após o julgamento do caso.<sup>436</sup> O secretário de estado americano à época, Mike Pompeo, chegou a declarar publicamente seu “profundo desapontamento” com a decisão da Corte, alegando que os prejuízos imediatos ultrapassaram a casa dos sete milhões de dólares.<sup>437</sup>

Cabe salientar, entretanto, que o fato de não existir uma decisão de adequação para um determinado país não torna a transferência de dados proibida, pois os art. 46 e 49 do GDPR enumeram outras hipóteses em que essas transferências podem ocorrer,<sup>438</sup> como por exemplo, por meio da estipulação de cláusulas-tipo de proteção de dados entre as entidades de origem e de destino dos dados pessoais,<sup>439</sup> formulação de códigos e conduta<sup>440</sup> e, até mesmo, por simples consentimento do titular dos dados em casos específicos.<sup>441</sup>

---

<sup>432</sup> Os casos *Schrems I* e *II* receberam essa nomenclatura, pois ambos foram movidos pelo ativista austríaco Maximillian Schrems.

<sup>433</sup> TJUE. C-311/18. Caso *Schrems II*. Julgado em 2020.

<sup>434</sup> *Ibid.*

<sup>435</sup> *Ibid.*

<sup>436</sup> PARLAMENTO EUROPEU. **The CJEU judgment in the Schrems II case**. Disponível em: <[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS\\_ATA\(2020\)652073\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)>. Acesso em: 23/03/2021.

<sup>437</sup> REUTERS. Pompeo 'deeply disappointed' in EU court decision to ditch trans-Atlantic data transfer deal. Disponível em: <<https://www.reuters.com/article/us-facebook-privacy-eu-usa-idUSKCN24I2GS>>. Acesso em: 23/03/2021.

<sup>438</sup> CEPD. Recomendações 01/2020. *Op. cit.* pág.12-13.

<sup>439</sup> GDPR. Art. 46.2.d.

<sup>440</sup> GDPR. Art.46.2.e

<sup>441</sup> GDPR. Art. 49.1.a.

Conforme ressalta Osman e Soares, os impactos extraterritoriais do regime de transferência internacional de dados pessoais do GDPR são claramente perceptíveis quando se analisa o caso dos EUA – mencionado acima – e também de outros países que mantêm relações comerciais com o bloco.<sup>442</sup> Por meio do mecanismo das decisões de adequação, a UE exerce influência sobre outros países para que estes adotem medidas legislativas e regulatórias semelhantes às suas.<sup>443</sup> O mesmo fenômeno ocorreu com relação ao Brasil, com a adoção de bases principiológicas e dispositivos com claras inspirações no GDPR na sua própria legislação de proteção de dados, a LGPD.<sup>444</sup> Dentro dessa perspectiva, segundo Fonseca, o regime de transferência de dados do GDPR caracteriza-se como uma verdadeira “exportação” dos padrões regulatórios da União Europeia,<sup>445</sup> fazendo dessa organização um “regulador global” ou “empreendedor normativo”.<sup>446</sup>

Bradford explica essa influência regulatória global da União Europeia por meio do conceito de *Brussels Effect* (Efeito Bruxelas, em tradução livre).<sup>447</sup> O termo decorre do chamado *California Effect*, que foi cunhado pela doutrina norte-americana para se referir à capacidade do estado da Califórnia em ditar os padrões regulatórios aplicados aos demais estados dos EUA, em razão do tamanho do seu mercado e pela sua disposição em adotar regras rígidas, principalmente nos campos do direito ambiental e do consumidor.<sup>448</sup>

Conforme afirma a autora, apesar dos diversos desafios estruturais e conjunturais que a União Europeia enfrenta atualmente – tais como as desconfiças geradas pelo Brexit, o crescimento do euroceticismo, pressões geopolíticas da Rússia, entre outros –, o bloco europeu detém ainda um poder unilateral de regulador global.<sup>449</sup> Para Bradford, isso se dá porque as empresas que operam na União Europeia ou que estabelecem relações comerciais com o bloco acabam voluntariamente aplicando os padrões que lhes são exigidos nos países da UE para suas subsidiárias e sucursais nos demais países do mundo, evitando os custos de ter que implantar programas de conformidade para cada legislação local.<sup>450</sup> Além disso, como os padrões

---

<sup>442</sup> OSMAN, Bruna Homem de Souza; SOARES, Jéssica Aparecida. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS: A extraterritorialidade do GDPR europeu e seus impactos. In: WACHOWICZ, Marcos (org.). **Proteção de Dados em Perspectiva: LGPD e RGPD na ótica do Direito Comparado**. Curitiba: Gedai, UFPR 2020. pág. 583.

<sup>443</sup> *Ibid.*

<sup>444</sup> *Ibid.*

<sup>445</sup> FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. *Op. cit.* pág. 292.

<sup>446</sup> *Ibid.*

<sup>447</sup> BRADFORD, Anu. **The Brussels Effect: How the European Union Rules the World**. Nova Iorque: Oxford University Press, 2020.

<sup>448</sup> *Ibid.* pág. 3.

<sup>449</sup> *Ibid.* pág. XIV.

<sup>450</sup> *Ibid.* pág. XIV

regulatórios na EU em diversos campos são os mais altos do mundo, a conformidade com o direito da UE implica, em certa medida, na conformidade com os padrões internacionais em diferentes campos do direito.<sup>451</sup>

Dessa forma, sem nenhuma necessidade de coerção, a UE vai expandindo os efeitos das suas normas para além do Velho Continente. Contudo, segundo a autora, esse fenômeno não deve ser somente atribuído à importância econômica do mercado europeu no contexto internacional.<sup>452</sup> Não fosse assim, poder-se-ia também falar em “*Washington Effect*” ou, até mesmo, em “*Beijing Effect*”. Trata-se, portanto, de uma combinação de fatores, quais sejam: “tamanho do mercado, capacidade regulatória, padrões rigorosos, destinatários inelásticos e não-divisibilidade.”<sup>453</sup>

Sem a intenção de explorar as minúcias de cada fator descrito acima, cabe comentar, brevemente, os mais importantes deles. O tamanho do mercado está ligado à quantidade de consumidores e às características desses consumidores, como a sua renda.<sup>454</sup> Com uma população de cerca de 448 milhões de pessoas<sup>455</sup> e um PIB per capita de aproximadamente 35 mil dólares,<sup>456</sup> a União Europeia é um mercado atrativo para qualquer empresa que busca a internacionalização. Além disso, quando contabilizado pelo conjunto dos países que a compõem, a UE tem o segundo maior PIB do mundo, atrás somente dos EUA.<sup>457</sup>

A capacidade regulatória, por sua vez, tem relação com a “habilidade de promulgar e executar regulamentos” do bloco europeu, que somente é possível pela existência de instituições sofisticadas e bem estruturadas, conforme elucidado no primeiro capítulo deste trabalho.<sup>458</sup> Em conjunto com a capacidade regulatória, também caminha a disposição da UE em criar normas mais rigorosas em campos sensíveis para sociedade, como, por exemplo, a proteção do meio ambiente, do consumidor e de dados pessoais.<sup>459</sup>

---

<sup>451</sup> *Ibid.* pág. XV.

<sup>452</sup> *Ibid.* pág. 25.

<sup>453</sup> *Ibid.*

<sup>454</sup> *Ibid.* pág 16-17.

<sup>455</sup> EUROSTAT. EU population in 2020: almost 448 million. Disponível em: <[<sup>456</sup> BANCO MUNDIAL. GDP per capita \(current US\\$\) - European Union. Disponível em: <<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=EU>>. Acesso em: 23/03/2021.](https://ec.europa.eu/eurostat/documents/2995521/11081093/3-10072020-AP-EN.pdf/d2f799bf-4412-05cc-a357-7b49b93615f1#:~:text=On%201%20January%202020%2C%20the,States%20on%201%20January%202019.>.</a>>. Acesso em: 23/03/2021.</p>
</div>
<div data-bbox=)

<sup>457</sup> BANCO MUNDIAL. GDP (current US\$) - European Union, United States, China. Disponível em: <[https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN&name\\_desc=true](https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN&name_desc=true)>. Acesso em: 23/03/2021.

<sup>458</sup> BRADFORD, Anu. *Op. cit.* pág. 30-31.

<sup>459</sup> *Ibid.* 37-38.

O conceito de inelasticidade dos destinatários dos Regulamentos da UE está intrinsicamente ligado à coibição do chamado *Forum Shopping*, termo que já foi explicado anteriormente neste trabalho. Ao utilizar dispositivos que tornam ineficaz qualquer tentativa dos agentes econômicos de contornar a legislação do bloco, buscando outras jurisdições mais favoráveis, a UE torna seus alvos regulatórios mais fixos e, portanto, consegue atuar extraterritorialmente de maneira mais eficaz.<sup>460</sup>

Por fim, o critério da não-divisibilidade diz respeito à ação das corporações com atuação internacional no sentido de padronizar sua produção e suas práticas gerenciais.<sup>461</sup> Para a autora, esse movimento só ocorre quando “os benefícios de economias de escala pela padronização excedem os custos de renunciar à busca por custos mais baixos em mercados menos regulados.”<sup>462</sup> O maior benefício desse tipo de prática, conforme já ressaltado, é poder estar de acordo com várias legislações ao mesmo tempo a partir da conformidade com a mais exigente delas.

Em se tratando especificamente do contexto da proteção de dados, a autora ressalta que o GDPR criou um “*De Facto Brussels Effect*” e “*De Jure Brussels Effect*”.<sup>463</sup> *De Facto Brussels Effect*, porque para as grandes empresas de tecnologia é, na prática, inviável sair do mercado europeu e, do mesmo modo, seria muito custoso – além tecnicamente inviável – implementar diferentes maneiras de tratamento de dados para cada país do mundo. Portanto, elas acabam enquadrando-se nos dispositivos art. 3º do Regulamento.<sup>464</sup> E *De Jure Brussels Effect*, porque o GDPR – e a Diretiva 95/46 antes dele – é a inspiração para grande parte das quase 120 legislações de proteção de dados que atualmente existem ao redor do mundo.<sup>465</sup>

Diante do que foi até aqui exposto, verifica-se que a extraterritorialidade do GDPR pode se manifestar tanto diretamente quanto indiretamente. Pela via direta, quando as empresas realizam o tratamento de dados pessoais de indivíduos que se encontram na UE por meio de um estabelecimento em algum país do bloco ou destinando seus produtos e serviços ou ainda monitorando o comportamento dessas pessoas. Já a manifestação indireta ocorre pelas regras que regulamentam a transferência internacional de dados pessoais ou, até mesmo, pelas próprias empresas que padronizam seus processos de tratamento de dados pessoais internacionalmente de acordo com os *standards* europeus.

---

<sup>460</sup> *Ibid.* 48-49.

<sup>461</sup> *Ibid.* 53-54.

<sup>462</sup> *Ibid.* pág. 54.

<sup>463</sup> *Ibid.* pág. 142.

<sup>464</sup> *Ibid.* pág. 143.

<sup>465</sup> *Ibid.* pág. 148.

#### 4 OS IMPACTOS DA APLICAÇÃO EXTRATERRITORIAL DO GDPR PARA AS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO EM FLORIANÓPOLIS - SC

O município de Florianópolis, capital do estado de Santa Catarina, além de ser conhecido por seu potencial turístico, com suas 42 praias e diversas outras atrações, tem ganhado cada vez mais notoriedade pelo crescimento do seu setor de tecnologia. A cidade, inclusive, tem sido apelidada por alguns veículos de imprensa como a “ilha do silício,”<sup>466</sup> em alusão ao denominado Vale do Silício nos EUA – região onde estão concentradas as maiores empresas de tecnologia do mundo.<sup>467</sup>

De fato, atualmente a capital catarinense apresenta a maior densidade de empresas de tecnologia por habitante no país, segundo estudo realizado pela ACATE.<sup>468</sup> Além disso, no ano de 2019, o faturamento desses empreendimentos na região metropolitana de Florianópolis alcançou cifra aproximada de 9 bilhões de reais, com cerca de 30 mil funcionários e 7 mil empreendedores.<sup>469</sup>

Considerando especificamente o campo da Tecnologia da Informação e Comunicação em Florianópolis, diversas são as empresas que trabalham diretamente com o processamento de dados pessoais no município. Algumas delas alcançam, direta ou indiretamente, uma atuação internacional, seja prestando serviços para outras empresas transnacionais ou oferecendo seus próprios serviços externamente.<sup>470</sup> Isso faz com que essas empresas possam estar sujeitas a normas e padrões estrangeiros, como é o caso do GDPR.

Ressalta-se que, ainda que existam muitas semelhanças entre a LGDP brasileira e o GDPR<sup>471</sup>, não se pode afirmar que a conformidade com a primeira norma implique,

<sup>466</sup> G1 Santa Catarina. **Ilha do Silício, Florianópolis lidera o bom desempenho catarinense no setor de tecnologia.** Disponível em: <<https://g1.globo.com/sc/santa-catarina/techsc/noticia/2019/11/14/ilha-do-silicio-florianopolis-lidera-o-bom-desempenho-catarinense-no-setor-de-tecnologia.ghtml>>. Acesso em: 24/03/2021. Também nesse sentido: INFOMONEY. **Além da “Ilha do Silício”: como Santa Catarina está levando fábricas de startups ao interior.** Disponível em: <<https://www.infomoney.com.br/negocios/alem-da-ilha-do-silicio-como-santa-catarina-esta-levando-fabricas-de-startups-ao-interior/>>. Acesso em: 24/03/2021.

<sup>467</sup> CAMBRIDGE DICTIONARY. **Silicon Valley.** Disponível em: <<https://dictionary.cambridge.org/pt/dicionario/ingles/silicon-valley>>. Acesso em: 24/03/2021.

<sup>468</sup> ACATE. **Tech Report 2020.** Disponível em: <<https://www.techreportsc.com/>> Acesso em: 24/03/2021. pág. 23.

<sup>469</sup> *Ibid.* pág. 26.

<sup>470</sup> A título de mera ilustração, a empresa Neoway, que tem sede em Florianópolis, é tida atualmente como a maior empresa da América Latina em serviços de *Big Data Analytics*.

<sup>471</sup> MOURA, Aline Beltrame de. GNOATTON, Letícia Mulinari. **Os Desafios Da Aplicação Extraterritorial Do Regulamento Geral De Proteção De Dados Pessoais Da União Europeia.** In: GHILARDI, Dóris; SASS, Liz Beatriz (coords.) *Temas Atuais De Direito Privado E Sociedade Da Informação: O Direito Na Era Digital.* 1ª ed. – Florianópolis: Habitus, 2020.

necessariamente, em total conformidade com a segunda. Portanto, uma vez verificada a incidência da aplicação direta do GDPR para alguma empresa brasileira, esta deverá analisar, dentro de sua dinâmica interna, quais métodos e práticas precisam ser ajustados para atender aos dispositivos específicos do Regulamento – o que, conseqüentemente, implica em aumento de custos.

Dentro dessa perspectiva, conforme demonstram Moura e Gnoatton, em 2018, “o mercado brasileiro, preocupado com a possibilidade de aplicação extraterritorial do Regulamento europeu, passou a tomar as medidas necessárias para a adequação ao GDPR”. Obviamente, essas medidas vêm sempre acompanhadas de um incremento de custos e mudanças nas dinâmicas internas das empresas. Ademais, para aquelas empresas que se encontram dentro do escopo de aplicação extraterritorial do GDPR por força do art. 3.2, além dos custos de conformidade, soma-se a responsabilidade de designar um representante junto à autoridade de dados do país europeu para o qual direciona majoritariamente seus serviços, conforme determina o art. 27 do GDPR.

Desse modo, no intuito de analisar os principais impactos diretos que a aplicação extraterritorial do GDPR pode ter para as empresas de TIC de Florianópolis, o presente capítulo será dividido da seguinte forma: primeiramente, serão brevemente rememorados alguns aspectos teóricos do art. 3º para se identificar as hipóteses em que o fenômeno da extraterritorialidade poderia alcançar as empresas objeto desta pesquisa; em seguida, serão apresentados e discutidos os resultados de uma pesquisa empírica realizada com algumas empresas do setor, que buscou verificar se as hipóteses aventadas podem ser identificadas na prática.

#### 4.1 CONSIDERAÇÕES SOBRE AS HIPÓTESES DE APLICAÇÃO DO GDPR ÀS EMPRESAS DE TIC DE FLORIANÓPOLIS

Conforme elucidado no capítulo 3 deste trabalho, existem algumas formas pelas quais o GDPR pode ser diretamente aplicável a uma empresa estrangeira. A primeira delas é através do critério do estabelecimento, elencado no art. 3.1 do Regulamento. Para ser abrangida por esse critério, uma empresa de TIC sediada em Florianópolis deve ter alguma filial, sucursal ou qualquer outra presença física que constitua um estabelecimento em algum Estado-membro da UE. Além disso, a empresa deve realizar o tratamento de dados pessoais no contexto das atividades deste estabelecimento.

---

Tendo em conta os desafios que se impõem para a implementação de instalações físicas em país estrangeiro<sup>472</sup> – o que exige não somente capacidade financeira, mas também técnica e jurídica – bem como a possibilidade que as empresas de TIC têm de desenvolver suas atividades de forma remota, acredita-se que a hipótese de incidência do art. 3.1 não tenha tanta potencialidade de atingir as empresas objeto desta pesquisa. Além disso, conforme indicam as teorias de internacionalização de empresas, a presença física, por meio de filiais ou sucursais, é a última etapa dentro de um longo processo de aprendizado e criação de vínculos de uma empresa com países estrangeiros.<sup>473</sup>

O segundo fator que atrai a aplicação do GDPR para empresas estrangeiras é o critério da destinação (*targeting*), consignado no art. 3.2 do Regulamento. Rememora-se que, segundo esse critério, não há a necessidade de que a empresa estrangeira tenha qualquer presença física no território da UE. Exige-se, tão somente, que ela esteja realizando o tratamento de dados para a oferta de bens e serviços ou por mecanismos de monitoramento de comportamento de pessoas que se encontrem no bloco.

Dessa forma, por ter uma natureza mais ampla e, de certo modo, mais flexível, acredita-se que pelo critério da destinação há maiores chances de que as empresas de TIC de Florianópolis possam ser diretamente alcançadas pelo escopo de aplicação extraterritorial do GDPR.

Resta, por fim, verificar se tais hipóteses podem ser comprovadas na prática ou, ao menos, ter uma noção mais precisa de como as empresas objeto deste estudo têm, de fato, percebido a extraterritorialidade do GPDR.

#### 4.2 ANÁLISE PRÁTICA DA APLICAÇÃO EXTRATERRITORIAL DO GDPR: PESQUISA EMPÍRICA

Uma vez esclarecidas as hipóteses em que as empresas de TIC de Florianópolis poderiam se enquadrar dentro do escopo de aplicação do GDPR, cabe agora confrontar tais premissas com a prática mercadológica. Nesse sentido, foi realizada no âmbito deste trabalho

---

<sup>472</sup> CORTEZIA, Sandro Luís Diesel; SOUZA, Yeda Swirski de. **Uma análise sobre a internacionalização de pequenas empresas brasileiras da indústria de software**. Brazilian Business Review. v. 8, n.4. Vitória, Out. - Dez. 2011. ISSN 1807-734X DOI: <http://dx.doi.org/10.15728/bbr.2011.8.4.2>

<sup>473</sup> SOUZA, Crisomar Lôbo de. **Estratégias de internacionalização: um estudo sobre a influência dos fatores de riscos sobre a estratégia e objetivos estratégicos em empresas exportadoras brasileiras**. 2017. Tese (Doutorado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2017. doi:10.11606/T.12.2017.tde-13062017-164539. Acesso em: 2021-04-07.

uma pesquisa empírica com o objetivo de compreender como as empresas estão reagindo aos possíveis impactos da aplicação extraterritorial do Regulamento, principalmente com relação ao incremento de custos ao processo produtivo.

Dessa forma, será apresentada abaixo a metodologia da pesquisa e, em seguida, os resultados obtidos. Pretende-se, ainda, comparar, naquilo que houver compatibilidade, os dados obtidos neste trabalho com duas outras pesquisas. Uma delas foi realizada pela empresa Serasa Experian, e é intitulada “O que os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito?”. Essa pesquisa ouviu 508 empresas de todas as regiões do Brasil, entre os meses de fevereiro e março de 2019.<sup>474</sup> A segunda pesquisa foi realizada pelo SEBRAE e levou o título de “Panorama LGPD em Santa Catarina: Conhecimento das pequenas empresas sobre a Lei Geral de Proteção e Dados”. Esse estudo, por sua vez, contou com a participação de 810 micro e pequenos empreendedores de todo o estado de Santa Catarina, entre os dias 04 e 25 de janeiro de 2021.<sup>475</sup>

#### 4.2.1 Metodologia

O estudo empírico consistiu na elaboração de formulário por meio da plataforma *Google Forms* que, posteriormente, foi enviado para empresas que trabalham no setor de TIC e que estejam listadas no sítio eletrônico da ACATE. Foram selecionadas somente empresas com atuação em Florianópolis - SC.<sup>476</sup>

No sentido de esclarecer pontos importantes aos participantes da pesquisa, a página de entrada do questionário continha um cabeçalho com informações gerais, além de links que direcionavam para sites com maiores informações sobre o GDPR da União Europeia e sobre a LGPD do Brasil. Após a leitura do cabeçalho do formulário, os respondentes eram direcionados para uma página contendo 16 perguntas em formato de múltipla escolha. As perguntas ainda foram divididas em duas seções: informações gerais da empresa e questões específicas sobre a proteção de dados pessoais.

---

<sup>474</sup> SERASA EXPERIAN. O que os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito? Disponível em: <<https://www.serasaexperian.com.br/conteudos/protecao-de-dados/pesquisa-o-que-os-consumidores-e-as-empresas-sabem-sobre-lgpd-e-o-que-estao-fazendo-a-respeito/>>. Acesso em: 26/01/2021.

<sup>475</sup> SEBRAE. Panorama LGPD em Santa Catarina: Conhecimento das pequenas empresas sobre a Lei Geral de Proteção e Dados. Disponível em: <<http://sebrae.sc/panoramalgpd>>. Acesso em: 04/04/2021.

<sup>476</sup> A listagem completa das empresas pode ser consultada no seguinte endereço eletrônico: <<https://www.acate.com.br/associados/>> Acesso em: 26/01/2021.

O endereço eletrônico para acesso ao formulário foi enviado para o total de 362 empresas e ficou aberto para receber respostas na plataforma *Google Forms* entre os dias 20/02/2020 e 08/05/2020. A plataforma oferece um mecanismo de validação de endereço de e-mails para garantir maior segurança e confiabilidade das informações.<sup>477</sup>

Do total das empresas que receberam o formulário, somente 24 responderam à totalidade das questões. A baixa adesão obtida pela pesquisa pode ser justificada pelo período em que o formulário foi lançado, que coincidiu com o início da pandemia de Covid-19 e as medidas de distanciamento dela decorrentes, que resultaram na readaptação das atividades de diversas empresas.

Após o envio das respostas pelos participantes, a plataforma utilizada realizou a tabulação das informações e gerou gráficos para melhor ilustrar os resultados. Esses números serão demonstrados e analisados no subcapítulo “resultados”. Devido ao caráter confidencial da pesquisa, os nomes das empresas participantes não serão divulgados, sendo apresentados somente os gráficos gerados a partir das respostas obtidas.

É imperioso ressaltar que, pela impossibilidade de distinguir o número exato de empresas de TIC que estavam em funcionamento em Florianópolis durante o envio do formulário, não foi possível calcular o universo total da pesquisa. Consequentemente, não se pode mensurar com a necessária certeza a margem de erro do estudo. Dessa forma, os resultados apresentados abaixo não podem ser tomados em termos quantitativos, mas servem para demonstrar qualitativamente a percepção dos empresários da área acerca dos possíveis impactos da aplicação extraterritorial do GPDR.

Cabe considerar, por fim, que no período em que o formulário da presente pesquisa estava recebendo respostas, a Lei Geral de Proteção de Dados do Brasil ainda não estava em vigor, fato que só ocorreria em 18 de setembro de 2020, ao menos para a maior parte dos dispositivos da lei.

## **4.2.2 Resultados**

### **4.2.2.1. Perfil das empresas**

Com relação ao perfil das empresas participantes, foram feitos os seguintes questionamentos: (1) “Sua empresa tem sede ou filial no Município de Florianópolis-SC?”; (2)

---

<sup>477</sup> Para saber mais sobre a plataforma Google Formulários:< <https://www.google.com/intl/pt-BR/forms/about/>>. Acesso em: 26/01/2021.

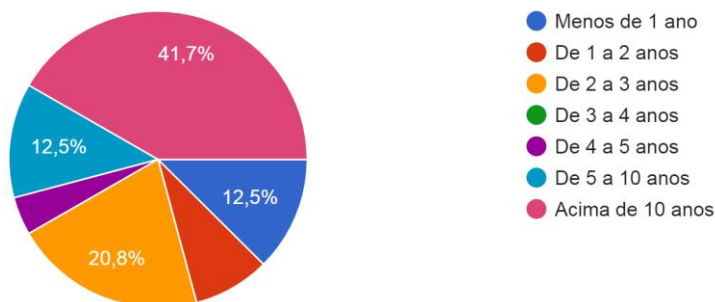
“Sua empresa é considerada uma startup?”; e (3) “Há quanto tempo sua empresa atua no mercado?”.

Todas as empresas responderam que têm sede ou filial no município de Florianópolis e, portanto, estão dentro do escopo da pesquisa. No que diz respeito à segunda pergunta, metade das empresas consideraram-se *startups*, ou seja, são empresas “estruturadas para crescer rápido e continuamente” dentro de um mercado em contínua expansão.<sup>478</sup> Já com relação à terceira pergunta, houve maior divergência nas respostas, conforme verifica-se na Figura 1:

Figura 1- Gráfico das respostas compiladas da pergunta número 3 do questionário

3. Há quanto tempo sua empresa atua no mercado?

24 respostas



Fonte: o autor.

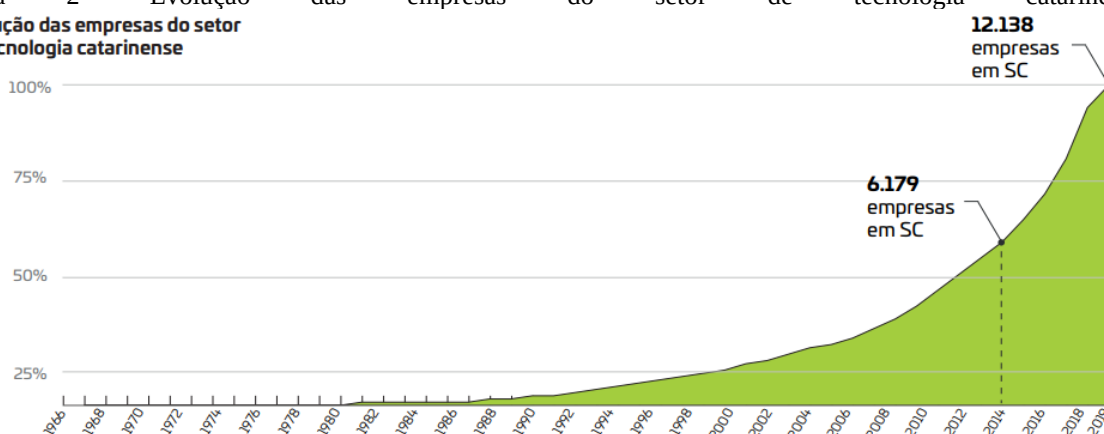
Embora cerca de 41% das empresas entrevistadas tenham mais de 10 anos de atuação no mercado, percebe-se que a maioria delas (58,3%) atua há menor tempo, o que reflete o crescimento relativamente recente do mercado da Tecnologia da Informação e Comunicação, acompanhando a própria evolução das novas tecnologias. Esses resultados também estão em harmonia com os dados apresentados pela ACATE, que apontam que a média de idade das empresas de Tecnologia em Florianópolis é de 8 anos.<sup>479</sup>

Esse panorama de recente expansão pode ser de igual forma percebido ao analisar a Figura 2, que demonstra a evolução do número de empresas de Tecnologia em todo o estado de Santa Catarina nos últimos anos. Verifica-se que do ano de 2014 até 2019 o setor teve um crescimento aproximado de 100%.

<sup>478</sup>BEHRENS, Jéssica Soares Braga. **Startup na prática: desafios e oportunidades**. 2015. 41 f., il. Monografia (Bacharelado em Comunicação Social)—Universidade de Brasília, Brasília, 2015.

<sup>479</sup> ACATE. **Tech Report 2018**. Disponível em: <<https://www.acate.com.br/wp-content/uploads/2018/11/ACATE-Observat%C3%B3rio-2018.pdf>> Acesso em: 24/03/2021. pág. 33.

Figura 2- Evolução das empresas do setor de tecnologia catarinense



Fonte: ACATE. Tech Report 2020.

#### 4.2.2.2. A realização de tratamento de dados pessoais como atividade das empresas entrevistadas

A primeira questão que as empresas participantes responderam relativamente ao tratamento de dados pessoais no âmbito das suas atividades foi a seguinte: “sua empresa atua realizando operações que podem envolver a coleta, armazenamento ou processamento de dados pessoais?”. Considerando a abrangência do conceito de tratamento de dados pessoais elucidado no capítulo 3 deste trabalho, esperava-se que a grande maioria das empresas respondesse positivamente a esta questão. De fato, com exceção de uma respondente, todas as outras responderam que realizam a coleta de dados pessoais em suas atividades.

A presente pesquisa não questionou quais os meios utilizados pelas empresas para realizar a coleta dos dados pessoais dos clientes, mas os resultados do estudo realizado pela Serasa Experian demonstraram que há uma tendência entre as empresas de menor porte de colherem os dados pessoais de seus clientes, principalmente por meio de contato pessoal e de mídias sociais. À medida que cresce o porte da empresa, a coleta dos dados pessoais torna-se mais sofisticada e passa a ser realizada principalmente por meios eletrônicos. Especificamente sobre o setor de tecnologia, a pesquisa da Serasa Experian demonstrou que a coleta de dados pessoais é feita majoritariamente por websites, call centers, empresas de bancos de dados e loyalty.<sup>480</sup>

Caso fosse considerado somente o escopo material do GDPR contida em seu art. 2.1, o Regulamento poderia, portanto, ser aplicável a quase a totalidade das empresas entrevistadas.

<sup>480</sup> SERASA EXPERIAN. *Op. cit.*

Contudo, como não se pode analisar uma norma levando em consideração somente seu âmbito material, deve-se passar ao próximo tópico de análise.

#### 4.2.2.3 Presença das empresas na União Europeia

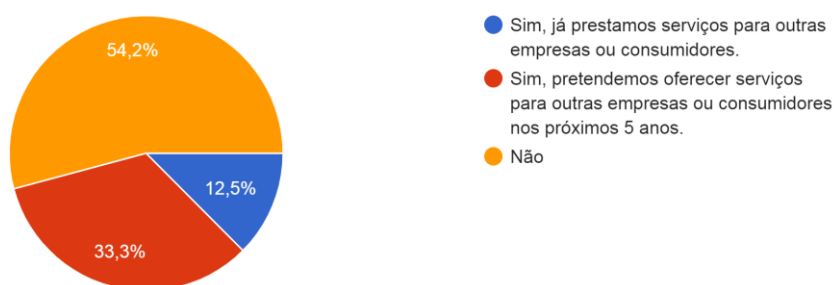
No que concerne à presença das empresas entrevistadas na União Europeia, nenhuma delas alegou ter filial, sucursal ou representação nos países do bloco. Sendo assim, o GPDR não lhes poderia ser aplicável por força do art. 3.1. Isso não impede, entretanto, que as empresas tenham que estar em conformidade com o Regulamento, caso sejam contratadas para prestar serviços por empresas que atuem na União Europeia.

Foi pensando nessa última hipótese que foi elaborada a seguinte pergunta: “Sua empresa já prestou ou pretende oferecer serviços para outras empresas/entidades ou consumidores localizados na União Europeia?”. Os resultados demonstraram que somente 12,5% das empresas entrevistadas já prestaram serviços para outras empresas ou consumidores na União Europeia, e que 33% delas ainda pretendem realizar tais atividades nos próximos 5 anos.

Figura 3- Gráfico das respostas compiladas da pergunta número 9 do questionário

9. Sua empresa já prestou ou pretende oferecer serviços para outras empresas/entidades ou consumidores localizados na União Europeia?

24 respostas



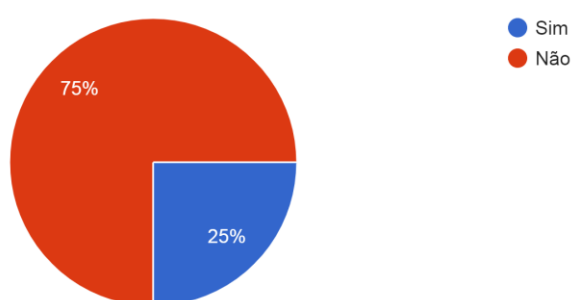
Fonte: o autor.

Conclui-se, dessa forma que, mesmo não tendo filial no território da União Europeia, o GDPR pode vir a ser diretamente aplicável para as empresas que já prestaram ou pretendem prestar serviços para controladores da UE – caso esses serviços envolvam o tratamento de dados pessoais de indivíduos que estejam localizados nos países bloco.

A questão número 8 indagou ainda se as empresas tinham como objetivo constituir filial ou representação em algum país da União Europeia dentro dos próximos cinco anos, haja vista que a maioria delas ainda se encontram na fase inicial de suas operações. Como resultado, 25% das empresas responderam positivamente, ou seja, expressaram seu objetivo de estabelecer sua presença fisicamente em algum país do bloco.

Figura 4- Gráfico das respostas compiladas da pergunta número 8 do questionário

8. Sua empresa tem como objetivo constituir filial ou representação em algum país da União Europeia nos próximos 5 anos?  
24 respostas



Fonte: o autor.

Esse cenário demonstra a importância do conhecimento sobre as regras estabelecidas no GDPR para as empresas que têm a internacionalização como perspectiva a curto e médio prazo.

#### 4.2.2.4 Conhecimento das empresas sobre o GDPR

A presente pesquisa também buscou investigar o nível de conhecimento que as empresas detinham sobre o GPDR, partindo da hipótese de que a maioria das respondentes teria pouco ou nenhum conhecimento sobre. Isso porque, dada a sua natureza de norma estrangeira, é natural que haja relativa dificuldade de acesso às informações sobre o Regulamento, mesmo considerando a publicidade que foi dada por sites especializados da área de tecnologia da informação, alguns deles em língua portuguesa.

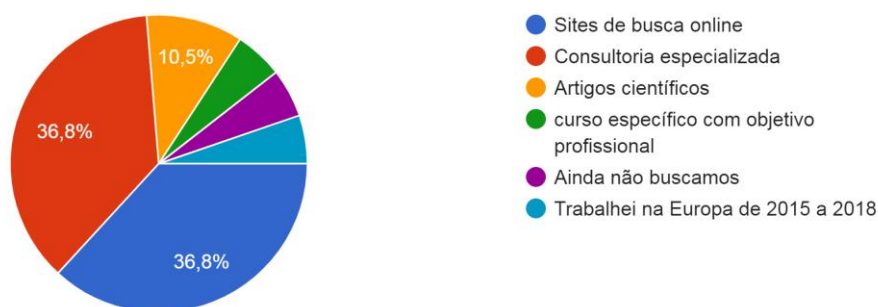
Os resultados da pesquisa refutaram essa hipótese, mostrando que cerca de 70% das empresas entrevistadas já haviam buscado algum tipo de informação sobre a norma ao tempo da coleta do questionário. Desses 70%, o número de empresas que obtiveram informações por

meio de sites de busca na internet foi igual ao daqueles que buscaram tais informações por meio de consultoria jurídica especializada, conforme constata-se pela análise da figura 5

Figura 5- Gráfico das respostas compiladas da pergunta número 10 do questionário.

10.1 Caso positivo a resposta anterior, o acesso a tal informação se deu através de qual meio?

19 respostas



Fonte: o autor.

Os dados apresentados demonstram a crescente importância que os meios digitais têm alcançado para a difusão de conteúdos jurídicos, mesmo que nem sempre se possa garantir a confiabilidade das informações constantes nesses meios. Para isso, conclui-se, desde já, que é necessária uma maior divulgação de trabalhos acadêmicos sobre a temática, bem como uma maior conscientização das empresas sobre a relevância de buscar auxílio pela contratação de serviços jurídicos especializados.

#### 4.2.2.5 Impactos do GDPR para as empresas a partir da perspectiva do art. 3.2

Conforme pontuado no subcapítulo 4.1 deste trabalho, o dispositivo que tem maior potencial de tornar o GDPR diretamente aplicável às empresas de TIC de Florianópolis é o art. 3.2 do Regulamento. À luz do artigo mencionado, não é necessário que uma empresa tenha presença física no território dos Estados-membros da União Europeia para ter a obrigação de estar em conformidade com o GDPR, bastando somente que realize o tratamento de dados pessoais de indivíduos que lá estejam localizados quando da realização de oferta de bens e serviços ou do controle de comportamento dessas pessoas.<sup>481</sup>

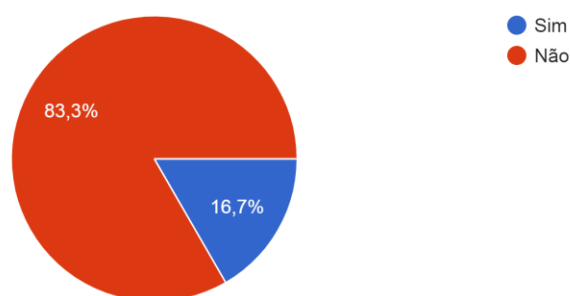
<sup>481</sup> GDPR. Art. 3.2.

Dentro dessa perspectiva, as empresas participantes da pesquisa foram questionadas sobre a realização da coleta, o processamento ou o armazenamento de dados pessoais de indivíduos que estejam localizados no território de algum Estado-membro da União Europeia. Os resultados foram compilados e estão representados na figura 6.

Figura 6 - Gráfico das respostas compiladas da pergunta número 5 do questionário.

5. Sua empresa já realizou a coleta, processamento, ou armazenamento de dados pessoais de indivíduos, independente da nacionalidade, que se encontrem no território da União Europeia?

24 respostas



Fonte: o autor.

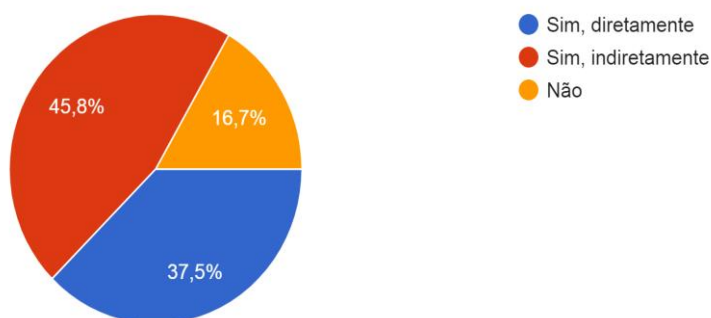
As respostas compiladas na figura acima confirmam a hipótese desta pesquisa de que o GDPR pode ser aplicável às empresas de Tecnologia da Informação de Florianópolis e, consequentemente, pode ter impactos diretos para essas entidades – ainda que somente para um percentual pequeno delas.

Também no mesmo sentido é a própria percepção das empresas entrevistadas, uma vez que a maioria delas (83, 3%) afirma que possa vir a ser impactada pelas normas previstas no GDPR, direta ou indiretamente, conforme demonstra a figura 7:

Figura 7- Gráfico das respostas compiladas da pergunta número 11 do questionário.

11. Sua empresa avalia que possa ser impactada pelas normas estabelecidas no GDPR?

24 respostas



Fonte: o autor.

Para fins de comparação, ilustra-se que, na Índia, país que é atualmente é destaque pelo seu crescimento no setor de tecnologia, uma pesquisa desenvolvida em 2018 pela Deloitte e com metodologia similar a do presente trabalho também demonstrou que o GDPR seria aplicável a cerca de 23% das empresas do setor de Tecnologia por força das disposições do art. 3.2 do Regulamento.<sup>482</sup>

Como se percebe, portanto, os impactos da aplicação extraterritorial do GDPR podem ser observados em diferentes partes do mundo – o que demonstra a afirmação da UE como um regulador de nível global.<sup>483</sup>

#### 4.2.2.6 Impactos diretos para as empresas pela perspectiva de incremento de custos

A presente subseção tem como objetivo pontuar os impactos da aplicação extraterritorial do GDPR para as empresas entrevistadas sob o viés do incremento dos custos operacionais.

Sabe-se que, para se adequar às obrigações impostas pelas normas de proteção de dados pessoais, algumas empresas optam por implementar programas específicos de *compliance*<sup>484</sup>, cuja complexidade pode variar de acordo com o tamanho da organização.

<sup>482</sup> DELOITTE. GDPR Preparedness Survey Report. Disponível em: <<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-riks-gdpr-preparedness-survey-report-noexp.pdf>>. Acesso em: 15/10/2020.

<sup>483</sup> BRADFORD, Anu. *Op. cit.*

<sup>484</sup> Entende-se por *compliance* o “conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.” FRAZÃO, Ana. **Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos**

Outras, por outro lado, preferem permanecer inertes e não implementar nenhuma medida de adequação, sujeitando-se ao risco de sofrer as sanções estipuladas nas legislações vigentes. Em ambos os casos, seja pela via preventiva ou repressiva, as empresas que exercem atividades relacionadas ao tratamento de dados pessoais deverão perceber um aumento nos seus custos de produção, em razão das novas obrigações criadas pelos regulamentos.

De acordo com Gonçalves, desconsiderando as imperfeições do mercado, um aumento nos custos operacionais das empresas pela necessidade de adequação às novas legislações impacta diretamente na curva de oferta do setor, resultando em um acréscimo nos preços dos serviços prestados ou nos lucros obtidos.<sup>485</sup> No caso das empresas impactadas pelo GDPR, o aumento de custos está relacionado a diversos fatores, tais como: a readaptação dos sistemas para garantir maior segurança no tratamento e armazenamento dos dados pessoais dentro da perspectiva estipulada no art. 25 do GDPR, que prevê a proteção de dados desde a concepção<sup>486</sup>; a reformulação da política de privacidade; treinamento de pessoal; contratação do encarregado de proteção de dados (*Data Protection Officer - DPO*);<sup>487</sup> além da contratação de representante junto à UE, nos casos das empresas que se enquadram nas hipóteses do art. 3.2 do GDPR.<sup>488</sup>

Nos Estados Unidos, por exemplo, uma pesquisa elaborada em 2017 pela instituição PwC e que envolveu mais de 200 empresas apontou que 77% delas planejavam alocar mais de 1 milhão de dólares para se adequarem às normas do GDPR.<sup>489</sup>

Um dos incentivos para os gastos com adequação às normas do Regulamento são suas altas multas, que podem ser aplicadas às empresas infratoras, conforme estabelecido no seu art. 83. Em alguns casos, como na infringência de alguma disposição relativa à transferência internacional de dados, a multa aplicável pode chegar a 4% do rendimento anual a nível internacional da empresa ou 20 milhões de Euros, dependendo de qual for o valor maior. Por outro lado, conforme explicam Ferreira, Gonçalves e Queiroz, os custos de implementação de um programa de *Compliance* também podem ser altos, uma vez que se trata de um procedimento complexo, que envolve equipe multidisciplinar de conhecimento jurídico

---

**administrativos.** In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42

<sup>485</sup> GONÇALVES, Everton das Neves. **A Teoria de Posner e sua Aplicabilidade à Ordem Constitucional Econômica Brasileira de 1988.** Dissertação de Mestrado em Direito – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, Florianópolis, Santa Catarina. 1997. Disponível em <http://tede.ufsc.br/teses/PDPC0258-D.pdf>. Acesso em 25/01/2021. pág. 72-73.

<sup>486</sup> GDPR, Art. 25.

<sup>487</sup> GDPR, Art. 37.

<sup>488</sup> GDPR, Art. 27.

<sup>489</sup> PWC. **GDPR Preparedness Pulse Survey.** Disponível em: <<https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html>> Acesso em 25/01/2021.

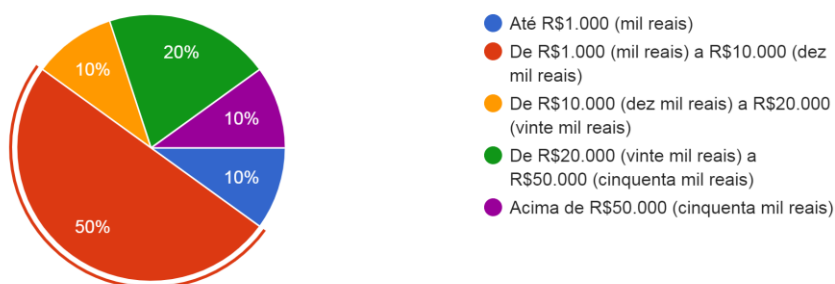
diversificado.<sup>490</sup> O alto custo desses procedimentos pode ser, portanto, um desincentivo para as empresas de menor porte e uma vantagem para as grandes empresas de tecnologia, conforme indicam alguns analistas.<sup>491</sup>

Dentro dessa perspectiva, a presente pesquisa constatou que 62,5% das empresas entrevistadas julgam necessário a realização de investimentos para se adequarem às normas do GDPR. Quando perguntadas se de fato já realizaram algum investimento nesse sentido, 41,7% delas responderam que sim – dado que indica mais uma vez o impacto direto da aplicação extraterritorial do GDPR.

Para as empresas que afirmaram já terem tido custos para se adequar ao GDPR foi questionado qual a faixa de valores despendidos. As opções de respostas foram divididas em cinco faixas, a saber: até R\$1.000 (mil reais); de R\$1.000 (mil reais) a R\$10.000 (dez mil reais); de R\$10.000 (dez mil reais) a R\$20.000 (vinte mil reais); de R\$20.000 (vinte mil reais) a R\$50.000 (cinquenta mil reais); e acima de R\$50.000 (cinquenta mil reais). Os resultados estão demonstrados na figura 8:

Figura 8 - Gráfico das respostas compiladas da pergunta número 13.1 do questionário.

13.1 Caso positiva a resposta anterior, qual a média de valores que sua empresa já investiu para se adequar ao GDPR?  
10 respostas



Fonte: o autor.

<sup>490</sup> FERREIRA, Bráulio Cavalcanti; QUEIROZ, Bruna Pamplona de; GONÇALVES, Everton das Neves. Análise Econômica do Direito e o Compliance Empresarial: apreciação jurídico-econômica dos programas de conformidade e dos custos de prevenção. **Economic Analysis Of Law Review**, Brasília, v. 9, n. 1, p. 259-276, Janeiro-Abril de 2018. Quadrimestral. Disponível em: <<https://portalrevistas.ucb.br/index.php/EALR/issue/view/490>>. Acesso em: 21 jan. 2021.

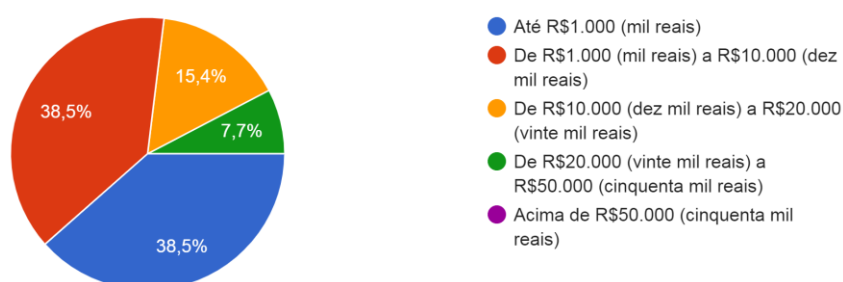
<sup>491</sup> THE NEW YORK TIMES. How Facebook and Google Could Benefit From the G.D.P.R., Europe's New Privacy Law. Disponível em: <<https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html>>. Acesso em: 24/03/2021. THE WALL STREET JOURNAL. GDPR Has Been a Boon for Google and Facebook. Disponível em: <<https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219>>. Acesso em 24/03/2021. FORBES. GDPR Is Great News For Google And Facebook, Really. Disponível em: <<https://www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/?sh=f57c18348f63>>. Acesso em: 24/03/2021.

Vislumbra-se, portanto, que a maioria das empresas entrevistadas gastou entre mil e dez mil reais, e que 30% delas gastaram mais do que 20 mil reais para se adequar ao GDPR. Esses números estão de acordo com o perfil das empresas entrevistadas, já que a maior parte delas tem pouco tempo de atuação no mercado e são caracterizadas como *startups*.

A pesquisa também questionou se as empresas já haviam investido em cursos de capacitação para os seus colaboradores sobre o GDPR. A metade das empresas respondeu positivamente. Destas, a grande maioria (77%) gastou até 10 mil reais em capacitação dos colaboradores, conforme ilustrado no gráfico abaixo:

Figura 9 - Gráfico das respostas compiladas da pergunta número 14.1 do questionário.

14.1 Caso positiva a resposta anterior, qual a média de valores que sua empresa despendeu ou julga necessária despende em cursos de capacitação de funcionários/colaboradores sobre o GDPR?  
13 respostas



Fonte: o autor.

#### 4.2.2.7 Percepção das empresas sobre a LGPD do Brasil

Como demonstrado no capítulo 3 deste trabalho, a LGPD brasileira contém muitos dispositivos similares ao GDPR da União Europeia, uma vez que buscou nesta norma a sua inspiração. Esse fato contribui para minimizar os custos de *compliance* para as empresas que se enquadram no âmbito de aplicação territorial de ambas as normas. Isso porque, ao estarem em conformidade com a LGPD, as empresas brasileiras acabam atendendo a diversos requisitos também estipulados pelo GDPR, ainda que sejam necessárias medidas adicionais para o total alinhamento com os dispositivos do Regulamento.

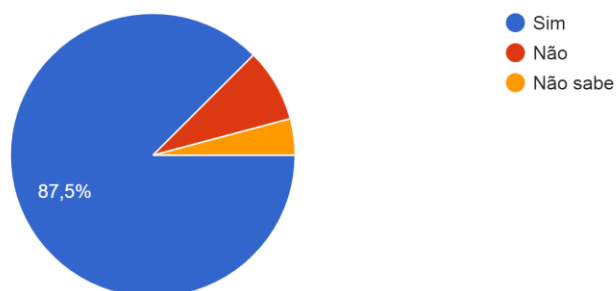
Em razão dessas semelhanças, a presente pesquisa procurou também saber qual era a percepção das empresas entrevistadas sobre os possíveis impactos da LGPD do Brasil para os seus negócios. Deve-se considerar, repisa-se, que no período em que o questionário esteve

aberto para as respostas, a LGPD ainda não estava em vigor no Brasil. Os resultados foram compilados nas figuras que serão apresentadas a seguir.

Figura 10 - Gráfico das respostas compiladas da pergunta número 15 do questionário.

15. Sua empresa avalia que poderá ser impactada pelas normas estabelecidas na Lei Geral de Proteção de Dados (LGPD) do Brasil?

24 respostas



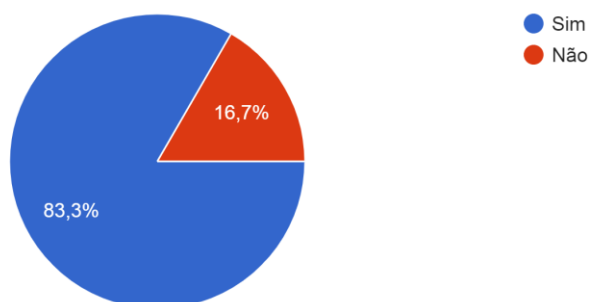
Fonte: os autores.

Pode-se verificar da figura acima que grande maioria das empresas entrevistadas acredita que pode sim ser impactada pela LGPD. Além disso, quando questionadas especificamente sobre a necessidade de realização de investimentos para se adequarem à lei brasileira, somente 16,7% delas responderam que não seria necessário realizar qualquer investimento, número que demonstra a preocupação da grande maioria em investir para adequar sua empresa à lei brasileira.

Figura 11 - Gráfico das respostas compiladas da pergunta número 16 do questionário.

16. Sua empresa julga necessária a realização de investimentos para se adequar às normas estabelecidas na LGPD do Brasil?

24 respostas



Fonte: os autores.

Analisando os resultados obtidos, pode-se inferir que a maioria das empresas entrevistadas está ciente da abrangência da LGPD e da necessidade de adequação das suas atividades empresariais à norma.

Ao contrastar os números desta pesquisa com aqueles obtidos com a pesquisa do SEBRAE, que entrevistou pequenas e microempresas de diversos setores de todo o estado de Santa Catarina, verifica-se que o nível geral de conhecimento sobre a LGPD no estado é ligeiramente menor. Segundo a pesquisa do Sebrae, cerca de 80,8% das pequenas empresas e 74,2% das microempresas do estado já ouviram falar sobre a LGPD. Nesse mesmo estudo, quando questionadas sobre o nível de adequação à LGPD, 78,1% das pequenas empresas alegaram que já estão adequadas ou estão em processo de adequação à norma em comparação com 69,6% das microempresas.<sup>492</sup>

Ao comparar o nível de adequação por setor de atividade, a pesquisa do SEBRAE constatou que o setor com maior adequação até o início de 2021 era o de serviços – onde estão também classificadas as empresas de TIC, seguido pelo setor de comércio e, por fim, o da indústria.<sup>493</sup>

A partir desses dados, pode-se inferir que quanto maior o porte da empresa, maior é a facilidade de acesso à informação sobre as normas de proteção de dados pessoais e maior também é o nível de conformidade com a legislação. Esse fenômeno vem ao encontro da percepção de alguns analistas, mencionada anteriormente neste capítulo, de que as novas legislações de proteção de dados pessoais podem favorecer as empresas que possuam uma maior capacidade financeira para se adequar.

A pesquisa realizada em nível nacional pela Serasa Experian,<sup>494</sup> também questionou as empresas participantes sobre os possíveis impactos da LGPD. O estudo chegou ao resultado de que quanto maior o porte das empresas maior era o impacto esperado por elas com relação aos recursos necessários para se adequarem à norma. Nas empresas de maior porte (com até 999 funcionários) o número das que acreditam que poderiam ser impactadas pelo LGPD chegou a 81%, conforme exposto na figura abaixo:

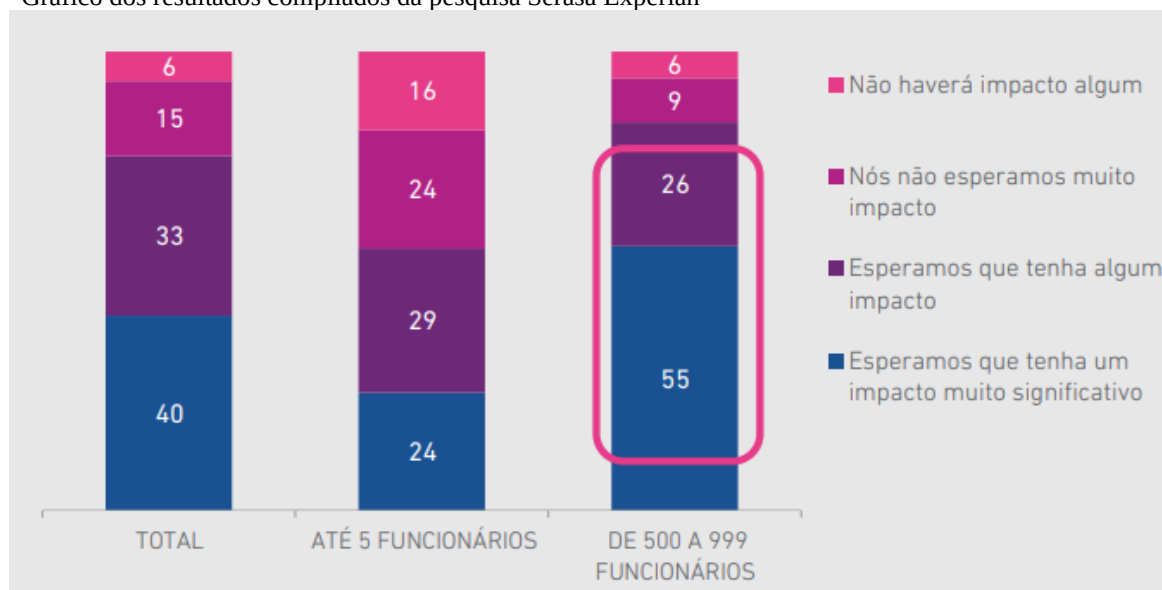
---

<sup>492</sup> SEBRAE. Panorama LGPD em Santa Catarina. *Op. cit.*

<sup>493</sup> *Ibid.*

<sup>494</sup> SERASA EXPERIAN. *Op. cit.* pág. 12.

Figura 12 - Gráfico dos resultados compilados da pesquisa Serasa Experian



Fonte: Serasa Experian. Op. cit. pág. 12.

Quando considerado o total das empresas entrevistadas, independente do seu porte, pode-se concluir que os resultados apresentados pela pesquisa elaborada pela Serasa Experian quanto à expectativa de impacto da LGPD é cerca de 13% menor do que o apontado pela pesquisa realizada no âmbito do presente trabalho. Tal fenômeno pode ser explicado pelo fato de que, assim como a pesquisa do SEBRAE, a pesquisa da Serasa Experian entrevistou empresas de diferentes setores, enquanto o presente estudo somente coletou respostas de empresas do setor de Tecnologia da Informação, que tende a ser o mais afetado pela LGPD.

Com relação aos investimentos necessários para a adequação das empresas às obrigações estabelecidas pela legislação, a pesquisa Serasa Experian identificou que os maiores desafios elencados pelas empresas para a implementação da LGP são: “treinamento da equipe (41%); identificação de correções e tecnologias adotadas (39%); que o setor TI inclua projetos referentes à lei no fluxo de trabalho (34%); concordar com uma interpretação da lei (31%); e encontrar pessoas com habilidades certas para o trabalho (30%).”<sup>495</sup>

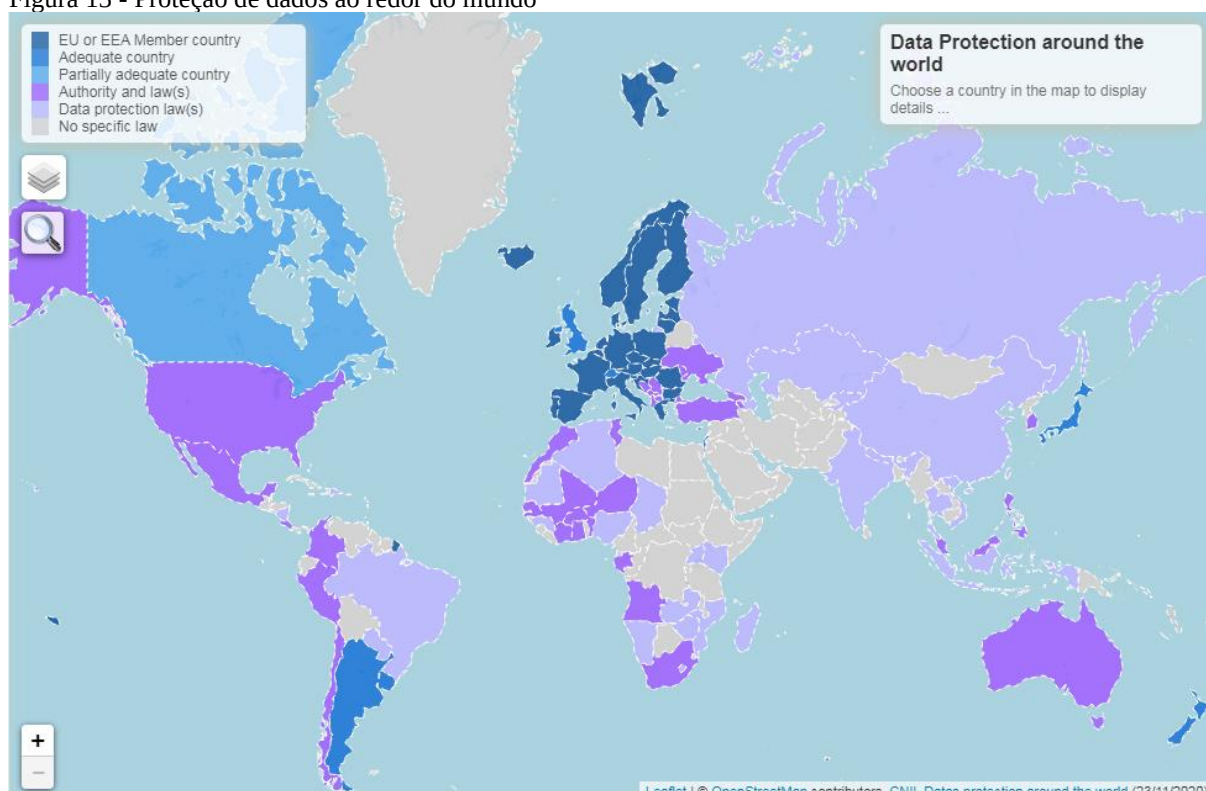
O enfrentamento dos desafios elencados acima poderá ser facilitado à medida que avance a estruturação da Autoridade Nacional de Proteção de Dados brasileira (ANPD). A criação da ANPD já estava prevista no texto inicial da LGPD, mas somente se concretizou a partir da edição do Decreto nº 10.474, de 26 de agosto de 2020. Dentre diversas outras funções, compete à ANPD: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais;

<sup>495</sup> SERASA EXPERIAN. Op. cit., pág. 12.

orientar os agentes na aplicação das normas sobre o tema; cooperar com órgãos nacionais e internacionais; e investigar e punir administrativamente às infrações à LGPD.<sup>496</sup>

O fato de a ANPD ainda não estar plenamente consolidada, além de estar ainda vinculada diretamente à Presidência da República – o que poderia macular sua independência – é um dos fatores pelos quais o Brasil ainda não é considerado pela União Europeia como um dos países que apresentam nível adequado de proteção de dados pessoais.<sup>497</sup> A figura abaixo, que demonstra o mapa dos países considerados adequados pela UE, ilustra como o Brasil precisa ainda evoluir nesse sentido para estar no mesmo patamar de países vizinhos como Argentina e Uruguai, que também são membros do Mercosul.

Figura 13 - Proteção de dados ao redor do mundo



Fonte: CNIL, 2020.

A partir da figura acima, pode-se de igual modo inferir que o esforço rumo à construção de um *standard* global de proteção de dados ainda irá demandar inúmeras iniciativas de cooperação internacional e diálogos multilaterais. Somente quando for alcançado esse

<sup>496</sup> LGPD, Art. 55-J.

<sup>497</sup> MARIO, Viola. **Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira**. Rio de Janeiro: Instituto Tecnologia e Sociedade, 2019.

patamar é que dispositivos com vocação extraterritorial como o art. 3º do GPDR não se farão mais necessários. Até lá, entretanto, as empresas ao redor do mundo e, no caso, as empresas de TIC de Florianópolis devem permanecer atentas e em conformidade com os regulamentos pertinentes à proteção de dados pessoais.

#### **4.2.3 Conclusões parciais sobre a pesquisa empírica**

O estudo realizado com algumas empresas de Tecnologia da Informação e Comunicação vai ao encontro da hipótese desta pesquisa de que a aplicação extraterritorial do GDPR tem gerado impactos diretos para o setor no município de Florianópolis. Isso porque, apesar de nenhuma das empresas entrevistadas terem presença física nos países que compõem a União Europeia, algumas delas já realizaram o tratamento de dados de indivíduos que se encontram no território do bloco ou já prestaram serviços para outras empresas do continente que tenham relação com o tratamento de dados pessoais. Dessa forma, 41% das empresas afirmaram já ter realizado algum investimento no sentido de buscar conformidade com o Regulamento – o que evidencia os impactos já presentes no que diz respeito ao incremento de custos operacionais das empresas.

Além disso, a pesquisa também demonstrou a pretensão de algumas empresas em buscar a internacionalização de seus negócios e, dessa forma, alcançar o mercado europeu dentro dos próximos 5 anos. Essa constatação, aliada ao fato de que a maioria delas ainda são consideradas *startups* e, portanto, têm como objetivo o rápido crescimento, aumenta as chances de que sejam alcançadas pelo escopo de aplicação do GDPR em médio prazo.

Deve-se ressaltar, neste ponto, que durante a análise dos dados colhidos, constatou-se a necessidade da realização de uma pesquisa futura para verificar se os investimentos executados pelas empresas para se adequarem ao GDPR não poderiam ser também decorrência de obrigações contratuais com outras empresas ou, até mesmo, para ganhar um melhor posicionamento no mercado, ainda que somente cerca de 12% das empresas entrevistadas tenha declarado já ter prestado serviços para outras organizações da União Europeia.

Com relação à LGPD, verificou-se que 87% das empresas acreditam que possam ser diretamente impactadas pela nova legislação brasileira e 83% delas afirmaram ser necessária a realização de investimentos para estar em conformidade com a norma. Esses números são similares aos coletados pelas pesquisas realizadas pelo SEBRAE e Serasa Experian, e

demonstram como a preocupação em se adequar à LGDP também se estende a nível regional e nacional.

## 5 CONCLUSÃO

Considerando a relevância do município de Florianópolis-SC como polo de empresas de Tecnologia da Informação e Comunicação, o presente trabalho teve como objetivo investigar os possíveis impactos diretos que a aplicação extraterritorial do GDPR poderia trazer para o setor. Esse debate tem ganhado importância à medida que a sociedade se torna cada vez mais interconectada por meio das TICs e, ao mesmo tempo, a capacidade de processamento de dados dessas tecnologias aumenta vertiginosamente, podendo colocar em risco o direito à proteção de dados dos indivíduos.

Dentro dessa perspectiva, buscou-se primeiramente analisar a formação histórica da União Europeia e como o Direito à Proteção de Dados Pessoais emergiu dentro dela para se tornar, atualmente, o paradigma internacional neste campo. Para tanto, ressaltou-se o funcionamento das instituições que compõem o bloco europeu a fim de demonstrar como a complexidade e sofisticação dessas instituições permitem que a UE atue como um regulador global. Ao trazer o recorte histórico da formação da proteção de dados pessoais, pontuou-se as primeiras iniciativas legislativas sobre o tema na Europa, os primeiros instrumentos internacionais e, por fim, as normas específicas do Direito da União Europeia, a saber, a Diretiva 95/46/CE, a Carta de Direitos Fundamentais da União Europeia e o próprio GDPR.

No segundo capítulo foram conceituados os termos que compõem o escopo material do GDPR, como o conceito de dados pessoais e de tratamento de dados. Em seguida, foram expostas as bases teóricas e as justificativas sob as quais se assenta o fenômeno jurídico da aplicação extraterritorial do GDPR. Viu-se que o art. 3.1 encontra tutela no próprio princípio da territorialidade, mas também pode ter aplicação extraterritorial quando uma empresa estrangeira realiza o tratamento de dados no contexto de um estabelecimento localizado na UE, conforme fixado pelo caso *Google Spain*. O art. 3.2, por sua vez, está baseado na teoria dos efeitos e no critério do direcionamento. Segundo tais critérios, uma empresa que realize o tratamento de dados pessoais de pessoas que se encontram na UE, seja pela oferta de bens e serviços ou pelo monitoramento de comportamento, também deve estar em conformidade com os dispositivos do Regulamento, ainda que não tenha qualquer presença física no bloco.

Ainda no segundo capítulo, verificou-se que, apesar de haver divergências, a maioria da doutrina entende que a aplicação extraterritorial do GDPR, em termos de jurisdição prescritiva, é legítima. Isso porque, segundo os doutrinadores, deve-se levar em consideração os desafios que as novas tecnologias impõem à eficácia da tutela do direito à proteção de dados

pessoais. Entretanto, constatou-se que a alargada abrangência do escopo (extra)territorial do GDPR impõe de igual modo grandes desafios à União Europeia em termos de jurisdição executiva, haja vista a dificuldade de implementação de multas e outras sanções para entidades sem presença física no bloco. A falta de recursos humanos e técnicos das Autoridades Nacionais de Proteção de Dados e a pouca cooperação internacional existente nesse campo agravam a situação. Apesar disso, por força do chamado Efeito Bruxelas, verificou-se que diversos países ao redor do mundo caminham em direção à conformidade com os padrões estabelecidos no GDPR, a exemplo da própria LGPD brasileira.

Uma vez percorrido sobre os aspectos teóricos que orbitam a extraterritorialidade do GDPR, o terceiro capítulo apresentou e discutiu os resultados do questionário aplicado a algumas empresas de TIC de Florianópolis sobre o tema. Apesar de nenhuma das empresas participantes da pesquisa ter presença física em qualquer país da União Europeia, chegou-se à conclusão de que o GDPR pode ser diretamente aplicável para algumas das empresas participantes, por força do seu art. 3.2, isto é, quando realizam o tratamento de dados pessoais de indivíduos que se encontram na UE por meio da oferta de bens ou serviços ou por meio do monitoramento do comportamento dessas pessoas. Além disso, algumas empresas já apresentaram incremento de custos devido à necessidade de adequação às normas do GDPR, que demanda investimento tanto na área técnica quanto de treinamento de pessoal.

Essas constatações confirmaram a hipótese básica deste trabalho de que algumas empresas do setor de TIC de Florianópolis podem se enquadrar dentro do escopo de aplicação extraterritorial do GDPR, e que tal fenômeno já impactou diretamente tais organizações. Ainda assim, ressalta-se a necessidade de maiores investigações futuras para averiguar se os investimentos executados pelas empresas para se adequarem às normas do GDPR não são também decorrência de obrigações contratuais ou de outras influências indiretas.

A pesquisa também demonstrou que algumas empresas do setor têm interesse em constituir alguma filial ou representação na União Europeia nos próximos cinco anos – o que torna a difusão de conhecimento sobre os dispositivos do GDPR ainda mais importante. Ao mapear as fontes de informações sobre o GDPR, observou-se que os meios mais utilizados pelas empresas participantes são pesquisas em sites de buscas e a consultoria jurídica especializada.

Tendo em vista as similaridades existentes entre a LGPD brasileira e o GDPR – o que pode, em parte, facilitar a adequação a ambas as normas –, o presente trabalho também buscou investigar a percepção dos empresários sobre os impactos da lei brasileira para seus negócios. Constatou-se que a grande maioria das empresas (87,5%) acredita que poderá ser

impactada pela LGPD, número muito próximo do obtido por outra pesquisa realizada em âmbito nacional pela Serasa Experian com empresas de grande porte (81%). A comparação dos números obtidos nesta pesquisa com outros estudos similares demonstrou que a preocupação das empresas quanto às medidas necessárias à adequação às normas de Proteção de Dados Pessoais não se limita ao setor de Tecnologia da Informação de Florianópolis, mas é um fenômeno de abrangência nacional e internacional.

Por fim, ressalta-se que, apesar dos impactos globais causados pela extraterritorialidade do GDPR, somente pela via da cooperação internacional e do debate nos organismos multilaterais é que se alcançará um nível adequado de proteção de dados pessoais para todos os indivíduos. Além disso, só assim se garantirá a segurança jurídica necessária para os agentes econômicos que operam no contexto da nova economia de dados. Esse equilíbrio entre a proteção de dados pessoais e o desenvolvimento tecnológico é, portanto, demanda urgente a ser tratada pela comunidade internacional para que o Direito à Proteção de Dados não seja somente privilégio de europeus ou brasileiros, mas sim de todos os indivíduos.

## REFERÊNCIAS

ACATE. **Tech Report 2018**. Disponível em: <<https://www.acate.com.br/wp-content/uploads/2018/11/ACATE-Observat%C3%B3rio-2018.pdf>> Acesso em: 24/03/2021.

ACATE. **Tech Report 2020**. Disponível em: <<https://www.techreportsc.com/>> Acesso em: 24/03/2021.

ACCIOLY, Hildebrando; CASELLA, Paulo Borba; SILVA, G E. do Nascimento e. **Manual de Direito Internacional Público**. 20ª edição. São Paulo: Saraiva, 2012.

ACUNHA, Fernando José Gonçalves. Democracia e transconstitucionalismo: “direito ao esquecimento”, extraterritorialidade e conflito entre ordens jurídicas. **Revista Direito Gv**, São Paulo, v. 12, n. 3, p. 748-775, set. 2016. Quadrimestral.

ALSENOY, B. Van; KOEKKOEK, Mariek. **Internet and Jurisdiction after Google Spain: the Extraterritorial Reach of the Right to be Delisted**. International Data Privacy Law Review. Vol. 5. 2015.

ALSENOY, Brendan Van. **Data Protection in the EU: Roles, responsibilities and liability**. Intersentia Ltd: Cambridge, 2019.

ALSENOY, Brendan Van. Reconciling the (extra)territorial reach of the GDPR with public international law. In: VERMEULEN, Gert; LIEVENS, Eva. **Data Protection and Privacy under Pressure**. Maklu: Portland, 2017.

Art. 29 Working Party. **Opinion 4/2007 on the concept of personal data**. 2007.

AZZI, Adèle. **The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation**. JIPITEC. 126 para 126. (2018).

BANCO MUNDIAL. GDP per capita (current US\$) - European Union. Disponível em: <<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=EU>>. Acesso em: 23/03/2021.

BANCO MUNDIAL. GDP (current US\$) - European Union, United States, China. Disponível em: <[https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN&name\\_desc=true](https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN&name_desc=true)>. Acesso em: 23/03/2021.

BANCO MUNDIAL. World Development Indicators. Disponível em: <<https://databank.worldbank.org/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=>>>. Acesso em: 23/03/2021.

BEDERMAN, David J. **Globalization and International Law**. Palgrave Macmillan: Nova Iorque, 2008.

BEHRENS, Jéssica Soares Braga. **Startup na prática: desafios e oportunidades**. 2015. 41 f., il. Monografia (Bacharelado em Comunicação Social)—Universidade de Brasília, Brasília, 2015.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: as funções e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRADFORD, Anu. **The Brussels Effect: How the European Union Rules the World**. Nova Iorque: Oxford University Press, 2020.

BRKAN, Maja. The Unstoppable Expansion of the EU Fundamental Right to Data Protection. **Maastricht Journal Of European And Comparative Law**, [S.L.], v. 23, n. 5, p. 812-841, out. 2016. SAGE Publications. <http://dx.doi.org/10.1177/1023263x1602300505>.

BUXBAUM, Hannah L. **Territory, Territoriality, and the Resolution of Jurisdictional Conflict** (2009). Articles by Maurer Faculty. 132. pág. 11.

CAREY, Peter. **Data Protection: A Practical Guide to UK and EU Law**. 5ª Ed. Oxford: Oxford University Press, 2018.

CASELLA, P. B. **Extraterritorialidade e proteção da livre-concorrência**. Revista da Faculdade de Direito, Universidade de São Paulo, [S. l.], v. 96, p. 501-519, 2001. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67514>. Acesso em: 28/02/2021.

CASTELLUCCIA, Claude. Behavioural Tracking on the Internet: A Technical Perspective. In: GUTWITH, Serge et al. (eds.) **European Data Protection: In Good Health?** Springer: Londres, 2012.

CDI. **Report on the Work of its Fifty-Eight Session**. 1 May-9 June and 3 July-11 August 2006. Doc. A/61/10. Annex E, n.º 2. Disponível em: <[http://legal.un.org/ilc/documentation/english/reports/a\\_61\\_10.pdf](http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf)> Acesso em: 01/03/2021.”

CEPD. Contribution of the EDPB to the evaluation of the GDPR under Article 97. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_contributiongdprevaluation\\_20200218.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf)>. Acesso em: 20/03/2021.

CEPD. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE. Disponível em: <[https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_recommendations\\_202001\\_supplementarymeasurestransferstools\\_pt.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pt.pdf)>. Acesso em 22/03/2021.

CHAIMOVICH, Mariana Midea Cuccovia. **O direito da integração nas constituições dos estados membros da União Europeia**. Dissertação de Mestrado. Faculdade de Direito da USP. São Paulo: USP, 2011. Disponível em: <[https://teses.usp.br/teses/disponiveis/2/2135/tde-15052012-090748/publico/Mariana\\_Midea\\_Cuccovia\\_Chaimovich\\_ME.pdf](https://teses.usp.br/teses/disponiveis/2/2135/tde-15052012-090748/publico/Mariana_Midea_Cuccovia_Chaimovich_ME.pdf)>. Acesso em: 24/03/2020.

CLAES, Monica. The Primacy of EU Law in European and National Law. In: ARNULL, Anthony; CHALMERS, Damian (ed.). **The Oxford Handbook of European Union Law**. Oxford: Oxford University Press, 2015.

COMISSÃO EUROPEIA. Adequacy decisions. Disponível em: <[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea)>. Acesso em 22/03/2021.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981.

CONSELHO DA EUROPA. **Handbook on European Data Protection Law**, Belgium: Council of Europe, 2018. p. 24.

CORTEZIA, Sandro Luís Diesel; SOUZA, Yeda Swirski de. **Uma análise sobre a internacionalização de pequenas empresas brasileiras da indústria de software**. Brazilian Business Review. v. 8, n.4. Vitória, Out. - Dez. 2011. ISSN 1807-734X DOI: <http://dx.doi.org/10.15728/bbr.2011.8.4.2>

COSTA, Olivier. **A União Europeia e sua política exterior (história, instituições e processo de tomada de decisão)**. Brasília: FUNAG, 2017. Disponível em: <[http://funag.gov.br/biblioteca/download/1189-Uniao\\_europeia\\_e\\_sua\\_politica\\_exterior.pdf](http://funag.gov.br/biblioteca/download/1189-Uniao_europeia_e_sua_politica_exterior.pdf)>. Acesso em: 24/03/2020.

CZERNIAWSKI, Michal; HERT, Paul de. **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**. *International Data Privacy Law*. Vol. 6, No. 3. Oxford: Oxford University Press, 2016.

DAL RI, Arno. **A Cidadania Europeia e a Livre Circulação de Pessoas**. In: DAL RI, Arno; OLIVEIRA, Odete de. (Orgs.) *Cidadania e Nacionalidade: efeitos e perspectivas regionais, nacionais e globais*. Ijuí: Unijuí, 2002.

DELOITTE. GDPR Preparedness Survey Report. Disponível em: <<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-riks-gdpr-preparedness-survey-report-noexp.pdf>>. Acesso em: 15/10/2020.

DINAN, Dismon. **Europe Recast: A History of European Union**. 2ª Edição. Lynne Rienner: Boulder, 2014.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. *Tratado de proteção de dados pessoais*. 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7.

ELLIOT, Mark; MACKEY, Elaine; MOURBY, Miranda; et al. **Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the**

UK. Computer Law & Security Review. Volume 34, nº2. 2018. Pages 222-233. ISSN 0267-3649. <https://doi.org/10.1016/j.clsr.2018.01.002>.

EUROSTAT. **EU population in 2020**: almost 448 million. Disponível em: <<https://ec.europa.eu/eurostat/documents/2995521/11081093/3-10072020-AP-EN.pdf/d2f799bf-4412-05cc-a357-7b49b93615f1#:~:text=On%201%20January%202020%2C%20the,States%20on%201%20January%202019.>>>. Acesso em: 23/03/2021.

FAIRHURST, John. **Law of the European Union**. 11. ed. Harlow: Pearson Education Limited, 2016.

FALK, Matheus. **A necessidade de proteção aos dados pessoais no direito brasileiro: tutela jurídica na era da modernidade líquida e da surveillance**. 2017. 192 f. Dissertação (Mestrado) - Curso de Direito, Universidade Federal do Paraná, Curitiba, 2017. Disponível em: <https://acervodigital.ufpr.br/handle/1884/47787>. Acesso em: 15 jun. 2020

FERREIRA, Bráulio Cavalcanti; QUEIROZ, Bruna Pamplona de; GONÇALVES, Everton das Neves. Análise Econômica do Direito e o Compliance Empresarial: apreciação jurídico-econômica dos programas de conformidade e dos custos de prevenção. **Economic Analysis Of Law Review**, Brasília, v. 9, n. 1, p. 259-276, Janeiro-Abril de 2018. Quadrimestral.

FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. **A Extraterritorialidade Do Regime Geral De Proteção De Dados Pessoais Da União Europeia: Manifestações E Limites**. 2018. 356 f. Tese (Doutorado) - Curso de Direito, Universidade Nova de Lisboa, Lisboa, 2018.

FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. **Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do GDPR**. UNIO - EU Law Journal. Vol. 4, No. 2, Julho 2018, pág. 119-131.

FONSECA, Maria da Graça Almeida de Eça do Canto Moniz Adão da. **As Implicações em Países Terceiros Do Regime Geral de Proteção de Dados Pessoais da União Europeia: a sua Extraterritorialidade**. Direito Comparado. RFD, vol. 1 nº 1. Lisboa, 2018. pág. 631.

FRAZÃO, Ana. **Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos**. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007.

FUSTER, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Springer: Bruxelas, 2014.

GONÇALVES, Everton das Neves. **A Teoria de Posner e sua Aplicabilidade à Ordem Constitucional Econômica Brasileira de 1988**. Dissertação de Mestrado em Direito – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas. Programa de Pós-

Graduação em Direito, Florianópolis, Santa Catarina. 1997. Disponível em <http://tede.ufsc.br/teses/PDPC0258-D.pdf>. Acesso em 25/01/2021.

GREZE, Benjamin. **The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives**. International Data Privacy Law,, Vol. 9, No. 2. 2019.

HARTLEY, Trevor. **Overlapping jurisdiction in EC law**. In: International Commercial Litigation: Text, Cases and Materials on Private International Law (pp. 237-264). Cambridge: Cambridge University Press, 2009. doi:10.1017/CBO9780511808739.011

HERT, Paul de; CZERNIAWSKI, Michal. **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**. International Data Privacy Law. Volume 6. Número 3. Agosto de 2016. <https://doi.org/10.1093/idpl/ipw008>.

HOBBSBAWM, Eric J. **Era dos Extremos: o breve século XX**. 2ª edição. São Paulo: Companhia das letras, 2019.

HOLMES, Dawn E. **Big Data: a very short introduction**. 1ª ed. Oxford: Oxford University Press, 2017.

IBGE. Memória IBGE: Censos Demográficos. Disponível em: <<https://memoria.ibge.gov.br/historia-do-ibge/historico-dos-censos/censos-demograficos.html>>. Acesso em: 10/04/2021.

JOHNSON, David Reynold; POST, David G. **Law and Borders - the Rise of Law in Cyberspace**. Stanford Law Review. Vol. 48, p. 1367. Stanford: 1996, Disponível em: <<https://ssrn.com/abstract=535> or <http://dx.doi.org/10.2139/ssrn.535>> Acesso em: 27/02/2021.

KAVA, Samuel. **The Extraterritorial Application of the Sherman Anti-Trust Act in the Age of Globalization: The Need to Amend the Foreign Trade Antitrust Improvements Act (FTAIA) & Vigorously Apply International Comity**. Journal of Business and Technology Law. V. 15, nº 1. 135. 2019. Disponível em: <<https://digitalcommons.law.umaryland.edu/jbtl/vol15/iss1/5>>. Acesso em 01/03/2021.

KLOSA, Dariusz; SVANTESSON, Dan Jerker; (eds.) **Trans-atlantic Data Privacy Relations as a Challenge for Democracy**. European Integration and Democracy Series. Volume 4. Cambridge: Intersentia, 2017.

KOTSCHY, Waltraut. Article 6. Lawfulness of processing. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation (GDPR): a commentary**. Oxford: Oxford University Press, 2020. p. 329.

KUNER, Christopher. **Extraterritoriality and regulation of international data transfers in EU data protection law**, International Data Privacy Law. Vol 5, n. 4. Novembro de 2015. páginas 235–245. DOI: <https://doi.org/10.1093/idpl/ipv019>.

KUNER, Christopher. **The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law**. Bloomberg BNA Privacy and Security Law Report. 2012.

LEE, Sang Woo. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing**. Tese de Doutorado. China University of Political Science and Law: Pequim, 2018.

LEOPOLDINO, Juliana. **REGIME JURÍDICO DAS SOCIEDADES TRANSNACIONAIS E EFEITOS EXTRATERRITORIAIS DAS LEIS**. 2008. 88 f. Dissertação (Mestrado) - Curso de Direito, Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

LOHMANN, Sacha. **Extraterritorial U.S. Sanctions**. SWP Comment. nº 5. Fev. 2019. Disponível em: <<https://www.swp-berlin.org/10.18449/2019C05/>> Acesso em: 27/02/2021.

LYNSKEY. Orla. **The Foundations of EU Data Protection Law**. Oxford University Press: Oxford, 2015.

MAIO, Claudio di; TOMÁS, Ana. **La ciudadanía europea ante el reto de la unidad política: ¿mero estatuto de libertades o motor para una sólida integración de la Unión Europea?** Derecho del Estado n.º 40, Universidad Externado de Colombia, Janeiro-Junho de 2018, pp. 181- 208. DOI: <https://doi.org/10.18601/01229893.n40.08>.

MARIO, Viola. **Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira**. Rio de Janeiro: Instituto Tecnologia e Sociedade, 2019.

MARKKULA, Jouni; ROHUNEN, Anna; TIKKINEN-PIRI, Christina. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. **Computer Law & Security Review.**, [S.L.], vol. 34, nº. 1, , pág. 134-153, fev. 2018. <https://doi.org/10.1016/j.clsr.2017.05.015>

MEDEIROS, Marcelo de Almeida; CAMPOS, Cinthia Regina. **União Européia, reformas institucionais e déficit democrático: uma análise a partir do mecanismo de co-decisão**. Rev. bras. polít. int., Brasília , v. 52, n. 1, p. 29-52, June 2009. Disponível em: <[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0034-73292009000100002&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292009000100002&lng=en&nrm=iso)>. Acesso em: 20/04/2020.

MENTHE, Darrel C. **Jurisdiction in Cyberspace: A Theory of International Spaces**. 4 Mich. Telecomm. & Tech. L. Rev. 69. (1998). Disponível em: <<http://repository.law.umich.edu/mttlr/vol4/iss1/3>>. Acesso em: 27/02/2021  
MENTHE, Darrel C. op. cit. pág. 71. TAYLOR, Mistale. Op. cit. pág. 3. BELETSK, Roman. **Critical assessment of the extraterritoriality of the EU General Data Protection Regulation**. University of Helsinki: Helsinki, 2019. pág. 12.

MICOLTA PORTOCARRERO, Ma. Catalina. **El proceso legislativo en el Tratado de Lisboa: privilegio de la eficacia en detrimento de la democracia**. Pap.polit., Bogotá , v. 19, n. 1, p. 237-263, June 2014 . Disponível em:

<[http://www.scielo.org.co/scielo.php?script=sci\\_arttext&pid=S0122-44092014000100012&lng=en&nrm=iso](http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-44092014000100012&lng=en&nrm=iso)>. Acesso em: 20/04/2020.

MONDSCHNEIN, Christopher. **The Regulation of Targeted Behavioural Advertising in the European Union**. MCEL Master Working Paper 2017/2. Maastricht Centre for European Law: Maastricht, 2017. pág. 11. Disponível em: <[https://www.maastrichtuniversity.nl/sites/default/files/mcel\\_master\\_working\\_paper\\_20172\\_mondschein\\_2.pdf](https://www.maastrichtuniversity.nl/sites/default/files/mcel_master_working_paper_20172_mondschein_2.pdf)> Acesso em: 03/03/2021.

MONTELEONE, Shara; PUCCIO, Laura. **From Safe Harbour to Privacy Shield Advances and shortcomings of the new EU-US data transfer rules**. Bruxelas: União Europeia, 2017. pág. 1. Disponível em: <[https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS\\_IDA\(2017\)595892\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf)>. Acesso em 23/03/2021.

MOURA, Aline Beltrame de. **Cidadania europeia: uma verdadeira e própria cidadania?** Direito em Debate, v. 32, p. 09-34, 2009.

MOURA, Aline Beltrame de. **Paradoxos e limites de uma cidadania sem deveres: o caso da cidadania da União Européia**. Âmbito Jurídico, v. 90, p. 1-8, 2011.

MOURA, Aline Beltrame de. **O âmbito político do princípio da subsidiariedade no Direito Comunitário europeu**. In: **8º Congresso Brasileiro de Direito Internacional**, 2010, Foz do Iguaçu. Estudos de Direito Internacional. Curitiba: Juruá Editora, 2010. v. XIX. p. 51-60.

MOURA, Aline Beltrame de. **O Direito Internacional Privado entre a Nacionalidade de Mancini e a Cidadania da União Europeia**. Revista Eletrônica Direito e Política, v. 7, p. 1058-1084, 2012.

MOURA, Aline Beltrame de. **As Bases Principiológicas do Sistema Jurídico da União Europeia**. In: Gustavo Ferraz de Campos Monaco; Maria Rosa Loula; Coordenadores. (Org.). **Direito Internacional e Comparado: Trajetória e Perspectivas**. 1ª ed. São Paulo: Quartier Latin do Brasil, 2021, v. 2, p. 43-58.

MOURA, Aline Beltrame de. GNOATTON, Letícia Mulinari; MOURA, Aline Beltrame de. **Os Desafios Da Aplicação Extraterritorial Do Regulamento Geral De Proteção De Dados Pessoais Da União Europeia**. In: GHILARDI, Dóris; SASS, Liz Beatriz (coords.) **Temas Atuais De Direito Privado E Sociedade Da Informação: O Direito Na Era Digital**. 1ª ed. Florianópolis: Habitus, 2020.

MOURA, Aline Beltrame de. **O critério de conexão da nacionalidade na doutrina e na legislação de direito internacional privado brasileiro (1863-1973)**. SEQUÊNCIA (UFSC), v. 39, 2018. pág. 198.

New York Times. Google Is Fined \$57 Million Under Europe's Data Privacy Law. Disponível em: <<https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>> Acesso em: 03/03/2020.

NUNES, Amandino Teixeira Júnior. **A União Europeia e suas instituições**. Revista de Informação Legislativa. 48 n. 192. Senado Federal: Brasília: out./dez. 2011. Disponível

em:<[https://www12.senado.leg.br/ril/edicoes/48/192/ril\\_v48\\_n192\\_p21.pdf](https://www12.senado.leg.br/ril/edicoes/48/192/ril_v48_n192_p21.pdf)>. Acesso em: 24/03/2020.

OIZUMI, Monica Yumi Shida. **Conflito de Jurisdição no Direito Concorrencial no Âmbito Internacional**. 2017. Dissertação (Mestrado) - Curso de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2017.

OSMAN, Bruna Homem de Souza; SOARES, Jéssica Aparecida. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS: A extraterritorialidade do GDPR europeu e seus impactos. In: WACHOWICZ, Marcos (org.). **Proteção de Dados em Perspectiva: LGPD e RGPD na ótica do Direito Comparado**. Curitiba: Gedai, UFPR 2020. pág. 583.

OSTER, Jan. Data Protection. In: **European and International Media Law** (pp. 304-369). Cambridge: Cambridge University Press, 2016. doi:10.1017/9781139208116.009

PARLAMENTO EUROPEU. **The CJEU judgment in the Schrems II case**. Disponível em:<[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS\\_ATA\(2020\)652073\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)>. Acesso em: 23/03/2021.

PHINNEMORE, David. **The European Union: Establishment and Development**. In: BORRAGÁN, Nieves Pérez-Solórzano; CINI, Michelle. **European Union Politics**. 5ª edição. Oxford University Press: New York, 2016.

PINDER, John; USHERWOOD, Simon. **The European Union: a very short introduction**. 3ª edição. Oxford University Press: Oxford, 2013. pág. 52.

PORTUGAL. Constituição (1976). **Constituição da República Portuguesa**, de 02 de abril de 1976. Redação original.

POULLET, Yves. **Transborder Data Flows and Extraterritoriality: the European Position**. *Journal of International Commercial Law and Technology*, vol. 2, no. 3, 2007, páginas. 141-153.

PURTOVA, Nadezhda. **The law of everything. Broad concept of personal data and future of EU data protection law**. *Law, Innovation and Technology*. Volume 10, n. 1. Londres: 2018.

PWC. **GDPR Preparedness Pulse Survey**. Disponível em:<<https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html>> Acesso em 25/01/2021.

REICHEL, Jane; LIND, Anna-sara. **Regulating Data Protection within the European Union**. In: DÖRR, Dieter; WEAVER, Russell L.. **Perspectives on Privacy Increasing**. Berlin: de Gruyter, 2014. Cap. 3. p. 22-45.

REINO UNIDO. Information Commissioner's Office. **Legitimate interests**. Disponível em:<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>> Acesso em: 21/08/2020.

REINO UNIDO. Information Commissioner's Office. **Data Protection and the EU-UK Trade Deal**. Disponível em: <<https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-uk-trade-deal/>>. Acesso em: 01/03/2021.

REINO UNIDO. Information Commissioner's Office. **ICO statement in response to the publication of a draft adequacy decision from the European Commission**. Disponível em: <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/02/ico-statement-in-response-to-the-publication-of-a-draft-adequacy-decision-from-the-european-commission/>> Acesso em: 01/03/2021.

REZEK, Francisco. **Direito Internacional Público: curso elementar**. 13ª edição. São Paulo: Saraiva, 2011. pág. 193.

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

SANTOS, Milton. **A Natureza do Espaço: Técnica e Tempo, Razão e Emoção**. 4. ed. São Paulo: Editora da Universidade de São Paulo, 2006.

SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo. Tratado de proteção de dados pessoais. 1. ed. Rio de Janeiro: Forense, 2021. p. 3-20. ISBN 978-85-309-9151-7.

SCHULTZ, Thomas. **Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface**. The European Journal of International Law Vol. 19 no.4. 2008.

SCHÜNEMANN, Wolf J.; BAUMANN, Max-Otto (ed.). **Privacy, Data Protection and Cybersecurity in Europe**. Cham: Springer, 2017. pág. 2.

SEBRAE. **Panorama LGPD em Santa Catarina: Conhecimento das pequenas empresas sobre a Lei Geral de Proteção e Dados**. Disponível em: <<http://sebrae.sc/panoramalgpd>>. Acesso em: 04/04/2021.

SERASA EXPERIAN. **O que os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito?** Disponível em: <<https://www.serasaexperian.com.br/conteudos/protecao-de-dados/pesquisa-o-que-os-consumidores-e-as-empresas-sabem-sobre-lgpd-e-o-que-estao-fazendo-a-respeito/>>. Acesso em: 26/01/2021.

Shabani, M., Borry, P. **Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation**. Eur J Hum Genet 26, 149–156 (2018). <https://doi.org/10.1038/s41431-017-0045-7>

SHARMA, Sanjay. **Data Privacy and GDPR Handbook**. Hoboken: John Wiley & Sons, 2020.

SOARES, Antonio Goucha. A União Europeia como potência global? As alterações do Tratado de Lisboa na política externa e de defesa. **Rev. bras. polít. int.**, Brasília, v. 54, n. 1, p. 87-104, 2011. Disponível

em:<[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0034-73292011000100006&lng=en&nrm=iso](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292011000100006&lng=en&nrm=iso)>. Acesso em: 28/04/2020.  
<https://doi.org/10.1590/S0034-73292011000100006>.

SOUZA, Crisomar Lôbo de. **Estratégias de internacionalização: um estudo sobre a influência dos fatores de riscos sobre a estratégia e objetivos estratégicos em empresas exportadoras brasileiras**. 2017. Tese (Doutorado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2017. doi:10.11606/T.12.2017.tde-13062017-164539. Acesso em: 2021-04-07.

SVANTESSON, Dan Jerker. **Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation**. *International Data Privacy Law*. Vol. 5, No. 4. 2015. pág. 232.

SVANTESSON, Dan Jerker B.. Article 3. Territorial scope. In: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. **The EU General Data Protection Regulation (GDPR): a commentary**. Oxford: Oxford University Press, 2020. p. 82.

SVANTESSON, Dan Jerker B. **Extraterritoriality in data privacy law**. Ex Tuto Publishing: Copenhagen, 2013.

SVANTESSON. Dan Jerker. **A “layered approach” to the extraterritoriality of data privacy laws**. *International Data Privacy Law*. Vol. 3, n. 4. 2013.

SVANTESSON. Dan Jerker. **Extraterritoriality in the context of Data Privacy Regulation**. *Masaryk University Journal of Law and Technology*. Vol. 7, .1. 2012.

SYRPIS, Phil. **The Relationship Between Primary and Secondary Law in the EU**. *Common Market Law Review*. Vol. 52. p 461–488. Kluwer Law International: United Kingdom, 2015.

TAYLOR, Mistale. **Permissions and Prohibitions In Data Protection Jurisdiction**. Brussels Privacy Hub Working Paper. Vol. 2, nº6. Maio de 2016.

TENE, Omer; WOLF, Christopher. **Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation**. *Future of Law Privacy Forum*. 2013. Disponível em:<<https://fpf.org/wp-content/uploads/2013/01/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-201311.pdf>> Acesso em: 04/03/2021.

UNIÃO EUROPEIA. Art. 29 Working Party. **Opinion 4/2007 on the concept of personal data**. 2007.

UNIÃO EUROPEIA. Article 29 Working Party. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.** Disponível em: <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf)>.

UNIÃO EUROPEIA. **Comunicação da Comissão Europeia relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais na Comunidade e à segurança dos sistemas de informação.** Bruxelas: 1990. Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:51990DC0314&from=EN>>. Acesso em: 05/07/2020

UNIÃO EUROPEIA. Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção 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://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520>>. Acesso em: 23/03/2021.

UNIÃO EUROPEIA. Decisão de Adequação da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: <[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.207.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG)>. Acesso em: 23/03/2021.

UNIÃO EUROPEIA. **Diretrizes 07/2020 sobre os conceitos de controlador e processador de dados no GDPR do Comitê Europeu de Proteção de Dados.** Disponível em: <[https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_202007\\_controllerprocessor\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf)>. Acesso em: 27/02/2020. pág. 4.

UNIÃO EUROPEIA. **Diretrizes 3/2018 sobre o âmbito de aplicação territorial do GDPR (Art.3º) do Comitê Europeu de Proteção de Dados.** Disponível em: <[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_pt.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf)> Acesso em: 01/03/2021. pág. 5.

UNIÃO EUROPEIA. **EU administration - staff, languages and location.** Disponível em <[https://europa.eu/european-union/about-eu/figures/administration\\_en](https://europa.eu/european-union/about-eu/figures/administration_en)>. Acesso em: 08/04/2020.

UNIÃO EUROPEIA. **EU Law.** Disponível em <[https://e-justice.europa.eu/content\\_eu\\_law-3-en.do](https://e-justice.europa.eu/content_eu_law-3-en.do)>. Acesso em 05/04/2020.

UNIÃO EUROPEIA. **European Parliament: powers and procedures.** Disponível em: <<https://www.europarl.europa.eu/about-parliament/en/powers-and-procedures>>. Acesso em: 28/04/2020.

UNIÃO EUROPEIA. **Guidelines 05/2020 on consent under Regulation 2016/679.** Disponível em:

<[https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf)>. Acesso em: 20/08/2020.

UNIÃO EUROPEIA. **Information Guide to the Court of Justice of the European Union.** Disponível em: <[http://aei.pitt.edu/74891/1/Court\\_of\\_Justice.pdf](http://aei.pitt.edu/74891/1/Court_of_Justice.pdf)>. Acesso em: 24/03/2020.

UNIÃO EUROPEIA. **O PE após o Tratado de Lisboa: um papel reforçado na construção da Europa.** Disponível em: <<https://www.europarl.europa.eu/about-parliament/pt/powers-and-procedures/the-lisbon-treaty>> Acesso em: 28/04/2020.

UNIÃO EUROPEIA. **Opinião nº8/2010 do Grupo de Trabalho do Art. 29 (versão original).** Disponível em: <[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf)>. Acesso em: 01/03/2021.

UNIÃO EUROPEIA. **Parecer nº. 1 de 2010 do Grupo de Trabalho do Artigo 29 sobre o conceito de controlador e processador.** Bruxelas: UE, 2010. pág. 15.

UNIÃO EUROPEIA. **Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century.** UE: Bruxelas, 2012. Disponível em <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>>. Acesso em 17/12/2020.

UNIÃO EUROPEIA. **The common agricultural policy at a glance.** Disponível em: <[https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance\\_en](https://ec.europa.eu/info/food-farming-fisheries/key-policies/common-agricultural-policy/cap-glance_en)>. Acesso em: 24/06/2020.

UNIÃO EUROPEIA. **The European Parliament: historical background.** Disponível em: <<https://www.europarl.europa.eu/factsheets/en/sheet/11/the-european-parliament-historical-background>>. Acesso em: 24/03/2020.

UNIÃO EUROPEIA. **The History of the General Data Protection Regulation.** Disponível em: <[https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en#](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#)>. Acesso em: 18/12/2020.

UNIÃO EUROPEIA. **Tratado Sobre Funcionamento Da União Europeia.** Artigo 288°. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>>. Acesso em: <05/04/2020.

USTARAN, Eduardo (ed.). **European Data Protection Law and Practice.** New Hampshire: International Association Of Privacy Professionals, 2018.

VAINZOF, Rony. Capítulo I - Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de dados comentada.** 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-85-5321-925-4.

VILA MAIOR, Paulo. **A União Europeia após a queda do muro de Berlim: sucesso e desafios.** Revista da Faculdade de Ciências Humanas e Sociais. Porto: Edições Universidade Fernando Pessoa, 2009. Disponível em: <[https://bdigital.ufp.pt/bitstream/10284/1329/1/196-205\\_FCHS06-4.pdf](https://bdigital.ufp.pt/bitstream/10284/1329/1/196-205_FCHS06-4.pdf)>. Acesso em 30/03/2020.

WALKER, Neil. The Philosophy of European Union. In: ARNULL, Anthony; CHALMERS, Damian (ed.). **The Oxford Handbook of European Union Law**. Oxford: Oxford University Press, 2015.

WELFARE, Damien; CAREY, Peter. Territorial Scope and Terminology. In: CAREY, Peter (ed.). **Data Protection: a practical guide to uk and eu law**. 5. ed. Oxford: Oxford University Press, 2018. Cap. 1. p. 1-32.

WILHELM, Ernst-Oliver. **A brief history of the General Data Protection Regulation**. International Association of Privacy Professionals (IAPP). Disponível em: <<https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>> . Acesso em: 18/12/2020.

XIA, Yue. **Assessing Extraterritorial Application of EU Competition Law**. Ghent University: Ghent, 2017. ág. 8. Ver também: TJEU. Caso C-48/69. Imperial Chemical Industries Limited v. Commission [1972] E.C.R. 619.

**Textos legislativos consultados:**

BRASIL. DECRETO Nº 7.030, DE 14 DE DEZEMBRO DE 2009. Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, art. 70.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Lei Geral de Proteção de Dados. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)> Acesso em: 05/03/2021.

PORTUGAL. Constituição (1976). Constituição da República Portuguesa, de 02 de abril de 1976. Redação original.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>>. Acesso em: 05/07/2020.

UNIÃO EUROPEIA. DIRETIVA (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

**Casos consultados:**

BRASIL. Tribunal de Justiça de São Paulo. Ação. nº 0005243-38.2013.8.26.0011. Luizeani Altenhofen. Eudes Gondim Junior. Pinheiros, SC, 04 de abril de 2013. Diário de Justiça do Tribunal de Justiça de São Paulo. São Paulo.

CORTE PERMANENTE DE JUSTIÇA INTERNACIONAL. Caso “Lotus” (França v Turquia), Julgamento nº 9 de 7 Setembro 1927. P.C.I.J. Reports 1928. Series A. No. 10. pág.18-19.

SUPREMA CORTE DOS ESTADOS UNIDOS DA AMÉRICA. Alcoa S. S. Co. v. United States, 338 U. S. 421 (1949).

TJUE, C-04/73, Caso Nold II, julgado em 14/05/1974

TJUE, C-11/70, Caso Internationale Handelsgesellschaft, julgado em 17/12/1970

TJUE, C-29/69, Caso Stauder, julgado em 12/11/1969.

TJUE. C-131/12. Caso Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González.

TJUE. C-210/16. Caso Wirtschaftsakademie. Julgado em 2018.

TJUE. C-230/14. Caso Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság.

TJUE. C-272/18. Caso Verein für Konsumenteninformation. Julgado em 2019.

TJUE. C-311/18. Caso Schrems II. Julgado em 16/07/2020.

TJUE. C-362/14. Caso Schrems. Julgado em 06/10/2015.

TJUE. C-366/10. Caso Air Transport Association of America and Others v. Secretary of State for Energy and Climate Change. Julgado em 2010.

TJUE. C-507/17. Caso Google LLC contra Commission Nationale de l’Informatique et de Libertés. Julgado em: 24/09/2019.

TJUE. C-582/14. Caso Breyer./Federal Republic of Germany. Julgado em 19 de outubro de 2016.

TJUE. C-585/08.. Caso Pammer and Hotel Alpenhof. Julgado em 2010.

TJUE. Caso C-275/06 Productores de Música de España (Promusicae) v Telefónica de España. Julgado em 2008.