UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI

VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM CIÊNCIA JURÍDICA – PPCJ

CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ

ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO

ANÁLISE COMPARATIVA DA COOPERAÇÃO INTERNACIONAL, DAS SANÇÕES ADMINISTRATIVAS E DO CONTROLE JUDICIAL NA PROTEÇÃO DE DADOS NA UNIÃO EUROPÉIA E NO BRASIL

MATHEUS ADRIANO PAULO

Orientador: Professor Doutor Osvaldo Agripino de Castro Junior

Itajaí-SC, 20 de janeiro de 2021.

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI

VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM CIÊNCIA JURÍDICA – PPCJ

CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ

ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO

ANÁLISE COMPARATIVA DA COOPERAÇÃO INTERNACIONAL, DAS SANÇÕES ADMINISTRATIVAS E DO CONTROLE JUDICIAL NA PROTEÇÃO DE DADOS NA UNIÃO EUROPÉIA E NO BRASIL

MATHEUS ADRIANO PAULO

Dissertação submetida ao Curso de Mestrado em Ciência Jurídica da Universidade do Vale do Itajaí – UNIVALI, como requisito parcial à obtenção do título de Mestre em Ciência Jurídica.

Orientador: Professor Doutor Osvaldo Agripino de Castro Junior

Itajaí-SC, 20 de janeiro de 2021.

AGRADECIMENTOS

Agradeço, primeiramente, a meus pais, Maria Diair da Silva e Marcio Roberto Paulo pelos princípios éticos que me foram ensinados. Também, à minha esposa pelo apoio incondicional.

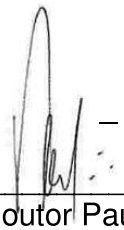
Ao meu orientador, Dr. Osvaldo Agripino de Castro Junior, por toda a paciência e zelo na elaboração do presente trabalho, sempre se mostrando compreensível com as dificuldades do dia a dia e com o tema proposto.

Ao coordenador do programa, Dr. Paulo Márcio Cruz, que sempre se fez presente em todo o programa, recebendo dicas, sugestões, auxiliando na elaboração dos trabalhos e buscando auxiliar todos com sua formidável equipe.

DEDICATÓRIA

Este trabalho é dedicado, primeiramente, a meus pais, Maria Diair da Silva e Marcio Roberto Paulo pelos princípios éticos que me foram ensinados. Também, à minha esposa pelo apoio incondicional. Por fim, ao meu orientador por acreditar no meu trabalho e por todas as oportunidades que me foram dadas e me fizeram chegar até aqui.

Esta Dissertação foi julgada APTA para a obtenção do título de Mestre em Ciência Jurídica e aprovada, em sua forma final, pela Coordenação do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica – PPCJ/UNIVALI.



Professor Doutor Paulo Márcio da Cruz
Coordenador/PPCJ

OSVALDO AGRIPINO DE CASTRO JUNIOR

Assinado de forma digital por OSVALDO AGRIPINO DE CASTRO JUNIOR
DN: c=BR, o=ICP-Brasil, ou=Autenticado por AR CERTISIGN OAB, ou=Assinatura Tipo A3, ou=0003125812, ou=ADVOGADO, cn=OSVALDO AGRIPINO DE CASTRO JUNIOR, email=agripino@univali.br
Dados: 2020.06.01 22:28:46 -03'00'

Doutor Osvaldo Agripino de Castro Junior (UNIVALI) – Orientador

Apresentada perante a Banca Examinadora composta pelos Professores

OSVALDO AGRIPINO DE CASTRO JUNIOR

Assinado de forma digital por OSVALDO AGRIPINO DE CASTRO JUNIOR
DN: c=BR, o=ICP-Brasil, ou=Autenticado por AR CERTISIGN OAB, ou=Assinatura Tipo A3, ou=0003125812, ou=ADVOGADO, cn=OSVALDO AGRIPINO DE CASTRO JUNIOR, email=agripino@univali.br
Dados: 2020.06.01 22:31:08 -03'00'

Doutor Osvaldo Agripino de Castro Junior (UNIVALI) – Presidente

Doutor Frederico Eduardo Zenedin Glitz (UNICURITIBAI) - Membro

ROBERTO EPIFANIO TOMAZ

Assinado de forma digital por ROBERTO EPIFANIO TOMAZ
Dados: 2020.06.03 13:41:26 -03'00'

Doutor Roberto Epifânio Tomaz (UNIVALI) - Membro

Itajaí(SC), 02 de abril de 2020

Este documento foi assinado digitalmente por Frederico Eduardo Zenedin Glitz.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 916D-2448-6ABF-1D78.

Este documento foi assinado digitalmente por Frederico Eduardo Zenedin Glitz.
Para verificar as assinaturas vá ao site https://oab.portaldeassinaturas.com.br:443 e utilize o código 916D-2448-6ABF-1D78.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal OAB. Para verificar as assinaturas clique no link: https://oab.portaldeassinaturas.com.br/Verificar/916D-2448-6ABF-1D78 ou vá até o site https://oab.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 916D-2448-6ABF-1D78

Hash do Documento

B0B49B065831516CBEB807CBEA36377B4E050817C869B39E7CCC20F3C44D6D7E

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 03/06/2020 é(são) :

☑ Frederico Eduardo Zenedin Glitz - 023.633.589-88 em 03/06/2020 14:16 UTC-03:00
Tipo: Certificado Digital

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, 20 de janeiro de 2021.

Matheus Adriano Paulo
Mestrando

ROL DE ABREVIATURAS E SIGLAS

ANSA	Agência Nacional de Segurança Americana
CC/2002	Código Civil de 2002
CDC	Código de Defesa do Consumidor
CRFB	Constituição da República Federativa do Brasil de 1988
CEPD	Comitê Europeu para a Proteção de Dados
DPOs	*Data Protection Officer*
FIPPs	*Fair Information Practice Principles*
GDPR	*General Data Protection Regulation*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IMBD	*Internet Movies Databases*
IP	*Internet Protocol* (protocolo de internet)
LGPD	Lei Geral de Proteção de Dados
NSA	*National Security Agency* (Agência Nacional de Segurança)
PL	Projeto de Lei
RGPD	Regulamento Geral de Proteção de Dados

LISTA DE TABELAS E QUADROS

Quadro 1 – Quadro comparativo LGPD/RGPD 105
Tabela 1 – Dados Anonimizados 121

ROL DE CATEGORIAS –

Agentes de tratamento: o controlador e o operador.[1]

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo[2]. Segundo Bioni, são os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.[3]

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional[4].

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.[5]

***Big Data*:** Segundo Larissa Kakizaki de Alcantara[6], *Big Data*, em tradução literal, significa “grandes dados” e, um de seus grandes desafios, é interpretar esses dados corretamente. Tudo o que nós fazemos deixa um “traço digital” ou “dados”, na qual existe a possibilidade de utilizar e analisar.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade

---

[1] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[2] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[3] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais. Comentários à Lei n. 13.709/2018 LGPD.** Saraiva Educação. Edição do Kindle, 2018. Posição 291.
[4] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[5] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[6] ALCANTARA, Larissa Kakizaki de. **Big Data e IoT**: Desafios da Privacidade e da Proteção de Dados no Direito Digital. Edição do Kindle, posição 168.

determinada.[7]

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.[8]

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.[9]

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) [10]. De acordo com pesquisa feita pelo "*International Association of Privacy Professionals*", que trata do *Regulamento Geral de Proteção de Dados* (RGPD) Europeu, será preciso mais de 28 mil encarregados pelo tratamento de dados para receber todas as reclamações.[11]

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador[12]. Eles devem manter os registros das operações dos dados tratados e o órgão competente determinará a forma da guarda deste registro. Como explicado no art. 5°, IX da Lei Geral de Proteção de Dados (Lei n° 13.709/2018), o operador está subordinado ao responsável, em que o primeiro só realizará o tratamento determinado pelo segundo.[13]

---

[7] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[8] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[9] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[10] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[11] HEIMES, Rita; PFEIFLE, Sam. Study: **at least 28.000 DPOs needed to meet GDPR requirements**. Disponível em: <https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/#>. Acesso em: 16 jan. 2020.
[12] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[13] SOUZA. Luiza Ribeiro de Menezes. proteção de dados pessoais: estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro N. 5.276/2016. **IDP**. Escola de Direito de Brasília. Disponível em < https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153/1484>. Acesso em: 16 jan.

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.[14]

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.[15]

Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[16]

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.[17]

Transnacionalidade: "[...] os novos espaços públicos não vinculados a um território específico, que perpassam a ideia tradicional de Nação Jurídica, aceitam a pluralidade como premissa e possibilitam o exercício de poder a partir de uma pauta axiológica de comum consensual destinada a viabilizar a proposição de um novo pacto de civilização [...]".[18]

2020, p. 31.

[14] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[15] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[16] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[17]BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[18] CRUZ, Paulo Márcio; BODNAR, Zenildo. A transnacionalidade e a emergência do Estado e do

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.[19]

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.[20]

Cooperação Jurídica Internacional: A cooperação jurídica internacional pode ser entendida como um modo formal de solicitar a outro país alguma medida judicial, investigativa ou administrativa necessária para um caso concreto em andamento. A efetividade da justiça, dentro de um cenário de intensificação das relações entre as nações e seus povos, seja no âmbito comercial, migratório ou informacional, demanda cada vez mais um Estado proativo e colaborativo. As relações jurídicas não se processam mais unicamente dentro de um só Estado Soberano, pelo contrário, é necessário cooperar e pedir a cooperação de outros Estados para que se satisfaçam as pretensões por justiça do indivíduo e da sociedade.[21]

Cooperação Transnacional: Segundo o Conselho da Europa, em seu Glossário de Desenvolvimento Territorial publicado em 2011, a cooperação transnacional é um tipo mais recente de cooperação territorial, que cruza as fronteiras nacionais abrangendo vastas áreas de diversos países[22]. A cooperação transnacional é

Direito transnacionais. **Revista eletrônica do CEJUR**, v. 1, n. 4, 2009. disponível em <https://revistas.ufpr.br/cejur/article/download/15054/11488>. Acesso em: 20 out. 2019.

[19] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[20] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[21] Justiça e Segurança Pública – Governo Federal. Disponível em <https://www.justica.gov.br/sua-protecao/cooperacao-internacional>. Acesso em: 27 abr. 2020.

[22] CONSELHO DA EUROPA – **Glossário do Desenvolvimento Territorial. Conferência Europeia dos Ministros Responsáveis pelo Ordenamento do Território do Conselho da Europa (CEMAT).** Lisboa: DGOTDU, 2011, página 21. Disponível em <https://rm.coe.int/16806f7d5d>. Acesso em 27 abr. 2020.

particularmente relevante para determinadas questões estratégicas, como as redes de áreas metropolitanas, a promoção da economia marítima das regiões costeiras, a melhoria geral das acessibilidades, as medidas de grande escala relacionadas com a valorização do património cultural e natural, etc.

SUMÁRIO

RESUMO **16**

ABSTRACT **17**

INTRODUÇÃO **18**

CAPÍTULO 1: TEORIA GERAL DA PROTEÇÃO DE DADOS **21**

1.1. Histórico 21

1.1.1. No Mundo 25

1.1.2. Na União Europeia 29

1.1.3. No Brasil 34

1.2. Conceitos Relevantes 41

1.2.1. *Cookies* 41

1.2.2. *Big Data* 41

1.2.3. Dado Pessoal 42

1.2.4. Dado Pessoal Sensível 43

1.2.5. Dado Anonimizado 44

1.2.6. Controlador 44

1.2.7. Operador 45

1.2.8. Encarregado 46

1.2.9. Agente de tratamento 46

1.2.10. Tratamento 46

1.2.11. Anonimização 47

1.2.12. Consentimento 47

1.2.13. Transferência Internacional de Dados 48

1.2.14. Uso compartilhado de dados 48

1.2.15. Transnacionalidade 49

1.3. Elementos Determinantes 50

1.4. Cooperação internacional 51
1.5. Sanções administrativas 54
1.6. Controle judicial do ato administrativo 59
1.7. Método comparativo sincrônico 61
1.8. Método comparativo diacrônico 62
CAPÍTULO 2: ELEMENTOS DETERMINANTES DOS MODELOS DE PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA E NO BRASIL 64
2.1. União Europeia 64
2.1.1. Cooperação internacional 66
2.1.2. Sanções administrativas 71
2.1.3. Controle judicial 76
2.1.3.1. *Deutsche Bahn* 78
2.1.3.2. *Maximilian Schrems Vs Data Protection Commissioner* 79
2.1.3.3. *Sony Playstation Network* Vs Comissão Nacional de Informações e Liberdade (CNIL) 81
2.1.3.4. *Google* Vs Comissão Nacional de Informações e Liberdade (CNIL) da França 82
2.2. Brasil 84
2.2.1. Cooperação internacional 85
2.2.2. Sanções administrativas 87
2.2.3. Controle judicial 92
2.1.3.1. Sistema de *scoring* 95
2.1.3.2. Recurso em Mandado de Segurança nº 55.019/DF39 96
2.1.3.3. Recurso Especial nº 1.660.168/RJ 97
2.1.3.4. Recurso Especial nº 1.348.532/SP 100
2.1.3.5. *Cambridge Analytica* 102

CAPÍTULO 3: ANÁLISE COMPARATIVA DOS ELEMENTOS DETERMINANTES DA PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA E NO BRASIL 104

3.1. Cooperação internacional 108

3.2. Sanções administrativas 115

3.3. Controle judicial 123

CONSIDERAÇÕES FINAIS 138

REFERÊNCIAS BIBLIOGRÁFICAS 142

RESUMO

O objetivo desta pesquisa é contribuir para o aperfeiçoamento do modelo brasileiro de proteção de dados, tendo em vista a edição da Lei Geral de Proteção de Dados, que criou a Agência Nacional de Proteção de Dados, e se insere na área de concentração Fundamentos do Direito Positivo e da Linha de Pesquisa Direito e Jurisdição. O problema é a insegurança jurídica em relação ao marco regulatório específico da proteção de dados como a LGPD, assim como de jurisprudência consolidada que possa dar maior efetividade à nova legislação. A escolha do modelo europeu decorre da experiência de mais de vinte anos de aplicação de normas sobre a matéria e do sistema romano-germânico. A hipótese da pesquisa é que a análise comparativa dos três elementos determinantes adiante mencionados contribuirá para o aperfeiçoamento do modelo brasileiro de proteção de dados. A pesquisa ocorrerá por meio da análise comparativa dos elementos determinantes dos modelos europeu e brasileiro, quais sejam cooperação internacional, sanções administrativas e controle judicial dos atos administrativos relacionados à proteção de dados, o que será feito em três capítulos. Para tanto, no Capítulo 1 a pesquisa discorre sobre uma Teoria Geral da Proteção de Dados, suas categorias relevantes, com ênfase na cooperação internacional, nas sanções administrativas e controle judicial dos atos administrativos dos referidos sistemas. O Capítulo 2 apresenta e aprofunda os elementos determinantes acima nos modelos europeu e brasileiro de proteção de dados. O Capítulo 3 efetua a análise comparativa dos referidos elementos determinantes, através de análise de casos judiciais e administrativos em cada modelo. A hipótese da pesquisa foi confirmada e a pesquisa termina com considerações finais e sugestões para a melhoria do modelo brasileiro. O Método a ser utilizado na fase de Investigação será o indutivo e comparativo-sincrônico.

Palavras-chave: Lei Geral de Proteção de Dados; Privacidade; Direito Comparado; União Europeia e Brasil.

ABSTRACT

The aim of this research is to contribute to improving the Brazilian data protection model, in light of the publication of the General Data Protection Law, which created the National Data Protection Agency. It falls under the area of concentration Fundamentals of the Constitution, and the line of research Law and Jurisdiction. The problem is the legal uncertainty that surrounds the specific regulatory framework for data protection such as the Data Protection Law, as well the consolidated jurisprudence that can make the new legislation more effective. The choice of the European model arose out of more than twenty years of experience applying standards on the subject, and from the Roman-Germanic system. The research hypothesis is that a comparative analysis of the three determining elements mentioned below will contribute to improving the Brazilian data protection model. The research involved a comparative analysis of the determining elements of the European and Brazilian models: international cooperation, administrative sanctions, and judicial control of administrative acts related to data protection. The work is arranged in three chapters. Chapter 1 discusses a General Theory of Data Protection and its relevant categories, with emphasis on international cooperation, administrative sanctions and judicial control of the administrative acts of these systems. Chapter 2 delves more deeply into the abovementioned determining elements in the European and Brazilian data protection models. Chapter 3 gives a comparative analysis of these elements, analyzing some judicial and administrative cases in each model. At the end, the research hypothesis is confirmed and some final considerations are given, with suggestions for improving the Brazilian model. The inductive and comparative-synchronous method is used in the Investigation phase.

Keywords: General Data Protection Law; Privacy; Comparative law; European Union and Brazil.

INTRODUÇÃO

A presente dissertação, que é produção da área de concentração Fundamentos do Direito Positivo, e da linha de pesquisa Direito e Jurisdição do Programa de Mestrado e Doutorado em Ciência Jurídica da Universidade do Vale do Itajaí, tem como objetivo geral contribuir para o aperfeiçoamento do modelo brasileiro de proteção de dados, por meio da análise comparativa da cooperação internacional, das sanções administrativas e do controle judicial dos atos administrativos dos modelos de proteção de dados da União Europeia e do Brasil.

No Capítulo 1 buscou-se discorrer sobre uma Teoria Geral da Proteção de Dados, apresentando os conceitos e categorias relevantes, seguido da apresentação do conceito do que são os elementos determinantes e quais são os elementos estudados nesta pesquisa, quais sejam, Cooperação Internacional, Sanções Administrativas e Controle Judicial dos atos administrativos envolvendo a matéria nos modelos de Proteção de Dados da União Europeia e do Brasil, estudando-se o histórico de cada um dos regulamentos analisados, trazendo exemplos de outros países à título de exemplificação, como os modelos da Austrália e do Canadá.

Além disso, buscou-se esmiuçar a legislação brasileira e Europeia, objetivando entender o contexto histórico de ambas as regiões para, assim, entender a necessidade de uma Lei Geral de Proteção de Dados, apresentando dados acerca da construção histórica da União Europeia e como a legislação daquela região pode contribuir para a aperfeiçoamento do modelo brasileiro, que conforme será visto, não possui um histórico tão aprofundado quanto o da União Europeia.

Ainda no Capítulo 1, buscou-se apresentar alguns conceitos operacionais para a correta compreensão da pesquisa, conceitos estes apresentados pela Lei Geral de Proteção de Dados da União Europeia e do Brasil tais como o conceito de “Dados Pessoais” e “Cooperação Internacional”, podendo compreender melhor a pesquisa a partir da sua correta interpretação.

Por fim, apresentou-se também no Capitulo 1, além das novidades instituídas pela LGPD descritas acima, a criação de uma Agência Reguladora, denominada Autoridade Nacional de Proteção de Dados (ANPD), que possui diversas atribuições, dentre elas promover ações de cooperação com autoridades de

proteção de dados pessoais de outros países, buscando através da cooperação trazer maior segurança jurídica para os titulares de dados. Da mesma forma, a União Europeia também possui um órgão regulador, denominado de Comitê Europeu de Proteção de Dados, e como será visto, além do Comitê Europeu, os países-membros da União Europeia possuem forte autonomia através de suas entidades supervisoras locais.

No Capítulo 2 tratou-se de apresentar os elementos determinantes da cooperação internacional, da aplicação das sanções administrativas e do controle judicial dos atos administrativos nos modelos europeu e brasileiro de proteção de dados.

Com isso, objetivou-se estudar os elementos determinantes destacados acima para apurar como já funciona o então vigente Regulamento Geral de Proteção de Dados da União Europeia, através do Comitê Europeu de Proteção de Dados.

Como será visto, a União Europeia já possuía legislação acerca de proteção de dados ao menos desde 1995, com a Diretiva nº 46. Além disso, antes mesmo da União Europeia, os países-membros daquela região já tinham forte histórico de leis sobre proteção de dados pessoais.

Já no Brasil, objetivou-se estudar os elementos determinantes destacados na Lei Geral de Proteção de Dados e como vem sendo discutido este assunto sem a vigência de uma Lei Geral de Proteção de Dados, podendo-se perceber que a ausência de uma Lei de Proteção de Dados fez grande falta na construção de precedentes dos Tribunais Superiores acerca desta matéria.

O Capítulo 3 dedica-se a efetuar a análise comparativa dos elementos determinantes da cooperação internacional, da aplicação das sanções administrativas nos modelos europeu e brasileiro de proteção de dados e do controle judicial do ato administrativo, estudando as decisões judiciais em cada país para auferir a aplicabilidade nas esferas administrativa e judicial da Lei Geral de Proteção de Dados europeia e brasileira.

Ao final, buscou-se, com a análise comparativa dos elementos determinantes da cooperação internacional e das sanções administrativas dos modelos europeu e brasileiro de proteção de dados contribuir para o aperfeiçoamento do modelo brasileiro, tendo em vista que o modelo europeu já está

em vigência.

Assim, buscou-se apresentar os principais aspectos do seu funcionamento, visando contribuir para maior celeridade na resolução dos problemas que surgirão no modelo brasileiro.

A presente Dissertação se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões sobre Proteção de Dados.

O Método utilizado na fase de Investigação será o indutivo e comparativo-sincrônico.

Nesta Dissertação as categorias principais estão grafadas com a letra inicial em maiúscula e os seus conceitos operacionais são apresentados em glossário inicial.[23]

[23] Sobre Categorias e Conceitos Operacionais vide: PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica:** Teoria e Prática. 14.ed.rev.atual. e amp. Florianópolis: EMais, 2018. p.31-60.

CAPÍTULO 1 – TEORIA GERAL DA PROTEÇÃO DE DADOS

1.1. Histórico

Iniciando a pesquisa acerca do tema “Proteção de Dados”, denota-se que o mesmo é relativamente novo, mas está diretamente vinculado à uma ideia já antiga, que é a de “Privacidade”. Afinal, só há interesse na proteção de dados pessoais e sigilosos se houver interesse na manutenção da privacidade, na vida privada e na inviolabilidade da intimidade.

Para compreender a necessidade da Proteção de Dados no Brasil, é fundamental entender como a privacidade tornou-se um direito fundamental, sujeito à proteção pelo estado jurisdicional, e como se tornou ainda mais importante com o avanço das tecnologias[24].

Ressalta-se que a Constituição da República Federativa do Brasil de 1988 (CRFB/88) dispõe no art. 5º XII[25] acerca da inviolabilidade de dados e das comunicações telefônicas, dentre outros:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Através de uma análise histórica, Rafael Fernandes Maciel ajuda a confirmar o fato de ser a privacidade um valor desejado, ainda que alguns tenham sustentado que em troca dos benefícios proporcionados pela imensidão de serviços gratuitos na *internet*, as pessoas renunciariam, ou não se importariam, com a violação a esse direito[26].

Todavia, evidentemente que a preocupação com a privacidade é visível, inclusive a proteção da privacidade foi instituída no artigo 3º da Lei nº 12.965/2014 (Marco Civil da Internet)[27].

---

[24] MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019. Edição do Kindle. Posição 134.

[25] BRASIL. **Constituição da República Federativa do Brasil de 1988.** Art. 5ª, XII. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 27 abr. 2020.

[26] MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019. Edição do Kindle. Posição 134.

[27] BRASIL. **Marco Civil da Internet. Lei 12.965/2014.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 27 abr. 2020.

Pois bem, inicia-se falando da privacidade em 1824, onde a Constituição do Império reconhecia um certo direito à privacidade, ao proteger o “segredo da carta” e a “inviolabilidade da casa”. No entanto, naquele momento, a privacidade estava submetida a um conceito mais lastreado na propriedade, ou seja, a Carta Magna protegia o meio físico e não o conteúdo em si. Por isso, vê-se apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio. Perceba-se que não há uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo, o que se protegia ali era a invasão, o ato de romper barreiras físicas.[28]

Mas em 1890, dois advogados norte-americanos, Samuel Warren e Louis Brandeis, escreveram o artigo *The Right to Privacy* publicado na *Harvard Law Review*[29].

Esse artigo é considerado por muitos como o que mais influenciou o direito à privacidade. O interesse em divulgar fatos da vida privada de forma sensacionalista e fofocas cada vez mais sendo estampadas nos jornais, somados ao avanço tecnológico com o uso de câmeras fotográficas portáteis, motivou os advogados a criarem a necessidade de se pensar em um direito à privacidade mais amplo e não apenas sobre meios físicos, como o sigilo da carta ou a violação de domicílio[30].

Era preciso, segundo os autores, que a lei assegurasse aos indivíduos em qual extensão desejassem comunicar seus pensamentos, sentimentos e emoções para outros. Esses direitos não eram baseados em propriedade, mas em um “*direito geral de o indivíduo ser deixado só*” e sua violação configuraria um delito ao direito da personalidade, sujeito a medidas judiciais apropriadas.[31]

Em 1948, com a Declaração Universal dos Direitos Humanos[32], foi possível reconhecer o direito da inviolabilidade à vida privada como um direito

---

[28] MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais**: Atualizado com a Medida Provisória nº 869/18. RM Digital Education. Edição do Kindle. Posição 145.

[29] WARREN, Samuel D. Brandeis, Louis D. **The Right to Privacy.** Disponível em:<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 12 dez. 2019.

[30] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais**: Atualizado com a Medida Provisória nº 869/18 . RM Digital Education. Edição do Kindle. Posição 154.

[31] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais**: Atualizado com a Medida Provisória nº 869/18 . RM Digital Education. Edição do Kindle. Posição 164.

[32] United Nations Human Rights – Office of the High Commissioner. Disponível em <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>. Acesso em: 12 jan. 2020.

fundamental do homem. O artigo 12 da referida declaração estatuiu:

> Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques

Já em 1970, no Estado alemão de Hesse, surge a primeira lei mundial de proteção aos dados pessoais, em uma década em que começam a surgir inúmeras legislações de proteção, com o reconhecimento de que os "*dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte*"[33].

Em 1981, o Conselho da Europa aprovou o *Data Protection Convention - Treaty 108* (Convenção de Proteção de Dados – Tratado 108)[34], tornando-se o primeiro instrumento legal internacional que visava proteger o indivíduo contra abusos na coleta e no processamento de dados pessoais, regulando o fluxo transfronteiriço.

Ainda mais relevante, em 1983, na Alemanha, a Corte Constitucional reconheceu o direito à autodeterminação informacional, declarando inconstitucional a "*Lei do Censo*"[35] no tocante à obrigatoriedade de os cidadãos fornecerem os dados, sob pena de multa, permitindo ainda que os mesmos fossem compartilhados entre órgãos públicos federais[36].

No Brasil, em 1990, o Código de Defesa do Consumidor (Lei nº 8.078/90),

---

[33] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais**: Atualizado com a Medida Provisória nº 869/18 . RM Digital Education. Edição do Kindle. Posição 164.

[34] Tratado nº 108 da Convenção de Proteção de Dados da Europa. Disponível em <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 09 abr. 2020.

[35] Por meio da Lei do Censo (Volkszählungsgesetz) de 1983, promulgada em 25 de março de 1982 (BGBl. I, p. 369), ordenou-se o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho, para fins estatísticos. O objetivo declarado da lei era reunir, por meio de levantamentos feitos por pesquisadores credenciados, dados sobre o estágio do crescimento populacional, a distribuição espacial da população no território federal, sua composição segundo características demográficas e sociais, assim como também sobre sua atividade econômica. Tais dados sempre foram considerados indispensáveis para quaisquer decisões político-econômicas da União, Estados e municípios Disponível em <https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877>. Acesso em: 11 dez. 2019.

[36] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:** Atualizado com a Medida Provisória nº 869/18. RM Digital Education. Edição do Kindle. Posição 174.

regulou o uso de banco de dados de consumidores[37] em seu artigo 43. O artigo previu o direito de o consumidor ter acesso a "*informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele*", permitindo a correção em caso de inexatidão. Ademais, embora o CDC não tenha previsto o consentimento para coletar tais dados, exigiu que o consumidor seja informado sobre a abertura do cadastro.

Em 1996, a Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/96)[38] reconheceu o direito à privacidade, ao restringir o uso de tal método investigativo a determinadas hipóteses e sempre sob o amparo de uma ordem judicial[39]. Em 1997, a Lei do *Habeas Data* (Lei nº 9.507/97)[40] foi promulgada, regulando o direito constitucional e o rito de acesso e correção de informações pessoais.

Maciel ainda destaca que, em meados da década de 90, na Europa, mais precisamente em 1995, foi aprovada a Diretiva nº 46 da União Europeia. Um diploma amplo visando a proteção de dados pessoais e que foi um dos mais propalados ao redor do mundo até a aprovação do GDPR (*General Data Protection Regulation*)[41] que será melhor abordado em tópico oportuno. A diretiva, embora não tivesse força legal perante os países membros, serviu de baliza para legislações nacionais, bem como teve seus princípios mais relevantes mantidos no GDPR[42].

Importante mencionar a lição de Danilo Doneda, no livro *Da privacidade à proteção de dados pessoais*[43], o qual destaca que uma crescente preocupação em

---

[37] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. BRASIL. **Lei nº 8.078/1990 – Código De Defesa do Consumidor.** Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 12 dez. 2019.

[38] BRASIL. **Lei 9.296/1996**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 12 dez 2019.

[39] Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. BRASIL. **Lei 9.296/1996.** Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 12 dez 2019.

[40] BRASIL. **Lei 9507/1997 – Habeas Data.** Disponível em <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 12 dez. 2019.

[41] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).–** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[42] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais**: Atualizado com a Medida Provisória nº 869/18. RM Digital Education. Edição do Kindle. Posição 202.

[43] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Ed. Renovar. 2006, p. 91.

relação à tutela da privacidade é própria de nosso tempo:

> A ideia de privacidade em si não é recente – com os diversos sentidos que apresenta, pode ser identificada em outras épocas e em outras sociedades. Porém, com suas características atuais, ela começou a se fazer notar pelo ordenamento jurídico somente no final do século XIX e assumiu suas feições atuais apenas nas últimas décadas.

O autor ainda menciona que, mesmo com a privacidade hoje consagrada como um direito fundamental, traços do contexto individualista do qual é originária ainda se fazem notar. E não teria nem como ser diferente, até pelo seu grande potencial de ressaltar as individualidades na vida em relação, sendo prudente destacar o fato de que se trata de um direito surgido como "tipicamente burguês" na chamada "idade de ouro da privacidade" – a segunda metade do século XIX, não por acaso no apogeu do liberalismo jurídico clássico[44].

A relevância histórica sobre a privacidade, no qual se percebe a inserção de um direito à privacidade em ordenamentos de cunho eminentemente patrimonialista e que fizeram dela uma prerrogativa reservada a extratos sociais bem determinados. A bem da verdade, o substrato individualista em torno da proteção da privacidade foi por demais forte durante muito tempo. Casos clássicos em relação à privacidade aconteceram na Inglaterra, França e Itália, conforme menciona Doneda:

> Aproveitando-nos do distanciamento temporal, podemos observar a crônica judiciária do passado referente à privacidade para deparar-nos com algo semelhante a um elenco de celebridades de cada época: na Inglaterra, o caso que é mencionado como o exórdio da matéria nos tribunais envolve os literatos Alexander Pope e Jonathan Swift e outro ainda o próprio casal real, Príncipe Albert e Rainha Vitória; na França, o primeiro caso que envolveu a *vie privée* foi o *affaire* Rachel, envolvendo a então famosa atriz francesa Elisa Rachel Félix; na Itália, dentre os primeiros julgados que envolviam (propriamente ou não) a privacidade, encontramos envolvidos nomes como o do tenor Enrico Caruso ou então do ditador Benito Mussolini e sua amante Clara Petacci[45].

---

[44] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro. Ed. Renovar. 2006, p. 91.

[45] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro. Ed. Renovar.

Assim, é latente a necessidade de privacidade e a proteção desta como direito fundamental, e consequentemente, como a proteção de dados está diretamente vinculada à ideia de privacidade, tanto no Brasil quanto no mundo, pode-se afirmar que a proteção de dados é também direito fundamental, conforme será verificado nos tópicos subsequentes.

1.1.1. No mundo

Em muitos países já se pensa em privacidade e proteção de dados. Na página “DLA Piper”[46], os autores do estudo apresentam uma pesquisa aprofundada de todas as legislações do mundo inteiro sobre proteção de dados, qualificando cada país em “Limitado, Moderado, Robusto e Pesado” no que se refere à legislação sobre proteção de dados em cada um dos países analisados. Os dados são atualizados até 2019.

Vale ressaltar que essa preocupação no mundo com a proteção da privacidade é consequência do como nossa sociedade vive hoje, como sendo o período chamado de “sociedade da informação”.

Sobre o assunto, Manuel Castells[47] conceitua a ideia de sociedade da informação e sociedade informacional, dispondo que:

> O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolatiscismo, ou seja, no geral uma infraestrutura intelectual. Ao contrário, o termo informacional indica o atributo de uma forma especifica de organização social em que a geração, o processamento e a transmissão da informação tornaram-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. [...] Por exemplo, uma das

---

2006, p. 8.

[46] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

[47] CASTELLS, Manuel. **A Sociedade em Rede.** Tradutor: Roneide Venancio Majer. 17. Ed, 2016, p. 46.

> características principais da sociedade informacional é a lógica de sua estrutura básica em redes, o que explica o uso do conceito de ‘sociedade em redes‘ [...].

Fato é que em relação à proteção de dados, um dos maiores desafios para a aplicação efetiva de uma legislação regulando o tema é o controle sobre o fluxo internacional de dados.

Segundo Maciel[48], a liquidez dos dados permite que sejam transmitidos com uma velocidade enorme para outra jurisdição. O titular, na maioria das vezes, nem fica sabendo onde suas informações foram parar.

O autor destaca, ainda, que é impossível coibir o dinamismo da inovação que, muitas vezes, utiliza facilidades de *data centers* em outros países e se beneficia de acordos comerciais com empresas estrangeiras. Essas, muitas vezes, são responsáveis por aportar capital de investimento, ou mesmo, pela própria razão de que a *internet* não possui fronteiras delineadas, sendo que o dado de uma pessoa natural coletado no Brasil pode estar sendo obtido a partir de uma outra nação[49].

No Brasil, foi promulgada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. Outros regulamentos similares à LGPD no Brasil, são o *General Data Protection Regulation* (GDPR)[50] na União Europeia, que passou a ser obrigatório em 25 de maio de 2018, e aplicável a todos os países da União Europeia (UE) e o *California Consumer Privacy Act of 2018* (CCPA)[51], nos Estados Unidos da América, implementado através de uma iniciativa em âmbito estadual, na Califórnia, onde foi aprovado no dia 28 de junho de 2018.

Nos Estados Unidos, o CCPA não é a única legislação sobre proteção de dados, conforme destaca o escritório americano DLA PIPER:

---

[48] MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018)**. Cidade: Editora RM Digital Education. 1ª Edição. 2019, Edição do Kindle. Posição 1155.

[49] MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).** RM Digital Education. 1ª Edição. 2019, Edição do Kindle. Posição 1163.

[50] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 55-a –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[51]CALIFORNIA. **Consumer Privacy Act of 2018** – Disponível em <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121>. Acesso em: 10 dez. 2019.

> Os EUA também têm centenas de privacidade e segurança de dados entre seus 50 estados e territórios, como requisitos para proteção de dados, descarte de dados, políticas de privacidade, uso apropriado de números do Seguro Social e notificação de violação de dados. Somente a Califórnia possui mais de 25 leis estaduais de privacidade e segurança de dados, incluindo a Lei de Privacidade do Consumidor da Califórnia (CCPA), de promulgação em 2018 (1 de janeiro de 2020). A CCPA aplica vários setores e apresenta definições abrangentes e amplos direitos individuais e impõe requisitos e restrições substanciais à coleta, uso e divulgação de informações pessoais, que são definidas de maneira muito ampla, conforme explicado abaixo.[52]

Segundo o DLA Piper, existem outros países que possuem uma legislação considerada “forte” acerca de proteção de dados pessoais. Uma delas é o Canadá[53].

Nesse país há 28 estatutos federais, provinciais e territoriais de privacidade (excluindo as disposições legais, requisitos de privacidade sob outra legislação, legislação federal *antispam*, roubo de identidade, código criminal etc.), que legislam sobre a proteção de informações pessoais nas áreas privada e pública. Embora cada estatuto varie em escopo, requisitos, recursos e disposições de aplicação, todos estabelecem um regime abrangente para a coleta, uso e divulgação de informações pessoais[54].

Dentre as legislações que envolvem proteção de dados no Canadá, as principais são a *Lei de Proteção de Informações Pessoais e Documentos Eletrônicos* e a *Lei de Proteção de Informações Pessoais e Prevenção de Roubo de Identidade.* Foi também encontrada uma lei que trata da proteção de informações pessoais no

---

[52]Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

[53] Consoante consta na pesquisa do DLA PIPER: “The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification. California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020. The CCPA applies cross-sector and introduces sweeping definitions and broad individual rights, and imposes substantial requirements and restrictions on the collection, use and disclosure of personal information, which is very broadly defined as explained below” - Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

[54] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

setor privado, denominada *Quebec Privacy Act*[55].

A Austrália[56] regula a privacidade e a proteção de dados por meio de uma mistura de leis federais, estaduais e territoriais. A *Lei Federal de Privacidade* de 1988 (Lei de Privacidade) e seus *Princípios de Privacidade da Austrália* (*APPs*) aplicam-se a entidades do setor privado com um faturamento anual de pelo menos US$ 3.000.000,00 (três milhões de dólares) e a todas as agências do Governo da Commonwealth e do Governo do Território da Capital Australiana[57].

De acordo com a Lei de Privacidade da Austrália, o Comissário de Privacidade tem autoridade para conduzir investigações para aplicar a Lei de Privacidade e buscar sanções civis por violações graves e flagrantes ou por violações repetidas dos *APPs* em que uma entidade falhou em implementar esforços corretivos.

A maioria dos estados e territórios da Austrália (exceto Austrália Ocidental e Austrália do Sul) possui sua própria legislação de proteção de dados aplicável a agências governamentais estaduais e às empresas privadas que interagem com agências governamentais estaduais. Essas normas incluem: a *Lei de Privacidade de Informações de 2014* (Território da Capital Australiana), a *Lei da Informação de 2002* (Território do Norte), a *Lei de Privacidade e Proteção de Informações Pessoais de 1998* (Nova Gales do Sul), a *Lei de Privacidade de Informações 2009* (Queensland), a *Lei de Proteção de Informações Pessoais de 2004* (Tasmânia) e a *Lei de Privacidade e Proteção de Dados de 2014* (Victoria)

Assim, denota-se que esses países com uma legislação mais rígida em relação a proteção de dados, começaram a se preocupar com a privacidade já há bastante tempo, e a maioria deles tende a acompanhar esse crescimento pela proteção de dados em todo o mundo.

Pela pesquisa realizada pela DLA Piper, ainda há muitos países não pesquisados ou sem informações suficientes, e outros com uma legislação fraca sobre o assunto. Porém, denota-se que a tendência é pelo fortalecimento da

---

[55] Quebec Privacy Act. Disponível em <http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1>. Acesso em: 02 fev. 2020.

[56] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

legislação em todos os países.

Agora, analisaremos especificamente a União Europeia e em seguida o Brasil.

1.1.2. Na União Europeia

Regras sobre proteção de dados pessoais na União Europeia já existiam desde 1995 e foram substituídas e aprimoradas. A *Diretiva de Proteção de D*ados de 1995 (DPD95)[58] foi substituída em 2016 por um novo regulamento mais amplo de proteção de dados.

O novo regulamento é formalmente chamado de *Regulamento Geral de Proteção de Dados* (RGPD ou em inglês GDPR). O GDPR é o maior e mais importante regulamento de dados pessoais e de proteção de dados dos últimos vinte anos. Segundo Paul Lambert, o GDPR é um dos desenvolvimentos mais importantes para a União Europeia e para o mundo, sobretudo, para os Estados Unidos[59].

Embora exista uma longa história de evolução e preocupações com a proteção de dados, verifica-se o aumento de segurança em face dos *hackers* e da violação de dados e perda de dados.

Em relação à proteção dos dados pessoais de pessoas físicas, este é direito fundamental na União Europeia. O Artigo 8º, nº 1, da Carta da União Europeia[60] e o artigo 16, nº 1[61] do mesmo diploma legal, preveem que todos têm direito à proteção de seus dados pessoais. Os princípios e regras de proteção dos dados pessoais dos indivíduos devem, independentemente da nacionalidade ou

---

[58] UNIÃO EUROPEIA. **Diretiva 95/46/EC do Parlamento Europeu**. Disponível em <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Acesso em: 23 jan. 2020.

[59] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 24.

[60] Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR >. Acesso em: 23 jan. 2020.

[61] É reconhecida a liberdade de empresa, de acordo com o direito da União e as legislações e práticas nacionais. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 23 jan. 2020.

residência do indivíduo, ser respeitados por quem está na União Europeia[62].

Hoje a União Europeia possui o já mencionado RGPD (*Regulamento Geral de Proteção de Dados*)[63] que começou a vigorar a partir de maio de 2018 e que visa a Proteção de dados em toda a União Europeia.

O RGPD nasceu através do Regulamento nº 2016/679 e foi sancionado em 2016. Após um período de transição de dois anos, tornou-se lei diretamente aplicável em todos os Estados-Membros da União Europeia, mais precisamente em 25 de maio de 2018. [64]

O regulamento é diretamente aplicável e tem efeito imediato em todos os Estados-Membros. Existem mais de 50 países abrangidos pela RGPD, todos possuindo autonomia para legislar de maneira distinta em suas próprias leis nacionais de proteção de dados, possibilitando que cada Estado-Membro interprete a RGPD de acordo com a necessidade e situação local[65].

O foco principal de aplicação da GDPR gira em torno de uma entidade ou empresa que deve estar estabelecida na União Europeia. No entanto, o GDPR também tem efeito extraterritorial. Uma empresa que não esteja estabelecida na União Europeia continuará sujeita ao GDPR se processar dados pessoais de titulares de dados que estão na União Europeia.

No seu artigo 1º o GDPR dispõe que é destinado às regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, bem como defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. Por fim, estabelece que a livre circulação de dados pessoais no interior da União não é restringida e nem proibida por motivos relacionados com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais[66].

---

[62] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 247.

[63] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 99 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out 2019.

[64] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

[65] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

[66] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 1 –** Disponível na versão

Robert Walters, Leon Trakman e Bruno Zeller, no livro "*Data Protection Law – A comparative Analysis of Asia-Pacific and European Approaches-Springe*r"[67] destacam que o GDPR respeita todos os direitos fundamentais, particularmente o direito à privacidade, à família, à vida, à casa e às comunicações, à proteção de dados pessoais, às liberdades de pensamento, consciência e religião e às liberdades de expressão e informação.

Além disso, destacam os autores que o GDPR respeita a liberdade de conduzir um negócio, o direito a uma solução eficaz e julgamento justo e diversidade cultural, religiosa e linguística e que a União Europeia manteve o equilíbrio desses direitos, sendo o objetivo geral da União Europeia manter e fortalecer o mercado econômico comum.

Lecionam, ainda, que:

> O GDPR reforça esse ponto dentro do preâmbulo pelo qual afirma que a tecnologia permite que empresas privadas e autoridades públicas façam uso de dados pessoais em uma escala sem precedentes, a fim de prosseguir suas atividades[68]

A Lei Europeia também traz a ideia de proteção de dados denominada por Paul de Hert, Ronald Leenes e Serge Gutwirth de proteção "por projeto", introduzido no regulamento, que obrigam os controladores e processadores de dados a garantir que sejam implementadas medidas e procedimentos técnicos e organizacionais para proteger os dados pessoais[69].

---

português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[67] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019. p. 70.

[68] Tradução direta do autor. Texto original: "The GDPR respects all fundamental rights, particularly the right to private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information.47 Additionally, the GDPR respects the freedom to conduct a business, the right to an effective remedy and a fair trial, and cultural, religious and linguistic diversity. The EU has retained the balance of these rights, with the overall object of the Union to retain and strengthen the common economic market. The GDPR reinforces this point within the preamble whereby at it states that technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities". ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019. p. 70.

[69] GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de. **Reforming European Data Protection Law**. Law, Governance and Technology Series 20. Springer Netherlands, 2015, p. 56.

Ainda, a RGPD não trouxe uma definição propriamente dita a “dados pessoais”, porém, a consideração nº 51[70] destaca a proteção específica aos dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, tendo em vista que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.

Tais dados são conhecidos como “dados sensíveis”. São os dados pessoais que revelem a origem racial ou étnica. Vejamos:

> Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.[71]

Além disso, em um trecho da consideração nº 51, o legislador dispõe que o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais caracterizações denotam a grande preocupação do legislador em conceituar separadamente cada um dos institutos.

Outro ponto fundamental que deve-se destacar é que em determinadas

---

[70] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 51. –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[71] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 51. –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

situações, os dados pessoais não deverão ser objeto de tratamento, tendo em vista o direito dos Estados-Membros de estabelecerem disposições de proteção de dados específicas. Tudo isso a fim de adaptar a aplicação das regras do regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública que está investido o responsável pelo tratamento.

Assim, a Lei Geral de Proteção de Dados da União Europeia parece, em primeira análise, a mais completa legislação sobre proteção de dados, principalmente por que engloba diversos países e permite que os países também legislem suprindo as omissões em face da realidade local que uma Lei em âmbito transnacional pode gerar.

1.1.3. No Brasil

Diferentemente do que acontece com a União Europeia, no Brasil a legislação demorou para se preocupar com a ideia de Proteção de Dados.

Em 2002, o Código Civil Brasileiro trouxe, finalmente, um capítulo sobre os Direitos da Personalidade[72], incluindo a vida privada e fornecendo instrumentos para coibir a violação de tal direito. A relevância dessa inclusão, ainda que tardia, revela a privacidade como um direito subjetivo e não focado no direito à propriedade.[73]

Ainda em 2013, o mundo presenciou os acontecimentos catalisadores da pressa pela renovação das legislações de proteção de dados em vários países, bem como para uma maior consciência sobre a necessidade de proteger as informações pessoais.

Segundo Maciel, a divulgação, por Edward Snowden, então analista da NSA (*National Security Agency*), dos detalhes dos programas utilizados para monitoramento e vigilância global das informações trafegadas pela *web*, por intermédio do *software* PRISM e outros correlatos, chocou o mundo e, não diferente,

---

[72] BRASIL. **Lei 10.406/2002 – Código Civil**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 30 jan. 2020.

[73] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 202.

os brasileiros menos afetos à tecnologia, que descobriram o quão vulnerável é a privacidade em um ambiente digital.[74]

Assim, no início de setembro de 2013, quando foi noticiado que a então Presidente da República, Dilma Rousseff, e os seus principais assessores haviam sido alvos diretos de espionagem da agência norte-americana, uma das ações tomadas pelo governo brasileiro foi a de colocar em tramitação do PL nº. 2126/11 (Marco Civil da Internet)[75] sob regime de urgência, como uma forma de "resposta à espionagem" [76].

Ainda que o texto do Marco Civil[77] não trouxesse qualquer proteção real à espionagem internacional, fato é que os valores nele trazidos, sobretudo relacionados à privacidade e à proteção dos registros de conexão e de acesso a aplicações, iriam ao encontro dos valores afrontados pela prática de vigilância em massa e que motivaram Edward Snowden a arriscar sua própria vida ao dar-lhe publicidade[78].

Segundo Oliver Alexandre Reinis, tratando sobre os dados da última *Pesquisa Nacional por Amostra de Domicílios Contínua* (PNAD C) divulgada pelo IBGE, o Brasil terminou o ano de 2016 com 116 milhões de pessoas conectadas à *internet*, o equivalente a 64,7% da população com idade acima de 10 anos[79].

A solução implementada no GDPR e que inspirou a LGPD para tentar minimizar os riscos dos titulares foi a de criar uma série de regras para que as transferências internacionais possam ser consideradas adequadas. Sem atendimento a tais regras, as transferências são ilegais. Lembrando que é considerada internacional a transferência de dados pessoais, tanto para país estrangeiro ou para organismo internacional do qual o país seja membro[80].

---

[74] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18** . RM Digital Education. Edição do Kindle. Posição 252.
[75] BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.
[76] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18** . RM Digital Education. Edição do Kindle. Posição 263.
[77] BRASIL. **Marco Civil da Internet. Lei 12.965/2014.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 27 abr. 2020.
[78] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18** . RM Digital Education. Edição do Kindle. Posição 263.
[79] REINIS, Oliver Alexandre. **Lei Brasileira de Proteção de Dados**: Lei n. 13.709, de 14 de agosto de 2018**.** Edição do Kindle. Posição 13.
[80] MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)**. RM Digital Education. 1ª Edição. 2019, Posição 1163.

Na LGPD, nove incisos tratam da transferência internacional de dados previstos no artigo 33, dentre eles, destacam-se os quatro primeiros:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos.
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> [...][81]

Além destas previsões, nos incisos seguintes (V, VI, VII, VIII e IX) a legislação também prevê a transferência internacional de dados pessoais quando a autoridade nacional autorizar a transferência, quando a transferência resultar em compromisso assumido em acordo de cooperação internacional, quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do art. 23 da LGPD.

Por fim, a LGPD também autoriza a transferência internacional de dados quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades ou quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º da lei.

---

[81] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

Vale ressaltar que a Proteção de Dados no Brasil já é um tema amplamente debatido pelo Poder Legislativo, o qual continha diversos projetos de lei com o intuito de proteção de dados, porém, que tomou força nos últimos anos em razão de alguns fatores externos, dentre eles, o escândalo de privacidade do *Facebook*[82].

Um dos mais relevantes foi o PL nº 5276/2016, que abordou o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, apresentado em 13 de maio de 2016, mas que foi arquivado em razão do PL nº 4060/2012[83], apresentado em 13 de junho de 2012, que foi transformado posteriormente na Lei Ordinária nº 13.709/2018, que é a Lei Geral de Proteção de Dados.

Ainda, sobre proteção de dados, há o PL nº 6291/2016, que alterou o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de *internet*, apresentado em 11 de outubro de 2016 e que também foi prejudicado em razão da Lei nº 13.709/2018 e do PL nº 330/2013, também prejudicado em razão da Lei Ordinária nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

Hoje, dentre as normas que tratam ou possuem relação com os temas “privacidade” e “proteção de dados”, podem ser citadas a Lei do Cadastro Positivo, Lei nº 12.414, de 2011, que estabelece em seu art. 1º que a lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 (Código de Proteção e Defesa do Consumidor)[84], tratando a legislação acerca da formação e a consulta a banco de dados.

Além disso, há vigente a Lei de Acesso à Informação, Lei nº 12.527, de

---

[82] A empresa Cambridge Analytica utilizou de dados dos usuários para que pudessem fazer uma campanha política mais assertiva em favor do atual presidente dos Estados Unidos Donald Trump. Facebook e Cambridge Analytica trabalharam para Trump após vazamento de dados. **O Globo**. Disponível em <https://oglobo.globo.com/mundo/facebook-cambridge-analytica-trabalharam-para-trump-apos-vazamento-de-dados-1-22510991>. Acesso em: 10 dez. 2019.

[83] BRASIL. **PL 4060/2012**. Disponível em <https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 10 dez. 2019.

[84] BRASIL, **Lei 12.414 de 9 de junho de 2011.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 10 dez. 2019.

2011, que estabelece no artigo 1ª os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal[85].

Por fim, não menos importante, destaca-se também a Lei nº 12.965, de 2014, que é o “Marco Civil da Internet”, dispondo em seu artigo 1ª:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Desde a Constituição da República Federativa do Brasil de 1988, o Brasil se preocupa com os aspectos da personalidade, e, consequentemente, protege, indiretamente, o sigilo de dados, com a proteção, por exemplo da dignidade da pessoa humana no art. 1º, III da CRFB/88[86].

Ainda, a CRFB/88 também traz no art. 5º, X, a inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, todos aspectos relacionados à personalidade da pessoa.

A terminologia “dado” aparece na CRFB/88, sobretudo, no inciso XII do art. 5º, que representa o direito fundamental ao sigilo e faz menção expressa à inviolabilidade de dados:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer

---

[85] BRASIL. **Lei 12.527 de 2011**. Art. 1º. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 dez. 2019.

[86] BRASIL, **Constituição da República Federativa do Brasil de 1988**. Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: I - a soberania; II - a cidadania; III - a dignidade da pessoa humana. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 10 dez. 2019.

> para fins de investigação criminal ou instrução processual penal;

A Constituição da República Federativa do Brasil é de 1988, ou seja, não se tem no conceito operacional de “dados” naquela época a mesma ideia de hoje, que é mais ampla e muito mais evoluída, e é por isso que nos últimos anos observamos uma evolução histórica da legislação nacional e internacional sobre o assunto.

Já em legislações especiais, é possível observar que os artigos 20 e 21 do Código Civil[87] estabelecem a proteção à intimidade e à vida privada, não fazendo referência à proteção de dados:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. (Vide ADIN 4815)
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

No Código de Defesa do Consumidor (CDC), o artigo 43 estabelece que:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. [88]

Ou seja, estabelece o limite do acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre a

---

[87] BRASIL. **Lei 10.406/2002 – Código Civil**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 30 jan. 2020.
[88] BRASIL, **Lei nº 8.078/1990 – Código de Defesa do Consumidor**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 10 dez. 2019.

própria pessoa, tratando-se de direito personalíssimo.

Por último, temos a então recente e ainda não vigente Lei Geral de Proteção de Dados no Brasil (LGPD), Lei nº 13709/2018 mencionada acima, que apresenta diversos aspectos inéditos em relação à proteção de dados no país.

O seu artigo 1º esclarece que a legislação dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Dentre as novidades instituídas, está a criação de uma agência reguladora, denominada Autoridade Nacional de Proteção de Dados (ANPD)[89], que possui diversas atribuições, dentre elas promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional.

De acordo com Patrícia Peck Pinheiro[90], a LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil.

Por fim, Robert Walters, Leon Trakman e Bruno Zeller, destacam que privacidade, para a indústria, não é a mesma coisa que proteção de dados, e trazem outro problema jurídico na sua extensa pesquisa, tema este que será melhor abordado ao longo da pesquisa:

> Privacidade e proteção de dados significam coisas diferentes para a indústria, governos e a comunidade em geral. Ao contrário de outras áreas do direito que possuem conceitos, normas e princípios legais bem estabelecidos, é uma área do direito que atualmente está longe de ser resolvida. Há mais de 40 anos, Zelman Cowan afirmou que um homem sem

[89] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 55-a –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[90] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD**. Saraiva Educação. Edição do Kindle. Posição 321.

> privacidade é um homem sem dignidade. No entanto, a privacidade e a proteção de dados representam um desafio significativo para o governo, a sociedade e a indústria. Esse desafio é ainda mais acentuado do que nunca na nova economia digital, com milhões de pessoas acessando a Internet diariamente e sem saber se a sua privacidade pessoal está sendo violada.[91]

Assim, tendo em vista o objetivo de contribuir para uma Teoria Geral da Proteção de Dados, passamos à análise de alguns conceitos relevantes para a melhor compreensão do tema.

1.2. Conceitos relevantes (União Europeia e Brasil)

1.2.1. Cookies

Cookies são utilizados para capturar os dados do usuário e registrá-los em um servidor da *web.* A análise é muito útil para classificar as atividades das pessoas na *web*. É possível, inclusive, testar a produtividade dos empregados de uma empresa, utilizando tal técnica[92].

Cada vez que acessamos uma página na internet, esta página está monitorando o modo como operamos, preferências etc. Assim, todos esses dados são armazenados para diversos fins, desde simplesmente registrar os dados dos usuários, como também designar as preferências para aquele tipo de usuário.

Assim, é possível saber exatamente o que o usuário se interessa e melhorar a plataforma ou também para o trabalho de propaganda que será realizado posteriormente.

---

[91] Tradução livre do autor. Texto original: “Privacy and data protection mean different things to industry, governments and the general community. Unlike other areas of law that have well settled legal concepts, norms and principles, it is an area of law that currently is far from settled. More than 40 years ago, Zelman Cowan stated that a man without privacy is a man without dignity.1 However, privacy and data protection pose a significant challenge for government, society and industry. This challenge is even more pronounced than ever in the new digital economy, with millions of people accessing the Internet daily, and not knowing whether their personal privacy is being infringed.” ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. Data Protection Law – **A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 04.

[92] SILVEIRA, Sergio Amadeu de. **Tudo sobre todos**. São Paulo. Editora Edições Sesc SP. 2017. Edição do Kindle. Posição 1058.

1.2.2. Big Data

Segundo Larissa Kakizaki de Alcantara[93], *Big Data*, em tradução literal, significa “grandes dados” e, um de seus grandes desafios, é interpretar esses dados corretamente. Tudo o que nós fazemos deixa um “traço digital” ou “dados”, na qual existe a possibilidade de utilizar e analisar.

O avanço tecnológico e o aumento de dados foi algo alarmante e tende a apenas aumentar ao longo dos anos. Ou seja, há uma espécie de avalanche de dados criada diariamente e, com isso, unidades de medida como o *gigabyte* não são mais suficientes para comportar esses dados.

Assim, diante dessa explosão de números e de tudo o que foi exposto, o *Big Data* é representada por cada página acessada, pelo celular, *tablet* ou computador, que envia uma quantidade de informações para quem a requisitou. As coisas mais simples feitas no dia a dia de alguém geram dados. Não se trata apenas de informações produzidas pelas grandes companhias, pois cada usuário tem um perfil e, para melhor complementá-lo, são utilizados suas ligações, mensagens, cartões de crédito e viagens.

Com isso, tais dados ficam armazenados para serem utilizados, seja como forma de publicidade, para saber os gostos e desejos de seus usuários, seja como forma de melhorar produtos, mapear o trânsito, a medicina, ou qualquer outro serviço existente que possa utilizar isso[94].

1.2.3. Dado pessoal

Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do *Internet Protocol* (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados à pessoa natural viva[95].

---

[93] ALCANTARA, Larissa Kakizaki de. **Big Data e IoT**: Desafios da Privacidade e da Proteção de Dados no Direito Digital . Edição do Kindle, posição 168.
[94] ALCANTARA, Larissa Kakizaki de. **Big Data e IoT**: Desafios da Privacidade e da Proteção de Dados no Direito Digital . Edição do Kindle, Posição 149.
[95] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018**

A Lei Geral de Proteção de Dados Pessoais define dado pessoal como sendo qualquer “informação relacionada à pessoa natural identificada ou identificável”. Colhemos dessa definição que um dado pessoal não são apenas os tradicionais nomes, prenomes, endereços e número de cadastro de pessoa física. Dado pessoal é toda informação que pode identificar um indivíduo ainda que não diretamente. Portanto, incluem-se na referida definição, por exemplo, os números de *Internet Protocol – IP*, número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas. Isso em razão da presença do léxico “identificável”, que amplia a definição de dados pessoais.[96]

Outrossim, não é considerado dado pessoal o dado anônimo, considerado como aquele em que o indivíduo “*não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*”. Um dado pessoal pode deixar de ser alvo de proteção, caso seja anonimizado, com a “*utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*”.[97]

Pela RGPD, dados pessoais são a informação relativa a uma pessoa singular identificada ou identificável, conceituando também titular dos dados que é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular[98].

1.2.4. Dado pessoal sensível

LGPD. Saraiva Educação. Edição do Kindle. Posição 281.

[96] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18** . RM Digital Education. Edição do Kindle.Posição 544.

[97] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18** . RM Digital Education. Edição do Kindle. Posição 564.

[98] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 4, Item 1 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural[99].

Dispõe Maciel que tais dados podem gerar riscos significativos para os direitos e liberdades fundamentais a depender do contexto de sua utilização e, por essa razão, são submetidos a um regime especial para tratamento mais rigoroso[100].

Bruno Bioni[101] destaca que dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação.

Destaca ainda que quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos de sua personalidade.

1.2.5. Dado Anonimizado

São os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento[102].

Bruno Ricardo Bioni conceitua dados anônimos como a antítese do conceito de dados pessoais, por ser incapaz de revelar a identidade de uma pessoa e destaca:

> Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto. Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre os dados e seus respectivos titulares, o que é

[99] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD.** Saraiva Educação. Edição do Kindle. Posição 286.
[100] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 594.
[101] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 85.
[102] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD**. Saraiva Educação. Edição do Kindle. Posição 291.

> chamado de anonimização. Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados, variando entre a) supressão; b) generalização; c) randomização e; d) pseudoanonimização. [103]

Assim, a função do dado anonimizado é trazer maior segurança aos dados que estão sendo tratados, evitando a invasão por hackers ou, no caso de invasão, a inutilidade dos dados, tarefa esta que grandes empresas vêm adotando como prática de governança.

1.2.6. Controlador

Já o controlador é sempre a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais[104].

O Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, conceitua o controlador como a pessoa que sozinho ou em conjunto com outros, determina os propósitos e os meios do processamento de dados pessoais[105].

No caso da União Europeia, quando os objetivos e os meios desse tratamento forem determinados pela legislação da União ou do Estado-Membro, o responsável pelo tratamento ou os critérios específicos para a sua nomeação poderão ser previstos pela legislação da União ou do Estado-Membro.

1.2.7. Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador[106]. Nesse passo, Maciel[107]

---

[103] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 71.

[104] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[105] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 4, item 7 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

[106] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

ressalta que:

> A maior parte das obrigações da lei recai, naturalmente, sobre o controlador, uma vez que é ele que possui a relação direta com o titular dos dados. Ao operador recaem obrigações acessórias, as quais devem estar, na maioria, definidas em contrato firmado com o controlador, para que possa atender às necessidades desse de forma rápida e plena, a fim de evitar que o controlador seja punido por tratamento indevido dos dados pessoais.

Tanto o controlador como o operador devem manter registro (art. 37) das operações de tratamento, especialmente quando baseado no legítimo interesse. Recomenda-se o registro em todas as situações, até mesmo para ressalva de responsabilidades.

1.2.8. Encarregado

Pela LGPD, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)[108].

Em síntese do que foi visto até o momento, pode-se concluir que o tratamento dos dados se dará pelos agentes de tratamento, que tratam dados de titulares, e estão indiretamente vinculados também ao encarregado, que ficará responsável pela intermediação das comunicações entre o agente de tratamento denominado “controlador”, o titular dos dados e o órgão regulador.

1.2.9. Agentes de tratamento

Resumidamente, os agentes de tratamento são o controlador e o operador[109], considerados os responsáveis pelo tratamento de dados. Conforme

---

[107] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 1297

[108] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[109] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

mencionado acima, o controlador é sempre a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais e o operador é sempre a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Assim, os agentes de tratamento estão diretamente ligados e são diretamente responsáveis pelos dados dos titulares que estão sendo tratados.

1.2.10. Tratamento

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração[110].

Segundo a RGDP, tratamento é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição[111].

1.2.11. Anonimização

É a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta

---

[110] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[111] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 4, item 2 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

ou indireta, a um indivíduo[112].

Vale ressaltar que a anonimização do dado visa manter a privacidade do titular e/ou evitar a utilização dos dados por terceiros não autorizados. Assim, mantendo-se anonimizada uma parte dos dados, ao menos o que se pretende é dar maior segurança jurídica ao dado que está sendo tratado, evitando-se o furto de dados por *hackers* ou qualquer interessado, seja para fins lícitos ou ilícitos.

1.2.12. Consentimento

Nos termos do Regulamento Geral de Proteção de Dados o consentimento do titular dos dados é representado por qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados pelos quais ele ou ela, por uma declaração ou por uma ação afirmativa clara, que signifiquem concordância com o tratamento de dados pessoais relacionados a ele ou ela[113];

Na Lei Geral de Proteção de Dados Brasileira o conceito aparece de maneira mais resumida, dispondo que o consentimento nada mais é do que a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[114].

Assim, a LGPD é mais específica acerca do conceito de consentimento, trazendo a ideia de considerá-lo como válido somente para uma finalidade determinada. O RGPD, por sua vez, traz de maneira mais ampla, e trata de qualquer concordância inequívoca acerca do tratamento de dados do titular.

1.2.13. Transferência internacional de dados

Considera-se transferência internacional de dados pessoais toda

---

[112] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[113] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 4, item 11 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

[114] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

transferência para país estrangeiro ou organismo internacional do qual o país seja membro[115].

Em outras palavras, a transferência, por exemplo, de dados para órgão regulador eventualmente existente no Mercosul, é considerada uma transferência internacional de dados.

1.2.14. Uso compartilhado de dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados[116].

1.2.15. Transnacionalidade

Segundo Paulo Marcio Cruz e Carla Piffer, transnacionalidade pode ser entendida como os novos espaços públicos não vinculados a um território específico, que perpassam a ideia tradicional de Nação Jurídica, aceitam a pluralidade como premissa e possibilitam o exercício de poder a partir de uma pauta axiológica de comum consensual destinada a viabilizar a proposição de um novo pacto de civilização[117].

Os autores ainda trazem a ideia e a conceituação de transnacionalidade e direito transnacional[118], na definição de direito transnacional, que utiliza as figuras “da era do computador” para explicar sua teoria:

---

[115] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[116] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[117] CRUZ, Paulo Márcio; BODNAR, Zenildo. A transnacionalidade e a emergência do Estado e do Direito transnacionais. **Revista eletrônica do CEJUR**, v. 1, n. 4, 2009. disponível em <https://revistas.ufpr.br/cejur/article/download/15054/11488>. Acesso em: 20 out. 2019.
[118] CRUZ, Paulo Marcio. Piffer, Carla. **O DIREITO TRANSNACIONAL COMO DISCIPLINA EM CURSOS JURÍDICO S 2018** | v. 12 | n. 1 | p. 11-28 | ISSN 2317-2622. Disponível em <http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v12n1p11-28>. Acesso em: 23 jan. 2020.

> Para o autor, o direito transnacional seria: 1. aquele direito “baixado” do direito internacional para o direito doméstico, como algumas normas internacionais de direitos humanos internalizadas por muitos Estados; 2. o direito “carregado e então baixado”, como uma regra originada de uma ordem jurídica interna que posteriormente se torna parte do direito internacional; e 3. o direito que é “horizontalmente transplantado” de um sistema doméstico para o outro, citando como exemplo a doutrina do *unclean hands* ou ficha limpa, cuja origem remonta ao direito britânico e que migrou para vários outros sistemas jurídicos.

E complementam:

> Diante dessas reflexões acerca do direito transnacional, entende-se que os acontecimentos de hoje são transnacionais porque ocorrem de forma recorrente para além das fronteiras nacionais e requerem um compromisso regular e significativo de todos os participantes, pois, à medida que a globalização desenvolve sua dinâmica, cresce a necessidade de os envolvidos se localizarem em novos cenários e encontrarem maneiras de contrabalançar as novas tendências e limitar os novos poderes desterritorializados.

A correta interpretação da ideia de Transnacionalidade é fundamental para a compreensão da Cooperação Internacional, uma vez que a Transnacionalidade é algo que transpassa a ideia do Estado Nacional, bem como pode se afirmar que os Dados Pessoais hoje transpassam a ideia do Estado Nacional, sendo considerado, portanto, Transnacionais.

1.3. Elementos determinantes

O objetivo desta pesquisa é comparar a aplicação da Lei Geral de Proteção de dados no Brasil com a aplicação do Regulamento Geral de Proteção de Dados na União Europeia.

A melhor forma de comparar as legislações é trazendo os elementos determinantes que estão sendo comparados e, dessa forma, apontar como funciona

em cada um dos modelos de proteção de dados.

Nos ensinamentos de Osvaldo Agripino de Castro Junior, no direito comparado, os chamados elementos determinantes têm sua importância mais genérica, central e relevante, pois constituem a estrutura econômica, a ideologia oficial, o princípio da separação ou unidade do poder no Estado, as relações de certeza ou incertezas que ligam o direito aos fatores que eles abordaram, são as instituições jurídicas que influenciam de maneira direta ou indireta toda a ordem jurídica e determinam de forma necessária todas as outras partículas jurídicas elementares, bem como o perfil estrutural da ordem jurídica.[119]

Ainda, o autor destaca que os elementos determinantes constituem-se na matéria prima da comparação, a partir da qual a comparação será feita, de modo que, modificar estes elementos é alterar a estrutura específica da ordem jurídica considerada.

Neste sentido, uma das tarefas principais da análise comparativa é a busca da identificação dos elementos e/ou fatores que são responsáveis ou contribuem para certos desenvolvimentos no sistema judicial.

Os elementos determinantes determinam a estrutura fundamental da ordem jurídica, tendo em vista que modificá-los ou trocá-los significa alterar o perfil da ordem jurídica na qual atuam. O autor destaca:

> Assim, a análise comparativa não tem significado quando em condições de identidade, pois total identidade ou total diferença são, dessa forma, totalmente inúteis neste tipo de método, já que a tarefa do comparativista, através do contraste dos elementos determinantes, é fazer a comparação entre semelhança e diferença, e divergência e convergência, a fim de colaborar para o entendimento e/ou reforma do mencionado elemento do sistema. Trata-se de método extremamente importante num quadro de enorme diversidade cultural, em face da grande quantidade de sistemas jurídicos e, consequentemente, judiciais no mundo, todos operando num período de intensa transnacionalização do direito, o que torna a tarefa do direito comparado mais urgente e relevante do que nunca.[120]

---

[119] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 85.

[120] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e**

Dessa forma, anota-se que os elementos determinantes da presente pesquisa são as sanções administrativas, que serão analisadas em cada uma das legislações, tanto brasileira quanto da União Europeia, objetivando descobrir as similaridades, diferenças, e efetividade, a cooperação internacional, de que modo ambas as legislações garantiram a cooperação internacional, tão fundamental nos dias atuais e, por fim, o controle judicial, pois as decisões têm grande influência na consolidação do marco regulatório.

1.4. Cooperação Internacional

A cooperação entre os países é algo previsto pela Lei Geral de Proteção de Dados no Brasil em diversos momentos. Primeiro, o legislador trata da cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, quando aborda a questão da transferência internacional de dados[121].

Ainda, é permitida a transferência internacional de dados somente quando o país ou o organismo internacional proporciona grau de proteção de dados pessoais adequados ao previsto na Lei Geral de Proteção de Dados Brasileira.

Quando não houver, o controlador oferece garantias de cumprimento de princípios dos direitos do titular e do regime de proteção de dados previsto na Lei na forma de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos.

Também é possível a transferência internacional de dados quando for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, quando for necessária para a proteção da vida ou a incolumidade física do titular ou de terceiros, quando a autoridade nacional autorizar a transferência, quando resultar de um acordo de cooperação internacional, dentre outras

---

Desenvolvimento: Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 86.

[121] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 33º, Inciso I – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

hipóteses.[122]

Ainda, a LGPD também determina que o órgão regulador (ANPD – Agência Nacional de Proteção de Dados) promova ações de cooperação com autoridades de proteção de dados de outros países, de natureza internacional ou transnacional.[123]

Já a GDPR (*General Data Protection Regulation*) da União Europeia, traz em suas considerações iniciais a necessidade da cooperação entre estados-membros:

> A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros.[124]

Em seguida, na Consideração 101 da GDPR, destacou-se que:

> A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para

---

[122] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 33 – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[123] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-J, Inciso IV – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[124] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 11 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out 2019.

> subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante

Em seguida, na legislação propriamente dita, a GRPD estabelece no artigo 50 que a comissão e as autoridades de controle devem tomar medidas para estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais, prestar assistência mútua em nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações. E ainda prestar assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais.

Ademais, devem associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais e, por fim, estabelecem que devem promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros.[125]

1.5. Sanções administrativas

[125] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 50 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

No GDPR, mais especificamente disposto na “Consideração 148”, o legislador menciona que a imposição de sanções é necessária para o fim de reforçar a execução das regras do regulamento, incluindo coimas (multas), por violação do regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controle[126].

Determina, ainda, na “Consideração 149”, que os Estados-Membros poderão definir as normas relativas às sanções penais aplicáveis por violação do regulamento, inclusive por violação das normas nacionais adotadas em conformidade com o regulamento, e dentro dos seus limites.

Essas sanções penais podem inclusive prever a privação dos lucros auferidos em virtude da violação do regulamento. Contudo, a imposição de sanções penais por infração às referidas normas nacionais, bem como de sanções administrativas, não deverá implicar a violação do princípio *bis in idem,* conforme interpretação já consolidada pelo Tribunal de Justiça Europeu[127].

É interessante trazer à tona que o RGPD, em relação às multas, não se aplica na forma que foi proposta pelo legislador na Dinamarca e à Estônia, conforme expressamente disposto na “Consideração 151”:

> Os sistemas jurídicos da Dinamarca e da Estónia não conhecem as coimas tal como são previstas no presente regulamento. As regras relativas às coimas podem ser aplicadas de modo que a coima seja imposta, na Dinamarca, pelos tribunais nacionais competentes como sanção penal e, na Estónia, pela autoridade de controlo no âmbito de um processo por infração menor, na condição de tal aplicação das regras nestes Estados-Membros ter um efeito equivalente às coimas impostas pelas autoridades de controlo. Por esse motivo, os tribunais nacionais competentes deverão ter em conta a recomendação da autoridade de controlo que propõe a coima. Em todo o caso, as coimas impostas deverão ser efetivas, proporcionadas e

[126] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 148 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

[127] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 149 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

> dissuasivas.[128]

Em seguida, o Capítulo XIII trata das vias de recurso, da responsabilidade e das sanções administrativas (artigos 77 a 84 da RGPD). O artigo 83 estabelece que cada autoridade de controle assegura que a aplicação de multas relativamente a violações do regulamento é, em cada caso individual, efetiva, proporcional e dissuasiva.

Sobre a aplicação, destaca o item 2 do artigo 83 que, dependendo das circunstâncias de cada caso, as multas são aplicadas em conformidade com as medidas referidas no artigo 58, nº 2, alíneas “a” a “h” e “j”. Assim, ao decidir sobre a aplicação de uma multa e sobre o montante da multa em cada caso individual, deve-se considerar o seguinte:

> a) A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos;
> b) O caráter intencional ou negligente da infração;
> c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares;
> d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25 e 32;
> e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante;

Ainda, é levado em consideração o grau de cooperação com a autoridade de controle, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos, as categorias específicas de dados pessoais afetadas pela infração, a forma como a autoridade de controle tomou conhecimento da infração e, em especial, se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram.

---

[128] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 151 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

Em outras palavras, percebe-se aqui a grande importância de um programa de integridade dentro de uma empresa, que garanta uma auditoria interna capaz de verificar as infrações e responsabilizar o funcionário antes mesmo que a demanda seja remetida ao órgão regulador.

Também deve-se considerar o cumprimento das medidas a que se refere o artigo 58, nº 2 (Advertências e medidas para o cumprimento da RGPD), caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria.

Deve-se considerar também o cumprimento de códigos de conduta (programas de integridade) aprovados nos termos do artigo 40 da RGPD ou de procedimento de certificação aprovados nos termos do artigo 42 da Legislação Europeia, e, por fim, qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.

Acerca da penalidade financeira, a RGPD estabelece duas situações. A primeira, é pela violação das disposições previstas no artigo 83, item 4, alíneas a, b e c. Estas, estarão sujeitas, em conformidade com o nº 2, a multas de até EUR 10.000.000,00 (dez milhões de euros) ou, no caso de uma empresa, até 2% do seu faturamento correspondente ao exercício financeiro anterior, dependendo do montante que for mais elevado[129].

A segunda está disposta no artigo 83, item 5 da RPGD. A violação das disposições descritas nas alíneas do item 5, em conformidade com o nº 2, estão sujeitas a multas de até EUR 20.000.000,00 (vinte milhões de euros) ou, no caso de uma empresa, até 4 % do seu faturamento correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

Á título de exemplo, as infrações previstas no item 5 são:

> a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5º, 6º, 7º e 9º;
>
> b) Os direitos dos titulares dos dados nos termos dos artigos 12 a 22;

[129] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 83, item 4 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

> c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44 a 49;
> d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX;
> e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58.o, nº 2, ou o facto de não facultar acesso, em violação do artigo 58.o, nº 1.

Além dos casos exemplificados, o RGPD prevê também que nos casos de descumprimento de uma ordem emitida pela autoridade de controle a que se refere o artigo 58, nº 2, está sujeito, em conformidade com o nº 2 do referido artigo, a multas também de até 20.000.000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual em nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado[130], ou seja, mesma penalidade descrita acima, aplicado neste caso em razão do descumprimento de uma simples ordem.

No Brasil, a Lei Geral de Proteção de Dados (Lei 13.709/2018) dispõe no artigo 52 que os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na citada norma, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional[131]:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua

[130] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 83, Item 5 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.
[131] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 52 – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

> regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;

Para aplicação das advertências acima, a Lei Geral de Proteção de Dados prevê no §1º do artigo 52 um prévio procedimento administrativo que possibilite o contraditório e a ampla defesa, de acordo com as peculiaridades do caso concreto e considerando alguns parâmetros. São eles:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Assim, a primeira impressão é que a GRPD tem uma penalidade muito mais severa do que a Lei de Proteção de Dados Brasileira, o que será melhor apurado nos capítulos posteriores.

Vale dizer que a LGPD somente aplicará as penalidades de suspensão parcial do funcionamento do banco de dados e do exercício da atividade após a reincidência ou caso os controladores estejam submetidos a outros órgãos e entidades de competência sancionatória[132].

Por fim, na linha de priorizar a conciliação que o judiciário brasileiro vem tratando os diversos assuntos, o parágrafo sétimo do mesmo artigo destaca que o

---

[132] BRASIL. **Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).** Artigo 52, §6, Incisos I e II – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

vazamento individual de dado ou acesso não autorizado poderá ser objeto de conciliação direta entre o controlador e o titular de dados.

Passamos agora à análise teórica acerca do controle judicial do ato administrativo na Lei Geral de Proteção de Dados e no Regulamento Geral de Proteção de Dados Europeu

1.6. Controle judicial do ato administrativo

A Lei Geral de Proteção de Dados no Brasil trouxe diversas hipóteses de controle judicial.

Em um primeiro momento, permitiu a discussão da matéria em âmbito administrativo. Para tanto, criou a figura da Autoridade Nacional de Proteção de Dados, que é uma agência reguladora que visa zelar pela proteção de dados pessoais, fiscalizar e aplicar sanções em caso de infrações à LGPD, dentre outras atribuições previstas no artigo 55-J.

As agências reguladoras praticam atos administrativos na pessoa dos agentes públicos que foram investidos na função. Por isso, é fundamental que os agentes de proteção de dados observem o ato administrativo lançado, o seu agente, objeto, motivo, forma e finalidade.

A natureza jurídica da Agência Nacional de Proteção de Dados (ANPD) é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. Esta transformação deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD[133].

Os membros do conselho da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, com mandato de 4 (quatro) anos[134].

Assim, a LGPD se preocupou em trazer à agência reguladora uma

---

[133] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-A, §§ 1 e 2 – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[134] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-A, §§ 1 e 2 – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

rotatividade da gestão que evitará esquemas de corrupção, bem como possivelmente trará maior eficácia às decisões, tal como funciona no Conselho Administrativo de Defesa Econômica (CADE)[135], por exemplo.

Destaca-se que o ato administrativo é uma forma de expressar as decisões tomadas por órgãos e autoridades da administração pública e que produz efeitos jurídicos, especialmente em reconhecer, modificar ou extinguir direitos ou, ainda, impor obrigações ou restrições, observada a legalidade. E ainda:

> Deverá ser tomado por agente competente, objeto lícito, formal (e aqui, dando ciência aos cidadãos, a outros órgãos da administração e órgãos de controle), incluindo, ainda, o modo de divulgação, motivação, portanto, as circunstâncias que provocaram aquela decisão e a finalidade que geralmente se traduz no interesse público.[136]

Para compreender melhor a autonomia e legitimidade da ANPD (Agência Nacional de Proteção de Dados) criada pela LGPD, importante trazer o conceito de órgão regulador na visão de Paulo Roberto Ferreira Motta, que dispõe que agência reguladora é "*um ente administrativo dotado de autonomia, sendo que a sua criação deve ser realizada por lei específica, com personalidade jurídica de direito público interno, patrimônio próprio e competências perfeitamente especificadas no texto legal criador daquela*"[137]

Embora o termo agência reguladora possa sugerir associação da função reguladora com desempenho normativo, há de se explicar que o seu bojo é muito mais completo e amplo, pois além do poder de polícia que lhes é conferido, têm em seu espectro de atuação, o poder de agir também na composição de conflitos e aplicação de possíveis sanções. Dentre as suas funções, incluem o controle de tarifas, a universalização dos serviços, a instigação à competitividade, fiscalização de contratos de concessão, dirimir conflitos entre partes envolvidas.[138]

---

[135] BRASIL. **Lei 12.529/2011**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.htm>. Acesso em 13 mai. 2020.
[136] ALMEIDA. Paula Joyce de Carvalho Andrade de. O controle da atuação das Agências Reguladoras Federais Brasileiras. **Dissertação de Mestrado**. Universidade Presbiteriana Mackenzie. São Paulo. 2007, p. 34.
[137] MOTTA, Paulo Roberto Ferreira. **Agências reguladoras**. Barueri: Manole, 2003. p. 101.
[138] ALMEIDA. Paula Joyce de Carvalho Andrade de. O controle da atuação das Agências Reguladoras Federais Brasileiras. **Dissertação de Mestrado**. Universidade Presbiteriana Mackenzie. São Paulo.

Assim, em que pese a liberdade que é conferida ao órgão regulador e a presunção de veracidade do ato administrativo, todo ato administrativo pode ser submetido ao Poder Judiciário para que este exerça seu poder de controle e evite abusividades perpetradas pelo órgão recém-criado.

Assim, caso não seja solucionada ou a solução não seja adequada para alguma das partes, a LGPD possibilitou que a matéria seja discutida judicialmente, possibilitando o exercício da ampla defesa e do contraditório, direitos garantidos pela CRFB/88.

Agora, passamos a entender o método abordado na presente pesquisa.

1.7. Método comparativo sincrônico

O objetivo do método comparativo sincrônico consiste em pesquisar dois ou mais fenômenos, tal como sistemas jurídicos e sistemas judiciais, identificando as semelhanças, através da consideração das diferenças[139].

Os métodos comparativos sincrônico e diacrônico são fundamentais para a melhora de um país através da pesquisa, pois, pode-se obter uma melhor possibilidade de eficiência em determinado assunto nos estudos comparativos.

O método comparativo sincrônico tem como um dos seus objetivos o estudo dos exemplos de causas que explicam as semelhanças ou diferenças dos termos a serem comparados, o que possibilita um melhor conhecimento do direito que está sendo comparado.

Nesse sentido, Osvaldo Agripino de Castro Junior[140] destaca:

> Deste modo, considerar após a comparação, o seu próprio direito numa nova ótica é compreende-lo melhor, justamente por que se pode descobrir novos aspectos, contornos e relevos que até então não eram percebidos. As falhas e fraquezas de certas instituições jurídicas nacionais aparecem mais

---

2007, p. 34.

[139] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 148.

[140] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 148.

> claramente. A comparação permite que o observador olhe o direito nacional com um novo olhar mais maduro, porque mais experimentado, mais crítico, porque mais informado. É um primeiro efeito benéfico dos conhecimentos obtidos pela comparação.

Assim, denota-se a importância dos métodos comparativos, sobretudo o método sincrônico.

1.8. Método comparativo diacrônico

Este método é também conhecido como “método comparativo-histórico”, que visa, resumidamente estudar o passado para se projetar o futuro. Nas palavras do autor acima, a história não se reduz simplesmente ao conhecimento do passado, mas engloba também a observação do presente. Ao direito do passado, deve-se opor o direito do presente. Os dois devem ser compreendidos como estágios de evolução do espírito integrado à evolução da história. Além disso, o direito comparado não é só o prolongamento do presente que se constitui história no passado. É a história que se realiza[141].

Sergio Schneider e Cláudio Job Schmitt[142] tratando do método comparativo destacam que:

> A comparação, enquanto momento da atividade cognitiva, pode ser considerada como inerente ao processo de construção do conhecimento nas ciências sociais. É lançando mão de um tipo de raciocínio comparativo que podemos descobrir regularidades, perceber deslocamentos e transformações, construir modelos e tipologias, identificando continuidades e descontinuidades, semelhanças e diferenças, e explicitando as determinações mais gerais que regem os fenômenos sociais.

Reconhecer a historicidade, cuja dimensão é a História do Direito, é admitir simplesmente que o fenômeno jurídico parcial – como as instituições jurídicas, ou global, como as ordens jurídicas – é condicionado, pois inexiste fenômeno jurídico puro que seja descolado do seu meio socio-histórico. O valor

---

[141] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 143

[142] SCHNEIDER, Sergio; SCHIMITT, Cláudia Job. **O uso do método comparativo nas Ciências Sociais.** Cadernos de Sociologia, Porto Alegre, v. 9,1998 p. 49.

atemporal uma vez que é sujeito de uma ordem que é sempre histórica, que compreende estruturas políticas, sociais e econômicas especificas de determinada época.

Desta forma, o direito deve ser examinado a luz de sua história e nas suas estruturas políticas, econômicas e sociais, sem esquecer a concepção ideológica que, de forma incerta e difusa ou de maneira precisa e clara, orienta suas soluções jurídicas num sentido ou noutro[143]. E complementa:

> O método comparativo-histórico, por sua vez, proporciona a possibilidade de uma avaliação objetiva, embora não absoluta, abstraída das contingências de espaço e tempo, e relacionada a determinado problema particular. Weber, por sua vez, intrigado com as diferenças que via entre o mundo moderno e não moderno, mergulhou na vida da civilização ocidental para compreender os campos da religião, do governo, e da economia, e , embora educado para ser advogado, desenvolveu importantes pesquisas comparativas sobre a história do direito e a sociologia do direito, com o objetivo de desvendar os mistérios das diferentes ordens sociais da sociedade ocidental e, particularmente, da ordem econômica, enfim, de descobrir a racionalidade destes campos. Desde Weber, todavia, poucos acadêmicos tem se empenhado para alcançar o nível de seus estudos nos campos da história, direito, economia e sociologia.

Assim, após a apresentação dos conceitos relevantes para a compreensão do tema, busca-se apresentar os elementos determinantes dos modelos de proteção de dados na União Europeia e no Brasil, através do método sincrônico, o que será feito no Capítulo 2.

---

[143] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 143.

CAPÍTULO 2: ELEMENTOS DETERMINANTES DOS MODELOS DE PROTEÇÃO DE DADOS NA UNIÃO EUROPÉIA E NO BRASIL

Conforme já mencionado no capítulo primeiro, no direito comparado, os chamados elementos determinantes têm sua importância mais genérica, central e relevante, pois constituem a estrutura econômica, a ideologia oficial, o princípio da separação ou unidade do poder no Estado, as relações de certeza ou incertezas que ligam o direito aos fatores que eles abordaram, são as instituições jurídicas que influenciam de maneira direta ou indireta toda a ordem jurídica e determinam de forma necessária todas as outras partículas jurídicas elementares, bem como o perfil estrutural da ordem jurídica[144].

Neste sentido, uma das tarefas principais da análise comparativa é a busca da identificação dos elementos e/ou fatores que são responsáveis ou contribuem para certos desenvolvimentos no sistema judicial.

Conforme visto anteriormente os modelos de proteção de dados no mundo estão em constante evolução, razão pela qual se faz necessário o presente estudo.

Nesta pesquisa objetivou-se pesquisar somente a legislação da União Europeia e do Brasil, objetivando comparar os elementos determinantes, quais sejam: Cooperação Internacional, Sanções Administrativas e Controle Judicial.

Assim, prosseguiremos com a pesquisa acerca da União Europeia, trazendo decisões dos tribunais acerca de Proteção de Dados, e em seguida apresentaremos também os dados em relação ao Brasil.

2.1. União Europeia

A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados necessariamente, mas a

---

[144] CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002, p. 85.

pessoa que é titular desses dados[145].

Destaca Bruno Ricardo Bioni[146], que o direito comunitário Europeu exprime bem a travessia do consentimento no percurso geracional das leis de proteção de dados pessoais, cuja linha evolutiva permanece em curso até hoje, a começar pela influência das *guidelines* (orientações) da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) que promoveu as primeiras normatizações sobre o tema no direito comunitário Europeu.

A Convenção 108[147], por exemplo, da década de 1980, de Strasbourg, do Conselho da Europa, é resultado do movimento promovido pela OCDE para facilitar a harmonização das legislações de proteção de dados pessoais.

Duas décadas depois surge a *Diretiva Europeia de Proteção de Dados Pessoais (*Diretiva 95/46/CE), que assegura aos indivíduos o controle sobre as suas informações pessoais.

A referida diretiva, não impõe somente o direito de o titular dos dados pessoais controlá-los, mas, simetricamente, deveres aos *data controllers* – que é quem processa os dados pessoais – para aperfeiçoar tal estratégia regulatória[148].

Em seguida surge também a *Diretiva Europeia 2002/58*[149], que trata do tratamento de dados e da proteção da privacidade nas comunidades eletrônicas.

Analisando o breve histórico acima apresentado, o que se percebe é que a União Europeia há décadas já entendeu a necessidade de proteger os dados das pessoas e a privacidade.

Outrossim, com a evolução global da transmissão de dados e informações, tornou-se mais do que necessário a evolução da legislação, sobretudo porque tais legislações protegiam os dados, mas era omissa em pontos fundamentais.

---

[145] MENDES, Laura Schertel - **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014, p. 262

[146] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 122.

[147] Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. **CNPD**. Disponível em <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 15 jan. 2020.

[148] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 123.

[149] Relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Disponível em <https://www.anacom.pt/render.jsp?contentId=964154.>. Acesso em: 15 jan. 2020.

Importante frisar que a cooperação internacional é fundamental para a viabilidade de qualquer Lei de Proteção de Dados, justamente por que os dados são transmissíveis facilmente de um país para outro por meio da rede mundial de *internet*.

De outro lado, não basta apenas a cooperação internacional, mas também a implementação de sanções e multas administrativas pelo descumprimento da legislação.

Os dois elementos acima citados, somados à uma legislação mais robusta, traduz-se em uma grande conquista de maior segurança jurídica e institucional dos dados que são diariamente compartilhados com pequenas, médias e grandes corporações, bem como com o Estado, que, vale dizer, também tem responsabilidade por seus dados.

Assim, passa-se a analisar a cooperação internacional, as sanções e multas administrativas previstas na RGPD e LGPD.

2.1.1. Cooperação Internacional

O *Regulamento Geral sobre a Proteção de Dados* (RGPD) da União Europeia aplica-se ao tratamento de dados pessoais, realizado dentro ou fora da União Europeia.

É o que dispõe o artigo 3º da RGPD[150], que determina que o regulamento aplica-se "*ao tratamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou processador na União Europeia, independentemente de o processamento ocorrer dentro ou fora da União Europeia*".

Zeller, Trakman e Walters[151] discorrendo sobre a RGPD da União Europeia destacam que há circunstâncias em que as leis de um país estrangeiro podem diferir significativamente das leis da União Europeia, mas que os dados ainda podem ser transferidos, desde que respeitadas algumas regras impostas pelos órgãos regulamentadores da RGPD Europeia.

---

[150] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 3 -** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12/12/2019.

[151] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 69.

Por exemplo, o controlador de dados, responsável pela informação que será transmitida, através de regras corporativas vinculativas, pode estabelecer um acordo para facilitar a transferência dos dados.

Além disso, quando um acordo for aprovado ou for emitido algum tipo de certificação aprovada pelo órgão regulador e as garantias da lei forem atendidas, o controlador de dados poderá obter autorização para transferir os dados pessoais para fora da União Europeia.

Em resumo, o alcance do RGPD é bastante extenso, e ampliou o alcance trazido pela antiga *Diretiva 95/46/CE*[152] que, a bem da verdade, era a Lei de Proteção de Dados que vigorava antes da aprovação do GDPR.

Em outras palavras, o *Regulamento de Proteção de Dados da União Europeia* poderá ser aplicada mesmo que as operações de mecanismos de busca sejam realizadas por meio de uma filial ou escritório em qualquer Estado-Membro da União Europeia, ainda que a empresa principal tenha origem e esteja sediada fora da União Europeia, conforme já mencionado acima.

Portanto, em termos práticos, o RGPD pode ser interpretado como não apenas uma Lei Regional, mas também Internacional de proteção de dados, o que por si só auxilia na Cooperação Internacional de Proteção de Dados.

Destacam Zeller, Trakman e Walters:

> Por exemplo, quando registradores e registros estabelecidos fora da União Europeia prestam seus serviços de registro de nomes de domínio a pessoas físicas na União Europeia, o GDPR pode ser aplicado. Além disso, tanto a autoridade nacional de proteção de dados dos Estados membros como o Conselho Europeu de Proteção de Dados têm um papel no monitoramento da aplicação e implementação do RGPD[153].

---

[152] Diretiva 95/46/CE é uma legislação 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: 16 jan. 2020.

[153]Tradução livre do autor. Texto original: “For example, when registrars and registrations established outside the European Union provide their domain name registration services to individuals within the European Union, the GDPR may apply. In addition, both the Member States' national data protection authorities and the European Data Protection Council have a role in monitoring the implementation and implementation of the RGPD”. ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 69.

Deste modo, pode-se afirmar que a transferência de dados através das fronteiras internacionais não é assunto novo na União Europeia. Para ajudar a facilitar esse processo, a RGPD, através do artigo 44, estabelece que:

> Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento[154].

O artigo 45 permite que o Comitê Europeu avalie a adequação da proteção à transferência de dados. A transferência para um país fora da União Europeia pode ser realizada desde que sejam aplicadas as garantias de proteção de dados adotadas pela Comissão da União Europeia[155].

Até a finalização da presente pesquisa, os únicos países que obtiveram reconhecimento de adequação definidos pela União Europeia são Andorra, Argentina, Canadá, Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos. Pode-se dizer que a União Europeia está declarando para países fora da União Europeia que, os países que oferecerem um nível de proteção que é considerado adequado, podem transferir dados através das fronteiras internacionais[156].

Explicam Zeller, Trakman e Walters que os países que desejam a

---

[154] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 44 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

[155] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 45 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

[156] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. Data Protection Law – **A Comparative analysis of Asia-Pacific And European Approaches**. Ed. Springers, 2019, p. 74.

transferência de dados e que não fazem parte da União Europeia, podem incluir garantias em um tipo de contrato que poderá ser realizado entre a *ICANN* (Corporação da Internet para Atribuição de Nomes e Números)[157] e os registradores de dados, a fim de garantir a legalidade das transferências dos dados para países terceiros.

E destaca:

> No entanto, deve notar-se que as garantias incluídas nos contratos existentes foram objeto de críticas e que a sua validade deve ser julgada pelo Tribunal de Justiça da União Europeia. Sua validade futura, pelo menos em sua forma atual, é um tanto incerta. Além disso, o Artigo 47 garante que existem regras corporativas vinculativas que podem ser aplicadas[158].

Além disso, vale frisar que as regras corporativas criam uma estrutura autorregulatória pela qual uma organização deve cumprir suas próprias regras. Este é um sinal positivo, pois atribui maior responsabilidade à indústria de se autorregular, em vez da posição tradicional do governo em desempenhar esse papel em nome da comunidade.

Ainda, a Comissão da União Europeia é responsável por determinar se um país estrangeiro ou organização internacional garante um nível adequado de proteção. A transferência transfronteiriça de dados pessoais pode estar exposta a muitas variáveis.

Assim, a União Europeia considera que uma organização deve estabelecer processos e sistemas sólidos, para garantir que todos os dados pessoais coletados, armazenados e usados sejam precisos. Quaisquer dados imprecisos devem ser excluídos.

Além disso, há um Comitê Europeu para a Proteção de Dados (CEPD)[159]

---

[157] Para alcançar outra pessoa na Internet, você precisa digitar um endereço no seu computador - um nome ou um número. Esse endereço deve ser exclusivo para que os computadores saibam onde se encontrar. A ICANN coordena esses identificadores exclusivos em todo o mundo. Sem essa coordenação, não teríamos uma Internet global. **INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS**. Disponível em <https://www.icann.org/resources/pages/welcome-2012-02-25-en>. Acesso em: 16 jan 2020.

[158] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert**. Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches**. Ed. Springers, 2019, p. 74.

[159] O Comité Europeu para a Proteção de Dados (CEPD) é um organismo europeu independente que contribui para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e

que fornece à Comissão Europeia uma opinião avaliando a adequação do nível de proteção de dados de um país ou organização.

O CEPD é responsável por orientar os controladores, processadores e empresas a cumprir e determinar disputas entre as autoridades nacionais de supervisão. A ênfase da Comissão é determinar se o país estrangeiro possui garantias satisfatórias para proteger a transferência de dados.

Por exemplo, considerando o sistema atual de proteção de dados, não é razoável que a Comissão autorize a transferência de dados para Cingapura ou Austrália, pois são dois países que não possuem leis de privacidade maduras o suficiente para a proteção dos dados naqueles países.

Entretanto, no caso em que a Comissão considere que a transferência de dados não terá proteção adequada, essa transferência ainda sim poderá ocorrer, desde que o responsável pelo tratamento estabeleça regras corporativas vinculativas aprovadas pela Comissão.

Além disso, o controlador deve possuir um contrato em vigor descrevendo as cláusulas padrões de proteção de dados e a certificação eventualmente aprovada[160].

Já os artigos 48 e 49 do RGPD também se referem à transferência de dados em circunstâncias em que um tribunal ou órgão administrativo estrangeiro ordenou a transferência que não é permitida ou quando não foram estabelecidas garantias apropriadas:

> As decisões judiciais e as decisões de autoridades administrativas de um terceiro país que exijam que o responsável pelo tratamento ou o subcontratante transfiram ou divulguem dados pessoais só são reconhecidas ou executadas se tiverem como base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o terceiro país em causa e a União ou um dos Estados-Membros, sem prejuízo de outros motivos de transferência nos termos do presente capítulo.

---

promove a cooperação entre as autoridades de proteção de dados da UE**.** **European Data Protection Board – Comite Europeu para a Proteção de Dados**. Disponível em:<https://edpb.europa.eu/edpb_pt>. Acesso em: 16 jan. 2020.

[160] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. Data Protection Law – **A Comparative analysis of Asia-Pacific And European Approaches**. Singapura: Springers, 2019, p. 75.

> Na falta de uma decisão de adequação nos termos do artigo 45.o, nºo 3, ou de garantias adequadas nos termos do artigo 46.o, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países estrangeiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições: [...][161].

Assim, verifica-se que o RGPD Europeia delineou bem as possibilidades de transferência de dado para outros países que não fazem parte da União Europeia, com diversos métodos de transparência e segurança administrativas, sem que tenha que recorrer ao judiciário europeu para tanto.

Passamos a analisar as Sanções Administrativas no âmbito da RGPD.

2.1.2. Sanções Administrativas

Para reforçar a aplicação das regras do Regulamento Geral de Proteção de Dados (RGPD), explica Paul Lambert,[162] que devem ser aplicadas sanções, incluindo multas administrativas, por qualquer infração ao RGPD, além de medidas apropriadas impostas pela autoridade supervisora de proteção de dados de acordo com o RGPD.

No caso de uma infração menor ou se a multa passível de ser aplicada constituir um ônus desproporcional para uma pessoa física, a RGPD possibilita que seja emitida uma repreensão em vez de uma multa (advertência, por exemplo).

Ainda, a legislação prevê que se deve levar em consideração diversos fatores, tais como a natureza, gravidade e duração da infração, o caráter intencional da infração, as ações tomadas para mitigar os danos sofridos e o grau de responsabilidade.

Além disso, deve-se levar em consideração também se já houve ou não infrações anteriores, a maneira pela qual a infração se tornou conhecida pela autoridade supervisora de proteção de dados, a conformidade com as medidas

---

[161] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 48 e 49 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez 2019.
[162] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 251.

ordenadas contra o controlador ou processador, bem como qualquer outro fator agravante ou atenuante e, por fim, a adesão a um código de conduta (programas de Integridade/Compliance)[163].

A imposição de sanções, incluindo multas administrativas, deve estar sujeita a garantias processuais adequadas, de acordo com os princípios gerais do direito da União Europeia e da Carta da União Europeia, incluindo proteção judicial efetiva e devido processo legal.[164]

Para fortalecer e harmonizar as sanções administrativas por infrações ao RGPD, cada autoridade supervisora de proteção de dados deve ter o poder de aplicar multas administrativas.

Dispõe Paul Lambert:

> O RGPD deve indicar infrações e o limite superior e os critérios para a definição das multas administrativas relacionadas, que devem ser determinadas pela autoridade supervisora competente em proteção de dados em cada caso individual, levando em consideração todas as circunstâncias relevantes da situação específica. Deve, também, levar em consideração:
> A natureza, gravidade e duração da infração;
> Suas consequências;
> As medidas adotadas para garantir o cumprimento das obrigações sob o RGPD e para prevenir ou mitigar as consequências da infração.[165]

Robert Walters, Leon Trakman e Bruno Zeller inclusive destacam que há sinais de que os governos estão levando o uso ilegal de dados mais a sério nos últimos tempos, e citam como exemplo a própria União Europeia[166].

Ainda, quando multas administrativas são impostas a pessoas que não são empresas, a autoridade supervisora de proteção de dados deve levar em

---

[163] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 148 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez 2019.
[164] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 252.
[165] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 252.
[166] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. Data Protection Law – **A Comparative analysis of Asia-Pacific And European Approaches**. Ed. Springers, 2019, p. 443.

consideração o nível geral de renda no Estado-Membro, bem como a situação econômica da pessoa ao considerar o valor apropriado da multa. O mecanismo de consistência também pode ser usado para promover uma aplicação consistente de multas administrativas[167].

De outro turno, cabe aos Estados-membros determinar se e em que medida as autoridades públicas devem estar sujeitas a multas administrativas. A aplicação de uma multa administrativa ou de uma advertência não afeta a aplicação de outros poderes das autoridades de supervisão de proteção de dados ou de outras sanções previstas no RGPD[168].

Conforme já abordado sucintamente no capítulo 1, as violações da RGPD estão sujeitas a multas administrativas de até EUR 10.000.000,00 (dez milhões de euros) ou, no caso de uma organização, até 2% do faturamento anual total do exercício financeiro anterior, o que for maior.

Além disso, em outras circunstâncias, é possível a aplicação de multas de até EUR 20.000.000,00 (vinte milhões de euros) ou, no caso de uma organização, até 4% do volume de negócios anual total do exercício financeiro anterior, o que for maior, quando violarem[169]:

> Os princípios básicos de processamento, incluindo condições de consentimento, de acordo com os Artigos 5, 6, 7 e 9;
> Os direitos dos titulares de dados;
> As transferências de dados pessoais para um destinatário em um país terceiro ou país organização internacional;
> Quaisquer obrigações nos termos da lei do estado membro;
> Não cumprimento de uma ordem ou limitação temporária ou definitiva no processamento ou suspensão dos fluxos de dados pela autoridade supervisora de proteção de dados§ ou falha no fornecimento de acesso em: violação a Artigo 58º, item 1.

---

[167] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 252.
[168] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 252.
[169] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Art. 83, Item 4. Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

Em relação às multas por desconformidade com a ordem da autoridade supervisora de proteção de dados, a lei estabelece que o não cumprimento de uma ordem da autoridade supervisora de proteção de dados a que se refere o artigo 58 deve ser sujeita a multas administrativas até EUR 20.000.000,00 (vinte milhões de euros), ou, no caso de uma organização, até 4% do faturamento anual total do exercício financeiro anterior, o que for maior.

Sem prejuízo dos poderes corretivos das autoridades de supervisão da proteção de dados nos termos do artigo 58º, item 2, cada Estado-Membro pode estabelecer regras acerca de quando as multas administrativas podem ser impostas às autoridades e organismos públicos estabelecidos no respectivo Estado-Membro.

O exercício pela autoridade supervisora de proteção de dados de seus poderes nos termos do referido artigo deve estar sujeito a garantias processuais apropriadas, de acordo com a legislação da União Europeia e do Estado-membro, incluindo remédio judicial eficaz e o devido processo legal.

Quando o sistema jurídico do Estado-membro não fornecer multas administrativas, o artigo pode ser aplicado de forma que a multa seja iniciada pela autoridade supervisora de proteção de dados competente e imposta pelos tribunais nacionais competentes, garantindo ao mesmo tempo que esses recursos legais sejam eficazes e tenham um efeito equivalente às multas administrativas impostas pelas autoridades de supervisão da proteção de dados.

Ainda, completa Lambert[170]:

> De qualquer forma, as multas aplicadas devem ser efetivas, proporcionadas e dissuasivas. Sem prejuízo dos poderes corretivos das autoridades de supervisão de proteção de dados nos termos do artigo 58, cada Estado membro pode estabelecer regras sobre se e em que medida multas administrativas podem ser impostas às autoridades e órgãos públicos estabelecidos nesse estado membro. Portanto, existe algum potencial de não conformidade e violações para o setor público serem classificadas de alguma forma no setor comercial, se determinadas leis nacionais tentarem estabelecer padrões duplos. Deve-se ter em mente que existem muitas violações de dados relatadas em termos do setor público, portanto as

[170] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 255.

preocupações não se limitam ao setor privado.

Se um controlador ou processador, intencional ou negligentemente, para as mesmas operações de processamento ou vinculadas, infringir várias disposições do RGPD, o valor total da multa administrativa não deve exceder o valor especificado para a infração mais grave[171].

É possível prever que essa disposição limitada pode ser contestada em casos particulares. As nuances desta disposição levarão algum tempo para serem totalmente apreciadas. Será interessante ver se isso contrasta com as disposições de certas normas dos EUA que preveem penalidades por comunicação de *spam*, o que pode resultar em multas totais significativas mesmo que apenas uma amostra das violações seja levada em consideração[172].

Em relação às sanções, o artigo 84 do RGPD[173] dispõe que os Estados-Membros devem estabelecer as regras sobre outras sanções aplicáveis às violações do RGPD, em particular para as infrações não sujeitas a multas administrativas nos termos do artigo 83, e devem tomar todas as medidas necessárias para garantir sua aplicação. Tais penalidades devem ser efetivas, proporcionais e dissuasivas.

Portanto, além do regime de multas descrita acima, as organizações precisam estar cientes do potencial de penalidades adicionais decorrentes. Os Estados-Membros devem estabelecer as regras sobre outras sanções aplicáveis às violações do RGPD, em particular para as infrações não sujeitas a multas administrativas nos termos do artigo 83, e devem tomar todas as medidas necessárias para garantir sua aplicação. Tais sanções devem ser efetivas, proporcionais e dissuasivas[174].

---

171 LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 258.

172 LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 258.

173 Os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 83, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 84 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

174 LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 259.

Assim, as organizações precisarão revisar seus programas de integridade, trazendo estes detalhes específicos, bem como quaisquer alterações que possam ocorrer ou serem introduzidas ao longo do tempo.

Como observado anteriormente, o GDPR estabelece disposições significativas ao regime de multas. A criação de novas penalidades aprimoradas no novo regime de proteção de dados será um estímulo significativo para muitas organizações considerarem seriamente a adequação com a proteção de dados.

Paul Lambert complementa:

> Enquanto a Comissão Federal do Comércio (bem como as regras do direito da concorrência) nos EUA impuseram, e também concordaram consensualmente, multas significativas em relação a questões de proteção de dados, o aumento de multas e penalidades na UE - incluindo uma porcentagem da rotatividade mundial nível - aumenta os riscos de erros de conformidade. Embora seja importante obter a conformidade correta, também é importante garantir a conformidade e o cumprimento dos pedidos de maneira rápida e oportuna. Caso contrário, isso também abre potencial para penalidades[175].

Assim, a LGPD da União Europeia trata a questão de multas e sanções com bastante seriedade, o que será melhor estudado no capítulo seguinte quando analisados os casos de aplicação da lei até a presente data.

2.1.3. Controle judicial

Toda lei pode ser submetida à análise do judiciário a qualquer momento. Quando a lei é nova, isso acontece com maior frequência, pois as partes teoricamente lesadas com as sanções e multas, muito provavelmente buscarão o judiciário para ver reduzidas ou eximidas as multas ou sanções aplicadas, até que se forme um entendimento pacificado sobre determinado assunto.

Pensando nisso, a própria legislação Europeia trouxe no seu artigo 78 o

---

[175] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 260.

que Walters, Trakman e Zeller[176] chamam de remédio judicial:

> Artigo 78. Direito à ação judicial contra uma autoridade de controlo
> 1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todas as pessoas singulares ou coletivas têm direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito.
> 2. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, os titulares dos dados têm direito à ação judicial se a autoridade de controlo competente nos termos dos artigos 55.oe 56.o não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado nos termos do artigo 77.o.
> 3. Os recursos contra as autoridades de controlo são interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidas.
> 4. Quando for interposto recurso de uma decisão de uma autoridade de controlo que tenha sido precedida de um parecer ou uma decisão do Comité no âmbito do procedimento de controlo da coerência, a autoridade de controlo transmite esse parecer ou decisão ao tribunal.

O artigo prevê a possibilidade de qualquer pessoa propor ações judiciais contra decisões juridicamente vinculativas das autoridades de controle, conforme dispõe o item 1 do artigo acima.

Importante destacar que a lei não obriga a interposição de primeiro um recurso administrativo, pois traz a possibilidade de propor ação judicial e o recurso administrativo, sem prejuízo um do outro, ou seja, totalmente independentes. A parte pode optar em propor somente a ação judicial para litigar sobre imposições administrativas, pode também em conjunto propor o recurso administrativo, ou somente o recurso administrativo.

Além disso, os próprios titulares de dados têm direito à ação judicial se a autoridade de controle não tratar a reclamação ou não informar sobre o andamento da reclamação que tenha apresentado nos termos do artigo 77, que dispõe que todos os titulares de dados têm direito a apresentar reclamação a uma autoridade de

[176] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. Data Protection Law – **A Comparative analysis of Asia-Pacific And European Approaches**. Ed. Springers, 2019, p. 78.

controle. Em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o regulamento.

Franzina[177] ressalta, no entanto, que se uma regra como a do artigo 25 do *Regulamento 2016/679* de Bruxelas[178] seja invocada para manter um acordo realizado entre partes, o artigo 79 da RGPD permitiria que um titular de dados também instaurasse nos tribunais uma ação em mais de um Estados-Membros.

Destaca Franzine que o RGPD não diz que a jurisdição é exclusiva. Além disso, o Artigo 79 não esclarece os motivos que podem ser derrogados ao abrigo de um acordo entre as partes

Assim, a aplicação de multas e sanções estão sujeitos ao controle judicial, caso uma das partes se sinta lesada ou não concorde com a penalidade aplicada, o que será melhor a seguir, com a análise dos casos práticos. Ademais, antes da RGPD, muitos casos já eram tratados sob a ótica da proteção de dados pela Diretiva Europeia 95/46/CE. Vejamos.

2.1.3.1. Deutsche Bahn

Em 2009, por exemplo, tornou-se público que os funcionários de uma empresa (*Deutsche Bahn*) foram pesquisados pela agência denominada "*Network Deutschland GmbH"*.

Ao longo de meses, outras informações vieram à tona sobre a extensão da troca de espionagem e dados. Não apenas funcionários, mas seus cônjuges também foram investigados em relação a suas finanças privadas, incluindo transferências de dinheiro, viagens, comportamento *Online* e dados biográficos.

As ordens para investigar esses dados foram dadas oralmente pelo departamento encarregado de "combater a corrupção". Pelas informações

---

[177] FRANZINA, Pietro. Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation, in Alberto de Franceschi (2016) **European contract law and the digital single market: the implications of the digital revolution**, Cambridge, Antwerp, Portland, Intersentia, p. 108.

[178] UNIÃO EUROPEIA. Regulamento 2016/679 do parlamento Europeu e do conselho. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 12 jan. 2020.

divulgadas, para realização da espionagem, o valor de aproximadamente EUR 800.000,00 (oitocentos mil euros) foi acordado sem transparência[179].

O suspeito por entregar as informações foi o CEO Hartmut Mehdorn, que teve que se demitir em março de 2009, tendo assumido o novo CEO Rüdiger.

Pelos desvios de dados, uma pena monetária foi imposta à empresa pelo Estado de Berlim. Foi a maior condenação na época acerca de proteção de dados na Alemanha, cerca de EUR 1.100.000,00 (um milhão e cem mil euros), pagos pela empresa sem objeção.

O lado positivo é que a lei de proteção de dados não é de natureza objetiva, mas sim subjetiva, ou seja, o texto legal precisa ser traduzido em relação a todas as atividades realizadas em uma empresa. A referida empresa reconheceu esse desafio e, após um grande fracasso, passou por um extenso processo de negociação das novas regras formais de privacidade e proteção de dados na empresa, além de comunicá-los a tantos funcionários e gerentes quanto possível[180].

2.1.3.2. Maximilian Schrems Vs Data Protection Commissioner

Um outro caso foi o que envolveu o Sr. Maximilian Schrems e o *Data Protection Commissioner*[181].

Neste caso, foi necessário o tribunal determinar se a transferência de dados pessoais tinha proteções adequadas do *Facebook* na União Europeia, mais especificamente na Irlanda, para servidores localizados nos Estados Unidos.

Tudo começou quando o Sr. Schrems apresentou uma queixa ao *Comissário Irlandês de Proteção de Dados*, dizendo que, à luz das revelações feitas em 2013 por Edward Snowden sobre as atividades dos serviços de inteligência dos Estados Unidos, a Agência de Segurança Nacional (NSA), a lei e a prática dos Estados Unidos não ofereceram proteção adequada contra a vigilância pelas

---

[179] FINN, Rachel L., WRIGHT, David, FRIEDEWALD, Michael, GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de, POULLET, Yves - **European Data Protection Coming of Age**. Ed Springer Netherlands, 2013, p. 383.

[180] FINN, Rachel L., WRIGHT, David, FRIEDEWALD, Michael, GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de, POULLET, Yves - **European Data Protection Coming of Age**. Ed Springer Netherlands, 2013, p. 383.

[181] UNIÃO EUROPEIA. Acordão do Tribunal de Justiça. **Processo nº C-362/14**. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&from=PT>. Acesso em: 28 jan. 2020.

autoridades públicas dos dados transferidos para esse país.

A autoridade irlandesa rejeitou a denúncia, considerando que uma investigação sobre as questões levantadas pelo Sr. Schrems era infundada e que não havia provas de que os dados pessoais do Sr. Schrems tivessem sido acessados pela NSA.

Além disso, o Comissário considerou que o as alegações feitas pelo Sr. Schrems teriam que ser determinadas de acordo com o acordo "*Safe Harbor 2000/520191"*, e a Comissão havia constatado que os Estados Unidos asseguravam um nível adequado de proteção.

Neste emblemático caso, o tribunal anulou o referido acordo transatlântico EUA-UE *Safe Harbor*, em vigor há 15 anos[182]. Esse acordo permitiu que as empresas transferissem dados da Europa para os Estados Unidos (EUA). Efetivamente, as empresas nos EUA poderiam certificar-se de que obedeceriam aos padrões de proteção de dados da UE para permitir a transferência de dados europeus para os Estados Unidos.

Assim, o Tribunal de Justiça da União Europeia constatou que os dados europeus não eram suficientemente protegidos nos Estados Unidos. Consequentemente, o mesmo Tribunal determinou que o órgão de supervisão de um Estado membro é independente e tem o poder de atestar a conformidade com as leis de proteção de dados.

Deve-se observar que um órgão nacional (o organismo de supervisão) pode verificar o nível de proteção concedido à transferência de dados para um país estrangeiro. É importante ressaltar que qualquer avaliação deve estar de acordo com as normas europeias, e não as de um país estrangeiro, a menos que haja uma isenção.

Assim, há um compromisso de garantir que as normas da União Europeia não sejam comprometidas, quando esses dados estiverem sendo transferidos para

---

[182] O Tribunal de Justiça da União Europeia produziu um julgamento invalidando o acordo de transferência de dados pessoais (conhecido como "Safe Harbor", "Porto Seguro" em tradução para o português) entre os Estados Unidos e a União Europeia. Esse acordo, que estava em vigor desde o ano de 2000, era o instrumento legal que autorizava empresas a transferirem dados coletados de cidadãos europeus para serem processados em seus estabelecimentos situados em território americano. Disponível em < http://www.editoramagister.com/doutrina_27076672_A_DECISAO_DA_CORTE_EUROPEIA_QUE_INVALIDOU_O_ACORDO_DE_TRANSFERENCIA_DE_DADOS_PESSOAIS.aspx>. Acesso em: 19 jan. 2020.

um país estrangeiro.

No início de 2017, os dados personalizados de troca e proteção de comunicações da União Europeia em um mundo globalizado tentaram chegar a uma decisão de adequação com o Japão e outros países.

Isso ocorreu como resultado do caso Schrems, que exige qualquer decisão de adequação para equilibrar as necessidades de acesso gratuito e o fluxo de dados pessoais para os países, mas deve ser realizado somente quando esse país tiver regras equivalentes de proteção de dados para a União Europeia[183].

2.1.3.3. Sony Playstation Network Vs Comissão Nacional de Informações e Liberdade (CNIL)

Importante abordar neste trabalho o caso midiático com a Sony. A autoridade britânica da área de informação multou a Sony em £ 250.000,00 (duzentos e cinquenta mil libras) porque a empresa não tomou medidas de segurança suficientes para evitar um ataque à sua rede *online* de jogos *PlayStation Network.*

O ataque ocorreu em abril de 2011 e teve como alvos dados de cartão de crédito e outras informações pessoais dos usuários armazenados na *PlayStation Network.* Apelidada pelos *gamers* de *Sony Epic Fail*, a invasão obrigou a empresa a bloquear o acesso à rede, deixando milhões de usuários sem poder jogar *multiplaye*r por vários dias[184].

Lambert, utilizando o caso para exemplificar a aplicação da GDPR, destaca que as vendas da Sony no terceiro trimestre de 2015 são de aproximadamente US$ 21.400.000.000,00 (vinte e um bilhões quatrocentos milhões de dólares), se multiplicadas por quatro trimestres, o faturamento chega a aproximadamente US$ 85.600.000.000,00 (oitenta e cinco bilhões seiscentos milhões de dólares).

Portanto, pela nova regra da GDPR, uma multa por uma violação de

---

[183] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches**. Ed. Springers, 2019, p. 76.

[184] Sony é multada no Reino Unido por invasão à PlayStation Network. **O Globo**. Disponível em <https://oglobo.globo.com/economia/sony-multada-no-reino-unido-por-invasao-playstation-network-7385801>. Acesso em: 22 jan. 2020.

dados de segurança, como este caso em que a empresa foi multada em £ 250.000,00 (duzentos e cinquenta mil libras), após o GDPR pode chegar a EUR 10.000.000 (dez milhões de euros) ou 2% de US$ 85.600.000.000,00 (oitenta e cinco bilhões e seiscentos milhões de dólares), o que for maior, o que dá aproximadamente US$ 1.710.000.000,00 (um bilhão e setecentos e dez milhões de dólares).

Ainda, em determinados casos a multa pode ser de até 4%. Considere uma organização com um faturamento anual de US$ 100.000.000.000,00 (cem bilhões) e uma multa de 4%, o que equivaleria a US$ 4.000.000.000,00 (quatro bilhões). Isso enfatiza a importância significativamente aprimorada da conformidade da proteção de dados pelas organizações. O custo da não conformidade foi bastante aumentado pelo novo GDPR[185], principalmente por que a penalidade é pelo faturamento, e não lucro da empresa.

2.1.3.4. Google Vs Comissão Nacional de Informações e Liberdade (CNIL) da França

Em relação à jurisprudência acerca da RGPD, o *Google* recebeu uma multa na França de EUR 50.000.000,00 (cinquenta milhões de euros) por "falta de transparência, informação incorreta e ausência de consentimento válido na publicidade personalizada[186]".

A decisão foi comunicada pela Comissão Nacional de Informações e Liberdade (CNIL), a autoridade francesa para proteção da privacidade. A punição foi dada com base nas diretrizes fixadas na RGPD. Esse já é o maior valor de multa aplicada desde que a legislação entrou em vigor, em maio de 2018.

O RGPD exige que as companhias expliquem de forma clara e compreensiva às pessoas como usam suas informações. Também exige que haja consentimento explícito para uso desses dados[187].

---

[185] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 256.

[186] Google recebe maior multa já aplicada por violar dados pessoais na Europa. **UOL**. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2019/01/21/google-e-multado-na-franca-por-violar-de-dados-pessoais.htm>. Acesso em: 22 jan. 2020.

[187] Google recebe maior multa já aplicada por violar dados pessoais na Europa. **UOL**. Disponível em

A CNIL justificou a sanção devido à "*gravidade das violações observadas nos princípios da proteção de dados: transparência, informação e consentimento*". A CNIL considerou que não é tão fácil achar as explicações do *Google* de como as informações são usadas. Informações sobre o processamento dos dados, por exemplo, não estavam presentes na mesma página que o detalhamento sobre o armazenamento de dados. Em alguns casos, o usuário teria de percorrer cinco ou seis páginas até achar a descrição dos processos do *Google.*

O pedido por consentimento foi outro problema identificado pela CNIL. Em alguns casos, a caixa de texto pedindo autorização do usuário já vinha preenchida. Segundo a CNIL, as irregularidades detectadas na multinacional norte-americana "*deixam os usuários sem suas garantias essenciais, já que pratica operações que podem revelar importantes partes da vida privada*".

A CNIL começou a analisar reclamações recebidas das associações *None Of Your Business* (NOYB) e *La Quadrature du Net* (LQDN). Para elas, o *Google* "*não tem base legal*" para processar informação pessoal de usuários com o objetivo de criar publicidade personalizada.

A informação sobre as operações de processamento para a personalização dos anúncios fica diluída em vários documentos e não permite ao usuário saber seu alcance real.

A título de comparação, o Google já recebeu outras multas dentro da União Europeia que atingiu a casa dos bilhões. No primeiro caso, a Comissão Europeia aplicou em 2017 uma multa de EUR 2.424.000.000,00 (dois bilhões quatrocentos e vinte e quatro milhões de euros) por usar sua ferramenta de busca para favorecer o comparador de preços *Google Shopping.* Dessa forma, a empresa impedia que rivais tivessem a mesma capacidade de competir.

O valor dessa multa já era o maior aplicado, até então, para condutas anticompetitivas. Só que, em julho de 2018, o *Google* quebrou sua própria marca: foi multado em EUR 4.340.000.000,00 (quatro bilhões trezentos e quarenta milhões de euros) por usar seu sistema operacional para *smartphones*, o Android, para impedir a livre competição no mundo dos *smartphones*. Isso fez a empresa ser obrigada a

---

<https://www.uol.com.br/tilt/noticias/redacao/2019/01/21/google-e-multado-na-franca-por-violar-de-dados-pessoais.htm>. Acesso em: 22 jan. 2020.

mudar o *Android*. Ainda cabe recurso acerca da multa aplicada[188].

Existem diversos casos práticos que poderiam ser apresentados nesta pesquisa, mas evitando-se tautologia, apresentou-se somente alguns casos mais pontuais e que demonstram os resultados esperados nesta pesquisa.

Agora, passamos a análise dos elementos determinantes no Brasil.

2.2. Brasil

No Brasil, existem diversas leis setoriais que trabalharão em conjunto com a Lei Geral de Proteção de Dados Pessoais. Dentre elas, o Código de Defesa do Consumidor, que disciplinou no artigo 43 os bancos de dados e cadastros de consumidores. Esse artigo, nas palavras de Bruno Ricardo Bioni[189], alcança todo e qualquer dado pessoal do consumido, indo muito além, portanto, dos bancos de dados e informações negativas para fins de concessão de crédito.

Importante ressaltar que a legislação consumerista optou por conferir ao consumidor o direito de controlar as suas informações pessoais, seguindo o padrão regulatório acima referenciado das *Fair Information Practice Principles* (FIPPs). Com efeito, toda normatização ali desenhada desemboca para que o consumidor seja capacitado para autodeterminar as suas informações pessoais.

Além desta, há também a Lei de Cadastro Positivo, Lei nº 12.414/2011, que veio disciplinar a formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito.

Também há o *Marco Civil da Internet*, Lei nº 12.965/2014, que inaugurou uma normativa específica para os direitos e garantias dos cidadãos nas relações travadas na *internet*[190] que, inclusive, prevê a proteção da privacidade e dos dados pessoais.

Por fim, veio a Lei Geral de Proteção de Dados (Lei 13.709/2018) que,

---

[188]Google é multado em € 50 milhões sob nova regra de dados da Europa. **Época Negócios Online**. Disponível em <https://epocanegocios.globo.com/Empresa/noticia/2019/01/google-e-multado-em-50-milhoes-sob-nova-regra-de-dados-da-europa.html>. Acesso em: 28 jan. 2020.

[189] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 127.

[190] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 130.

após quase uma década de debates, fez com que o Brasil aprovasse a referida legislação. Segundo Bruno Ricardo Bioni:

> É interessante notar que, na primeira versão do anteprojeto de lei colocada sob consulta pública em 2010, o consentimento era, em termos topográficos, a única base legal para o tratamento de dados pessoais. Isso se repetiu na segunda consulta pública em 2015, quando o que hoje são as demais bases legais da LGPD eram hipóteses nas quais o consentimento poderia ser dispensado[191].

Dentre alguns pontos relevantes, destacam-se os elementos determinantes da LGPD no que se refere à sua eficácia, quais sejam: a Cooperação Internacional e as Sanções Administrativas, que serão melhor abordadas a seguir.

2.2.1. Cooperação Internacional

O artigo 33 da Lei Geral de Proteção de Dados autoriza a transferência internacional de dados pessoais em alguns casos específicos, sobretudo quando a transferência for necessária para a cooperação internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, bem como quando a transferência resultar em compromisso assumido em acordo de cooperação internacional[192].

Além disso, a LGPD prevê no capítulo IX, Seção I, a criação da *Autoridade Nacional de Proteção de Dados, já abordado no capítulo primeiro*. Dentre as competências da ANPD, uma delas é promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional[193].

Não poderá ser admitida a transferência para países em que não houver

---

[191] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 133.
[192] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 33, VI – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.
[193] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-J, IX – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

tratado de cooperação em matéria cível, o que dificultaria eventual medida de defesa dos direitos dos titulares, ainda que o país tenha legislação e fiscalização efetiva sobre proteção de dados pessoais.

A LGPD é bem mais amena no tocante à aferição do nível de adequação do que o GDPR. Assim, se determinado país, tendo tratado de cooperação com o Brasil, é considerado adequado pela GDPR, certamente deverá também assim ser considerado pela ANPD[194].

Além disso, a LGPD dispõe que para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei Geral de Proteção de Dados, será permitida a transferência de dados.

O que se observa, é que a LGPD traz algumas disposições parecidas com a GDPR da União Europeia. No entanto, de maneira muito mais breve e resumida, de modo que a LGPD não abrange tantas hipóteses quanto a GDPR.

Cunha[195] destaca que, na prática, embora o texto da Lei neste ponto silencie, o natural será que a Autoridade Nacional, uma vez criada, diga à sociedade e ao mercado quais legislações estrangeiras ela percebe como adequadas e, mais importante, inadequadas.

DPOs (*Data Protection Officer* ou Encarregados) e Autoridades Nacionais de vários países devem, num futuro relativamente próximo, iniciar atividades de cooperação e de intercâmbio. Essas trocas têm tudo para ser muito positivas, no sentido do estabelecimento de boas práticas, bem como no de gradual uniformização das normas infra legais a serem editadas pelas várias autoridades.

Ainda, o inciso VI do artigo 33, dispõe que é possível a transferência de dados quando a transferência resultar em compromisso assumido em acordo de cooperação internacional.

Como a expressão “Cooperação Internacional” é usada sem nenhuma limitação de contorno, Cunha[196] destaca que o Mercosul, a OMS, a Unasul, e mesmo a OMC, passam a representar portas de saída facilitada para os dados

---

[194] MACIEL, Rafael. Manual prático sobre a **Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. Editora RM Digital Education. Edição do Kindle. Posição 1212 de 3284.

[195] CUNHA, Mauro Leonardo. **Comentários à Lei Geral de Proteção de Dados**. Edição Própria. 2018, Edição do Kindle. Posição 1324 de 2215.

[196] CUNHA, Mauro Leonardo. **Comentários à Lei Geral de Proteção de Dados**. Edição Própria. 2018, Edição do Kindle. Posição 1324 de 2215.

pessoais coletados no Brasil.

Atualmente, com a *internet*, grande parte do tratamento de dados pessoais de cidadãos de determinado país é realizada em um país estrangeiro. O artigo 33 prevê que essa transferência se dará somente junto a países que possuam um nível de proteção de dados semelhante, apresentando cinco critérios específicos de como será feita a comparação: quando o órgão competente autorizar a operação, e quando o titular tiver fornecido seu consentimento, com informação prévia e específica sobre o caráter internacional da operação. O artigo 35 ainda garante que tanto o responsável pelo tratamento quanto o operador respondam pelo tratamento de dados, independentemente de onde a operação se realize[197].

Melhor seria que o legislador houvesse especificado que espécies de cooperação internacional autorizam a migração de dados. Seria alentadora a criação com brevidade da Autoridade Nacional, cujo poder regulamentador teria o condão de limitar esse tipo de abertura radical ainda constante no texto da Lei[198].

Ainda, só poderá ser feita a transferência internacional de dados quando o titular obtiver informações de todos os aspectos da atividade, e consentir de forma específica e própria, além da necessidade de o país que receber oferecer o mesmo grau de proteção de dados, tem-se satisfeito esse requisito[199].

Assim, o que se percebe é que o órgão regulador terá que administrativamente buscar medidas para trazer maior segurança jurídica à ideia de transferência de dados e cooperação internacional, evitando-se assim a interpretação genérica por parte dos interessados em benefício próprio, o que poderá acarretar grandes prejuízos para quem tem seus dados operados no Brasil.

Nesse cenário, a correta implementação da LGPD projetará o Brasil como país que se preocupa e regulamenta a proteção dos dados pessoais, seguindo a tendência internacional capitaneada pela GDPR. Embora a lei brasileira, por si só, não garanta de imediato a transferência transfronteiriça de dados pessoais da Europa para o Brasil, futuramente ela poderá ser levada em consideração pela

---

[197] BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. **Proteção de dados pessoais no Brasil:** análise dos projetos de lei em tramitação no Congresso Nacional. 2017, p. 28.
[198] CUNHA, Mauro Leonardo. **Comentários à Lei Geral de Proteção de Dados**. Edição do Kindle. Posição 1356.
[199] BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. **Proteção de dados pessoais no Brasil:** análise dos projetos de lei em tramitação no Congresso Nacional. 2017, p. 34.

Comissão Europeia para avaliar se existe garantia de um nível de proteção adequado. Assim, tanto o responsável pelo tratamento (*data controller*, ou controlador), quanto o subcontratante (data processor ou processador) precisam estar adequados não só com a LGPD, mas também com a GDPR, caso haja interesse em exportar dados pessoais para fora da União Europeia.

2.2.2. Sanções Administrativas

A nossa legislação consumerista já previa algumas hipóteses de sanções, judiciais e administrativas, tais como as práticas abusivas, ensejando a atuação dos órgãos estatais de defesa do consumidor, em todos os níveis da Federação, de modo a fiscalizar e aplicar as sanções administrativas adequadas, nos termos dos artigos 56 e 57 do CDC[200].

Ainda, a Lei do Cadastro Positivo reforçou a fiscalização e o controle administrativo na hipótese de violação das suas normas, atribuindo poder aos órgãos de aplicarem medidas corretivas para a exclusão de informações incorretas e o cancelamento dos cadastros dos consumidores que não autorizaram a sua abertura (art. 17, § 2º)[201].

Além do controle administrativo, o Código de Defesa do Consumidor estabelece medidas penais, em seus artigos 72 e 73, em relação às condutas, respectivamente, de "*impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros*" e de "*deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata*"[202].

Tudo isso, entretanto, não seria suficiente para a defesa dos dados pessoais, e apenas abarrotaria o judiciário com mais ações judiciais. Assim, a LGPD trouxe diversas hipóteses de sanções administrativas pelo órgão regulador, de modo

---

[200] Código de Defesa do Consumidor. Lei 8.078/1990. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em 13. Mai. 2020.
[201] BRASIL, **Lei 12.414 de 9 de junho de 2011.** Art. 17, §2. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 10 dez. 2019.
[202] MENDES, Laura Schertel - **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014, p. 233.

a dar maior segurança jurídica para quem tem seus dados tratados e, inclusive, para quem detém os dados pessoais.

As sanções poderão ser aplicadas de forma gradativa, isolada ou cumulativa, de acordo com o caso concreto[203]. A LGPD dispõe no artigo 52 que os agentes de tratamento de dados, em razão das infrações cometidas, ficam sujeitas à diversas sanções administrativas aplicáveis pelo órgão regulador.

Dentre as penalidades previstas na LPGD, a mais branda é a pena de advertência, prevista no inciso I do artigo 52, com indicação de prazos para adoção de medidas corretivas, o que deixa margem para que o órgão regulador possa agir de acordo com o caso concreto.

As penas pecuniárias são as penas previstas nos incisos II e III do artigo 52, que preveem multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração e multa diária, limitada também ao valor de R$ 50.000.000,00 (cinquenta milhões de reais).

Vale ressaltar que, em que pese a sanção no valor acima pareça uma pena expressiva, trata-se de uma penalidade relativamente leve, considerando que a penalidade, na verdade, é de 2% do faturamento da empresa, ou seja, para que a empresa seja multada em R$ 50.000.000,00 (cinquenta milhões de reais), a mesma terá que ter um faturamento de R$ 2.500.000.000,00 (dois bilhões e quinhentos milhões de reais). Para uma empresa com faturamento de R$ 2.500.000.000,00 (dois bilhões e quinhentos mil reais), R$ 50.000.000,00 (cinquenta milhões de reais) não representa uma penalidade capaz de coagi-la a melhorar sua proteção de dados.

Além do mais, destaca-se que a penalidade de R$ 50.000.000,00 é a penalidade máxima por infração, não significando automaticamente que a empresa será penalizada neste valor, principalmente se não for reincidente.

No cálculo do valor da multa de que trata o inciso II do *caput* deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de

---

[203] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18 .** RM Digital Education. Edição do Kindle. Posição 1584 de 3284.

empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea[204].

Além das penalidades acima mencionadas, a LGPD também traz penalidades socioeducativas no artigo 52, como, por exemplo:

> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração.

Há também a possibilidade de suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador e a suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.

Por fim, a última penalidade prevista na LGPD é a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Evidentemente, as sanções serão só serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados alguns parâmetros, tais como:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência
> VI - o grau do dano;

[204] BRASIL. **Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).** Artigo 52, §4 – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Segundo o §6º do art. 52 da LGPD, as sanções previstas nos incisos X, XI e XII do mesmo artigo, que dispõe sobre a suspensão da atividade ou do funcionamento do banco de dados, bem como a proibição do exercício de atividades relacionadas ao tratamento de dados, só serão aplicadas somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput do artigo para o mesmo caso concreto; e em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.

Trazendo a ideia de conciliação e arbitragem, o parágrafo sétimo prevê que os vazamentos individuais ou os acessos não autorizados de que trata o *caput* do art. 46 da Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata o artigo.

Vale ressaltar que, em que pese a legislação já ter abordado a questão das penalidades em caso de descumprimento da lei, o Artigo 53 dispõe que a autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a LGPD, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. Desta forma, a lei garante maior autonomia para que o órgão regulador possa adequar a legislação ao momento que se está vivendo.

Tais metodologias devem respeitar os princípios de direito administrativo devendo ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos

os seus elementos, demonstrando a observância dos critérios previstos na Lei, consoante dispõe o §1º do artigo 53 da LGPD.

O órgão regulador também tem o dever de estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária, além de ter que observar a gravidade da falta e a extensão do dano ou prejuízo, consoante dispõe o artigo 54:

> Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional. Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

Interessante notar que o teto máximo de valor pecuniário para aplicação da multa prevista no inciso II é por infração e, em um mesmo procedimento administrativo, poderão ser encontradas várias infrações a partir de uma mesma denúncia. Por exemplo, um incidente de vazamento de dados em que, no decorrer do procedimento, seja apurado que também havia um tratamento de dados pessoais excessivo ou desproporcional.

Poderá haver uma infração pelo incidente e outra pela ilicitude do tratamento. Ainda, a autoridade nacional:

> poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea[205].

Finalizada à análise sobre o controle administrativo através das multas e sanções administrativas, é importante analisar o contexto na seara judicial, ou seja, qual a tendência de aplicação no Brasil.

---

[205] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 1577 de 3284.

2.2.3. Controle judicial

O Marco Civil da Internet (MCI), Lei nº 12.965/2014, estabeleceu regramento para guarda e disponibilização dos dados pessoais, demandando ordem judicial para acesso ao conteúdo e ainda trouxe os princípios da finalidade e adequação, vedando a guarda, por provedores de aplicações, dos "*registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente" e "dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular*" (art. 16)[206].

O Marco Civil da Internet trouxe diversas hipóteses de controle judicial, estabelecendo, a partir do artigo 7, que o acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados alguns direitos, dentre eles, a inviolabilidade e sigilo de suas comunicações privadas armazenadas, só podendo terceiros ter acesso mediante ordem judicial[207].

Já o artigo 10, trata da guarda e disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e de conteúdo de comunicações privadas, trazendo a ideia de que o provedor responsável pela guarda dos dados somente será obrigado a disponibilizar os dados pessoais ou outras informações mediante ordem judicial[208].

O § 2º ratifica o disposto no artigo 7, dispondo que § "*O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º*".

Em seguida, ainda na MCI, o artigo 13 aborda o sigilo dos registros e a guarda pelo prazo mínimo de 01 ano sendo que, caso algum interessado queira acesso aos referidos dados, deverá a autoridade requerente no prazo de 60 dias

---

[206] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 294 de 3284.

[207] BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Art. 7, III. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.

[208] BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Art. 10, §1. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.

ingressar com pedido judicial de acesso aos registros[209].

Destaca-se que um dos pilares do MCI é a proteção da privacidade e dos dados pessoais, ao lado da neutralidade de rede e da liberdade de expressão. Sua proeminência consolidou-se com o episódio do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos[210].

Ainda, a lei prevê no § 2º que a autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto acima. Todavia, caso o pedido não seja protocolado no prazo, ou seja indeferido, o provedor não fica responsável por período superior ao acima[211].

O MCI foi incisivo no sentido de afirmar que em qualquer hipótese, a disponibilização ao requerente dos registros deve ser sempre precedida de autorização judicial, não sendo permitida qualquer outra forma de disponibilização, deixando clara a ideia de proteção e segurança jurídica, uma vez que submete a um terceiro imparcial a necessidade da “invasão” de dados de terceiro.

O artigo 15 prevê também que uma Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

E, por fim, o artigo 22 traz a última previsão de controle judicial prevista no MCI, dispondo acerca de produção de prova judicial, onde a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

A LGPD não trouxe tantas previsões quanto a MCI acerca de controle judicial, trazendo uma maior importância ao órgão regulador e as sanções

---

[209] BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Art. 13, §3. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.
[210] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 130.
[211] BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Art. 13, §§ 2 e 4. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.

administrativas.

Vale ressaltar que, em 2014, a Corte Europeia reconheceu aos titulares dos dados o direito ao esquecimento perante os buscadores, como forma de proteção dos dados pessoais, estabelecendo os seguintes critérios para remoção, o que restou ratificado pela RGPD. Todavia, na LGDP não foi previsto dispositivo semelhante. Na realidade, Maciel entende que deixar ao critério dos provedores a decisão sobre a retirada ou não de conteúdo é bastante temerário, devendo ser precedido sempre de ordem judicial, porquanto somente o juiz poderá ponderar os direitos em conflito, conforme modelo adotado no Brasil[212].

Ainda, Maciel destaca que não há necessidade de consentimento para utilizar os dados pessoais da parte adversa num processo judicial, administrativo ou arbitral. Destaca:

> Imaginemos o contrário: não fosse uma base legal, cairíamos no absurdo de ser necessária autorização do processado para que ele permitisse utilizar seus dados para ser iniciado o processo. Essa base legal também legitima ao Poder Judiciário a gestão, autorizando que analise e utilize os dados não só para prestação jurisdicional[213].

Uma das formas de controle judicial prevista na LGPD é a do art. 7, que dispõe que o tratamento de dados pessoais somente poderá ser realizado, dentre outras hipóteses, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, nos termos da Lei de Arbitragem[214].

Já o artigo 11, trata dos dados pessoais sensíveis. Dispõe a LGPD que o tratamento deste tipo de dado somente poderá ocorrer no exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, também nos termos da Lei da Arbitragem (Lei 9.307/1996)[215].

---

[212] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 318 de 3284.

[213] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. RM Digital Education. Edição do Kindle. Posição 726 de 3284.

[214] BRASIL. **Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).** Artigo 7º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[215] BRASIL. **Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).** Artigo 11º, D – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out.

Um dos precursores e catalizadores no processo de evolução do conceito de privacidade foi certamente o Código de Defesa do Consumidor, que estabeleceu uma proteção integral da pessoa nas relações de consumo, seja dos seus interesses econômicos, seja da sua integridade e personalidade. Ademais, o caráter principiológico das suas normas tem se mostrado aberto o suficiente para oferecer soluções para os novos conflitos relacionados à tecnologia da informação, servindo de base para a jurisprudência referente à violação dos dados pessoais, conforme já exposto neste capítulo.

Vê-se, assim, que a capacidade do Código de Defesa do Consumidor de se adaptar a novas demandas e de oferecer novas respostas foi fundamental para o desenvolvimento contínuo de mecanismos de proteção da personalidade do consumidor, inclusive contra os riscos advindos do processamento de dados pessoais[216].

Assim, após a análise teórica da legislação e da doutrina acerca do tema no Brasil, faz-se necessária a análise jurisprudencial, objetivando buscar a efetividade da legislação brasileira.

2.2.3.1. Sistema de *Scoring*

Um dos casos mais falados na mídia, e que gerou milhares de ações judiciais no Brasil, foi o caso do sistema de *Scoring*. A discussão central era se violaria a privacidade ter seus dados avaliados por um sistema de *Scoring*. O STJ sumulou o assunto (Súmula 550) a qual dispõe que:

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo[217].

2019.

[216] MENDES, Laura Schertel - **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014, p. 204.

[217] BRASIL. Superior Tribunal de Justiça. **Súmula 550**. Disponível em < http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 02 fev. 2020.

Sobre a legalidade da utilização do mencionado sistema *credit scoring*, reitera-se o que foi dito na decisão, no sentido de que se trata de uma prática comercial lícita, autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei nº 12.414/2011, cuja utilização prescinde do consentimento prévio e expresso do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico.

Assim, com esta decisão, afastando a ideia de que não se trata de um banco de dados, o sistema de *scoring* pôde continuar vigente, e pelo fato da decisão ter interpretado não ser o sistema de *scoring* um banco de dados, não terá aplicação da LGPD, de modo que é bem provável que a decisão não será reavaliada.

2.2.3.2. Recurso em Mandado de Segurança nº 55.019/DF39

Ainda, cita-se o Recurso em Mandado de Segurança nº 55.019/DF39[218]. O referido Mandado de Segurança é de extrema relevância para esta pesquisa pois envolve proteção de dados e cooperação internacional.

A recorrente, *Yahoo do Brasil*, alega que tem direito líquido e certo de não cumprir decisão judicial que determinou a quebra de sigilo telemático da conta de e-mail *"j_castanheira@yahoo.com"*. Sustentou a ilegalidade da decisão judicial que determinou a quebra sob o argumento de ausência de indícios suficientes de autoria da prática delitiva, bem como de não ser responsável pelo fornecimento de dados que não estão sob sua guarda, mas sim sob a responsabilidade da empresa estrangeira *Yahoo Holdings Inc*.

Os fundados indícios da ocorrência do ilícito, dizem respeito à suposta violação do sigilo de informações relativas ao *Caso FCVS*, quando do envio de um e- mail por parte de Fábio Ferreira Cleto, então Vice-Presidente da Caixa Econômica Federal (CEF), para Jailton Zanon de Oliveira, então Diretor Jurídico do mesmo ente, com cópia para Jorge Hereda - à época, Presidente da instituição.

A medida justificava-se, pois com progresso das investigações, percebeu-se que o responsável por esse domínio junto ao registro seria o titular da conta de e-mail j_castanheira@yahoo.com, isto é, Joaquim Eduardo Castanheira. Por fim, o

[218] BRASIL. **Recurso em Mandado de Segurança Nº 55.019/DF39**. Disponível em < http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

período solicitado é o interregno entre 24 de setembro e 11 de dezembro de 2011.

O acórdão se harmoniza com o entendimento do Superior Tribunal de Justiça que preferiu julgado situação análoga à dos autos, envolvendo a empresa *FACEBOOK*, entendeu pela prescindibilidade de cooperação internacional, na hipótese de o pedido de quebra de sigilo telemático ser direcionado a empresa localizada no Brasil e, nessa condição, submetida à legislação brasileira

O entendimento pacificado é que por estar instituída e em atuação no país, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo.

A requisição de serviços à recorrente, enquanto provedora da conta de e-mail do investigado, estabelece, satisfatoriamente, o modo de realizar a interceptação de dados, não cabendo à destinatária da medida deixar de cumpri-la, pelo argumento de suposta ofensa a direitos fundamentais de terceiro.

2.2.3.3. Recurso Especial nº 1.660.168/RJ

Outro caso envolvendo provedores de internet é envolvendo a autora Denise Pieri Nunes e as empresas *Google Brasil Internet Ltda*, *Yahoo do Brasil Internet Ltda* e *Microsoft informática Ltda*[219].

Denise pleiteou a desindexação nos resultados das aplicações de busca mantidas pelas recorrentes de notícias relacionadas às suspeitas de fraude no XLI Concurso da Magistratura do Estado do Rio de Janeiro.

Na inicial, a recorrida alega que a indexação desses conteúdos seria causa de danos a sua dignidade e a sua privacidade e, assim, requer a filtragem dos resultados de buscas que utilizem seu nome como parâmetro, a fim de desvinculá-la das mencionadas reportagens.

Na mesma linha da decisão apontada acima, após inicialmente deferir a medida liminar pleiteada pela recorrida, julgou improcedente o pedido, por entender que as aplicações de buscas na internet não são responsáveis pelo conteúdo das notícias encontradas. O Tribunal, por sua vez, reformou a decisão para condenar as

[219] BRASIL. **Recurso Especial Nº 1.660.168/RJ44**. Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

recorrentes a filtrarem os resultados de busca que contivesse menção à recorrida.

As empresas interpuseram Recurso Especial.

Neste caso em específico, foi utilizado pela relatora Ministra Nancy Andrighi, para embasar seu voto, uma decisão de um caso na Europa, que vale a pena citar:

> Em 05/03/2010, M. Costeja González, cidadão espanhol, apresentou na Autoridade Espanhola de Proteção de Dados Pessoais – AEPD uma reclamação contra a La Vanguardia Ediciones SL, a Google Spain e a Google Inc. Alegava que, nos resultados das buscas feitas pelo Google com seu nome, obtinha menção a duas páginas do jornal da La Vanguardia de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de uma execução fiscal de dívidas junto à Segurança Social. Assim, pedia que: (i) La Vanguardia suprimisse ou alterasse referidas páginas; e (ii) Google suprimisse ou ocultasse os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa. A autoridade espanhola indeferiu o pedido relacionado à La Vanguardia, mas deferiu com relação à Google, ordenando que essa empresa promovesse a exclusão solicitada.[220]

A decisão supramencionada foi submetida à Justiça espanhola e, como havia questionamento sobre o alcance de legislação da União Europeia, o processo foi remetido ao Tribunal de Justiça Europeu. Em 13 de maio de 2014, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção de dados pessoais, mencionado Tribunal decidiu que:

> Um provedor de aplicação de buscas deve ser considerado responsável pelos dados pessoais, nos termos da legislação europeia; A responsabilidade existe mesmo quando o servidor do provedor de aplicação de buscas se encontra fora do território europeu; Preenchidos os requisitos legais, um provedor de aplicação de buscas é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as conexões a outras páginas web publicadas por

[220] UNIÃO EUROPEIA. **Acórdão Do Tribunal De Justiça Europeu.** Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=905559>. Acesso em: 22 jan. 2020.

> terceiros e que contenham informações sobre essa pessoa, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita; O indivíduo, ao exercer seu direito ao esquecimento, não pode causar prejuízo a outra pessoa. Em princípio, esse direito prevalece sobre o interesse econômico do buscador e sobre o interesse público em acessar a informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse caso se houver razões especiais (por exemplo, se o requerente houver desempenhado relevante papel na vida pública).

Todavia, em que pese o julgado contrariar a jurisprudência do STJ, o ministro entendeu que o Tribunal de Justiça Europeu parte de pressupostos legais muito distintos daqueles existentes no País. Destacou, ao menos na época, que o mais importante é a ausência de uma lei geral que disponha sobre a proteção de dados pessoais dos cidadãos brasileiros.

Destacou a importância acerca do direito ao esquecimento, porém, pontuou que somente quando as circunstâncias assim determinarem. E, concluiu que "*não há fundamento legal que permita impor aos provedores de pesquisa a obrigação de eliminar do seu sistema os resultados que apontem para uma foto ou texto específico, sob a alegação de implementar o direito ao esquecimento de qualquer requerente.*

Posteriormente, em agosto de 2017, o Ministro Marco Aurélio Bellizze em voto-vista proferiu julgado contrariando a jurisprudência construída pelo STJ, dando provimento ao pedido da autora, o que foi acompanhado pelos demais ministros, sob o principal argumento de que "*não se trata de efetivamente apagar o passado, mas de permitir que a pessoa envolvida siga sua vida com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca"*, o que denota grande avanço do judiciário brasileiro ao longo dos anos.

2.2.3.4. Recurso Especial nº 1.348.532/SP

Neste caso, a Associação Nacional de Defesa da Cidadania e do Consumidor - ANADEC ajuizou ação civil pública contra HSBC BANK BRASIL S.A. - Banco Múltiplo, pleiteando a declaração de nulidade de uma das cláusulas do

contrato de prestação de serviços de emissão, utilização e administração do cartão de crédito oferecido pelo réu. Esclareceu que consta nas condições gerais cláusula abusiva, à luz do Código de Defesa do Consumidor e da legislação Civil[221].

O julgado asseverou que:

> o réu "fere o direito do consumidor, ao inserir em seus contratos de adesão cláusula autorizando o fornecimento, digamos o repasse, aos seus parceiros (todas as empresas com quem as rés mantêm contrato ou convênio para oferecer serviços/produtos) e a todo o conglomerado (empresas do grupo do qual faz parte a ré), dos dados cadastrais (pessoais e de consumo fornecidos quando da contratação exclusiva com a ré)"[222].

Concluiu que a autorização constante na cláusula impugnada, na qual o consumidor "*autoriza (embora obrigado, por meio da assinatura do contrato de adesão) que seus dados cadastrais sejam repassados a terceiros, no país ou no exterior, mostra-se nula de pleno direito, por ofender o ordenamento jurídico".*

O juízo sentenciante acolheu o pedido, considerando abusiva a cláusula destacada na ação civil, condenando o réu a não mais inseri-la em seus contratos ou que previsse autorização compulsória de conteúdo equivalente, devendo, ainda, providenciar nova redação para o documento, em 30 (trinta) dias, sob pena de multa diária.

O réu interpôs apelação. O Tribunal de Justiça do Estado de São Paulo deu parcial provimento, mantendo a decisão, no mérito acerca do reconhecimento da abusividade.

Em seguida, foi interposto recurso especial pelo réu, alegando a inexistência de ilegalidade da cláusula contratual questionada nos autos, uma vez que não se vislumbra qualquer violação à intimidade ou à vida privada dos consumidores. Destaca que os consumidores autorizam a transferência de seus dados cadastrais, nos termos daquela cláusula, tratando-se de cadastro positivo do

---

[221] BRASIL. **Recurso Especial Nº 1.348.532/SP47.** Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

[222] BRASIL. **Recurso Especial Nº 1.348.532/SP47.** Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

consumidor, que contém dados correntes e nada sigilosos.

Assevera, ademais, que não se verifica violação à intimidade ou mesmo ilegalidade do contrato, porque, no ato da assinatura do termo de adesão, o cliente recebe as condições gerais, tendo pleno conhecimento de seus dos termos.

Argumenta que o Código de Defesa do Consumidor não proíbe a elaboração, organização, consulta e manutenção de bancos de dados sobre consumidores e sobre consumo, e que a troca de informações ocorre em prol do próprio consumidor, para a concessão de crédito, sendo, ainda, restrita às empresas do grupo HSBC.

Disse ainda que da mesma forma o ordenamento não veda o compartilhamento das informações cadastrais com órgãos de cadastro negativos de crédito, pois que o próprio CDC considera os bancos de dados como entidades de caráter público.

Reitera que nenhuma ilegalidade há no repasse de dados objetivos para essas entidades, que registram e arquivam as informações que lhe são passadas pelos bancos ou de que tenham conhecimento por iniciativa própria, em regra, referentes a aspectos relevantes à concessão de crédito aos clientes das instituições associadas.

Por fim, o STJ concluiu que é abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.

Ainda, definiu que a cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança.

De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.

2.2.3.5. *Cambridge Analytica*

Um outro caso de grande importância, mas desta vez envolvendo o Brasil, foi uma multa de R$ 6.600.000,00 (seis milhões e seiscentos mil reais) ao *Facebook* pelo vazamento de dados de ao menos 443.000 usuários brasileiros. A decisão foi do Ministério da Justiça e Segurança Pública que, por meio do Departamento de Proteção e Defesa do Consumidor, aplicou a multa em razão do compartilhamento indevido de dados de usuários brasileiros no caso *Cambridge Analytica*.

O caso começou a ser investigado depois de ser noticiado que brasileiros também tiveram seus dados compartilhados sem permissão pela consultoria de *marketing* político *Cambridge Analytica*. Fundada nos Estados Unidos, a consultoria que trabalhou para a campanha de Donald Trump, foi acusada em março de 2019 de ter feito o maior roubo de dados da história do *Facebook.* Na época, a empresa de Mark Zuckerberg admitiu “violações das regras” e baniu a empresa na rede social. Meses depois, os Estados Unidos multaram o *Facebook* em US$ 5.000.000.000,00 (cinco bilhões de dólares), valor recorde no setor de tecnologia na época.

No Brasil, o processo aberto investigou se houve violação dos dados pessoais dos consumidores e se alguém obteve acesso indevido a essas informações. O Departamento de Proteção e Defesa do Consumidor concluiu então que houve prática abusiva por parte do *Facebook*. De acordo com a decisão, “resta evidente que dados dos cerca de 443.000 usuários da plataforma estavam em disposição indevida pelos desenvolvedores do aplicativo “*thisisyourdigitallife*”. O aplicativo é um teste psicológico cujas respostas de milhares de pessoas que o fizeram teriam sido utilizadas para “finalidades no mínimo questionáveis”, segundo a decisão.

Ainda de acordo com a decisão, houve falha na informação adequada aos usuários do *Facebook* sobre as consequências do padrão de configuração de privacidade em relação aos dados compartilhados.

Após a decisão do processo, o *Facebook* até a conclusão da pesquisa não havia sido intimado, portanto, cabendo recurso. Por meio de sua assessoria de

imprensa, a empresa enviou uma nota afirmando está focada "*em proteger a privacidade das pessoas*" e que tem feito mudanças na plataforma, "*restringindo as informações que desenvolvedores de aplicativos podem acessar. Não há evidência de que dados de usuários no Brasil tenham sido transferidos para a Cambridge Analytica. Estamos avaliando nossas opções legais sobre este caso*." A nota foi acrescentada ao texto após a publicação da primeira versão desta reportagem[223].

Assim, após as considerações propostas no capítulo 2, partiremos para uma análise comparativa dos elementos determinantes, quais sejam: Sanções Administrativas, da Cooperação Internacional e Controle Judicial na União Europeia e no Brasil.

[223] ROSSI, Marina. Brasil multa Facebook em 6,6 milhões de reais pelo vazamento de dados no caso Cambridge Analytica**. EL PAIS**. <https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html>. Acesso em: 22 jan. 2020.

CAPÍTULO 3: ANÁLISE COMPARATIVA DOS ELEMENTOS DETERMINANTES DA PROTEÇÃO DE DADOS NA UNIÃO EUROPÉIA E NO BRASIL

Nesta altura da pesquisa, já foram apresentados o contexto histórico da Lei Geral de Proteção de Dados no Brasil e do Regulamento Geral de Proteção de Dados na União Europeia, assim como, no Capítulo 2, os elementos determinantes da Cooperação Internacional, Sanções Administrativas no âmbito da RGPD e da LGPD bem como o Controle Judicial.

O avanço tecnológico alimentou a digitalização de nossas sociedades por infraestruturas cada vez mais poderosas, baseadas em dispositivos digitais e programas. Atualmente a comunicação se tornou principalmente comunicação digital e, consequentemente, a informação tornou-se fácil de processar e armazenar através de “dados”, o que é ao mesmo tempo fluido e persistente.

A lógica, por exemplo, por detrás da “big data”, é que quanto mais se sabe, melhor se pode controlar os processos sociais e orientar o progresso da sociedade. "*Big Data*" parece ser uma “bola de cristal" que permite que aqueles que a usam não apenas olhem para o futuro, mas também obter informações que lhes permitam moldá-las de acordo com suas necessidades[224].

Stefano Rodotá[225] destaca que:

> “O ambiente no qual a noção de privacidade passa assim a ser caracterizado pelos três paradoxos já enunciados e por quatro tendências que podem ser sintetizadas da seguinte forma: Do direito de ser deixado só ao direito de manter controle sobre as informações que me digam respeito; Da privacidade ao direito à autodeterminação informativa; Da privacidade à não-discriminação Do sigilo ao controle

A proteção de dados é necessária em uma sociedade democrática para sustentar uma democracia vívida. O direito à não discriminação é igualmente importante. Não é por acaso que o Tribunal de Justiça da União Europeia, em dois

---

[224] GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de. **Reforming European Data Protection Law**. Law, Governance and Technology Series 20. Springer Netherlands, 2015, p. 24.
[225] RODOTÁ, Stefano. **A vida na sociedade da vigilância** – A privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro. Ed. Renovar, 2008, p. 97.

casos recentes relacionados a perfis invocaram a legislação sobre proteção de dados e antidiscriminação para proteger os direitos dos cidadãos[226].

A lei de proteção de dados é feita para facilitar o livre fluxo de informações, salvaguardando os dados pessoais. Nesse sentido, privacidade é uma questão de opacidade enquanto a proteção de dados está relacionada transparência[227].

Uma das mais importantes novidades no Brasil é a tramitação da PEC nº 17/2019, que altera a Constituição da República Federativa do Brasil de 1988 para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais[228].

Já o RGPD, introduz um novo direito do titular, sendo o direito de exigir do controlador de dados que ele exclua os dados pessoais do usuário ou, mais relevante para atividades *online*, que o controlador de dados pare de copiar ou replicar tais dados.

Assim, considerando a imensidão de novidades trazidas pela LGPD e pela GDPR, alterando o *status quo* dos dias atuais da proteção de dados em todo o mundo e a sua importância em um Estado Democrático, apresentar-se-á um quadro comparativo abaixo com as principais previsões da LGPD e GDPR e suas similaridades ou diferenças.

Quadro comparativo LGPD-GDPR

LGDP	GDPR
Sanções administrativas Previsão: Art. 52 As sanções vão desde advertências até multas pecuniárias de 2% sobre o faturamento, em caso de empresas, até R$	**Sanções Administrativas** Previsão: Art. 83 As sanções são de EUR 10.000.000,00 (dez milhões de euros) até 4% do faturamento, em caso de empresas, sem limite para pessoas

[226] GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de. **Reforming European Data Protection Law**. Law, Governance and Technology Series 20. Springer Netherlands, 2015, p. 36.
[227] GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de. **Reforming European Data Protection Law**. Law, Governance and Technology Series 20. Springer Netherlands, 2015, p. 36.
[228] CÂMARA DOS DEPUTADOS. **Proposta de Emenda Constitucional 17/2019**. Disponível em < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 02 fev. 2020.

50.000.000,00 (cinquenta milhões de reais);	jurídicas.
Tratamento de dados sensíveis Previsão: Art. 11 Pela LGPD, é autorizado o tratamento de dados pessoais sensíveis, nas hipóteses previstas no artigo 11 da LGPD.	**Tratamento de dados sensíveis** Previsão: Art. 9 Pela GDPR, é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, com algumas exceções
Tratamento de dados de menores Previsão: Art. 14 A LGPD traz o tratamento de dados de menores de forma genérica, permitindo o tratamento de dados, desde que realizado no melhor interesse do menor.	**Tratamento de dados de menores** Previsão: Art. 8 O tratamento é lícito a partir dos 16 anos. Caso seja menor de 16 anos, tratamento só será lícito com o consentimento dos responsáveis. É permitido à cada Estado-Membro permitir o tratamento sem consentimento para crianças a partir dos 13 anos.
Políticas de Proteção de dados Previsão: Art. 50 Os controladores e operadores recebem maior liberdade para formular regras de boas práticas e de governança que estabeleçam as condições de tratamento de dados.	**Políticas de proteção de dados** Previsão: Art. 24 O responsável pelo tratamento de dados deve aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o regulamento, sob pena de ser responsabilizado.
Responsabilização dos agentes Previsão: Art. 42 O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.	**Responsabilização dos agentes** Previsão: Art. 82 Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do regulamento tem direito a receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.
Comercialização de Dados Não há previsão	**Comercialização de dados** Previsão: Artigo 21 Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
Controlador e operador Previsão: Art. 39 O operador deverá realizar o tratamento segundo as instruções fornecidas pelo	**Controlador e operador** Previsão: Art. 28 Na GDPR, o controlador é denominado de “responsável” (na GDPR – PT), que é o

controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.	responsável pelo tratamento, que recorre ao subcontratante, que é o operador na LGPD. Para tanto, os subcontratantes devem oferecer garantias suficientes de medidas técnicas e organizativas adequadas de segurança do dado tratado.
Relatório de impacto Previsão: Art. 38 A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.	**Relatório de Impacto** Previsão: Art. 35 Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais.
Transferência internacional de dados Previsão: art. 33 A transferência internacional de dados é autoriza em casos específicos previsto nos incisos do artigo 33.	**Transferência internacional de dados** Previsão: Art. 44 A transferência de dados só é permitida se aprovada por uma comissão, avaliando, dentre vários princípios, o nível adequado de proteção que o país oferece.
Órgão regulador Previsão: art. 55 Autoridade Nacional de Proteção de Dados Foi criada a Autoridade Nacional de Proteção de Dados, sendo composto por 5 diretores, escolhidos pelo Presidente da República e por ele nomeado após aprovação no Senado Federal, com mandado de 4 anos e um Conselho Nacional de Proteção de Dados Pessoas e Privacidade.	**Órgão regulador** Previsão: art 68 Comitê Europeu para a Proteção de Dados Foi criado um Comité Europeu para a proteção de Dados como organismo da União, que é composto por um diretor da autoridade de controle de cada Estado-membro.
Compliance Previsão: Art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.	***Compliance*** Previsão: Art. 40 Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.

Fonte: Elaborado pelo autor a partir das duas normas acima citadas.

Assim, melhor compreendido o estudo até aqui, abaixo realizar-se-á uma análise comparativa dos elementos determinantes já apresentados no Capítulo 2, em relação à Proteção de Dados na União Europeia e no Brasil.

No Capítulo anterior buscou-se apresentar alguns casos objetivando conhecer os precedentes na União Europeia e no Brasil acerca de proteção de dados.

A RGPD na União Europeia está vigente desde maio de 2018. Assim, considerando que não há até a presente data muitos casos envolvendo a RGPD, apresentou-se um panorama dos casos mais midiáticos envolvendo a antiga Lei de Proteção de Dados, a Diretiva nº 95/45/CE.

No Brasil, todas as decisões envolvendo proteção de dados foram baseadas em leis esparsas, que em seu bojo tratavam sucintamente sobre proteção de dados.

Nesse cenário, é imprescindível uma análise comparativa das legislações e decisões envolvendo proteção de dados na União Europeia e no Brasil, que será feito inicialmente pela Cooperação Internacional.

3.1. Cooperação Internacional

A Cooperação Internacional está de certo modo interligado com a ideia de transnacionalidade. Isto porque, a importância da Cooperação Internacional existe em virtude da crescente necessidade por legislações transnacionais, e é em razão desta crescente necessidade que cada vez mais se torna necessário falar em “Cooperação Internacional”.

Conforme já mencionado no Capítulo 1, Paulo Marcio Cruz e Carla Piffer, definem “transnacionalidade” como os novos espaços públicos não vinculados a um território específico, que perpassam a ideia tradicional de Nação Jurídica, aceitam a pluralidade como premissa e possibilitam o exercício de poder a partir de uma pauta axiológica comum consensual destinada a viabilizar a proposição de um novo pacto de civilização[229].

[229] CRUZ, Paulo Márcio; BODNAR, Zenildo. A transnacionalidade e a emergência do Estado e do Direito transnacionais. **Revista eletrônica do CEJUR**, v. 1, n. 4, 2009. disponível em <https://revistas.ufpr.br/cejur/article/download/15054/11488>. Acesso em: 20 out. 2019.

Deste modo, ao tratar da Legislação Geral de Proteção de Dados em um mundo totalmente conectado, é imprescindível mencionar a ideia da transncionalidade, principalmente quando o assunto se refere a “dados”. As grandes empresas que tratam a maior quantidade da dados são empresas transnacionais.

De certo modo Paulo Marcio Cruz e Zenildo Bodnar já abordaram esta ideia:

> Em outras palavras, a Sociedade em rede conectada e cada vez mais *on line*, formada a partir da “globalização” promovida pela hegemonia capitalista consolidada a partir de 1989, remete a um “mundo novo”, uma espécie de continente não investigado que se abre a uma terra de ninguém transnacional, a um espaço intermediário entre o nacional e o local[230].

No mesmo artigo, os autores ainda indagam se as tecnologias de informação podem nos ajudar a propor, teoricamente, o necessário espaço público transnacional do século XXI. Concluem que é difícil responder a essa pergunta, mas defendem que seguramente elas permitiriam uma associação mais imediata dos cidadãos nas fases da proposta, da decisão e do controle.

Pelo que se está percebendo, as tecnologias de informação estão cada vez mais exigindo uma legislação transnacional, pois num espaço global, onde cada país legisla e trata seus dados de acordo com suas leis, o que se percebe é uma divergência de cultura gigantesca na aplicação de penalidades pela mesma infração em países diferentes, assim como no caso do *Facebook,* onde em um país a multa pode alcançar bilhões de dólares norte-americanos, e no Brasil a penalidade é significativamente menos severa. O que se acaba esquecendo é que o mesmo dado tratado no Brasil pode estar circulando na Europa, e vice-versa, e estas empresas analisarão sob a ótica estatística em quais dados é menos oneroso eventual penalidade no que se refere à tratamento de dados.

Em relação ao que dispõe a legislação no que se refere à Cooperação Internacional, o artigo 33 da Lei Geral de Proteção de Dados Brasileira autoriza a

---

[230] CRUZ, Paulo Márcio; BODNAR, Zenildo. Globalização, transnacionalidade e sustentabilidade. **Itajaí: Univali**, 2012. Disponível em < https://www.univali.br/vida-no-campus/editora-univali/e-books/Documents/ecjs/E-book%202012%20GLOBALIZA%C3%87%C3%83O,%20TRANSNACIONALIDADE%20E%20SUSTENTABILIDADE.pdf>. Acesso em: 02 fev. 2020, p. 32.

transferência internacional de dados pessoais em alguns casos específicos, sobretudo quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, bem como quando a transferência resultar em compromisso assumido em acordo de cooperação internacional[231].

Com isso, denota-se uma preocupação da LGPD em relação à Cooperação Internacional, de modo que tal preocupação é compatível com o momento atual, afinal, o mundo está conectado, e a transferência de dados do Brasil para outros países ou de outros países para o Brasil ocorre diariamente, o que é facilmente analisado nas redes sociais que, em sua maioria, são de servidores fora do Brasil.

No que se refere à RGPD da União Europeia, Zeller, Trakman e Walters[232] destacam que há circunstâncias em que as leis de um terceiro país podem diferir significativamente das leis da União Europeia, mas que os dados ainda podem ser transferidos, desde que respeitadas algumas regras.

Percebe-se, aqui, maior rigor para a transferência de dados para outros países, ou seja, não basta um país manifestar interesse nos dados, ele tem que requerer e a União Europeia através do seu órgão regulador, que irá aprovar ou não a transferência de dados.

Por exemplo, o controlador de dados, responsável pela informação que será transmitida, através de regras corporativas vinculativas, pode estabelecer um acordo para facilitar a transferência dos dados. Além disso, quando um acordo for aprovado ou for emitida algum tipo de certificação aprovada e as garantias da lei forem atendidas, os dados pessoais podem ser transferidos para fora da União Europeia.

Em resumo, o alcance do RGPD é bastante extenso, e ampliou o alcance trazida pela antiga Diretiva nº 95/46/CE[233] que figurava como a Lei de Proteção de

---

[231] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 33, VI – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[232] ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 69.

[233] Diretiva 95/46/CE é uma legislação do Parlamento Europeu e do Conselho, de 24 de Outubro de

Dados antes da aprovação do GDPR.

Tal ampliação trouxe também maior proteção aos dados que circulam na União Europeia, não permitindo que qualquer pessoa possa ter acesso.

Acredita-se que a lógica da LGPD seja a mesma, porém, a verdade é que a legislação brasileira está mais “leve” e não exige um tratamento mais robusto.

A legislação brasileira, ainda, prevê no capítulo IX, Seção I, a criação de uma Autoridade Nacional de Proteção de Dados[234]. Dentre as competências da ANPD, uma delas é promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional[235].

A legislação Europeia traz a ideia de um Comitê que decidirá pela União Europeia, mas também autoriza a fiscalização pelo Estado-Membro do responsável pelo tratamento de dados ou o subcontratante, obrigando-os a manter os registros de suas atividades[236].

Em razão da Supranacionalidade da União Europeia, as multas são impostas pela autoridade de controle de cada Estado-Membro:

> A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo nos termos do presente regulamento[237].

Inclusive, o artigo 83 traz a ideia de que cada autoridade de controle assegura que a aplicação de multas relativamente a violações do regulamento é, em

---

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: 16 jan. 2020.

[234] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-A – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[235] BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 55-J, IX – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

[236] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 82 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez 2019.

[237] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 148 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez 2019.

cada caso individual, efetiva, proporcionada e dissuasiva. Ou seja, cada país terá sua unidade de controle do ato administrativo, para apuração das multas.

À título de exemplo, o sítio eletrônico *Mydataprivacy*[238], com domínio na Europa, consta em seu rodapé como a unidade de controle a *Comissão Nacional de Proteção de Dados (CNPD)*, destinando para o sítio eletrônico "*https://www.cnpd.pt/".*

Por fim, o artigo 51 dispõe que cabe a uma ou mais autoridades públicas independentes, a responsabilidade pela fiscalização da aplicação do regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União.

Assim, em que pese a GDPR Europeia ser uma legislação transnacional, aplicável em toda União Europeia, cada Estado-Membro deve ter sua autoridade de controle para aplicação das penalidades.

A Lei de Proteção de Dados da União Europeia poderá ser aplicada mesmo que as operações de mecanismos de busca sejam realizadas por meio de uma filial ou escritório de divisão em qualquer Estado-Membro da União Europeia, ainda que a empresa principal tenha origem e esteja sediada fora da União Europeia, conforme já mencionado acima.

Portanto, em termos práticos, o GDPR pode ser interpretado como não apenas uma Lei Regional, mas também Transnacional de Proteção de Dados, o que por si só auxilia na Cooperação Internacional de Proteção de Dados. Destaca Zeller, Trakman e Walters:

> Por exemplo, quando registradores e registros estabelecidos fora da União Europeia prestam seus serviços de registro de nomes de domínio a pessoas físicas na União Europeia, o GDPR pode ser aplicado. Além disso, tanto a autoridade nacional de proteção de dados dos Estados membros como o Conselho Europeu de Proteção de Dados têm um papel no monitoramento da aplicação e implementação do RGPD[239].

---

[238] My Data Privacy. Disponível em <https://mydataprivacy.eu/o-regulamento/>. Acesso em: 23 jan. 2020.

[239]Tradução livre do autor. Texto original: "For example, when registrars and registrations established outside the European Union provide their domain name registration services to individuals within the European Union, the GDPR may apply. In addition, both the Member States' national data protection authorities and the European Data Protection Council have a role in monitoring the implementation

Ainda, conforme já mencionado, não poderá ser admitida a transferência para países em que não houver tratado de cooperação em matéria cível, o que dificultaria eventual medida de defesa dos direitos dos titulares, ainda que o país tenha legislação e fiscalização efetiva sobre proteção de dados pessoais.

Nestes aspectos (impactos transnacionais e internacionais), Paul Lambert em livro de sua autoria denominado *Understanding the New European Data Protection Rules,* trata no capítulo 33 especificamente sobre como funciona em relação aos dados saírem da União Europeia, principalmente quando empresas, visando reduzir custos, terceirizam serviços fora da União Europeia[240]:

> As organizações estão sob pressão cada vez maior para reduzir custos. Às vezes, isso pode levar em consideração a terceirização para países fora da UE. Quaisquer transferências, a menos que especificamente excluídas, são restritas. Além disso, a natureza global das atividades comerciais significa que as organizações como parte dos processos comerciais normais podem procurar transferir conjuntos particulares de dados pessoais para agrupar entidades que podem estar localizadas fora da UE. Pode haver situações semelhantes em que uma organização deseja fazer fluxos de dados transfronteiriços para agentes, parceiros ou processadores terceirizados.[241]

Assim, o autor explica que o Regulamento de Proteção de Dados controla e regula as transferências de dados da União Europeia para jurisdições fora da União Europeia. Essas transferências de dados para fora são denominadas de *Crossborder Transfers*[242].

---

and implementation of the RGPD". ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 69.

[240] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 351.

[241] Tradução livre do autor. Texto original: "Organizations are under ever-increasing pressure to reduce costs. This can sometimes involve consideration of outsourcing to countries outside of the EU. Any transfers, unless specifically excepted, are restricted. In addition, the global nature of commercial activities means that organizations as part of normal business processes may seek to transfer particular sets of personal data to group entities that may be located outside of the EU. There can be similar situations where an organization wishes to make trans-border data flows to agents, partners, or outsourced processors." ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019, p. 69.

[242] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC

Ressalta-se que esse tipo de procedimento tem aumentado muito, principalmente com o crescimento de segmentos *online* como o *eCommerce* e mídias sociais.

A LGPD é bem mais amena no tocante à aferição do nível de adequação do que o GDPR. Assim, se determinado país que pretende firmar tratado de cooperação com o Brasil for adequado para a GDPR, certamente deverá também assim ser considerado pela ANPD[243].

O que se observa, é que a LGPD traz algumas disposições parecidas coma GDPR da União Europeia, no entanto, de maneira mais breve e resumida, de modo que não abrange tantas hipóteses quanto a GDPR.

Assim, espera-se da ANPD que muitas lacunas sejam devidamente regulamentadas na via administrativa, destacando-se ainda mais a importância desta pesquisa para fins de auxiliar na construção necessária para implementação da LGPD.

Outrossim, conforme já disposto no Capítulo 1, os DPOs (*Data Protection Officers* ou Encarregados) e Autoridades Nacionais de vários países devem, num futuro relativamente próximo, iniciar atividades de cooperação e de intercâmbio. Essas trocas têm tudo para ser muito positivas, no sentido do estabelecimento de boas práticas, bem como no de gradual uniformização das normas infralegais a serem emitidas pelas várias autoridades.

Assim, a correta implementação da LGPD projetará o Brasil como país que se preocupa e regulamenta a proteção dos dados pessoais, seguindo a tendência internacional capitaneada pela GDPR.

Embora a lei brasileira, por si só, não garanta de imediato a transferência transfronteiriça de dados pessoais da Europa para o Brasil, futuramente ela poderá ser levada em consideração pela Comissão Europeia para avaliar se existe garantia de um nível de proteção adequado. Nesse contexto, tanto o responsável pelo tratamento (*data controller*, ou controlador), quanto o subcontratante (*data processor* ou processador) precisam estar adequados não só com a LGPD, mas também com a GDPR, caso haja interesse em exportar dados pessoais para fora da União

---

Press, 2017, p. 341.

[243] MACIEL, Rafael. Manual prático sobre a **Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18**. Editora RM Digital Education. Edição do Kindle.

Europeia.

Como a LGPD deu força total para que a ANPD regule a LGPD, o que por ora deve ser feito, em relação à Cooperação Internacional, é aguardar o início das atividades do órgão de proteção da LGPD, pois grande parte de sua regulamentação se dará em âmbito administrativo, já que a lei deixou em aberto diversas hipóteses.

3.2. Sanções administrativas

No que se refere às Sanções Administrativas, interessante notar que a LGPD é igualmente parecida com a GDPR em alguns aspectos. A LGPD trouxe diversas hipóteses de Sanções Administrativas pelo órgão regulador, de modo a dar maior segurança jurídica para quem tem seus dados tratados e inclusive para quem detém os dados pessoais.

As sanções poderão ser aplicadas de forma gradativa, isolada ou cumulativa, de acordo com o caso concreto[244]. A LGPD dispõe no artigo 52 que os agentes de tratamento de dados, em razão das infrações cometidas, ficam sujeitas à diversas sanções administrativas aplicáveis pelo órgão regulador.

Dentre as penalidades previstas na LPGD, a mais branda é a pena de advertência, prevista no inciso I do artigo 52, com indicação de prazos para adoção de medidas corretivas, o que deixa margem para que o órgão regulador possa agir de acordo com o caso concreto.

Neste ponto, a GDPR da União Europeia também prevê, no artigo 58, item 2, alínea a, que cada autoridade de controle pode aplicar advertências ao responsável pelo tratamento de dados. As penas pecuniárias são aquelas previstas nos incisos II e III da LGPD, que preveem multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração e multa diária, limitada também ao valor de R$ 50.000.000,00 (cinquenta milhões de reais).

Conforme já exposto acima, em que pese a sanção de R$ 50.000.000,00 (cinquenta milhões de reais) pareça uma pena expressiva, trata-se de uma

---

[244] MACIEL, Rafael. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais: Atualizado com a Medida Provisória nº 869/18.** RM Digital Education. Edição do Kindle.

penalidade consideravelmente leve, considerando que a penalidade, na verdade, é de 2% do faturamento da empresa, ou seja, para que a empresa seja multada em R$ 50.000.000,00 (cinquenta milhões de reais), a mesma terá que ter um faturamento de R$ 2.500.000.000,00 (dois bilhões e quinhentos milhões de reais). Para uma empresa com faturamento de R$ 2.500.000.000,00 (dois bilhões e quinhentos milhões de reais) anuais, R$ 50.000.000,00 (cinquenta milhões de reais) não surtirá o efeito coercitivo que se espera da LGPD.

Um outro exemplo, é uma empresa que tem o faturamento anual de até R$ 4.800.000,00 (quatro milhões e oitocentos mil reais), o que representa o faturamento de 99% das empresas no Brasil[245]. Esta empresa, em caso de violação de dados, poderá ser multada em até R$ 96.000,00 (noventa e seis mil reais), o equivalente a 2% do faturamento da pessoa jurídica.

Uma multa de R$ 96.000,00 (noventa e seis mil reais), para um desvio de dados de seus usuários, intencionalmente ou não, à primeira vista, ao que parece, não é algo que forçará as empresas a se protegerem mais, principalmente se o custo desta proteção for muito maior do que isso.

Em relação ao RGPD, as violações da RGPD estão sujeitas a multas administrativas de até EUR 10.000.000,00 (dez milhões de euros) ou, no caso de uma organização, até 2% do faturamento anual total do exercício financeiro anterior, o que for maior, em determinadas circunstâncias. Há previsão, também, de multas de até EUR 20.000.000,00 (vinte milhões de euros) ou, no caso de uma organização, até 4% do volume de negócios anual total do exercício financeiro anterior, o que for maior, quando violarem[246]:

> Os princípios básicos de processamento, incluindo condições de consentimento, de acordo com os Artigos 5, 6, 7 e 9.
>
> Os direitos dos titulares de dados.
>
> As transferências de dados pessoais para um destinatário em um país

[245] SEBRAE. Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD>. Acesso em: 30 jan. 2020.

[246] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Artigo 83 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez. 2019.

> terceiro ou país organização internacional.
> Quaisquer obrigações nos termos da lei do estado membro.
> Não cumprimento de uma ordem ou limitação temporária ou definitiva no processamento ou suspensão dos fluxos de dados pela autoridade supervisora de proteção de dados§ ou falha no fornecimento de acesso em: violação a Artigo 58°,n°1.

Ou seja, há penalidades mais brandas e mais severas, há depender do caso concreto.

Outrossim, em relação às multas por desconformidade com a ordem da autoridade supervisora de proteção de dados, a lei estabelece que o não cumprimento de uma ordem da autoridade supervisora de proteção de dados a que se refere o artigo 58 deve, de acordo com o item 2, sujeitará a multas administrativas até EUR 20.000.000,00 (vinte milhões de euros), ou, no caso de uma organização, até 4% do faturamento anual total do exercício financeiro anterior, o que for maior.

A marcante diferença entre as legislações de Proteção de Dados da União Europeia e Brasileira é o limite imposto pelo Brasil, de R$ 50.000.000,00 (cinquenta milhões de reais), enquanto a União Europeia não estabelece um limite, pois dependerá quase que exclusivamente do faturamento da empresa ou em conformidade com alguns requisitos previstos na lei.

Rafael Fernandes Maciel[247] defende a LGPD possua sanções pesadas, e que a legislação sopesa as punições àquelas empresas que possuem os cuidados mínimos com os dados pessoais dos titulares a elas confiados, e completa:

> [...] E é essa balança e compreensão de que incidentes de segurança são impossíveis de serem evitados completamente, que faz com que a regulamentação seja protetiva à privacidade sem impedir a inovação e os negócios forjados em informações pessoais. [...] os agentes de tratamento estão sujeitos à responsabilização civil pelo tratamento ilícito dos dados pessoais. Sem prejuízo, podem ser aplicadas sanções administrativas previstas no art. 52 da LGPD, aplicáveis pela autoridade nacional[248].

---

[247] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 52 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

[248] MACIEL, **Rafael Fernandes. Manual Prático sobre a Lei Geral de Proteção de Dados**

Patrícia Peck Pinheiro destaca que a versão nacional da Lei Geral de Proteção de Dados é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para subjetividade onde deveria ter sido mais assertiva.

Um exemplo disso ocorre em relação à determinação de prazos, pois enquanto o GDPR, na consideração 85, prevê prazos exatos, como de 72 (setenta e duas) horas, a LGPD prevê "prazo razoável"[249].

Ainda, sem prejuízo dos poderes corretivos das autoridades de supervisão da proteção de dados nos termos do artigo 58º, item 2, cada Estado-Membro pode estabelecer regras sobre se e em que medida multas administrativas podem ser impostas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.

Assim, na União Europeia existe uma legislação que prevê todas as hipóteses possíveis relacionadas à Proteção de Dados, mas deixa aberto aos países que quiserem adotar suas próprias regras legislarem sobre o assunto.

Importante frisar que em relação às penas, o RGPD da União Europeia não estipula a multa de EUR 20.000.000,00 (vinte milhões de euros) como seu limite, mas sugere, que a multa seja de até EUR 20.000.000,00 (vinte milhões de euros), ou seja, a autoridade de controle tem liberdade para decidir acerca da multa ou, no caso de empresas, de 4% sobre o faturamento total anual da empresa do exercício anterior, mesmo que ultrapasse os EUR 20.000.000,00 (vinte milhões de euros).

Ademais, a legislação Europeia prevê que se deve levar em consideração diversos fatores, tais como a natureza, a gravidade e a duração da infração, o caráter intencional da infração, as ações tomadas para mitigar os danos sofridos e o grau de responsabilidade. Além disso, se já houve ou não infrações anteriores, a maneira pela qual a infração se tornou conhecida pela autoridade supervisora de proteção de dados, a conformidade com as medidas ordenadas contra o controlador ou processador bem como qualquer outro fator agravante ou atenuante e, por fim

---

Pessoais (Lei nº 13.709/2018. RM Digital Education. 1ª Edição. 2019, Edição Kindle. Posição 1559.

[249] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais. Comentários à Lei n. 13.709/2018 LGPD.** Saraiva Educação. Edição do Kindle, 2018. Posição Kindle 254.

adesão a um código de conduta[250].

Para reforçar a aplicação das regras do Regulamento Geral de Proteção de Dados (RGPD), explica Paul Lambert[251] que devem ser aplicadas sanções, incluindo multas administrativas, por qualquer infração ao RGPD, além de, ou em vez de, medidas apropriadas impostas pela autoridade supervisora de proteção de dados de acordo com o RGPD. No caso de uma infração menor ou se a multa passível de ser aplicada constituir um ônus desproporcional para uma pessoa singular, pode ser emitida uma repreensão em vez de uma multa.

O que se percebe em relação ao sistema europeu, é que as sanções são mais firmes e parecem mais justas, de modo que a tendência é que grandes empresas que detém grandes quantidade de dados agirão mais ativamente na hora de decidir em investir na proteção dos dados pessoais tratados naqueles países.

Muito embora em relação a este ponto a legislação Brasileira e Europeia sejam parecidas, inclusive na “fórmula” para auferir o valor de uma penalidade, o fato de a legislação Europeia não ter imposto um limite na penalidade que poderá ser imposta, traduz-se em maior garantia para o órgão regulador exercer o seu poder dissuasório.

Outrossim, na União Europeia, quando o sistema jurídico do Estado-Membro não fornecer multas administrativas, o artigo pode ser aplicado de forma que a multa seja aplicada pela autoridade supervisora de proteção de dados competente e imposta pelos tribunais nacionais competentes, garantindo ao mesmo tempo que esses recursos legais sejam eficazes e tenham um efeito equivalente às multas administrativas impostas pelas autoridades de supervisão da proteção de dados.

Visando conferir maior segurança à proteção dos dados pessoais e objetivando não a aplicação de sanções administrativas, mas sim a segurança dos dados, a LGPD e a GDPR trazem a ideia do *compliance (*Programa de integridade*)*, que pode ser entendida como um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um

---

[250] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Consideração 148 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 12 dez 2019.
[251] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 251.

agente econômico e de qualquer um de seus sócios ou colaboradores[252].

Na doutrina surgem outros conceitos, como o elaborado por Vanessa Alessi Manzi[253] para quem *compliance* se constitui no "*ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da instituição, buscando mitigar o risco atrelado à reputação e ao regulatório/legal*".

Nesse passo, para Roberto Epifanio Tomaz[254] corporativamente *compliance* "*passou a identificar as ações, atitudes tomadas pela corporação, que são realizadas de acordo com as regras, éticas, legais e procedimentais, estabelecidas para regulação de suas atividades, tornando-se, portanto, sinônimo de postura correta na condução de seus negócios*".

Destarte o programa de *compliance* pode ser definido, como ponderam Ana Paula Candeloro, Maria Balbina Martins De Rizzo e Vinícius Pinho[255], como:

> Um conjunto de regras, padrões, procedimentos éticos e legais que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários; um instrumento capaz de controlar o risco de imagem e o risco legal, os chamados 'riscos de *Compliance*', a que se sujeitam as instituições no curso de suas atividades

Assim, em que pese não seja objeto do presente estudo, é de se salientar que o programa de *compliance*/integridade se tornou peça chave para que as empresas que realizam o tratamento de dados evitem sanções administrativas ou ao menos possam reduzir as penalidades caso a empresa possua o programa de integridade.

Além disso, uma forma preventiva de evitar as sanções é a prática de anonimização de dados. Bruno Bioni exemplifica em seu livro como na prática

---

[252] BRASIL. Guia Compliance – Versão Oficial**. Conselho Administrativo de Defesa Econômica – CADE.** Disponível em <http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-Compliance-versao-oficial.pdf>. Acesso em: 08 out. 2019.

[253] MANZI, Vanessa Alessi. **Compliance no Brasil**. São Paulo: Saint Paul Editora, 2008. p. 15.

[254] TOMAZ, Roberto Epifanio (org.). **Descomplicando o Compliance**. 1 ed. Florianópolis: Tirant Lo Blanch, 2018, p. 26.

[255] CANDELORO, Ana Paula P.; DE RIZZO, Maria Balbina Martins; PINHO, Vinícius. **Compliance 360º:** Riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012. p. 30

funcionaria a supressão e a generalização da anonimização de dados e, na tabela apresentada abaixo, o autor torna anônimo quatro dados.

Primeiro, *a supressão do CPF.* Por ser um identificador capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único, a sua disponibilização, ainda que parcial (por ex. cinco primeiros dígitos) não seria prudente.

Em seguida, a *generalização do nome completo.* Constaria apenas o prenome desde que fosse observado que os nomes da base de dados não são comuns. O objetivo é evitar que um nome possa ser atribuído a um indivíduo em específico.

Após, a *generalização da localização geográfica.* Em vez de disponibilizar o número completo do CEP, seriam divulgados apenas os seus primeiros dígitos. Assim, haveria uma localização menos detalhada, a fim de quebrar o vínculo de identificação desta informação com um sujeito.

Por fim, *a generalização da idade.* Em vez de divulgar a idade exata, seria divulgada a faixa etária para viabilizar a categorização dos indivíduos como jovens, adultos ou idosos (coluna e), e por outro lado, inviabilizar a sua individualização, dado o universo de pessoas que se enquadram naquela faixa etária[256].

A tabela ficaria da seguinte forma:

TABELA 1 - Base de Dados Relacionais Anonimizada:

Nome	**CPF**	**CEP**	**Faixa etária**	**Classificação/segmentação**
Bruno ~~dos santos~~	~~123.456-77~~	04055-~~000~~	18>	Jovem hipster
Bruno ~~dos santos~~	~~234.567-88~~	04055-~~111~~	18>	Jovem poupador
Bruno ~~dos santos~~	~~345.678-99~~	04055-~~222~~	18>	Jovem consumista
Bruno ~~Souza~~	~~456.789-10~~	01201-~~000~~	60<	Idoso com rentabilidade
Bruno ~~Souza~~	~~567.891-01~~	04201-~~111~~	60<	Idosa sem rentabilidade
Bruna ~~Schonber~~	~~222.333.44-55~~	04201-~~222~~	60<	Idosa com rentabilidade

[256] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 73.

Maria ~~Silva~~	~~157.890-88-66~~	09201-~~000~~	18<	Adulto desempregado
Maria ~~Silva~~	~~666.666.66-66~~	09201-~~000~~	18<	Adulto perfil executivo
Maria Sostenes	~~987.354.22-99~~	09201-~~222~~	18>	Jovem hipster

Fonte: BIONI, Bruno Ricardo. Proteção de Dados Pessoais: **A função e os limites do consentimento.** Rio de Janeiro: Forense, 2019, p.73.

Assim, a anonimização dos dados serviria também para evitar eventuais desvios de dados por *hackers*, evitando as penalidades da RGPD/LGPD. Todavia, Bruno defende que é mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível[257].

A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se com 100% (cem por cento) de eficiência, o anonimato das pessoas, na visão do autor, é um mito.

Para corroborar sua colocação, Bruno Ricardo Bioni menciona a pesquisa de *Arvind Narayanan* e *Vitaly Shmatikov* sobre o caso *Netflix Prize*, onde os autores reidentificaram diversas bases de dados anonimizados.

Os autores desenvolveram um algoritmo que calculava dentre outros fatores: a) quantos *bits* de informação seriam necessários para reverter o processo de anonimização; b) qual seria o melhor critério para a escolha de uma informação auxiliar, por exemplo, uma outra base de dados, para ser agregada para reverter o processo de anonimização e c) uma métrica sobre a probabilidade de acerto da reidentificação, evitando-se falsos positivos.

Na época, a *Netflix* havia criado um concurso que o desafio era melhorar o seu algoritmo de sugestão de filmes. Então a *Netflix* disponibilizou a sua base de dados com todas as avaliações dos filmes do seu catálogo entre 1998 e 2005, suprimindo os nomes dos usuários avaliadores e deixando somente a data e a nota de avaliação.

A fim de tornar o processo de reidentificação mais robusto, a *Netflix* utilizou de técnicas de randomização. Ela alterou algumas datas e *ratings* das

[257] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019, p. 73.

avaliações dos seus consumidores, o que aumentaria o risco de falsos positivos, a não ser pelo fato de o algoritmo dos pesquisadores ter sido projetado para isso.

Os pesquisadores rodaram tal algoritmo na base de dados disponibilizada, descobrindo que seria necessário entre 3 e 19 *bits* de informação para reverter o processo de anonimização. Esse *pool* de informações necessário estava publicamente disponível na *internet* e acessível na *Internet Movies Databases* (IMDB)[258].

Os pesquisadores cruzaram essas informações com a base de dados da *Netflix* correlacionando as datas das avaliações dos filmes e seus respectivos *scorings*. Assim, a peça faltante do quebra-cabeça, a identidade dos usuários da *Netflix*, foi desvendada com base nos nomes contidos nas avaliações do IMDB.

Mesmo assim, embora o autor do livro defenda que o método não é muito eficaz, ao menos é um método útil para fortalecer a segurança dos dados, que somado a outros métodos, pode gerar maior segurança jurídica e evitar o vazamento de dados.

Assim, após a conclusão acerca das Sanções Administrativas, passa-se à análise do Controle Judicial sobre os dados e a proteção de dados no Brasil e na União Europeia.

3.3. Controle Judicial

No Capítulo 2, realizou-se a apresentação dos elementos determinantes do Controle Judicial na União Europeia e no Brasil relacionadas à proteção de dados. Neste tópico será feita uma análise comparativa das decisões europeias e brasileiras no que se refere à proteção de dados pessoais, objetivando, em seguida, concluir se a LGPD e a RGPD estão em consonância com as decisões dos tribunais e de que modo as leis poderão ou estão contribuindo (no caso da União Europeia que já está vigente) para a segurança jurídica em relação à proteção de dados pessoais.

Em relação às possíveis demandas, a GDPR estabelece nos artigos 77 e seguintes o direito de apresentar reclamação a uma autoridade de controle, bem

[258] Site onde as pessoas compartilham suas impressões sobre filmes, utilizando-se na maioria das vezes, seus nomes reais. Disponível em <https://www.imdb.com/>. Acesso em: 12 jan. 2020.

como o direito à ação judicial contra uma autoridade de controle, dispondo que[259]:

> Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o presente regulamento. 2. A autoridade de controlo à qual tiver sido apresentada a reclamação informa o autor da reclamação sobre o andamento e o resultado da reclamação, inclusive sobre a possibilidade de intentar ação judicial nos termos do artigo 78º.

Ainda, a lei dispõe que, sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todas as pessoas singulares ou coletivas têm direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controle que lhes digam respeito, bem como os titulares dos dados têm direito à ação judicial se a autoridade de controle competente, nos termos dos artigos 55º e 56º, não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado nos termos do artigo 77º do RGPD.

Os recursos contra as autoridades de controle são interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidas e quando for interposto recurso de uma decisão de uma autoridade de controle que tenha sido precedida de um parecer ou uma decisão do Comitê. No âmbito do procedimento de controle, a autoridade transmite um parecer ou decisão ao tribunal.

Ainda, estabelece o direito à ação judicial contra o responsável pelo tratamento de dados:

> Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar reclamação a uma autoridade de controlo, nos termos do artigo 77º, todos os titulares de dados

[259] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR). Art. 77 e 78 –** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

> têm direito à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento. 2. Os recursos contra os responsáveis pelo tratamento ou os subcontratantes são propostos nos tribunais do Estado-Membro em que tenham estabelecimento. Em alternativa, os recursos podem ser interpostos nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual, salvo se o responsável pelo tratamento ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.

Já no artigo 83, a norma trata das condições gerais para aplicação de coimas (multas)[260], que são as penalidades em razão do descumprimento da Lei, e apontam uma análise mais subjetiva na aplicação da penalidade, conforme dispõe o item 2 e alíneas do referido artigo:

> Consoante as circunstâncias de cada caso, as coimas são aplicadas para além ou em vez das medidas referidas no artigo 58.o, nº 2, alíneas a) a h) e j).
> Ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte:
> a) A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos;
> b) O caráter intencional ou negligente da infração;
> c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares;
> d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25º e 32º;
> e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante;
> f) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos;

[260] Castigo ou pena que consiste num pagamento; sanção pecuniária. = MULTA "coima", in **Dicionário Priberam da Língua Portuguesa** [em linha], 2008-2013. Disponível em <https://dicionario.priberam.org/coima>. Acesso em: 23 out. 2019.

> g) As categorias específicas de dados pessoais afetadas pela infração;
> h) A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram;
> i) O cumprimento das medidas a que se refere o artigo 58º , nº 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria;
> j) O cumprimento de códigos de conduta aprovados nos termos do artigo 40º ou de procedimento de certificação aprovados nos termos do artigo 42º; e
> k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.

Nos itens seguintes (itens 4 e 5 do artigo 83 do RGPD) são estabelecidas multas de até EUR 20.000.000,00 (vinte milhões de euros), tema que será abordado a seguir. Por fim, destaca que os Estados-Membros estabelecerão as regras relativas às outras sanções aplicáveis em caso de violação do regulamento, previsto no artigo 84[261].

Deste modo, o que se percebe é que a legislação trata da possibilidade de ação judicial em diversas hipóteses, mas deixa margem para que cada Estado-Membro estabeleça suas sanções, dando maior liberdade para cada Estado decidir em seu âmbito local, porém, traz no seu texto algumas hipóteses de penalidades, caso o país não queira ou demore para legislar sobre, evitando-se assim uma lacuna na legislação.

Paul Lambert destaca que para qualquer infração à nova Lei de Proteção de Dados há uma penalidade que será imposta e, caso a penalidade seja desproporcional para a pessoa singular, pode ser emitida uma repreensão ao invés de uma multa, *in verbis*:

> Para reforçar a aplicação das regras do Regulamento Geral de Proteção de Dados (RGPD), devem ser aplicadas sanções, inclusive multas

[261] UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Art. 84 **–** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

> administrativas, por qualquer infração ao RGPD, além de, ou em vez de, medidas apropriadas impostas pela autoridade supervisora de proteção de dados nos termos do GDPR. No caso de uma infração menor ou se a multa passível de ser aplicada constituir um ônus desproporcional para uma pessoa singular, pode ser emitida uma repreensão em vez de uma multa[262].

Para que isso ocorra, devem ser analisados alguns aspectos, tais como a natureza, a gravidade e a duração da infração, o caráter intencional da infração, as ações tomadas para mitigar os danos sofridos e as eventuais infrações anteriores, bem como a adesão à um código de conduta (*compliance*)[263].

Assim, avaliar a LGPD pelo método comparativo é necessário tendo em vista a onda de invasão de *hackers* em bancos de dados de grandes empresas transnacionais como, por exemplo, a empresa Canvas, onde mais de 139 milhões de usuários tiveram seus dados vazados[264].

Destaca-se que os dados vazados foram obtidos por um “cibercriminoso” identificado como *GnosticPlayers* que, considerando todos os ataques já realizados por este *hacker*, somam mais de um bilhão de credenciais de usuários de 45 empresas que foram vazadas. Desde o início de 2019, dados de 932 milhões de usuários que foram roubados de 44 empresas ao redor do mundo, foram adicionados na *darkweb* pela *GnosticPlayers*[265].

O banco de dados do *Canvas* era protegido por um algoritmo chamado *bcrypt* – considerado um dos mais seguros que existem[266]. Ademais, o objetivo

---

[262] Traduçao direta do autor. Texto original: “To strengthen the enforcement of the rules of the General Data Protection Regulation (GDPR), penalties including administrative fines should be imposed for any infringement of the GDPR in addition to, or instead of, appropriate measures imposed by the data protection supervisory authority pursuant to the GDPR. In the case of a minor infringement, or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine”. LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 251.

[263] LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017, p. 251.

[264] FONSECA, Carol. Canva confirma invasão por hackers em sua plataforma. **Terra**. <https://www.terra.com.br/noticias/tecnologia/seguranca-digital/canva-confirma-invasao-por-hackers-em-sua-plataforma,2e9f83ba4d6c6221114ffc99145c3947j5jjavwb.html>. Acesso em: 23 jan. 2020.

[265] FONSECA, Carol. Canva confirma invasão por hackers em sua plataforma. **Terra**. <https://www.terra.com.br/noticias/tecnologia/seguranca-digital/canva-confirma-invasao-por-hackers-em-sua-plataforma,2e9f83ba4d6c6221114ffc99145c3947j5jjavwb.html>. Acesso em: 23 jan. 2020.

[266] FONSECA, Carol. Canva confirma invasão por hackers em sua plataforma. **Terra**. <https://www.terra.com.br/noticias/tecnologia/seguranca-digital/canva-confirma-invasao-por-hackers-em-sua-plataforma,2e9f83ba4d6c6221114ffc99145c3947j5jjavwb.html>. Acesso em: 23 jan. 2020.

deste (ou destes) *hackers,* conhecido como *GnosticPlayers*, ao que parece, é a comercialização dos dados[267], razão pela qual discutir os efeitos judiciais da LGPD e RGPD na aplicação de multas e sanções é tarefa imprescindível.

Ponto que se observa é que os titulares dos dados acabam não percebendo o impacto indireto que o vazamento de dados causa. É exatamente por estes vazamentos é que nossos telefones, e-mails, e diversos outros meios de comunicação são disponibilizados, as vazes ilegalmente, para empresas que prospectam clientes oferecendo seus serviços.

Este caso é um dos que, ao menos por ora, não teve nenhuma condenação em algum dos países onde se realiza o tratamento de dados, diferente do que acontece com empresas transnacionais como a *Google* e o *Facebook.*

Conforme apresentado no Capítulo 2, os casos *Google* e *Facebook* são os de maior incidência envolvendo dados, e a razão é justamente porque são as empresas que mais tratam dados em todo o mundo.

A *Google* tem aparecido na mídia com grande preocupação em reconstruir sua política de proteção de dados, embora defenda que seus dados são muito bem protegidos e que a empresa preza por esse tipo de proteção[268].

Grande parte dessa busca incansável por proteção dos dados tratados são as decisões observadas na União Europeia, que parece não pensar duas vezes antes de aplicar sanções em conformidade com a legislação.

Antes da RGPD, pode se perceber pelas decisões colacionadas no Capítulo 2, que a União Europeia já possuía uma legislação mais robusta em relação à proteção de dados, com aplicações de penalidades severas em relação ao assunto. A RGPD veio para suprir as lacunas que uma legislação datada de 1995 não poderia prever.

Enquanto a União Europeia já caminhava por um longo período de construção jurisprudencial com a Diretiva de 1995, o Brasil possuía poucas previsões em leis esparsas relacionadas à dados.

Assim, de outro lado, as decisões que se observa nos casos brasileiros

---

[267] ARBULU, Rafael. Hacker oferece 26 milhões de registros de usuário por US$ 5 mil em bitcoins. **Canaltech**. Disponível em: <https://canaltech.com.br/hacker/hacker-oferece-26-milhoes-de-registros-de-usuario-por-us-5-mil-em-bitcoins-135103/>. Acesso em: 23 jan. 2020.

[268] Termos de Privacidade do Google. Disponível em <https://privacy.google.com/?hl=pt_BR#>. Acesso em: 28 jan. 2020.

vão no sentido oposto. A jurisprudência do Superior Tribunal de Justiça com muita dificuldade reconhece a responsabilidade dos provedores de *internet* que tratam dados de milhões de brasileiros. Somente nos últimos anos é que as decisões passaram a proteger o titular dos dados.

Outrossim, realizada a análise dos julgados apresentados no Capítulo 2, percebeu-se uma grande dificuldade na construção da jurisprudência sobre proteção de dados no Brasil.

Até pouco tempo, as grandes corporações que detém os dados (*Yahoo, Facebook, Google*, etc.) no Brasil, eram vencedoras das demandas que objetivavam a exclusão de determinados termos da pesquisa dos seus provedores de internet. Tais precedentes que estão tomando forma no STJ estão cada vez mais buscando proteger o titular de dados que reclama alguma ilicitude ou desconforto no tratamento de seus dados pessoais.

Assim, observava-se grande divergência na jurisprudência brasileira e da União Europeia, no sentido de obrigar os provedores de internet a removerem conteúdo no qual a parte está requerendo a sua exclusão. No Brasil, a parte deve (ainda não há súmula sobre o assunto, mas conforme defendido acima, há decisões já em prol do titular de dados) apontar exatamente quem publicou para que o provedor possa excluir, não sendo responsabilidade direta do provedor. Na Europa, o provedor é responsável.

Grande parte desta linha de raciocínio, como se vê no julgado Recurso Especial nº 1.660.168/RJ, era a ausência de uma legislação de proteção de dados, como se tinha na Europa (Diretiva nº 95/CE).

Na União Europeia, já em 2009, por exemplo, no caso envolvendo a agência *Network Deutschland GmbH*, o Estado de Berlim multou a empresa *Deutsche Bahn* em EUR 1,1 bilhão , em 2009, sem a vigência da RGPD, ou seja, pode-se afirmar que a União Europeia já possui 11 anos de construção de precedentes em defesa dos dados pessoais.

Com a RGPD, a tendência é de multas mais severas, devendo ser observado os requisitos dispostos no art. 83, item 2. Então, seriam observados, no caso, a gravidade e a duração da infração e, em seguida, seria feita a análise do caráter intencional ou negligente da infração.

A *Deutsche Bahn* teve em 2019 (último dado divulgado)[269] um faturamento de aproximadamente EUR 45.000.000.000,00 (quarenta e cinco bilhões de euros). Se aplicada a penalidade máxima da RGPD, a multa sobre o faturamento da empresa, se o caso acontecesse em 2019, seria de EUR 1.800.000.000,00 (um bilhão e oitocentos milhões de euros).

Denota-se que antes mesmo da RGPD, as penalidades aplicadas eram próximas do que a RGPD hoje aborda, estando em consonância com os precedentes prolatados até então.

Já no Brasil, a tendência é a prática de penalidades menos severas. Por exemplo, no caso *Cambridge Analytica* envolvendo o Brasil, a multa aplicada foi de R$ 6.600.000,00 (seis milhões e seiscentos mil reais) ao *Facebook* pelo vazamento de dados de ao menos 443.000 usuários brasileiros. A decisão foi do Ministério da Justiça e Segurança Pública que, por meio do Departamento de Proteção e Defesa do Consumidor, aplicou a multa em razão do compartilhamento indevido de dados de usuários brasileiros no caso *Cambridge Analytica*.

O caso começou a ser investigado no Brasil depois de ser noticiado que brasileiros também tiveram seus dados compartilhados sem permissão pela consultoria de *marketing* político *Cambridge Analytica*. Na época, a empresa de Mark Zuckerberg admitiu que a empresa Cambridge Analytica violava as regras do *Facebook* e baniu a empresa na rede social.

Para o mesmo caso, os Estados Unidos aplicaram uma penalidade de US$ 5.000.000.000,00 (cinco bilhões de dólares), o que denota que os Estados Unidos possuem uma política muito mais forte em relação à proteção de dados, porém sem uma legislação unificada[270].

O que se pode observar com estes dados colhidos é uma grande divergência na aplicação de multa entre os países, sendo que o Brasil segue uma linha mais conservadora.

Para uma empresa com faturamento bilionário, uma multa de R$ 6.600.000,00 (seis milhões e seiscentos mil reais), aparentemente não servirá de

---

[269] Deutsche Bahn. Disponível em https://www.deutschebahn.com/resource/blob/4359656/6fea0b76a1c15164e7108d1b3edf3305/Rede-Lutz-Doll-HJ-2019-data.pdf>. Acesso em: 29 jan. 2020.

[270] Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotection.com/>. Acesso em: 23 jan. 2019.

coerção para que a situação force o *Facebook* a adotar outra política de Proteção de Dados no Brasil.

A LGPD traz em seu bojo previsões de penalidades de até 2% do faturamento da empresa. Todavia, deixa subjetiva a análise, e limite a penalidade máxima em R$ 50.000.000,00 (cinquenta milhões de reais). Já a RGPD não traz um valor de limite, mas estipula que pode ser de até 4% do valor do faturamento da empresa.

No caso *Maximillian Schrems* apresentado no Capítulo 2 é possível perceber que o Tribunal Europeu vem construindo sua jurisprudência no sentido de dar maior proteção aos dados pessoais. O Sr. Schrems apresentou uma queixa ao Comissário Irlandês de Proteção de Dados, dizendo que, à luz das revelações feitas em 2013 por Edward Snowden sobre as atividades dos serviços de inteligência dos Estados Unidos, a Agência de Segurança Nacional (NSA), a lei e a prática dos Estados Unidos não ofereceram proteção adequada contra a vigilância pelas autoridades públicas dos dados transferidos para o país.

A autoridade, num primeiro momento, rejeitou a denúncia, fundamentada em um acordo entre os Estados Unidos e a União Europeia denominada de *Safe Harbor 2000/520191*. Todavia, o Tribunal, de modo inteligente e atualizando a sua própria jurisprudência que estava ali sendo construída, anulou o acordo que estava em vigência há 15 anos. Com a anulação do acordo, cada Estado-Membro da União Europeia poderá analisar individualmente cada caso relacionado à Cooperação Internacional e à transferência de dados, desde que respeitado a RGPD.

Um caso bem interessante onde se pode observar a divergência de política interna acerca de proteção de dados foi o Recurso Especial nº 1.660.168/RJ. A ação, movida por *Denise Pieri Nunes* contra as empresas *Google Brasil Internet* Ltda, *Yahoo* do Brasil Internet Ltda e Microsoft informática Ltda, objetivava a obrigação de fazer em que pleiteava a desindexação nos resultados das aplicações de busca mantidas pelas recorrentes, de notícias relacionadas às suspeitas de fraude no XLI Concurso da Magistratura do Estado do Rio de Janeiro.

No mesmo caso, o acordão citou um caso europeu, envolvendo o Sr. *Mario Costeja González*, que objetivava exatamente o mesmo pedido do recurso especial: a remoção das aplicações de buscas mantidas pelas *Google Spain SL* e

Google Inc., dos dados pessoais do mesmo.

No acordão verifica-se que, para dirimir a questão, o tribunal pontuou a seguinte pergunta:

> Devem os direitos ao apagamento e bloqueio dos dados, regulados no artigo 12.°, alínea b), e o direito de oposição, previsto no artigo 14.°, [primeiro parágrafo,] alínea a), da Diretiva [95/46,] ser interpretados no sentido de que permitem que a pessoa em causa possa dirigir-se aos motores de busca para impedir a indexação da informação referente à sua pessoa, publicada em páginas web de terceiros, com base na sua vontade de que a mesma não seja conhecida pelos internautas quando considere que lhe pode ser prejudicial ou deseje que seja esquecida, mesmo tratando-se de uma informação publicada licitamente por terceiros?[271].

Ao final, inteligentemente, responde a citada pergunta:

> Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:
> 1) O artigo 2.°, alíneas b) e d), da 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, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de tratamento de dados pessoais, na acepção do artigo 2.°, alínea b), quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado responsável pelo dito tratamento, na acepção do referido artigo 2.°, alínea d)[272].

O acordão é rico em informações relevantes que levaram a esta

[271] UNIÃO EUROPEIA. **Acórdão Do Tribunal De Justiça Europeu.** Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=905559>. Acesso em: 22 jan. 2020.

[272] UNIÃO EUROPEIA. **Acórdão Do Tribunal De Justiça Europeu.** Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=905559>. Acesso em: 22 jan. 2020.

conclusão, mas o que mais chama a atenção é a análise minuciosa para um caso que parece pequeno, mas que tem relevância transnacional.

Em continuidade, em que pese a Ministra Relatora que analisou o caso tenha tido acesso à ao referido acordão europeu, destacou que "*o Tribunal de Justiça Europeu parte de pressupostos legais muito distintos daqueles existentes no País*". Ao final, declarou que ao menos na época, que o mais importante é a ausência de uma lei geral que disponha sobre a proteção de dados pessoais dos cidadãos brasileiros.

Por fim, reconheceu o direito fundamentado na teoria do direito ao esquecimento, por influência do Marco Civil da Internet, Lei nº 12.965/2014, art. 7º, incisos I e X, porém, sem reconhecer a responsabilidade do provedor de *internet.* Em outras palavras, a parte tem direito ao esquecimento, mas deve indicar em qual página o conteúdo está, sob pena do pedido não ser conhecido.

No julgado, o Ministro pontuou que "*não há fundamento legal que permita impor aos provedores de pesquisa a obrigação de eliminar do seu sistema os resultados que apontem para uma foto ou texto específico, sob a alegação de implementar o direito ao esquecimento de qualquer requerente*".

Posteriormente, em agosto de 2017, o Ministro em voto-vista proferiu julgado contrariando a jurisprudência construída pelo STJ, dando provimento ao pedido da autora, o que foi acompanhado pelos demais ministros, sob o principal argumento de que "*não se trata de efetivamente apagar o passado, mas de permitir que a pessoa envolvida siga sua vida com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca"*, o que denota grande avanço do judiciário brasileiro ao longo dos anos.

Sobre o julgado acerca do Sistema de *scoring*, em um dos processos analisados para ementar a súmula 550 (Recurso Especial nº 1.419.697/RS), o ministro realizou uma análise histórica do banco de dados do SPC:

> Em 1955, surge, em Porto Alegre, organizado pela Câmara de Dirigentes Lojistas (CDL), o primeiro banco de dados para integração dessas informações, sendo denominado de Serviço de Proteção ao Crédito (SPC) do Brasil. Posteriormente, foram criados em outros Municípios brasileiros,

> atingindo-se o expressivo número de 1600 CDLs instaladas em todo o Brasil. Com a facilidade de conexão pela internet, formou-se o SPC-Brasil, em 2002, administrando um imenso banco de dados com alguns milhões de registros, transformando-se em Rede Nacional de Informações Comerciais (RENIC). No setor privado, algumas empresas passaram a explorar economicamente o serviço de proteção ao crédito, com destaque para a *Serasa Experian*, com cerca de 50 anos de atuação no mercado brasileiro.

Mesmo que tenha sido amplamente debatida a questão do SPC formar um banco de dados, a avaliação da licitude do sistema *credit scoring* partiu da premissa de que não se trata de um cadastro ou banco de dados de consumidores, mas de uma metodologia de cálculo do risco de crédito, utilizando-se de modelos estatísticos e dos dados existentes no mercado acessíveis via *internet*.

De certo modo, parece um pouco controverso, pois, se o SPC forma um grande banco de dados, utilizar os dados para criar uma metodologia de cálculo do risco de crédito é violar o direito à privacidade. E se o cidadão não quer ser avaliado? No caso, não há essa opção.

Outro caso não comentado no Capítulo 2 é o caso da Uber *contra* a *Comissão Nacional de Informações e Liberdades* (CNIL). O mesmo órgão que multou a *Google* no caso mencionado no citado capítulo, também impôs uma multa de EUR 400.000,00 (quatrocentos mil euros) à *Uber* por ter "protegido insuficientemente os dados dos usuários" de seu serviço.

Em novembro de 2017, a *Uber* revelou que os dados de 57 milhões de seus usuários, clientes e motoristas foram *hackeados*. A CNIL considera que o ataque poderia ter sido evitado "*se tivessem adotado algumas medidas elementares em termos de segurança*".

Na realidade, o aplicativo havia sido informado sobre esta pirataria em novembro de 2016 pelos próprios *hackers.* A empresa havia dado a eles US$ 100 mil para que não revelassem as informações e apagassem os dados roubados.

A Uber, que sofreu vários casos de ataques virtuais, celebrou em setembro um acordo amigável de US$ 148.000.000,00 (cento e quarenta e oito milhões de dólares) com as autoridades americanas[273].

---

[273] França impõe multa de EUR 400 mil ao Uber por proteção insuficiente de dados. **UOL**. Disponível

O caso não ocorreu na União Europeia e nem no Brasil. Todavia, apresentou-se este caso por sua repercussão para fins de sugerir o aperfeiçoamento do modelo brasileiro de proteção de dados. No Brasil, considerando o histórico das decisões do Poder Judiciário e a ausência, ainda, de posição sobre o órgão regulador, não parece que a empresa teria a mesma penalidade.

Por fim, um outro caso de grande importância é o Recurso Especial nº 1.316.921/RJ, que é proveniente de uma ação ordinária inominada, ajuizada por Maria da Graça Xuxa Meneghel em desfavor da recorrente, *Google Brasil Internet Ltda*, objetivando compelir esta última a remover do seu *site* de pesquisas via Internet denominado *Google Search* os resultados relativos à busca pela expressão "xuxa pedófila" ou, ainda, qualquer outra que associe o nome da autora, escrito parcial ou integralmente, e independentemente de grafia, se correta ou equivocada, a uma prática criminosa qualquer (fls. 54/55, e-STJ).

O juiz de primeiro grau de jurisdição deferiu o pedido de tutela antecipada, determinando que a recorrente se abstenha de disponibilizar aos seus usuários, no site de buscas Google, quaisquer resultados/*links* na hipótese de utilização dos critérios de busca "Xuxa", "pedófila", "Xuxa Meneghel", ou qualquer grafia que se assemelhe a estas, isoladamente ou conjuntamente, com ou sem aspas, no prazo de 48 horas, a contar da intimação, sob pena de multa cominatória de R$ 20 mil por cada resultado positivo disponibilizado ao usuário. A decisão foi impugnada pela *Google* via agravo de instrumento.

Já o Acordão do Tribunal de Justiça do Rio de Janeiro deu parcial provimento ao agravo, restringindo a liminar apenas às imagens expressamente referidas pela parte agravada, ainda assim sem exclusão dos *links* na apresentação dos resultados de pesquisas (fls. 310-316, e-STJ).

Em seguida, foi proposto Recurso Especial da Google alegando violação dos arts. 461, §§ 4º e 6º do CPC; e 248 do Código Civil de 2002, bem como dissídio jurisprudencial (fls. 379-411, e-STJ).

Na ótica do Tribunal de Justiça do Rio de Janeiro, ainda que a agravante possa não ser juridicamente responsável pela veiculação dessas imagens na rede

---

em <https://economia.uol.com.br/noticias/afp/2018/12/20/franca-impoe-multa-de-eur-400-mil-ao-uber-por-protecao-insuficiente-de-dados.htm>. Acesso em: 22 jan. 2020.

de computadores, pode ela ser o destinatário da determinação judicial, em caráter cautelar, de sua cessação – considerando a quase inviabilidade fática de, para tal condão, demandar contra cada um dos *uploaders* isolados de imagens eróticas da agravada (fl. 315, e-STJ).

A Google se opôs a essa assertiva, afirmando que o citado tribunal ignorou por completo o fato de que não pode ser atribuída à recorrente a obrigação de impossível cumprimento considerando o estado da técnica atual, ressalvando que não é possível exigir que a Google realize o monitoramento de todo o conteúdo indicado como resultado em sua ferramenta de buscas a fim de verificar se as imagens ali indicadas são ou não referentes e ofensivas à recorrida.

Diante disso, conclui que o Tribunal Estadual deveria ter revogado a obrigação de fazer imposta à recorrente que, além de impossível, leva à censura prévia de conteúdo, antes mesmo de qualquer apreciação judicial (fls. 397-398, e-STJ).

Com isso, o STJ formulou algumas teses, relacionadas à dados pessoais, as quais cita-se:

> [...]
> 3. O provedor de pesquisa é uma espécie do gênero provedor de conteúdo, pois não inclui, hospeda, organiza ou de qualquer outra forma gerencia as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar links onde podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário. [...]
> 5. Os provedores de pesquisa realizam suas buscas dentro de um universo virtual, cujo acesso é público e irrestrito, ou seja, seu papel se restringe à identificação de páginas na web onde determinado dado ou informação, ainda que ilícito, estão sendo livremente veiculados. Dessa forma, ainda que seus mecanismos de busca facilitem o acesso e a consequente divulgação de páginas cujo conteúdo seja potencialmente ilegal, fato é que essas páginas são públicas e compõem a rede mundial de computadores e, por isso, aparecem no resultado dos sites de pesquisa.
> 6. Os provedores de pesquisa não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página.

> Documento.
> 7. Não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa.
> 8. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo – notadamente a identificação do URL dessa página – a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade da jurisdição. Se a vítima identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que, até então, se encontra publicamente disponível na rede para divulgação[274].

A decisão está bem fundamentada e rica de informações importantes na análise do caso, sobretudo envolvendo dados pessoais divulgados por terceiro. Todavia, o que se percebe em relação ao caso citado no Capítulo 2, o qual cita uma decisão Europeia, é a grande divergência acerca das penalidades aplicadas à grandes empresas.

No Brasil, resumidamente, entendeu-se que, como a empresa apenas intermedia a consulta de dados, não é responsável. Lá, por sua vez, é exatamente o inverso. A empresa é diretamente responsável por intermediar, o que parece mais aceitável, tendo em vista que, dependendo da quantidade de páginas que publicou o conteúdo ilícito ou ofensivo, é muito mais prudente bloquear diretamente na fonte (no intermediador que faz a consulta) do que em cada um dos que compartilharam.

Após tecidas estas breves considerações, conclui-se o capítulo no sentido de afirmar a grande divergência entre as decisões Europeias e Brasileiras, mas, por certo, o Brasil caminhará no sentido de tornar as decisões mais severas, principalmente por que os dados pessoais são transnacionais e enquanto a legislação for local, depende de uma boa construção cultural em prol dos titulares

---

[274] Superior Tribunal de Justiça. STJ. REsp 1407271 SP 2013/0239884-1. Disponível em <https://ww2.stj.jus.br/processo/pesquisa/?termo=REsp+1407271&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO>. Acesso em 13 mai. 2020.

dos dados.

CONSIDERAÇÕES FINAIS

No presente trabalho, objetivou-se discorrer sobre a Teoria Geral da Proteção de Dados, e em seguida sobre a análise comparativa dos elementos determinantes da Cooperação Internacional, as Sanções Administrativas e o Controle Judicial na Lei Geral de Proteção de Dados Brasileira e da União Europeia.

Isso porque, a recente edição da LGPD, suscita uma série de questionamentos aos operadores do direito decorrentes da sua interpretação e aplicação.

Um deles concerne à melhoria da qualidade da proteção de dados pela via da cooperação, já que as operações se dão em ambiente transnacional (Internet, por exemplo, com possibilidade de aumento da ineficácia da proteção).

O outro decorre da insegurança jurídica (aos regulados) do poder sancionatório que a ANPD poderá causar diante da inexistência de uma doutrina jurídica atualizada que possa contribuir para a proteção de dados de um lado, sem violar os direitos das empresas e pessoas.

Desta forma, acredita-se que a análise comparativa destes elementos determinantes no modelo Europeu e no modelo Brasileiro poderá contribuir para reduzir a insegurança jurídica no Brasil.

No Capítulo 1, buscou-se discorrer sobre a Teoria Geral da Proteção de Dados, com ênfase na Cooperação Internacional, na aplicação das Sanções Administrativas pela Lei Geral de Proteção de Dados da União Europeia e do Brasil, e por fim acerca do controle judicial do ato administrativo pelo órgão regulador, estudando-se o histórico acerca das legislações sobre proteção de dados no Brasil e na União Europeia e trazendo alguns exemplos também de outros países, como Austrália e Canada.

A presente pesquisa tem como objetivo geral contribuir para aperfeiçoar o modelo brasileiro de proteção de dados, por meio da análise comparativa da cooperação internacional, das sanções administrativas e do controle judicial dos atos administrativos dos modelos de proteção de dados da União Europeia e do Brasil.

No Capítulo 1 buscou-se discorrer sobre uma Teoria Geral da Proteção de Dados, apresentando os conceitos e categorias relevantes, seguido da apresentação do conceito do que são os elementos determinantes e quais são os

elementos estudados nesta pesquisa, quais sejam: cooperação internacional, sanções administrativas e controle judicial dos atos administrativos envolvendo a matéria nos modelos de Proteção de Dados da União Europeia e do Brasil, estudando-se o histórico de cada um dos regulamentos analisados e no mundo, trazendo exemplos de outros países à título de exemplificação, como os modelos da Austrália e do Canadá.

Além disso, buscou-se esmiuçar a legislação brasileira e Europeia, objetivando entender o contexto histórico de ambas as regiões para, assim, entender a necessidade de uma Lei Geral de Proteção de Dados, apresentando dados acerca da construção histórica da União Europeia e como aquela região pode contribuir para a aperfeiçoamento do modelo brasileiro, que conforme será visto, não possui um histórico tão aprofundado quanto o da União Europeia.

Ainda no Capítulo 1, buscou-se apresentar alguns conceitos operacionais para a correta compreensão da pesquisa, conceitos estes apresentados pela Lei Geral de Proteção de Dados da União Europeia e do Brasil tais como o conceito de “Dados Pessoais” e “Cooperação Internacional”, podendo compreender melhor a pesquisa a partir da sua correta interpretação.

Por fim, apresentou-se também no Capitulo 1, além das novidades instituídas pela LGPD descritas acima, a criação de uma Agência Reguladora, denominada Autoridade Nacional de Proteção de Dados (ANPD), que possui diversas atribuições, dentre elas promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, buscando através da cooperação trazer maior segurança jurídica para os titulares de dados. Da mesma forma, a União Europeia também possui um órgão regulador, denominado de Comitê Europeu de Proteção de Dados, mas como será visto, além do Comitê, os países-membros possuem forte autonomia através de suas entidades supervisoras locais.

No Capítulo 2 tratou-se de apresentar os elementos determinantes da cooperação internacional, da aplicação das sanções administrativas e do controle judicial dos atos administrativos nos modelos europeu e brasileiro de proteção de dados.

Com isso, objetivou-se estudar os elementos determinantes destacados acima para apurar como já funciona o então vigente Regulamento Geral de Proteção

de Dados da União Europeia, através do Comitê Europeu de Proteção de Dados.

Como será visto, a União Europeia já possuía legislação acerca de proteção de dados ao menos desde 1995, com a Diretiva nº 46. Além disso, antes mesmo da União Europeia, os países-membros daquela região já tinham forte histórico de leis sobre proteção de dados pessoais.

Já no Brasil, objetivou-se estudar os elementos determinantes destacados na Lei Geral de Proteção de Dados e como vem sendo discutido este assunto sem a vigência de uma Lei Geral de Proteção de Dados, podendo-se perceber que a ausência de uma Lei de Proteção de Dados fez grande falta na construção de precedentes dos Tribunais Superiores acerca desta matéria.

O Capítulo 3 dedica-se a efetuar a análise comparativa dos elementos determinantes da cooperação internacional, da aplicação das sanções administrativas nos modelos europeu e brasileiro de proteção de dados e do controle judicial do ato administrativo, estudando as decisões judiciais em cada país para auferir a aplicabilidade nas esferas administrativa e judicial da Lei Geral de Proteção de Dados europeia e brasileira.

Ao final, buscou-se, com a análise comparativa dos elementos determinantes da cooperação internacional e das sanções administrativas dos modelos europeu e brasileiro de proteção de dados contribuir para o aperfeiçoamento do modelo brasileiro, tendo em vista que o modelo europeu já está em vigência.

Após a pesquisa, pode-se concluir que:

1. A União Europeia já possuía legislação de proteção de dados desde 1995, ou seja, há pelo menos vinte e cinco anos a União Europeia vem se preocupando com a ideia de proteção de dados pessoais. Com isso, é evidente que as decisões daquela comunidade podem contribuir para as decisões brasileiras.

2. No Brasil, os julgados seguem uma linha menos severa, adotando precedentes voltados a evitar o enriquecimento ilícito da parte requerente e, consequentemente, não penalizando devidamente grandes empresas que tratam numerosas quantias de dados. Todavia, tal fator concorre para a manutenção do ato ilícito pela empresa praticante, pois o infrator saberá que a condenação não lhe prejudicará a sua atividade.

3. Com a comparação das decisões na União Europeia e no Brasil, o que se pôde concluir, consubstanciado inclusive nas conclusões apontadas acima, é que como a União Europeia já possuía um Regulamento de Proteção de Dados (Diretiva 95), as decisões que antecedem a RGPD já apresentavam grande segurança jurídica ao titular dos dados, com inclusive grandes penalidades em desfavor das empresas que fazem o tratamento de dados. Mesmo assim, como já se esperava, a preocupação ainda existente na União Europeia fez com que os legisladores adotassem a elaboração de uma Lei Geral de Proteção de Dados, principalmente buscando agora dar maior ênfase à Cooperação Internacional, sobretudo com os países estrangeiros que não fazem parte da União Europeia.

4. Por valer em diversos países, trata-se de uma legislação supranacional, com aplicabilidade em todos os Estados-Membros, facultando, inclusive, aos Estados-Membros da União Europeia estabelecerem regras distintas do Regulamento Geral, desde que queiram adotar uma postura mais severa. Não pode, entretanto, o país-membro adotar uma postura menos severa, pois isso contraria o Regulamento Geral.

5. Assim, o Brasil ainda precisará repensar o modelo adotado no País, principalmente pelo órgão regulador, que terá total responsabilidade para adotar medidas nos casos que surgirão na via administrativa, o que será uma grande novidade, pois antes de adentrar no judiciário, o titular poderá buscar a via administrativa para fazer valer seus direitos e garantir a proteção de seus dados.

Diante de tais conclusões, pode-se afirmar que a hipótese de que a análise comparativa dos elementos determinantes da cooperação internacional e das sanções administrativas dos modelos europeu e brasileiro de proteção de dados contribuirá para o aperfeiçoamento do modelo brasileiro, foi confirmada, sendo relevante fazer as seguintes sugestões para o referido aperfeiçoamento do modelo de proteção de dados no Brasil:

1. Retirar da Lei Geral de Proteção de Dados a limitação de multa de até R$ 50.000.000,00 (cinquenta milhões de reais), dando maior autonomia ao aplicador da sanção, em caso de empresas transnacionais que operam grande quantidade de dados, como *Facebook, Google, Instagram, etc***.**

2. A ANPD deve orientar as ME e EPP’s de que modo devem elas se

preocuparem com os dados tratados, tendo em vista que um mero cadastro para fins de agendamento já é considerado tratamento de dados pessoais e que podem gerar sanções em âmbito administrativo e judicial. Esta orientação serviria, em tese, como um norte inclusive para posteriormente possibilitar a defesa em âmbito administrativo e judicial. Vale ressaltar que estas empresas fazem parte de 99% das empresas no Brasil[275], e estas empresas muitas vezes não possuem orçamento ou ao menos não aplicam orçamento significante para a proteção de dados, estando sujeito a ataques virtuais e com maior vulnerabilidade do que as grandes corporações**.**

3. A LGPD deveria prever situações em que exigem o imediatismo, que dependem de uma decisão liminar, especificando situações pontuais em que a tutela deve ser deferida, trazendo assim, maior segurança jurídica em casos excepcionais, assim como o CDC trouxe a possibilidade da concessão da tutela liminarmente nas ações de obrigação de fazer, nos termos do artigo 84, §3º do CDC.

4. O Brasil deve buscar construir uma jurisprudência no sentido de responsabilizar o provedor de busca da *internet* em casos em que o titular dos dados requerer a exclusão dos dados do titular do provedor de busca, buscando proteger o titular de dados e não a empresa controladora e que realiza o tratamento de dados.

5. Utilizar como base e referência as decisões dos países membros da União Europeia, necessidade fundamental considerando que o assunto é matéria internacional e uma mesma empresa deve sentir a mesma coerção da União Europeia aqui no Brasil, sob pena de incorremos em um equívoco na proteção dos dados dos brasileiros.

6. A LGPD através da ANPD deverá regular de que modo se dará a Cooperação Internacional em situações envolvendo dados tratados no Brasil, mas por operadores de países estrangeiros.

7. A ANPD deve começar a pensar sobre a possibilidade de um direito Transnacional, realizando acordos com países que abririam parte de sua soberania no que se refere à tratamento de dados, submetendo à algum órgão de fiscalização e controle transnacional, do mesmo modo como já funciona (e muito bem) na União Europeia), porém, desta vez, em âmbito global.

---

[275] SEBRAE. Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD>. Acesso em: 30 jan. 2020.

8. A ANPD poderia propor incentivos para realização de políticas de integridade nas ME's e EPP's, pois estas representam 99% das empresas no Brasil[276], sendo que o programa de integridade poderá prever de que modo os dados serão tratados.

A pesquisa visa tão somente contribuir para a solução do problema, qual seja aperfeiçoar o modelo brasileiro de proteção de dados, através do método comparativo, tendo em vista a construção de precedentes realizado ao longo dos anos pela União Europeia, através da Cooperação Internacional, das Sanções Administrativas e do Controle Judicial.

[276] SEBRAE. Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD>. Acesso em: 30 jan. 2020.

REFERÊNCIA DAS FONTES CITADAS

ALCANTARA, Larissa Kakizaki de. **Big Data e IoT**: Desafios da Privacidade e da Proteção de Dados no Direito Digital . Edição do Kindle.

ALMEIDA. Paula Joyce de Carvalho Andrade de. O controle da atuação das Agências Reguladoras Federais Brasileiras. **Dissertação de Mestrado**. Universidade Presbiteriana Mackenzie. São Paulo. 2007.

ARBULU, Rafael. **Canaltech**. Disponível em: <https://canaltech.com.br/hacker/hacker-oferece-26-milhoes-de-registros-de-usuario-por-us-5-mil-em-bitcoins-135103/>. Acesso em: 23 jan. 2020.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. **Proteção de dados pessoais no Brasil:** análise dos projetos de lei em tramitação no Congresso Nacional. 2017.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro, Ed. Forense, 2019.

BRASIL, **Constituição da República Federativa do Brasil de 1988**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 10 dez. 2019.

BRASIL, **Lei 12.414 de 9 de junho de 2011.** Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 10 dez. 2019.

BRASIL, **Lei nº 8.078/1990 – Código de Defesa do Consumidor**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 10 dez. 2019.

BRASIL. Guia Compliance – Versão Oficial**. Conselho Administrativo de Defesa Econômica – CADE.** Disponível em <http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-Compliance-versao-oficial.pdf>. Acesso em: 08 out. 2019.

BRASIL. **Lei 10.406/2002 – Código Civil**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 30 jan. 2020.

BRASIL. **Lei 12.527 de 2011**. Art. 1º. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 dez. 2019.

BRASIL. Lei 12.965/2014 – **Marco Civil da Internet**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 16 jan. 2020.

BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD)** – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

BRASIL. **Lei 13.709/2018** - **Lei Geral de Proteção de Dados (LGPD).** Artigo 5º – Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 out. 2019.

BRASIL. **Lei 9.296/1996.** Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 12 dez 2019.

BRASIL. **Lei 9.296/1996**. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 12 dez 2019.

BRASIL. **Lei 9507/1997 – Habeas Data.** Disponível em <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 12 dez. 2019.

BRASIL. **Lei nº 8.078/1990 – Código De Defesa do Consumidor.** Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 12 dez. 2019.

BRASIL. **PL 4060/2012**. Disponível em <https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 10 dez. 2019.

BRASIL. **Recurso em Mandado de Segurança Nº 55.019/DF39**. Disponível em < http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

BRASIL. **Recurso Especial Nº 1.348.532/SP47.** Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

BRASIL. **Recurso Especial Nº 1.660.168/RJ44**. Disponível em <http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 22 jan. 2020.

BRASIL. Superior Tribunal de Justiça. **Súmula 550**. Disponível em < http://www.stj.jus.br/sites/portalp/Inicio>. Acesso em: 02 fev. 2020.

BRASIL. **Lei 12.529/2011**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.htm>. Acesso em 13 mai. 2020

CALIFORNIA. **Consumer Privacy Act of 2018** – Disponível em <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121>. Acesso em: 10 dez. 2019.

CÂMARA DOS DEPUTADOS. **Proposta de Emenda Constitucional 17/2019**. Disponível em < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 02 fev. 2020.

CANDELORO, Ana Paula P.; DE RIZZO, Maria Balbina Martins; PINHO, Vinícius. **Compliance 360º:** Riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

Carta dos Direitos Fundamentais da União Europeia. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 23 jan. 2020.

CASTELLS, Manuel. **A Sociedade em Rede.** Tradutor: Roneide Venancio Majer. 17. Ed, 2016,

CASTRO JUNIOR, Osvaldo Agripino de. **Teoria e Prática do Direito Comparado e Desenvolvimento:** Estados Unidos x Brasil. Florianópolis: fundação Boiteux, Unigranrio, Ibradd, 2002.

Comissão Nacional de Proteção de Dados. **CNPD**. Disponível em <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 15 jan. 2020.

CRUZ, Paulo Marcio. Piffer, Carla. **O DIREITO TRANSNACIONAL COMO DISCIPLINA EM CURSOS JURÍDICO S 2018** | v. 12 | nº 1 | p. 11-28 | ISSN 2317-2622. Disponível em <http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v12n1p11-28>. Acesso em: 23 jan. 2020.

CRUZ, Paulo Márcio; BODNAR, Zenildo. A transnacionalidade e a emergência do Estado e do Direito transnacionais. **Revista eletrônica do CEJUR**, v. 1, nº 4, 2009. disponível em <https://revistas.ufpr.br/cejur/article/download/15054/11488>. Acesso em: 20 out. 2019.

CRUZ, Paulo Márcio; BODNAR, Zenildo. Globalização, transnacionalidade e sustentabilidade. **Itajaí: Univali**, 2012. Disponível em < https://www.univali.br/vida-no-campus/editora-univali/e-books/Documents/ecjs/E-book%202012%20GLOBALIZA%C3%87%C3%83O,%20TRANSNACIONALIDADE%20E%20SUSTENTABILIDADE.pdf>. Acesso em: 02 fev. 2020, p. 32.

CUNHA, Mauro Leonardo. **Comentários à Lei Geral de Proteção de Dados**. Edição Própria. 2018, Edição do Kindle. Posição 1324 de 2215.

Data Protection Laws of the World. **DLA PIPER**. Disponível em <https://www.dlapiperdataprotectionºcom/>. Acesso em: 23 jan. 2019.

Deutsche Bahn. Disponível em https://www.deutschebahnºcom/resource/blob/4359656/6fea0b76a1c15164e7108d1b3edf3305/Rede-Lutz-Doll-HJ-2019-data.pdf>. Acesso em: 29 jan. 2020.

Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013. Disponível em <https://dicionario.priberam.org/coima>, Acesso em: 23 out. 2019.

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

European Data Protection Board – Comite Europeu para a Proteção de Dados. Disponível em:<https://edpb.europa.eu/edpb_pt>. Acesso em: 16 jan. 2020.

FINN, Rachel L., WRIGHT, David, FRIEDEWALD, Michael, GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de, POULLET, Yves - **European Data Protection Coming of Age**. Ed Springer Netherlands, 2013.

FONSECA, Carol. Canva confirma invasão por hackers em sua plataforma. **Terra**. <https://www.terra.com.br/noticias/tecnologia/seguranca-digital/canva-confirma-invasao-por-hackers-em-sua-plataforma,2e9f83ba4d6c6221114ffc99145c3947j5jjavwb.html>. Acesso em: 23 jan. 2020.

França impõe multa de EUR 400 mil ao Uber por proteção insuficiente de dados. **UOL**. Disponível em <https://economia.uol.com.br/noticias/afp/2018/12/20/franca-impoe-multa-de-eur-400-mil-ao-uber-por-protecao-insuficiente-de-dados.htm>. Acesso em: 22 jan. 2020.

FRANZINA, Pietro. Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation, in Alberto de Franceschi (2016) **European contract**

law and the digital single market: the implications of the digital revolution, Cambridge, Antwerp, Portland, Intersentia, p. 108.

Google é multado em € 50 milhões sob nova regra de dados da Europa. **Época Negócios Online**. Disponível em <https://epocanegocios.globo.com/Empresa/noticia/2019/01/google-e-multado-em-50-milhoes-sob-nova-regra-de-dados-da-europa.html>. Acesso em: 28 jan. 2020.
Google recebe maior multa já aplicada por violar dados pessoais na Europa. **UOL**. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2019/01/21/google-e-multado-na-franca-por-violar-de-dados-pessoais.htm>. Acesso em: 22 jan. 2020.

GUTWIRTH, Serge, LEENES, Ronald, HERT, Paul de. **Reforming European Data Protection Law**. Law, Governance and Technology Series 20. Springer Netherlands, 2015.
HEIMES, Rita; PFEIFLE, Sam. Study: **at least 28.000 DPOs needed to meet GDPR requirements**. Disponível em: <https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/#>. Acesso em: 16 jan. 2020.

Internet Corporation For Assigned Names And Numbers. Disponível em <https://www.icannºorg/resources/pages/welcome-2012-02-25-en>. Acesso em: 16 jan 2020.

LAMBERT, Paul. **Understanding the new European data protection rules**. Boca Raton. CRC Press, 2017.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). RM Digital Education. 1ª Edição. Goiânia – GO. 2019. Edição do Kindle.

MANZI, Vanessa Alessi. **Compliance no Brasil**. São Paulo: Saint Paul Editora, 2008.

MENDES, Laura Schertel - **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental – São Paulo: Saraiva, 2014.

MOTTA, Paulo Roberto Ferreira. **Agências reguladoras**. Barueri: Manole, 2003.

My Data Privacy. Disponível em <https://mydataprivacy.eu/o-regulamento/>. Acesso em: 23 jan. 2020.

O Globo. Disponível em <https://oglobo.globo.com/mundo/facebook-cambridge-analytica-trabalharam-para-trump-apos-vazamento-de-dados-1-22510991>. Acesso em: 10 dez. 2019.

O Tribunal de Justiça da União Europeia produziu um julgamento invalidando o acordo de transferência de dados pessoais (conhecido como "Safe Harbor", "Porto Seguro" em tradução para o português) entre os Estados Unidos e a União Europeia. Esse acordo, que estava em vigor desde o ano de 2000, era o instrumento legal que autorizava empresas a transferirem dados coletados de cidadãos europeus para serem processados em seus estabelecimentos situados em território americano. Disponível em < http://www.editoramagister.com/doutrina_27076672_A_DECISAO_DA_CORTE_EUROPEIA_QUE_INVALIDOU_O_ACORDO_DE_TRANSFERENCIA_DE_DADOS_PESSOAIS.aspx>. Acesso em: 19 jan. 2020.

PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica:** Teoria e Prática. 14.ed.rev.atual.

e amp. Florianópolis: EMais, 2018.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei nº 13.709/2018 LGPD**. Saraiva Educação. Edição do Kindle.

Por meio da Lei do Censo (Volkszählungsgesetz) de 1983, promulgada em 25 de março de 1982 (BGBl. I, p. 369), ordenou-se o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho, para fins estatísticos. O objetivo declarado da lei era reunir, por meio de levantamentos feitos por pesquisadores credenciados, dados sobre o estágio do crescimento populacional, a distribuição espacial da população no território federal, sua composição segundo características demográficas e sociais, assim como também sobre sua atividade econômica. Tais dados sempre foram considerados indispensáveis para quaisquer decisões político-econômicas da União, Estados e municípios Disponível em <https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877>. Acesso em: 11 dez. 2019.

Quebec Privacy Act. Disponível em <http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1>. Acesso em: 02 fev. 2020.

REINIS, Oliver Alexandre. **Lei Brasileira de Proteção de Dados**: Lei nº 13.709, de 14 de agosto de 2018**.** Edição do Kindle.

Relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Disponível em <https://www.anacom.pt/render.jsp?contentId=964154.>. Acesso em: 15 jan. 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância** – A privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro. Ed. Renovar, 2008.

ROSSI, Marina. Brasil multa Facebook em 6,6 milhões de reais pelo vazamento de dados no caso Cambridge Analytica**. EL PAIS**. <https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html>. Acesso em: 22 jan. 2020.

SCHNEIDER, Sergio; SCHIMITT, Cláudia Job**. O uso do método comparativo nas Ciências Sociais. Cadernos de Sociologia,** Porto Alegre, v. 9,1998 p. 49-87.

SEBRAE. Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD>. Acesso em: 30 jan. 2020.

SILVEIRA, Sergio Amadeu de. **Tudo sobre todos**. São Paulo. Editora Edições Sesc SP. 2017. Edição do Kindle.

Site onde as pessoas compartilham suas impressões sobre filmes, utilizando-se na maioria das vezes, seus nomes reais. Disponível em <https://www.imdb.com/>. Acesso em: 12 jan. 2020.

Sony é multada no Reino Unido por invasão à PlayStation Network. **O Globo**. Disponível em <https://oglobo.globo.com/economia/sony-multada-no-reino-unido-por-invasao-playstation-network-7385801>. Acesso em: 22 jan. 2020.

SOUZA. Luiza Ribeiro de Menezes. proteção de dados pessoais: estudo comparado do

regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro nº 5.276/2016. **IDP**. Escola de Direito de Brasília. Disponível em < https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153/1484>. Acesso em: 16 jan. 2020, p. 31.

Termos de Privacidade do Google. Disponível em <https://privacy.google.com/?hl=pt_BR#>. Acesso em: 28 jan. 2020.

Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR >. Acesso em: 23 jan. 2020.

TOMAZ, Roberto Epifanio (org.). **Descomplicando o Compliance**. 1 ed. Florianópolis: Tirant Lo Blanch, 2018.

UNIÃO EUROPEIA. **Acórdão Do Tribunal De Justiça Europeu.** Disponível em < http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=905559>. Acesso em: 22 jan. 2020.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 16 jan. 2020.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Disponível na versão português de Portugal em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 22 out. 2019.

UNIÃO EUROPEIA. Regulamento 2016/679 do parlamento Europeu e do conselho. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 12 jan 2020.

UNIÃO EUROPEIA. Acordão do Tribunal de Justiça. **Processo nº C-362/14**. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&from=PT>. Acesso em: 28 jan. 2020.

United Nations Human Rights – Office of the High Commissioner. Disponível em <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>. Acesso em: 12 jan. 2020

WARREN, Samuel D. Brandeis, Louis D. **The Right to Privacy.** Disponível em:<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 12 dez. 2019.

ZELLER, Bruno, TRAKMAN, Leon, WALTERS, Robert. **Data Protection Law – A Comparative analysis of Asia-Pacific And European Approaches.** Ed. Springers, 2019.