

**Pontifícia Universidade Católica de Campinas
PUC-Campinas**

Rafael Tedrus Bento

**A evolução dos conceitos de proteção de dados pessoais e privacidade na
jurisprudência do Tribunal de Justiça da União Europeia**

Mestrado em Direito

Orientador: Professor Doutor Lucas Catib de Laurentiis

Campinas

2021

Rafael Tedrus Bento

**A evolução dos conceitos de proteção de dados pessoais e privacidade na
jurisprudência do Tribunal de Justiça da União Europeia**

Dissertação apresentada ao Programa de Mestrado em Direito da Pontifícia Universidade Católica de Campinas – PUC, como requisito parcial para obtenção do título de Mestre em Direito, inserido na linha de pesquisa Cooperação Internacional e Direitos Humanos, sob a orientação do Professor Doutor Lucas Catib de Laurentiis.

Campinas

2021

Ficha catalográfica elaborada por Fabiana Rizziolli Pires CRB 8/6920
Sistema de Bibliotecas e Informação - SBI - PUC-Campinas

342.721 B478e	<p>Bento, Rafael Tedrus</p> <p>A evolução dos conceitos de proteção de dados pessoais e privacidade na jurisprudência do Tribunal de Justiça da União Europeia / Rafael Tedrus Bento. - Campinas: PUC-Campinas, 2021.</p> <p>172 f.</p> <p>Orientador: Lucas Catib de Laurentiis.</p> <p>Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito, Centro de Ciências Humanas e Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas, 2021.</p> <p>Inclui bibliografia.</p> <p>1. Direito a privacidade. 2. Proteção de dados. 3. Direitos fundamentais - União Européia. I. Laurentiis, Lucas Catib de. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Humanas e Sociais Aplicadas. Programa de Pós-Graduação em Direito. III. Título.</p> <p>CDU 342.721</p>
------------------	---

RAFAEL TEDRUS BENTO
**A evolução dos conceitos de proteção de dados
 pessoais e privacidade na jurisprudência
 do Tribunal de Justiça da União Europeia**

Este exemplar corresponde à redação final da Dissertação
 de Mestrado em Direito da PUC-Campinas, e aprovada
 pela Banca Examinadora.


APROVADO: 13 de dezembro de 2021.

Assinado por: **ALESSANDRA APARECIDA SOUZA
 DA SILVEIRA**
 Num. de Identificação: BI155179268
 Data: 2021.12.13 17:03:07+00'00'



DRA. ALESSANDRA APARECIDA SOUZA DA SILVEIRA (UNIVERSIDADE DO MINHO)


 DR. CLAUDIO JOSE FRANZOLIN (PUC-CAMPINAS)


 DR LUCAS CATIB DE LAURENTIIS – Presidente (PUC-CAMPINAS)

“We must not be confused about what freedom is. Basic human rights are simple and easily understood: freedom of speech and a free press; freedom of religion and worship; freedom of assembly and the right of petition; the right of men to be secure in their homes and free from unreasonable search and seizure and from arbitrary arrest and punishment.
(...)

“The future must see the broadening of human rights throughout the world. People who have glimpsed freedom will never be content until they have secured it for themselves. In a truest sense, human rights are a fundamental object of law and government in a just society. Human rights exist to the degree that they are respected by people in relations with each other and by governments in relations with their citizens.”

(Eleanor Roosevelt, 1948)

AGRADECIMENTOS

Fui privilegiado por ter conseguido terminar meus estudos e esta pesquisa, com saúde e sanidade íntegra. Praticamente o período completo deste curso foi marcado pela pandemia do COVID-19, o qual transformou nossa sociedade nestes últimos 2 (dois) anos. Nesse caminho, muitos foram os obstáculos e os erros, assim como as conquistas e os aprendizados.

E como nada se constrói sozinho nesta vida, tenho muito para agradecer. É impossível citar todas as pessoas que contribuíram para a conclusão dessa etapa, mas cada uma delas tem consciência de sua importância. Agradeço de coração a todas as pessoas. Apesar disso, é necessário destacar alguns nomes que tiveram influência direta e construtiva nesse ciclo.

Ao meu orientador, professor e grande exemplo de pessoa, Lucas Catib de Laurentiis, tenho muito que agradecer. Por ter confiado em mim desde o primeiro dia, pelos ensinamentos, pela calma em cuidar deste estudo e, principalmente, por nunca deixar de acreditar em meu potencial. Agradeço por seu apoio e estímulo constante, assim como pelas cobranças e críticas, sempre muito construtivas. Obrigado por ser este exemplo de pessoa e professor. Tudo que tem de positivo neste estudo, também é seu.

A todos professores e professoras da PUC-Campinas, muito obrigado. Em razão da proximidade e importância durante a Pós-Graduação, agradeço individualmente alguns. Guilherme Perez Cabral, Cláudio José Franzolin e Peter Panutto, agradeço pelas aulas, conselhos e apoio.

Agradeço à Universidade do Minho, por ter me selecionado a participar, como aluno especial, junto ao Mestrado em Direito da União Europeia, o qual teve papel central na evolução do entendimento dos conceitos trazidos à este estudo. Em especial, agradeço à Professora Doutora Alessandra Aparecida Souza da Silveira, a qual trouxe esta oportunidade única à minha vida e é um exemplo de pessoa e professora inigualável. Em especial, agradeço aos meus colegas daquele Mestrado, em nome do aluno Bruno Saraiva.

Aos funcionários da PUC-Campinas, sou grato pela alegria, empenho e trabalho de vocês para que todos os alunos e alunas consigam desfrutar da melhor experiência possível de aprendizado. De forma especial, agradeço ao Wagner Galvão por todo apoio e paciência.

Aos meus colegas da pós-graduação, obrigado por compartilharem tanto os momentos difíceis como os felizes comigo. Jamais esquecerei as discussões acadêmicas e as videoconferências durante a pandemia. Pelo apoio e contato frequente, agradeço especialmente à Raquel e ao André.

À minha esposa, Luise Duarte Ribeiro, agradeço pela paciência, pela parceria, pelo amor e cuidado contínuo. Sem você nada disso teria sido possível.

Ao meu sócio Thiago Terin Luz um agradecimento especial, por ter sido a primeira pessoa a me apresentar este direito, o qual serveria de meu estudo. Agradeço também pela paciência e cuidado neste período que me dediquei aos estudos.

À toda minha família, agradeço o amor, o carinho e as orações. Ao meu pai, Mario Tadeu Cezar Bento, minha madrasta, Cristina Rubio Barsotini, minha cunhada, Marília Martins Cavalcanti Bento, por sempre confiarem e estarem presentes em minha vida. Ao meu irmão, Marcos Vinicius Tedrus Cezar Bento, o registro de minha grande admiração pela pessoa e pelo profissional incrível que você é.

Por fim, à minha mãe, Gloria Maria Almeida Souza Tedrus o maior agradecimento deve ser registrado. Não tenho palavras para descrever o orgulho que é ser filho desta pessoa incrível, dedicada, única, a qual além de ser uma pessoa íntegra e correta, é uma professora doutora que merece todo o reconhecimento do mundo. Obrigado mãe.

RESUMO

BENTO, Rafael Tedrus. *A evolução dos conceitos de Proteção de Dados Pessoais e Privacidade na Jurisprudência Tribunal de Justiça da União Europeia*. 172 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de Campinas, 2021.

Este trabalho pretende analisar a relação, ou falta dela, entre os direitos à privacidade e a proteção dos dados pessoais, enquanto direitos fundamentais no ordenamento jurídico da União Europeia, em consonância com os julgados dos anos de 1989 a 2019, do Tribunal de Justiça da União Europeia. O objeto central do trabalho diz respeito ao conceito do direito fundamental aplicado por tal jurisprudência. Em meio a variações argumentativas e de concepções distintas a respeito das características deste direito, busca-se, em específico, verificar se a proteção de dados pessoais é identificada pela jurisprudência apenas como um instrumento para efetivação de outros direitos ou se é tratado como um direito autônomo, e quais são os reflexos dogmáticos dessa diferenciação. Este trabalho busca identificar padrões decisórios e características dogmáticas do direito fundamental à proteção de dados pessoais, assim, se insere, portanto, no campo da dogmática jurídica e da pesquisa jurisprudencial empírica do direito.

Palavras-chave: Proteção de dados pessoais. Privacidade. Carta dos direitos fundamentais da União Europeia. Tribunal de Justiça da União Europeia. Autodeterminação informacional.

ABSTRACT

BENTO, Rafael Tedrus. The evolution of the concepts of Personal Data Protection and Privacy in the Jurisprudence of the Court of Justice of the European Union. 172 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de Campinas, 2021.

This work intends to analyze the relationship, or lack of it, between the rights to privacy and the protection of personal data, as fundamental rights in the legal system of the European Union, in line with the judgments of the years 1989 to 2019, of the Court of Justice of the European Union. The central object of the work concerns the concept of the fundamental right applied by such jurisprudence. In the midst of argumentative variations and different conceptions regarding the characteristics of this right, it seeks, in particular, to verify whether the protection of personal data is identified by the jurisprudence only as an instrument for the realization of other rights or if it is treated as a right autonomous, and what are the dogmatic reflexes of this differentiation. This work seeks to identify decision-making patterns and dogmatic characteristics of the fundamental right to the protection of personal data, thus, it is inserted, therefore, in the field of legal dogmatics and empirical jurisprudential research of law.

Keywords: Protection of personal data. Privacy. Charter of fundamental rights of the European Union. Court of Justice of the European Union. Informational self-determination.

SUMÁRIO

Resumo	20
ABSTRACT	21
Sumário	22
INTRODUÇÃO	25
1 INSTITUIÇÕES JURÍDICAS DA UNIÃO EUROPEIA	30
1.1 Tratados originários da União Europeia.....	30
1.2 Tratados constitutivos da União Europeia.....	31
1.3 Normas da União Europeia	33
1.4 As normas relativas à proteção de dados pessoais na União Europeia	37
1.5 Carta dos Direitos Fundamentais da União Europeia e a Convenção nº 108 do Conselho da Europa	39
1.6 Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679	42
1.7 Diretiva E-Privacy e a Proposta de Regulamento Relativo à Privacidade e Comunicações Eletrônicas.....	46
1.8 Tribunal de Justiça da União Europeia e Tribunal Europeu de Direitos Humanos.....	49
1.9 Sistema de Reenvio Prejudicial e o Tribunal de Justiça da União Europeia.....	53
1.10 Conclusão parcial	55
2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE PERANTE O TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA	58
2.1 Objetivos da pesquisa sobre proteção de dados pessoais	58
2.2 Metodologia da coleta da jurisprudência do Tribunal de Justiça da União Europeia	59
2.3 Categorização de direitos abarcados na jurisprudência sobre direito à proteção de dados pessoais do Tribunal de Justiça da União Europeia	62
2.2.1 Transposição do direito da União à legislação nacional	63
2.2.1.1 Commission of the European Communities v. Kingdom of the Netherlands	63
2.2.1.2 Commission of the European Communities v. Grand Duchy of Luxemburg	64
2.2.1.3 Commission of the European Communities v. French Republic	65
2.2.2 Transferência internacional de dados pessoais, segurança nacional	66
2.2.2.1 Ireland v. European Parliament and Council of the European Union	66
2.2.2.2 Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeia	68
2.2.2.3 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources	70
2.2.2.4 Maximillian Schrems v. Data Protection Commissioner (Safe Harbor)	74
2.2.2.5 Tele2 (Netherlands) BV e o. v. Autoriteit Consument en Markt (ACM).....	78
2.2.2.6 Ministério Fiscal.....	80

2.2.2.7 Digital Rights Ireland Ltd v. Comissão Europeia	82
2.2.3 Privacidade e direito ao esquecimento	85
2.2.3.1 Google Spain SL v. Agencia Española de Protección de Datos.....	85
2.2.3.2 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni	89
2.2.3.3 GC e outros v. Commission nationale de l'informatique et des libertés – CNIL	91
2.2.3.4 Google LLC v. Commission nationale de l'informatique et des libertés – CNIL	95
2.2.4 Direitos autorais	99
2.2.4.1 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV.....	99
2.2.4.2 Digital Promusicae v. Telefónica de España SAU.....	102
2.2.4.3 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM.....	104
2.2.5 Direito do consumidor.....	105
2.2.5.1 Josef Probst v. mr.nexnet GmbH.....	105
2.2.5.2 Maximilian Schrems v. Facebook Ireland Limited.....	106
2.2.5.3 Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV.....	111
2.2.5.4 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH.....	114
2.2.5.5 Bavarian Lager.....	117
2.2.5.6 Deutsche Telekom AG v. Bundesrepublik Deutschland.....	119
2.2.6 Direito ao acesso dos dados pessoais	123
2.2.6.1 Patrick Kelly v. National University of Ireland.....	123
2.2.6.2 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert.....	124
2.2.6.3 Nils Svensson e outros v. Retriever Sverige AB.....	125
2.2.6.4 Tele2 Sverige AB v. Post-och telestyrelsen e Secretary of State for the Home Department v. Watson.....	127
2.2.6.5 Bodil Lindqvist.....	131
2.2.6.6 Rundfunk.....	133
2.2.6.7 Satamedia	134
2.3 Conclusão parcial	135
3 NOVAS PERSPECTIVAS PARA A PROTEÇÃO DE DADOS PESSOAIS	137
3.1 Globalização, dados pessoais e transferência internacional.....	137
3.2 Tendências das futuras atuações do Tribunal de Justiça da União Europeia	142
3.2.1 Privacy International e la Quadrature du Net e outros	142
3.2.2 Processo C-311/18 (Comissário de Proteção de Dados v. Facebook Ireland Ltd e Maximilian Schrems).....	143
3.2.3 Processo 620/19 (Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG).....	147

3.2.4 European Commission v. Kingdom of Spain.....	148
3.2.5 Facebook Ireland Limited e outros v. Gegevensbeschermingsautoriteit.....	149
3.2.6 Conclusão parcial	150
3.3 Ubiquidade do processamento de dados pessoais e as novas fronteiras.....	150
3.4 Proteção de dados pessoais um direito fundamental?	158
CONCLUSÃO.....	162
REFERÊNCIAS	166

INTRODUÇÃO

Atualmente, somos apanhados no meio de um cabo de guerra pelo controle sobre dados pessoais. Organizações privadas e governos têm um apetite insaciável por dados pessoais, confiando em sua capacidade de informar tomada de decisão e torná-lo mais eficiente. A quantidade de dados pessoais processados a cada ano continua a aumentar a exposição do indivíduo. O desenvolvimento tecnológico facilitou esse aumento dramático em volume de processamento de dados pessoais nas últimas décadas.

A tecnologia da informação e a Internet levaram à geração de mais dados pessoais. Uma vez gerados, esses dados são mais maleáveis e fáceis de editar e replicar graças à digitalização.

Embora o desenvolvimento tecnológico permita esse notável aumento do processamento de dados pessoais, o impulso para isso é explicado pelo aumento do valor de dados pessoais. Os dados pessoais são agora uma mercadoria; são valiosos e, portanto, procurados pela indústria privada e pelas autoridades públicas, fato que não escapou a atenção dos órgãos reguladores.

Informação é controle e controle é poder. Por isso, organizações privadas e governos têm um apetite insaciável pelo controle de dados, processo que é potencializado pelo desenvolvimento tecnológico, por meio do qual o processamento de dados pessoais foi facilitado nas últimas décadas. Como consequência, foi criado um sistema de proteção dos dados pessoais, sistema esse estruturado sobre o conceito da autodeterminação informacional. Essa é a reação do sistema jurídico à disputa pelo poder de controle dos dados, reação essa que, assim como a disputa pelos dados, se encontra em processo de desenvolvimento e consolidação.

A União Europeia inovou sobre o tema e continua sendo considerada como o principal modelo de regulamentação para responder ao fenômeno do processamento de dados pessoais. Formalmente, em 24 de outubro de 1995, aprovou-se a Diretiva 95/46/EC, relativa ao processamento de dados pessoais. A norma em questão exigia que cada Estado-Membro da União Europeia criasse uma agência ou tivesse um comissário de proteção de dados para supervisionar a aplicação dos princípios basilares deste direito, assim como exigiu que cada um destes Estados editasse leis nacionais sobre o processamento de dados pessoais. A Diretiva estabeleceu um prazo de 03 anos para tanto.

Como bem lembrou Viviane Reding, uma conhecida Comissária Europeia de Justiça, Direitos Fundamentais e Cidadania da União Europeia, quando o primeiro

instrumento legislativo a este respeito foi promulgado, apenas 1% da população da União Europeia tinha acesso direto à Internet e empresas tais como Google ainda não haviam sido lançados.¹

Essa mudança legislativa colocou desafios fundamentais para a regulamentação de proteção de dados pessoais. A diretiva estabeleceu um quadro de obrigações e salvaguardas que deveriam ser respeitadas por entidades envolvidas em processamento de dados pessoais, bem como direitos a serem exercidos por indivíduos. Tal regulamentação foi uma resposta clara ao fenômeno do processamento de dados pessoais.

O direito da União Europeia regulamentou a matéria da proteção de dados pessoais de forma autônoma e inovadora, buscando criar uma coerência interna em relação ao direito à privacidade. Mas essa previsão autônoma do direito à proteção de dados é um indício de que, ao contrário do que ocorre no direito norte-americano, no continente europeu a proteção de dados deve ser vista de forma diferenciada em relação ao direito à privacidade. Como essa diferenciação ocorre e o que isso significa para a proteção concreta desses direitos e para a tutela de seus titulares? E se a proteção de dados e a privacidade são, sob a ótica da União, direitos independentes e autônomos, seria possível a colisão desses direitos em situações específicas, com o afastamento da proteção de dados em razão da necessidade de se preservar a privacidade? Enfim, se a proteção de dados é um direito autônomo, a simples troca de informações pessoais já seria uma violação deste direito fundamental, independentemente dos efeitos concretos que esse ato venha a ocasionar?

A jurisprudência do Tribunal de Justiça União Europeia vem desenvolvendo a concepção prática a esse respeito. E a importância da determinação dos contornos desses direitos foi renovada por fatos e debates recentes. Vazamento de dados pessoais e escândalos públicos e privados, como as reveladas no episódio do compartilhamento não autorizado de dados entre *Facebook* e *Cambridge Analytica*,² deixam claro a atualidade da discussão sobre a privacidade e proteção de dados pessoais. Em uma sociedade constantemente vigiada e monitorada, indivíduos são identificados nos mínimos detalhes de sua vida pessoal. Como consequência, o poder dos controladores de dados pessoais (denominado Encarregado de Dados, na União Europeia) que se renova e multiplica com a coleta automatizada de dados pessoais. Todos esses fatores fazem com que a mesma pergunta seja constantemente e

¹ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 4.

² O caso envolveu a coleta não autorizada de aproximadamente 87 milhões de norte-americanos, ação que foi realizada com vistas a criar perfis comportamentais dos eleitores daquele país. A esse respeito, ver: ISAAK, J.; HANNA, M. J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, **Computer**, vol. 51, n. 8, p. 56-59, August 2018.

insistentemente repetida: afinal, o que significa e quais são os limites do direito à proteção de dados pessoais?

Nesse contexto, este estudo busca identificar as principais diretrizes da jurisprudência da União acerca da proteção dos direitos à privacidade e dados pessoais. Justifica-se, portanto, a análise dos julgados do Tribunal de Justiça da União Europeia, vez que se trata de uma comunidade de países que primordialmente debruçou-se o tema, inclusive com a adoção de normas que incentivaram outros países em muitas regiões do mundo a seguirem o seu exemplo. Essa é uma tendência verdadeiramente global, que vai do Chile³ à Coréia do Sul,⁴ do Brasil⁵ ao Quênia⁶ e da Índia⁷ ao estado da Califórnia,⁸ perpassando pela Indonésia.⁹

Além de ser uma oportunidade para revisitar conceitos-chave do regime de proteção de dados pessoais (dentre eles, os problemáticos conceitos de dados de pessoais e operações de tratamento), este exercício serve como antecipação de problemas jurídicos e práticos comuns a todos os órgãos nacionais ou internacionais que se proponham a regular essa matéria. Dentre eles, cite-se: as relações de tensão entre o conceito de proteção de dados pessoais e os direitos comunicativos em geral, especialmente os direitos a informar e ser informado, enfim, problemas decorrentes de operações de tratamento de dados (especialmente no âmbito da segurança ou saúde públicas), inclusive, as automatizadas e seus limites. Todos esses temas foram objeto de intenso debate na jurisprudência da União, que, neste sentido, pode e deve servir como um guia de possíveis caminhos para a solução desses conflitos. Observe-se que, na literatura brasileira não há registro de pesquisa a esse respeito nos portais *Scielo*, *Web of Science* e no portal de periódicos da CAPES.¹⁰ Dessa forma, a área do direito teria muito a ganhar com essa pesquisa, sobretudo tendo em vista o intenso debate a respeito da implantação do sistema nacional de proteção de dados pessoais.

³ Apesar da Lei chilena ser datada de 1999 (Lei 19.628), a partir da edição da GDPR, houve sua reforma para adequação aos termos europeus.

⁴ A Lei de Proteção de Informações Pessoais da Coréia do Sul foi promulgada em 2011 e atualizada em dezembro de 2018 para adequação aos termos europeus.

⁵ Houve a promulgação da Lei Geral de Proteção de Dados (LGPD) em 2018.

⁶ Em novembro de 2019, o Quênia promulgou a Lei de Proteção de Dados (Lei 24 de 2019).

⁷ Em 2019, a Índia aprovou a Lei de Proteção de Dados (PDPA).

⁸ Em 2018, a Califórnia aprovou a Lei de Privacidade do Consumidor (CCPA).

⁹ A Lei sobre Proteção de Dados Pessoais (PDP) da Indonésia foi aprovado em 2020.

¹⁰ Salienta-se que, na pesquisa de periódicos da CAPES, houve a identificação de 04 (quatro) artigos relativos ao direito ao esquecimento e o Tribunal de Justiça da União Europeia, o que compreende apenas uma fração ao que será estudado na presente pesquisa e poderão servir de base bibliográfica ao estudo. Em pesquisa independente, foi averiguada a Dissertação para obtenção do título de Mestrado de José Edilson Da Cunha Fontenelle Neto, com a seguinte nomenclatura “O DIREITO À PROTEÇÃO DE DADOS PESSOAIS (INFORMATIZADOS) ENQUANTO DIREITO FUNDAMENTAL AUTÔNOMO” (FONTENELLE NETO, José Edilson Da Cunha. O Direito À Proteção De Dados Pessoais (Informatizados) Enquanto Direito Fundamental Autônomo. Univali. Itajaí. 2019). Porém, não abarca por completo a pesquisa aqui intitulada, devido o estudo de casos realizado.

O objeto central do trabalho diz respeito ao conceito do direito fundamental aplicado por tal jurisprudência. Em meio a variações argumentativas e de concepções distintas a respeito das características deste direito, busca-se, em específico, verificar se a proteção de dados pessoais é identificada, pela jurisprudência da União, apenas como um instrumento para efetivação de outros direitos ou se é tratado como um direito autônomo, e quais são os reflexos dogmáticos dessa diferenciação. Parte da literatura europeia produzida a esse respeito é cética e crítica ao concluir que, com base na argumentação desenvolvida pelo Tribunal, não é possível concluir com clareza o caminho trilhado pelo Tribunal a esse respeito.¹¹

Importa, por isso, à esta pesquisa delimitar o conteúdo do direito à proteção de dados, tendo em conta a jurisprudência do Tribunal de Justiça da União Europeia (Tribunal). Para alcançar esse objetivo, serão utilizados textos acadêmicos a respeito do direito em questão, que servirão de fundamento para a determinação inicial do conteúdo da privacidade e dados pessoais. Esse material servirá como base teórica para a compreensão da jurisprudência coletada pela pesquisa. Ainda assim, será necessário delimitar a relação dos dois direitos e estabelecer o sentido do artigo 8º, para justificar sua inclusão na Carta dos Direitos Fundamentais da União Europeia. Afinal, se o direito à proteção de dados é realmente um mero subconjunto de privacidade e esses direitos deveriam se sobrepor, o acréscimo do artigo 8º à Carta seria destituído de significado e o direito à proteção de dados pessoais e poderia ser salvaguardado pela garantia à vida privada (artigo 7º), sem ter que fornecer regras de proteção de dados como um direito fundamental.

Assim, este trabalho acadêmico busca identificar padrões decisórios e características do direito fundamental abordado. Ele se insere, portanto, no campo da dogmática jurídica e da pesquisa jurisprudencial empírica do direito.¹² Divido em três partes, nele se pretende analisar a relação, ou falta dela, entre os direitos à privacidade e a proteção dos dados pessoais, enquanto direitos fundamentais no ordenamento jurídico da União Europeia, em consonância com os julgados dos anos de 1989 a 2019, do Tribunal de Justiça da União Europeia, com o intuito de delimitar o período temporal aos últimos 30 (trinta) anos do início do estudo.

Na primeira seção, será apresentado o Poder Judiciário da União Europeia, dispendo de breve histórico da sua criação até o funcionamento atual, assim como as bases jurídicas

¹¹ Nesse sentido: LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

¹² Note-se que utilizamos o termo “dogmática jurídica enquanto meio de trabalho do direito preocupado com a identificação de padrões normativos e com sua respectiva avaliação e sistematização” (FERRAZ JÚNIOR, Tércio Sampaio. *Introdução ao estudo do direito: técnica, decisão, dominação*. 10. ed. São Paulo: Atlas, 2018. p. 208-210).

relativas à proteção de dados pessoais existentes na União Europeia. Na segunda seção, será descrita a metodologia da coleta de casos para a pesquisa, com a categorização dos direitos abarcados nos julgados demonstrados na coleta, assim como a análise das perspectivas destes direitos, visando observar se há um direito autônomo à proteção de dados e a relação entre os direitos à proteção de dados pessoais e privacidade. Na terceira e última parte, far-se-á uma análise das novas perspectivas do direito à proteção de dados pessoais e os próximos desafios que este direito poderá enfrentar.

Este trabalho se alinha à área de concentração do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Campinas, uma vez que propicia o estudo de um importante Direito Fundamental garantido em Convenção Internacional (Convenção 108 do Conselho da Europa) e descrito na Carta de Direitos Fundamentais da União Europeia, sendo certo que constitui também direito previsto e garantido pelo sistema constitucional brasileiro.¹³ Fora isso, o tema mostra alinhamento direto com a Linha de Pesquisa “Cooperação Internacional e Direitos Humanos” ao pesquisar as repercussões da jurisprudência do Tribunal de Justiça da União Europeia frente a este direito, o que tem repercussões globais à sociedade da informação, notadamente no que se refere à orientação das atividades legislativas, jurisdicionais e administrativas.

¹³ Vale aqui registrar que em outubro de 2021, foi aprovada a Proposta de Emenda à Constituição (PEC) n.º 17, de 2019, que inclui a proteção de dados pessoais como um direito fundamental, no texto constitucional, introduzindo no art. 5º, da CF/88, o seguinte texto: “LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”. Anteriormente, o Supremo Tribunal Federal já havia garantido o direito à proteção de dados pessoais no Brasil, quando da análise acerca da ADI n.º 6387/2020. (SUPREMO TRIBUNAL FEDERAL. *ADI 6387*. Relatora Min. Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em 04 setembro 2021).

1 INSTITUIÇÕES JURÍDICAS DA UNIÃO EUROPEIA

1.1 Tratados originários da União Europeia

Na década seguinte do encerramento da 2ª Guerra Mundial, observou-se a construção de uma integração econômica entre países europeus, com a iniciativa dos Estados da Bélgica, Holanda e Luxemburgo em formar um Mercado Comum, com vistas ao crescimento e fortalecimento daquele continente, então desestruturado pelos efeitos daquela guerra.¹⁴ Na sequência, houve a criação da Comunidade Europeia do Carvão e do Aço (CECA), pelos Estados da Bélgica, França, República Federal da Alemanha, Luxemburgo, Itália e Países Baixos, sedimentando um acordo sólido com viés político e jurisdicional.¹⁵

Foram elaborados ainda dois Tratados de Roma, que entraram em vigor em 1958 e instituíram a Comunidade Econômica Europeia (CEE) e a Comunidade Europeia de Energia Atômica (EURATOM).¹⁶ A partir destes Tratados, houve a ampliação das “quatro liberdades” (de circulação dos trabalhadores, direito de estabelecimento, de prestação de serviços e circulação de capitais).¹⁷ Estes tratados são definidos como os tratados de fundação da Comunidade Europeia, posteriormente denominada União Europeia. Eles delegaram a soberania às instituições supranacionais e definiram os três importantes pilares do bloco europeu: a União Económica e Monetária (UEM), a Política Externa e de Segurança Comum (PESC) e a Justiça e Assuntos Internos (JAI).¹⁸ A criação da Comunidade Econômica Europeia estabeleceu ainda uma união aduaneira, que criou condições para integrar o mercado europeu e a integração dos mercados.¹⁹

No que diz respeito à capacidade institucional, os tratados fundadores introduziram um Poder Executivo supranacional, que tem independência para tomar decisões especialmente na

¹⁴ ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985. p. 50.

¹⁵ PIOVESAN, Flávia. *Direitos humanos e justiça internacional: um estudo comparativo dos sistemas regionais europeu, interamericano e africano*. 9. ed. rev., atual. e ampl. São Paulo: Saraiva, 2019. p. 33.

¹⁶ ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985. p. 50.

¹⁷ MANCINI, Federico G. *The making of a Constitution for Europe*. Common Market Law Review, 1989. p. 595-614. p. 603.

¹⁸ MANCINI, Federico G. *The making of a Constitution for Europe*. Common Market Law Review, 1989. p. 595-614. p. 604.

¹⁹ ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985. p. 51.

área de política de concorrência.²⁰ Desde a sua fundação, ao Tribunal de Justiça da União Europeia (inicialmente, denominado Tribunal de Justiça da Comunidade Europeia) foi atribuído o papel de Poder Judiciário da União.²¹ Paralelamente, houve a fundação do Parlamento Europeu, com poderes legislativos exercidos em conjunto ao Conselho de Ministros.²² A União Europeia é, portanto, uma construção única e singular no direito internacional e sua criação não só afetou as relações entre Estados-Membros europeus, mas também se tornou um importante ator internacional, especialmente no domínio do comércio e do desenvolvimento econômico.²³

1.2 Tratados constitutivos da União Europeia

Os tratados fundadores foram reformados (ou alterados) em diversas ocasiões, começando com o chamado Tratado de Fusão de 1965 e dois tratados relacionados ao orçamento, de 1970 e 1975. Seguiu-se uma reforma do Ato Único Europeu (SEA) de 1986, cujo objetivo principal foi criar a base institucional para a concretização do Mercado Comum, atualmente referido como o Mercado Interno.²⁴ O SEA foi um marco legal importante para o reconhecimento da soberania nacional, também denominado como princípio do reconhecimento mútuo²⁵, pela União e pelos Estados-Membros e da não discriminação com base na nacionalidade, vez que ele estipulava que “o Conselho, deliberando nos termos do disposto no artigo 100º-A, pode decidir que certas disposições em vigor num Estado-Membro devam ser reconhecidas como equivalentes às aplicadas por outro Estado-Membro”.²⁶ Este ato foi necessário após o julgamento do Processo C-120/78, conhecido como “Cassis de Dijon”, no qual uma fabricante francesa de licores foi excluída da comercialização de seus produtos na Alemanha com o fundamento no fato de que o seu teor alcoólico era demasiado

²⁰ LAURSEN, Finn. *The founding treaties of the European Union and their reform*. Oxford Research Encyclopedia of Politics, 2016. p. 1-28. p. 12.

²¹ LAURSEN, Finn. *The founding treaties of the European Union and their reform*. Oxford Research Encyclopedia of Politics, 2016. p. 1-28. p. 12.

²² LAURSEN, Finn. *The founding treaties of the European Union and their reform*. Oxford Research Encyclopedia of Politics, 2016. p. 1-28. p. 12.

²³ LAURSEN, Finn. *The founding treaties of the European Union and their reform*. Oxford Research Encyclopedia of Politics, 2016. p. 1-28. p. 13.

²⁴ ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985. p. 50.

²⁵ STORY, Jonathan. The origins, launching and consequences of ‘1992’ and the euro. In: WEBBER, D.; FORT, B. (org.). *Regional integration in Europe and East Asia: convergence or divergence?* London: Routledge, 2006. p. 85-108. p. 89.

²⁶ UNIÃO EUROPEIA. Artigo 100º B. *Ato Único Europeu*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:11986U/TXT&from=PT>. Acesso em: 19 fev. 2021.

baixo para ser classificado como licor ao abrigo do direito alemão.²⁷ O Tribunal decidiu que um Estado-Membro não pode aplicar a legislação nacional aos produtos importados de outro país-membro.²⁸

O próximo Tratado constitutivo foi o tratado formador da União Europeia propriamente dita, conhecido como Tratado de Maastricht, documento que foi assinado no dia 7 de fevereiro de 1992 pelos membros da Comunidade Europeia.²⁹ Com sua entrada em vigor no dia 1º de novembro de 1993, foi criada a União Europeia e foram lançadas as bases para a criação de uma moeda única europeia.³⁰ Com isso criou-se também uma nova instituição supranacional, o Banco Central Europeu (BCE), ao qual os governos nacionais delegaram a decisão em assuntos de política monetários supranacionais. O BCE tem independência para tomada de decisões.³¹ Na sequência deve ser citado o Tratado de Nice, assinado no ano de 2000. Com ele ocorreu uma mudança importante: o esperado alargamento da quantidade de membros ativos da União, o que gerou a necessidade da revisão nas modalidades de votação e a composição do Conselho europeu.³² No Tratado de Nice foi também redigida e aprovada a Carta dos Direitos Fundamentais da União Europeia.³³

Na sequência, houve a formulação do Tratado de Amsterdã, o qual alterou o Tratado da União Europeia e os Tratados constitutivos das Comunidades Europeias sendo que foi assinado em Amesterdão, em outubro de 1997, e entrou em vigor em 1 de maio de 1999. O tratado fez-se necessário para reforçar o papel de cooperação judiciária e policial da União, assim como, alterou as funções legislativas da União, sendo que o Parlamento Europeu e o Conselho tornaram-se colegisladores, com igualdade de poder para esta função.³⁴

²⁷ Processo C-120/78. *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*. Julgamento em: 20 fevereiro 1979.

²⁸ Processo C-120/78. *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*. Julgamento em: 20 fevereiro 1979.

²⁹ O tratado é considerado como um marco significativo no processo de integração europeia, uma vez que tinha como o objetivo econômico inicial das Comunidades Europeias, ultrapassou suas barreiras e tomou uma dimensão mais política e integralizadora. (NADER, Paulo. *Introdução ao estudo do direito*. 15. ed. Rio de Janeiro: Forense, 1997).

³⁰ ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985. p. 55.

³¹ STORY, Jonathan. The origins, launching and consequences of '1992' and the euro. In: WEBBER, D.; FORT, B. (org.). *Regional integration in Europe and East Asia: convergence or divergence?* London: Routledge, 2006. p. 85-108. p. 91.

³² LAURSEN, Finn. The treaty of Nice: the inadequate preparation of enlargement. In: LAURSEN, Finn. *Designing the European Union From Paris to Lisbon*. Palgrave Studies in European Union Politics, 2012. p. 196-216. p. 196.

³³ LAURSEN, Finn. The treaty of Nice: the inadequate preparation of enlargement. In: LAURSEN, Finn. *Designing the European Union From Paris to Lisbon*. Palgrave Studies in European Union Politics, 2012. p. 196-216. p. 196.

³⁴ JACQUÉ, Jean Paul. *Droit institutionnel de l'Union Européene*. 4. ed. Paris: Dalloz, 2006. p. 45

Posteriormente, o Tratado de Lisboa, também denominado “Tratado Reformador”, foi assinado pelos Estados-Membros da União Europeia, em 13 de dezembro de 2007. Tal documento reformou o funcionamento da União a partir de 1 de dezembro de 2009, quando entrou em vigor.³⁵ Ele alterou substancialmente a União Europeia e transformou a Carta dos Direitos Fundamentais em uma base jurídica para a União como um todo. A adesão da União à Carta passou a ser vista como uma obrigação da organização supranacional.³⁶ Por isso, este Tratado foi reconhecido como um avanço na proteção de liberdades e direitos, uma vez que tornou a Carta de Direitos Fundamentais da União Europeia formalmente vinculante³⁷ para as instituições da União e para os Estados-Membro, no domínio do Direito da União.³⁸

Salienta-se que a característica peculiar da Comunidade Europeia é realizar a cooperação internacional, realizada mediante o emprego de processos integradores capazes de consolidarem no grupo de suas partes um nível de coesão interna de expressão comunitária.³⁹ Destarte, o direito da União Europeia é composto de tratados constitutivos, classificados como normas de caráter originário e de atos normativos, classificados como normas derivadas, sendo que ambos são obrigatórios para os Estados-Membros e instituições.⁴⁰ Compõe-se, portanto, que os tratados formadores e constitutivos da União Europeia: o Tratado de Roma, o Ato Único Europeu e o Tratado da União Europeia. Já os reformadores são: o Tratado de Nice, o Tratado de Amsterdã, enfim, o Tratado de Lisboa, sendo os atos normativos derivados chamados de regulamentos, diretivas, decisões, recomendações e pareceres.

1.3 Normas da União Europeia

³⁵ PIOVESAN, Flávia. *Direitos humanos e justiça internacional: um estudo comparativo dos sistemas regionais europeu, interamericano e africano*. 9. ed. rev., atual. e ampl. São Paulo: Saraiva, 2019. p. 35.

³⁶ WENNERSTRÖM, Erik. *EU Accession to the European Convention on Human Rights: the creation of a european legal space for human rights or the last stand for the normative supremacy of the strasbourg system?* *Europarättslig Tidskrift*, 2013. v. 2. p. 375.

³⁷ Registra-se que há 02 (dois) países que, à época, registraram restrição formal à aplicação vinculante da Carta, conforme será mais bem discutido em tópico posterior. Para maior debate sobre a vinculação variável da Carta, ver: GROS-VERHEYDE, N. Une Charte à valeur juridique variable. *Europolitique*, n. 3407, 2007. p. 13.

³⁸ WENNERSTRÖM, Erik. *EU Accession to the European Convention on Human Rights: the creation of a european legal space for human rights or the last stand for the normative supremacy of the strasbourg system?* *Europarättslig Tidskrift*, 2013. v. 2. p. 375.

³⁹ SEGUELA, Ana de Bustos. Métodos de información. *Los documentos del Tribunal de Justicia de la Unión Europea*, Madrid, v. 3, n. 11-12, p. 54-59, maio/jul. 1996. p. 55.

⁴⁰ Nos primeiros instrumentos legais que instituíram as Comunidades Europeias havia o predomínio do papel econômico ante ao social, sobretudo em razão da natureza econômica contida nos tratados, sendo que à época não havia interesse pela interferência da legislação comunitária e dos direitos humanos nos direitos nacionais (JACQUÉ, Jean Paul. *Droit institutionnel de l'Union Européene*. 4. ed. Paris: Dalloz, 2006. p. 54).

Antes de adentrar no campo prático das normas legais relativas à proteção de dados pessoais na União Europeia, será apresentada breve explanação sobre as normas legais existentes naquele domínio. O Tratado de Funcionamento da União Europeia previa a criação de novas normas pelas instituições da União para dar seguimento aos seus objetivos. Estas legislações são frequentemente denominadas “legislações secundárias” e é importante observar que a União não tem um poder geral de legislar, mas somente pode legislar na medida em que tal poder lhe foi conferido pelos Tratados pertinentes.⁴¹ Há 05 (cinco) principais instrumentos normativos na União Europeia, quais sejam: (i) Regulamento; (ii) Diretiva; (iii) Decisão; (iv) Recomendação; (v) Parecer. A União tem liberdade na escolha destes instrumentos, mas existem dois tipos principais de legislações secundárias: as diretivas e os regulamentos.⁴²

As Diretivas estão previstas no artigo 288, do Tratado. Em princípio, trata-se de uma medida de alcance geral que exige que os Estados-Membros alcancem certos resultados, mas designa para cada um destes a forma e o método de sua implementação de forma nacional. Assim, uma diretiva prevê que os Estados-Membros terão de tomar medidas para aplicá-lo no próprio sistema jurídico desse Estado-Membro, ação que é desnecessária apenas nos casos em que o sistema jurídico do Estado-Membro já é adequado para alcançar os resultados em questão.⁴³ As Diretivas são utilizadas quando é considerado que as regras em questão podem precisar ser implementadas de diferentes maneiras nos diferentes Estados-Membros, tendo em conta diferentes circunstâncias – como diferentes aspectos administrativos, sociais ou políticos. São também úteis se não for prático fornecer todos os detalhes das regras, a nível da União. Em sua jurisprudência, o Tribunal de Justiça da União Europeia esclareceu aspectos da implementação nacional das diretivas.

O Tribunal considerou que as condições necessárias a implementar uma diretiva dependem de sua natureza. Isso quer dizer que a legislação nacional deve prever medidas que sejam eficazes para proteger os objetivos desta espécie legislativa.⁴⁴ Faz-se necessário ainda implementar medidas para que as regras da Diretiva sejam exequíveis dentro do sistema nacional contra terceiros.⁴⁵ Isto significa que, em geral, os Estados-Membros devem

⁴¹ NEWMAN, Abraham L. *Protectors of privacy: regulating personal data in the global economy*. Ithaca; London: Cornell University Press, 2008. p. 75.

⁴² NEWMAN, Abraham L. *Protectors of privacy: regulating personal data in the global economy*. Ithaca; London: Cornell University Press, 2008. p. 75.

⁴³ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001.

⁴⁴ Processo C-433/93. *Comissão das Comunidades Europeias contra República Federal da Alemanha*. Julgamento em: 11 agosto 1995.

⁴⁵ Processo C-433/93. *Comissão das Comunidades Europeias contra República Federal da Alemanha*. Julgamento em: 11 agosto 1995.

implementar as Diretivas, promulgando na legislação nacional normas que assumam forma legalmente vinculativas.⁴⁶

Uma questão importante na legislação da União ocorre quando um Estado-Membro não implementa uma Diretiva devidamente em sua legislação nacional, quando o prazo para implementação se evadiu, ou porque não implementou a medida, ou porque há algum tipo de erro, omissão ou outro defeito de implementação.⁴⁷ Há, inclusive, processos judiciais a respeito das legislações de proteção de dados pessoais que trataram desta questão, na qual a Comissão Europeia (ou outro Estado-Membro) apresentou ação para fazer com que algum Estado-Membro corrija a falha.⁴⁸

Nos casos de não implementação da diretiva no período determinado pela União, é possível que o Tribunal da União imponha uma multa pecuniária, com o intuito de reforçar a medida e garantir sua devida implementação, ainda que o Estado-Membro esteja em processo legislativo para sua implementação.⁴⁹ Fora isso, o Tribunal, em importante julgamento, admitiu que em alguns casos, as regras dispostas em diretivas podem ser aplicadas diretamente, sem a necessidade de transposição da medida ao Estado-Membro. Esta medida é denominada “doutrina do efeito direto das diretivas”.⁵⁰

Para ter efeito direto,⁵¹ uma disposição deve atender certas condições que foram desenvolvidas a partir do julgamento do caso *Van Gend en Loos*.⁵² Para isso, a Diretiva deve ser suficientemente clara e inequívoca em seu conteúdo, para fins judiciais (i) estabelecer uma obrigação incondicional (por exemplo, não deve ser sujeita a condições que exijam o exercício de uma escolha pelos Estados-Membros para a sua implementação) (ii) não depender de medidas adicionais a serem tomadas pelo Estado-Membro, enfim, (iii) ser capaz de criar direitos para os indivíduos.⁵³

⁴⁶ Processo C-433/93. *Comissão das Comunidades Europeias contra República Federal da Alemanha*. Julgamento em: 11 agosto 1995.

⁴⁷ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 96.

⁴⁸ Verificar o capítulo 3 desta dissertação.

⁴⁹ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 97.

⁵⁰ Processo C-26/62. *NV Algemene Transport en Expeditie Onderneming Van Gend & Loos contra Administração Fiscal neerlandesa*. Julgamento em: 05 fevereiro 1963.

⁵¹ Sobre o desenvolvimento da teoria dos “efeitos diretos”, ver: SWEET, Alec Stone. Constitutional dialogues in the european community. In: SLAUGHTER, Anne-Marie; SWEET, Alec Stone; WEILER, J. H. H. (org.). *The European Court and National Courts – doctrine and jurisprudence*. Legal Change in Its Social Context. Oxford: Hart Publishing, 1998. p. 305-330.

⁵² Salienta-se que, também, houve o desenvolvimento das teorias do “efeito indireto” e, posteriormente, da “responsabilidade governamental”. Sobre o tema: SWEET, Alec Stone. Constitutional dialogues in the european community. In: SLAUGHTER, Anne-Marie; SWEET, Alec Stone; WEILER, J. H. H. (org.). *The European Court and National Courts – doctrine and jurisprudence*. Legal Change in Its Social Context. Oxford: Hart Publishing, 1998. p. 305-330.

⁵³ Processo C-26/62. *NV Algemene Transport en Expeditie Onderneming Van Gend & Loos contra Administração Fiscal neerlandesa*. Julgamento em: 05 fevereiro 1963.

Já os Regulamentos são de aplicação geral e imediata. Eles vinculam de forma direta os Estados-Membros e indivíduos e anulam qualquer disposição inconstante da legislação nacional, assim como não necessitam de qualquer ação adicional pelos Estados-Membros para sua eficácia.⁵⁴ Trata-se, portanto, de norma que impõe um direito a toda a União, com validade uniforme e integral em todos os Estados-Membros. O direito à proteção de dados pessoais é um importante exemplo da diferença entre Diretiva e Regulamento, sendo certo que a primeira norma geral sobre o assunto foi uma Diretiva, a qual evoluiu para a construção de um Regulamento próprio e singular, que está em vigor no presente momento.

Outra espécie legislativa é a Decisão. As Decisões podem ser criadas por várias instituições da União, que atuam monocrática ou coletivamente e são geralmente relacionadas com a implementação de outra legislação abrangente, como a Diretiva ou Regulamento.⁵⁵ A Decisão é obrigatória em seus elementos, e somente tem aplicabilidade individual – quando designa seus destinatários. Caso não haja tal designação tem aplicação coletiva e difusa. Para esse efeito, basta que o universo dos destinatários seja identificável e que tal universo não possa, posteriormente, ser alterado. O conteúdo da Decisão deve ser adequado a produzir efeitos diretos e precisos, sendo vinculativa em todos os seus elementos e com aplicabilidade direta aos seus destinatários, o que a distingue da Diretiva.

Por fim, existem as categorias das Recomendações e Pareceres. Elas permitem às instituições da União disponibilizarem pronunciamentos de forma não vinculativa.⁵⁶ As Recomendações sugerem aos destinatários um dado comportamento, sem a existência da imposição legal. Já os Pareceres são emitidos pelas instituições da União, sempre que se revele oportuno apreciar uma dada situação. Em certos casos, os Pareceres podem criar condições à posterior formulação de atos vinculativos; ou seja, são informações prévias para a formulação de normativas vinculativas posteriores.⁵⁷ Deste modo, verifica-se que a normativa legal da União Europeia tem forte vinculação à legislação nacional.⁵⁸ Este aspecto da relação entre o direito da União Europeia e o direito nacional abrange os domínios em que ambos se completam mutuamente.⁵⁹

⁵⁴ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 54.

⁵⁵ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 58.

⁵⁶ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 59.

⁵⁷ Ver artigos 258 e 259, do Tratado.

⁵⁸ QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001. p. 60.

⁵⁹ O artigo 4º (3), do Tratado, ilustra esta relação: “Em virtude do princípio da cooperação leal, a União e os Estados-Membros respeitam-se e assistem-se mutuamente no cumprimento das missões decorrentes dos tratados. Os Estados-Membros tomam todas as medidas gerais ou específicas adequadas para garantir a execução das obrigações decorrentes dos tratados ou resultantes dos actos das instituições da União. Os Estados-Membros facilitam à União o cumprimento da sua missão e abstêm-se de qualquer medida susceptível de pôr em perigo a realização dos objetivos da União”.

1.4 As normas relativas à proteção de dados pessoais na União Europeia

As regulamentações sobre proteção à dados pessoais foram desenvolvidas em resposta à crescente quantidade de informações pessoais reunidas pelo Estado e grandes empresas, normalmente por meio de computadores.⁶⁰ Em relação às normativas sobre o direito à proteção de dados, a Convenção Europeia dos Direitos Humanos, de 1950, contém o direito à privacidade em seu bojo, conceito que tem vinculação direta com à proteção de dados pessoais.⁶¹ Assim, o artigo 8º, da Convenção protege o direito à vida privada e, em princípio, proíbe a interferência com o direito à privacidade.⁶² No entanto, o parágrafo 2º, mostra que esta proibição não é absoluta e, em muitos casos, o direito à privacidade pode ser limitado por outros interesses, como a segurança pública, ou direitos de terceiros.⁶³

Com base nesses parâmetros, diversos países europeus aprovaram na década de 1970 legislações sobre a proteção de dados. Algumas dessas leis continham restrições à exportação de dados pessoais, uma vez que os legisladores nacionais pretendiam evitar que os dados de seus cidadãos fossem exportados para países sem a proteção legal suficiente.⁶⁴ Para que fosse criada a futura resolução de forma continental sobre a matéria, foi editada em 1973 a Resolução (73) 22 (*Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector*), que incentivava os países da União Europeia a adotarem princípios mínimos sobre a matéria em comento com o intuito de aprofundarem as linhas comuns.⁶⁵ Em

⁶⁰ BENNETT, Colin. *Regulating privacy, data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992. p. 48.

⁶¹ No capítulo 2 da presente tese, debateremos essa vinculação entre os direitos.

⁶² Para um maior debate sobre a diferença entre “privacidade” e “vida privada”, ver: FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer. 2014. p. 214.

⁶³ De acordo com o texto do dispositivo: “1. Toda pessoa tem direito ao respeito por sua vida privada e familiar, seu lar e seu correspondência. 2. Não deve haver interferência de uma autoridade pública no exercício deste direito, exceto como está de acordo com a lei e é necessário em uma sociedade democrática no interesse de segurança nacional, segurança pública ou o bem-estar econômico do país, para a prevenção de desordem ou crime, para a proteção da saúde ou da moral, ou para a proteção dos direitos e liberdades de outros”.

⁶⁴ Sobre o tema: KOSTELNY JR., Albert J. *Emerging data protection in Europe: community law through the cases*. Fordham International Law Journal, v. 1, Issue 1, p. 71-75, 1997; MAYER-SCHÖNBERGER, Viktor. *Generational development of data protection in Europe*. Technology and privacy: the new landscape, 1997. p. 219-241.

⁶⁵ COMMITTEE of Ministers. Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973). Disponível em: <http://www.legislationline.org/documents/id/6498>. Acesso em: 24 mar. 2021.

1990, a União Europeia interveio para harmonizar a proteção de dados na União Europeia e apresentou uma proposta de Diretiva geral sobre o assunto.⁶⁶

Esta intervenção foi justificada pelo fato de a Comissão Europeia temer que as legislações nacionais fossem divergentes sobre a proteção de dados e prejudicassem o mercado interno comum. Neste mesmo ano, publicou-se uma proposta de Diretiva e, após cinco anos de negociações, a Diretiva de Proteção de Dados foi adotada.⁶⁷ Tal qual as demais diretivas da União, esta também exigia que os Estados-Membros aprovassem legislação de implementação. E esta Diretiva foi, provavelmente, a mais influente norma precursora sobre privacidade e proteção de dados pessoais no mundo.⁶⁸ Ela tinha dois objetivos. O primeiro era proteger as “liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais”.⁶⁹ O segundo foi salvaguardar o livre fluxo de dados pessoais entre Estados-Membros da União, indicando que os Estados “não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros”.⁷⁰

A Diretiva concedia, assim, direitos às pessoas físicas cujos dados eram processados e impunha obrigações às partes que realizem atos de tratamento de dados pessoais de forma segura e transparente (controladores de dados, no caso do Brasil e encarregados de dados, no caso da União Europeia).⁷¹ Continha ainda princípios para um processamento de dados justo, comparável aos princípios de práticas de informações justas.⁷² Como exemplo desta orientação, os dados pessoais deveriam ser processados de forma legal, justa e transparente (legalidade, justiça e transparência).⁷³ Fora isso, os dados pessoais coletados para uma finalidade não poderiam ser usados para fins diversos (limitação de propósito).⁷⁴ Os dados coletados deveriam ainda ser adequados, relevantes e limitados, ao que é necessário às finalidades de processamento (minimização de dados).⁷⁵

⁶⁶ SOLOVE, Daniel J.; SCHWARTZ, Paul M. *Information privacy law*. 7. ed. New York: Wolters Kluwer, 2021. p. 41.

⁶⁷ Sobre a história da Diretiva: NEWMAN, Abraham L. *Protectors of privacy: regulating personal data in the global economy*. Ithaca; London: Cornell University Press, 2008.

⁶⁸ SOLOVE, Daniel J.; SCHWARTZ, Paul M. *Information privacy law*. 7. ed. New York: Wolters Kluwer, 2021. p. 67.

⁶⁹ Artigo 1º, (1), da Diretiva relativa à proteção de dados.

⁷⁰ Artigo 1º, (2), da Diretiva relativa à proteção de dados.

⁷¹ NEWMAN, Abraham L. *Protectors of privacy: regulating personal data in the global economy*. Ithaca; London: Cornell University Press, 2008. p. 7.

⁷² GELLMAN, Robert. Fair information practices: a basic history. *SSRN Electronic Journal*, 2017. p. 14.

⁷³ Artigo 6º, da Diretiva de Proteção de Dados

⁷⁴ Artigo 6º, alínea “b”, da Diretiva Proteção de Dados.

⁷⁵ Artigo 6º alínea “c”, da Diretiva de Proteção de Dados.

Contudo, com o passar dos anos, foi verificada a falta de harmonização entre as transposições da Diretiva pelos Estados-Membros da União. Por isso, surge em 2016, porém entra em vigor em 2018 o Regulamento Geral sobre a Proteção de Dados, que substituiu a Diretiva. Embora seja baseado nos mesmos princípios, o Regulamento tem como objetivo construir um regime mais harmonizado sobre o tema, tema que será aprofundado no decorrer deste trabalho.⁷⁶ Em conclusão há que se observar que, tanto Convenções Internacionais, como o Direito da União protegem o direito à proteção de dados pessoais,⁷⁷ e que a proteção de dados foi construída de forma progressiva e complexa no ambiente europeu. Uma das tarefas deste trabalho é detalhar e expor este desenvolvimento.

Paralelamente, importante registra a existência de mais três instrumentos complementam o Regulamento Geral sobre a Proteção de Dados, em matéria de proteção de dados. Em primeiro lugar, a Diretiva 2016/680, aplica-se à proteção e tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Em segundo lugar, a Diretiva 2002/58/CE, aplica-se aos dados pessoais e à proteção da privacidade nas comunicações eletrônicas, no que diz respeito à segurança, violação de dados e confidencialidade das comunicações, a qual será melhor analisado posteriormente. Em terceiro lugar, o Regulamento 2018/1725 que estabelece as obrigações de proteção de dados das instituições e órgãos da União, durante o processamento de dados pessoais e o desenvolvimento de novas políticas públicas.

1.5 Carta dos Direitos Fundamentais da União Europeia e a Convenção nº 108 do Conselho da Europa

Em 1981 o Conselho da Europa (e não a União Europeia) adotou o primeiro instrumento transnacional sobre proteção de dados, a Convenção de Proteção de Dados nº 108 (Convenção).⁷⁸ Seu objetivo era proteger os indivíduos contra tratamento ilegal de dados pessoais, tanto na esfera privada como pública e também conciliar o respeito à privacidade e o

⁷⁶ Até que ponto o regulamento irá realmente harmonizar as regras de proteção de dados é uma questão em discussão, ver, por exemplo, BLUME, Peter. The myths pertaining to the proposed general data protection regulation. *International Data Privacy Law*, v. 4, n. 4, p. 269-273, 2014.

⁷⁷ LENAERTS, Koen; GUTIÉRREZ-FONS, José Antonio. The place of the Charter in the EU constitutional edifice. In: PEERS, Steve; HERVEY, Tamara; KENNER Jeff; WARD (org.). *The EU Charter of fundamental rights: a commentary*. Hart Publishing, 2014. p. 1559-1594. p. 1561.

⁷⁸ Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais CETS nº: 108, 28 de janeiro de 1981. A Convenção está em revisão: <http://www.coe.int/en/web/data-protection/modernisation-convenção108>.

livre fluxo de informações.⁷⁹ O texto exigia que os signatários promulgassem disposições nacionais sobre de proteção de dados e até hoje, a Convenção continua sendo a única peça vinculativa internacional para proteção de dados pessoais.⁸⁰ Em seu bojo, a Convenção contém disposições explicativas sobre a terminologia da proteção de dados, abordando conceitos como o de dados pessoais, processamento automático, controlador do arquivo ou arquivo de dados automatizado.⁸¹ Contém, também, os princípios da proteção de dados e a forma das disposições substantivas que os países devem garantir em seus sistemas jurídicos domésticos, o que inclui a obrigação de processamento justo e legal, armazenamento de dados para fins legítimos especificados e a proibição de uso fora do propósito declarado. De acordo com a Convenção, os dados em processamento automático devem ser adequados, relevantes, precisos e não excessivos no que diz respeito ao propósito de seu armazenamento, não podendo haver armazenamento por período maior do que o necessário.⁸²

Além disso, o texto prevê que a proteção aos denominados “dados sensíveis” (dados pessoais revelando origem racial, opiniões políticas ou religiosas ou outras crenças, como bem como as que dizem respeito à saúde ou à vida sexual) é reforçada, na medida em que a Convenção contém uma proibição geral de seu processamento automático na ausência de salvaguardas garantidas pelos sistemas jurídicos nacionais.⁸³ Por fim, a Convenção garante o direito de acesso do titular ao armazenamento de seus dados e o direito de providenciar sua correção ou exclusão.⁸⁴ E incorpora regras especiais sobre fluxos de dados transfronteiriços e mecanismos de assistência mútua para as partes contratuais.⁸⁵ Diante de sua relevância, em 1981 a Comissão Europeia (instituição da União Europeia) solicitou aos seus Estados-Membros a ratificação da Convenção de Proteção de Dados.⁸⁶ No entanto, até 1990 apenas sete Estados-Membros o fizeram.⁸⁷

Por outro lado, a Carta dos Direitos Fundamentais da União Europeia (Carta) foi redigida no ano de 2000 e se tornou vinculante no ano de 2009. Este é considerado o ato

⁷⁹ Considerando 4, da Convenção 108.

⁸⁰ EUROPEAN Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2014. p. 16. Disponível em: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. Acesso em 8 jan. 2021.

⁸¹ Artigo 2º, da Convenção 108.

⁸² Artigo 5º, da Convenção 108.

⁸³ Artigo 6º, da Convenção 108.

⁸⁴ Artigo 8º, da Convenção 108.

⁸⁵ Artigos 12-17, da Convenção 108.

⁸⁶ COMISSÃO Europeia. *Recomendação 81/679/CEE de 29 de julho de 1981 relativa à Convenção do Conselho da Europa para a proteção de pessoas no que diz respeito ao tratamento automático de dados pessoais*. 1981. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31981H0679&from=PT>. Acesso em: 19 jan. 2021.

⁸⁷ PLATTEN, N. Background to and history of the directive. In: BAINBRIDGE, D. *EC data protection directive*. London: Butterworths, 1996. p. 13-32. p. 14.

jurídico autônomo sobre o tema perante a União. O objetivo da Carta é expandir e abranger os direitos fundamentais à toda União.⁸⁸ Consiste em seis capítulos contendo direitos e um capítulo com disposições gerais sobre seu escopo.⁸⁹ De acordo com seu artigo 51, a Carta é aplicável apenas “às instituições, órgãos e agências da União, observância do princípio da subsidiariedade, bem como aos Estados-Membros apenas quando se aplicam Direito da União”. Os seis capítulos de conteúdo material contêm direitos com base em dignidade, liberdade, igualdade, solidariedade, cidadania e justiça. Por isso mesmo, a Carta deve ser aplicada a um leque diverso de matérias, entre as quais se incluem o apoio judiciário,⁹⁰ sanções às infrações aduaneiras,⁹¹ cartéis,⁹² doação de sangue,⁹³ exploração de máquinas de jogo de azar,⁹⁴ apoio ao desenvolvimento rural,⁹⁵ publicidade das organizações de radiodifusão,⁹⁶ divulgação de documentos contábeis,⁹⁷ obrigação de recolher impressões digitais de passaporte.⁹⁸

A Carta pode ser invocada por todas as pessoas que estejam no âmbito territorial da União,⁹⁹ inclusive por pessoas jurídicas de direito público.¹⁰⁰ A Polónia e o Reino Unido registraram a subordinação variável à Carta após tentativas de não haver vinculação direta aos seus termos, isso apesar de haver determinações do Tribunal de Justiça em sentido contrário.¹⁰¹ De fato, a supremacia e a primazia das normas da União sobre as de direito

⁸⁸ “Uma vez que os direitos fundamentais garantidos pela Carta devem [...] ser respeitados quando uma regulamentação nacional se enquadra no âmbito de aplicação do direito da União, não podem existir situações que estejam abrangidas pelo direito da União em que os referidos direitos fundamentais não sejam aplicados. A aplicabilidade do direito da União Europeia implica a aplicabilidade dos direitos fundamentais garantidos pela Carta” (Processo C-617/10. *Åklagaren v. Hans Åkerberg Fransson [GS]*. Julgamento em: 26 fevereiro 2013. Parágrafo 21).

⁸⁹ Dignidade (5 artigos), Liberdades (14 artigos), Igualdade (7 artigos), Solidariedade (12 artigos), Cidadania (8 artigos), Justiça (4 artigos) e Disposições gerais (4 artigos).

⁹⁰ Processo C-279/09. *DEB Deutsche Energiehandels – und Beratungsgesellschaft mbH v. Bundesrepublik Deutschland*. Julgamento em: 22 dezembro 2010.

⁹¹ Processo C-546/09. *Aurubis Bulgaria AD v. Nachalnik na Mitnitsa Stolichna*. Julgamento em: 31 março 2011.

⁹² Processo C-17/10. *Toshiba Corporation e outros v. Úřad pro ochranu hospodářské soutěže*. Julgamento em: 14 fevereiro 2012.

⁹³ Processo C-528/13. *Geoffrey Léger v. Ministre des Affaires sociales, de la Santé et des Droits des femmes e Etablissement français du sang*. Julgamento em: 29 abril 2015.

⁹⁴ Processo C-390/12. *Robert Pflieger e outros*. Julgamento em: 30 abril 2014.

⁹⁵ Processo C-401/11. *Blanka Soukupová v. Ministerstvo zemědělství*. Julgamento em: 11 abril 2013.

⁹⁶ Processo C-234/12. *Sky Italia Srl v. Autorità per le Garanzie nelle Comunicazioni*. Julgamento em: 18 julho 2013.

⁹⁷ Processo C-418/11. *Texdata Software GmbH*. Julgamento em: 26 setembro 2013.

⁹⁸ Processo C-291/12. *Michael Schwarz v. Stadt Bochum*. Julgamento em: 17 outubro 2013.

⁹⁹ Processo C-279/09. *DEB Deutsche Energiehandels – und Beratungsgesellschaft mbH v. Bundesrepublik Deutschland*. Julgamento em: 22 dezembro 2010.

¹⁰⁰ Processo C-176/13. *Conselho da União Europeia v. Bank Mellat*. Julgamento em: 18 fevereiro 2016.

¹⁰¹ Registra-se que os direitos fundamentais contidos na Carta não serão vinculativos para os tribunais britânicos e poloneses, salvo em casos que as legislações nacionais destes países detenham normas sobre os aspectos da União, conforme o Protocolo n.º 30 vinculado à Carta dos Direitos Fundamentais ou que os Direitos estejam

interno dos seus Estados-Membros possuem fundamentação jurisprudencial do Tribunal de Justiça da União Europeia.¹⁰²

Neste sentido, no caso *Costa & Enel*¹⁰³ o Tribunal determinou o primado da norma da União sobre a norma nacional, mesmo que o Estado nacional se oponha a este, o que é definido como a eficácia do Direito da União. Na mesma linha, no julgamento do caso *Internationale Handelsgesellschaft*,¹⁰⁴ o Tribunal decidiu que não se pode invocar normas nacionais para verificar a validade do Direito da União, sob pena de prejuízo do próprio caráter da União e da natureza da União Europeia. Nesta posição, a Carta constrói um sistema de proteção jurídica integral e eficaz, no qual se reconhece o direito de o indivíduo usufruir uma proteção legal dos direitos decorrentes da ordem jurídica, conforme disposto em seu artigo 47.

1.6 Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679

O Regulamento Geral sobre a Proteção de Dados (a sigla, em inglês, GDPR) é o modelo normativo criado pela União Europeia para abordar o direito à proteção de dados pessoais de forma harmônica e eficaz sobre todo o seu território.¹⁰⁵ Ele foi elaborado por meio de um processo legislativo complexo e duradouro. Em sua origem, os formuladores de políticas europeias iniciaram um processo que envolveu uma série de consultas a especialistas, o que gerou uma profunda sofisticação regulatória sobre como as práticas de informação podem ser manipuladas para escapar das metas regulatórias.¹⁰⁶ O motivo de sua criação está na fragmentação da proteção de dados nos Estados-Membros. Os resultados dessas incertezas jurisdicionais foram considerados obstáculos à busca das atividades econômicas a nível da União que conduziram a uma distorção da concorrência.¹⁰⁷ Com o objetivo de superar essas dificuldades, uma consulta inicial teve início em 2009 e a Comissão

inseridos em atos normativos diversos do da Carta. (disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12016E/PRO/30&from=ES>. Acesso em: 23 fev. 2021).

¹⁰² MANERO SALVADOR, A. El valor jurídico de la Carta de derechos fundamentales. De Niza a Lisboa. In: FERNANDEZ LIESA, C.; DIAZ BARRADO, C. *El tratado de Lisboa*. Análisis y perspectivas. Instituto universitario de estudios internacionales y europeos Francisco de Vitoria, Dykinson, 2009. p. 113-133.

¹⁰³ Processo 6/64. *Flaminio Costa v E.N.E.L.* Julgamento em: 15 julho 1964.

¹⁰⁴ Processo 11/70. *Internationale Handelsgesellschaft mbH v. Einfuhr – und Vorratsstelle für Getreide und Futtermittel*. Julgamento em: 17 dezembro 1970.

¹⁰⁵ VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 3.

¹⁰⁶ HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019. p. 68.

¹⁰⁷ Considerando 9, do Regulamento Geral sobre a Proteção de Dados.

Europeia publicou um texto de proposta em 2012.¹⁰⁸ Em dezembro de 2015, o Parlamento Europeu e o Conselho Europeu chegaram a um acordo sobre o texto. O Regulamento Geral sobre a Proteção de Dados foi oficialmente adotado em maio de 2016 e é aplicável desde maio de 2018.¹⁰⁹

Atualmente, o Regulamento Geral sobre a Proteção de Dados é exequível e sua interpretação é confiada aos tribunais, combinada com uma interpretação persuasiva, embora não vinculativa, do recém-criado Conselho Europeu de Proteção de Dados.¹¹⁰ Com isso, a União pretendeu reconquistar a confiança das pessoas no tratamento responsável dos seus dados pessoais, a fim de impulsionar a economia digital em todo o mercado interno.¹¹¹ Para a composição deste complexo normativo, o legislador europeu levou em conta os desafios de uma economia global, as novas tecnologias e os novos modelos de negócios, para com isso, criar um amplo escopo de aplicação que afetará inúmeras empresas. Com isso, foram criados não apenas deveres de proteção de dados, mas também as sanções foram aumentadas significativamente.¹¹²

O Regulamento consiste em um documento de quase 100 (cem) páginas. A extensão e complexidade da norma decorre do número de direitos para titulares de dados, dentre eles, o direito ao esquecimento, o direito à portabilidade de dados pessoais e o direito de resistir à criação de perfis automatizados. No mesmo sentido, o número de funções atribuídas aos controladores de dados pessoais (Encarregados de dados, no caso da União Europeia) foi significativamente alargadas através da introdução de um dever de responsabilidade, deveres relativos às avaliações de impacto de proteção de dados, o dever de nomear um oficial de proteção de dados pessoais e uma obrigação de notificação após a ocorrência de uma violação sobre os dados pessoais.¹¹³

Assim como a Diretiva de 1995, o primeiro artigo do Regulamento enfatiza que este conjunto normativo tem um objetivo duplo: promover o livre fluxo de dados pessoais dentro

¹⁰⁸ A Comissão Europeia é responsável pela executividade das medidas da União. Ver: *As prioridades da Comissão Europeia*. Disponível em: https://ec.europa.eu/commission/index_en. Acesso em: 13 jan. 2021.

¹⁰⁹ GDPR art 99 (2): “É aplicável a partir de 25 de maio de 2018”.

¹¹⁰ HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019. p. 71.

¹¹¹ Considerados 7 e 9, do Regulamento Geral sobre a Proteção de Dados.

¹¹² VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 31.

¹¹³ HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019. p. 73.

da União (para auxiliar o mercado comum) e proteger as pessoas e seus dados pessoais.¹¹⁴ De acordo com o texto, o direito à proteção de dados pessoais e o Regulamento serão aplicados em todas as situações em que dados pessoais – na definição do Regulamento, quaisquer dados relativos a uma pessoa identificada ou identificável – sejam processados.¹¹⁵

O Regulamento visa garantir a equanimidade em situações em que dados pessoais são processados. Ou seja, tais dados pessoais devem ser tratados dentro dos seguintes parâmetros: “lícito, leal e transparente em relação ao titular dos dados”.¹¹⁶ Neste sentido, o Regulamento busca construir um sistema amplo de proteção de dados pessoais e direitos correlatos, como a proteção das informações pessoais,¹¹⁷ a proteção dos dados pessoais em si.¹¹⁸ Visa ainda proteger as pessoas contra os efeitos discriminatórios do processamento de dados pessoais de forma automatizada.¹¹⁹ Em termos conceituais, há similitudes com a Diretiva. O conceito de tratamento de dados pessoais é praticamente idêntico ao adotado pela antiga Diretiva europeia, com duas “operações” de tratamento adicionadas em seu elenco (“estruturação” e “limitação” que substituiu o “bloqueio”).¹²⁰

Por isso, é possível dizer que a GDPR constitui a *lex generalis* no quadro jurídico da lei de proteção de dados pessoais e sua aplicação trouxe benefícios tanto para as empresas como para os cidadãos.¹²¹ De fato, aos indivíduos foram reconhecidos novos direitos e instrumentos de tutela – como o direito de ser esquecido, o acesso simplificado aos dados, o direito à portabilidade e o direito de saber quando os dados foram hackeados. Os controladores de dados (Encarregados de dados, no caso da União Europeia), por outro lado,

¹¹⁴ “Artigo 1º. Objeto e objetivos: 1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais”.

¹¹⁵ VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 4.

¹¹⁶ Artigo 1º alínea “a”, do Regulamento Geral sobre a Proteção de Dados.

¹¹⁷ SOLOVE, Daniel J.; SCHWARTZ, Paul M. *Information privacy law*. 7. ed. New York: Wolters Kluwer, 2021. p. 65.

¹¹⁸ HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIU, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019. p. 75.

¹¹⁹ Ver Considerando 71 e artigo 21, do Regulamento Geral sobre a Proteção de Dados. Para um registro mais específico sobre *Profiling* e o uso de dados pessoais, ver: PETKOVA, B.; BOEHM, F. Profiling and the essence of the right to data protection. In: SELINGER, E.; POLONETSKY, J.; TENE, O. (org.). *The Cambridge Handbook of Consumer Privacy*. Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2018. p. 285-300. p. 77.

¹²⁰ Art. 3 (2), do Regulamento.

¹²¹ KĘDZIOR, Magdalena. *GDPR and beyond – a year of changes in the data protection landscape of the European Union*. ERA Forum, 2019. v. 19. p. 505-509. p. 507.

foram obrigados a seguir o princípio da proteção de dados desde a concepção dos sistemas de tratamento (“privacy by design”) até a criação de meios de contenção de defeitos das operações (“privacy by default”).¹²² Já no plano institucional, a novidade foi a criação do Comitê Europeu de Proteção de Dados, que foi dotado da competência de emitir decisões vinculativas em casos de litígios entre autoridades nacionais de proteção de dados, além da atribuição de emitir orientações sobre a aplicação da GDPR no âmbito da União e de forma genérica e global.¹²³ Enfim, o Regulamento contém regras claras sobre as condições para a imposição de multas administrativas a pessoas que não cumpram as regras da União.

Especificamente acerca do tema deste trabalho, pode-se afirmar que a antiga Diretiva visava garantir “a proteção dos direitos e liberdades das pessoas, nomeadamente do seu direito à vida privada”.¹²⁴ Mas não detalhava quais outros direitos são protegidos. Já o Regulamento remove a maioria das referências ao direito à vida privada e, em vez disso, refere-se principalmente ao direito à proteção de dados.¹²⁵ Isso levanta questões sobre como a relação entre os dois direitos deve ser caracterizada. A proteção de dados pessoais pode ser definida como um direito distinto da privacidade, no aspecto regulamentar da União? Se sim, qual é o conteúdo do direito à proteção de dados? Quais são os objetivos distintos daqueles da privacidade?

Essas questões indicam que os objetivos do regime de proteção de dados da União continuam a ser ambíguos. Dois aspectos em particular continuam a provocar debate e desacordo. Em primeiro lugar, o amplo âmbito de aplicação do regime de proteção de dados da União foi duramente criticado. Em suas conclusões a respeito do julgamento do caso *Google Spain*, o Advogado-Geral da União Europeia, Sr. Jääskinen, comentou, por exemplo, com desaprovação, o alcance abrangente da antiga Diretiva e propôs uma interpretação restrita do conceito consagrado de “controlador de dados” (Encarregados de dados, no caso da União Europeia. Seu objetivo era limitar o âmbito pessoal da diretiva, o que não foi aprimorado no escopo do Regulamento.¹²⁶ Há também críticas que se dirigem contra o escopo material do regime de proteção na União, que seria excessivamente inclusivo e amplo, o que pode dificultar sua aplicação e tornar impossível o atingimento seus reais objetivos. Enfim,

¹²² VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 12.

¹²³ Artigo 51, do Regulamento.

¹²⁴ Considerando 68, da Diretiva 95/46/CE.

¹²⁵ A Diretiva 95/46/CE continha 13 (treze) referência à “vida privada”; já o Regulamento detém 01 (uma) referência ao termo.

¹²⁶ Processo C-131/12. *Conclusões Gerais do Advogado-Geral Niilo Jääskinen*. Apresentado em: 25 junho 2013. Parágrafos 79-81.

existem críticas conceituais contra o Regulamento que, erroneamente, teria dirigido seu foco sobre o conceito de dados pessoais, ao invés dos danos decorrentes do uso de dados.¹²⁷ Por tudo isso, como parte do direito à proteção de dados pessoais, faz-se necessária a análise abrangente desta questão, inclusive sobre os termos identificados na normativa a respeito desta matéria, o que será mais bem analisado nos próximos capítulos.

1.7 Diretiva E-Privacy e a Proposta de Regulamento Relativo à Privacidade e Comunicações Eletrônicas

A Diretiva e-Privacy¹²⁸ tem o objetivo geral de harmonizar as disposições dentro da União, necessárias a garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, em todos os Estados-Membros. Em específico, ela visa conferir uniformidade normativa ao direito à privacidade e confidencialidade no que diz respeito ao tratamento de dados pessoais realizados na comunicação eletrônica e garantir a livre circulação de tais dados e de equipamentos de comunicação eletrônica e serviços na União.¹²⁹ Visa, por conseguinte, garantir o respeito pelos direitos estabelecidos nos artigos 7º e 8º, da Carta dos Direitos Fundamentais da União Europeia.

A este respeito, a Diretiva complementa as disposições da GDPR no que diz respeito ao processamento de dados pessoais no setor de comunicação eletrônica.¹³⁰ Trata-se, portanto, de norma relativa à privacidade das comunicações eletrônicas, que pretendia fornecer um padrão mínimo para a regulamentação dos Estados-Membros acerca das solicitações comerciais, por meio de e-mails e tecnologias de telecomunicações. O artigo 13, da Diretiva de Privacidade Eletrônica estabelece uma regra básica de consentimento explícito (*opt-in*) para “comunicações não solicitadas, via chamadas automatizadas”.¹³¹

¹²⁷ BERGKAMP, Lucas. *EU data protection policy: the privacy fallacy: adverse effects of Europe’s data protection policy in an information-driven economy*. Computer Law & Security Review, 2002. v. 18. p. 31-47. p. 42.

¹²⁸ A Diretiva 2002/58/CE, é datada de julho de 2002 e trata do tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32002L0058>. Acesso em: 18 jan. 2021.

¹²⁹ VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. P. 3.

¹³⁰ Artigo 1 (2), da Diretiva 2002/58/CE.

¹³¹ “Artigo 13º. Comunicações não solicitadas: 1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrónico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio. 2. Sem prejuízo do n.º 1, se uma pessoa singular ou colectiva obtiver dos seus clientes coordenadas electrónicas de contacto para correio electrónico, no contexto da venda de um produto ou serviço, nos termos da Directiva 95/46/CE, essa pessoa singular ou colectiva poderá usar essas

Com relação à correios eletrônicos comerciais não solicitados uma exceção foi criada no artigo 13 (2) para os casos em que uma empresa forneceu um bem ou serviço a um indivíduo anteriormente. Neste caso, é possível o envio de e-mails não solicitados, desde que seja para anúncios de bens ou serviços semelhantes e seja fornecido ao cliente a oportunidade de “cancelar” o recebimento de e-mails futuros. Desta forma, é possível verificar momentos em que a Diretiva colidirá com os temas tratados na GDPR, fazendo com que haja divergências de entendimento e posicionamento sobre o assunto.¹³² Por isso, o Comité Europeu para a Proteção de Dados (a sigla, em inglês, EDPB)¹³³ emitiu a Opinião 5/2019, sobre a interpretação entre a Diretiva e-Privacy e a GDPR, indicando que, a partir do princípio da *lex specialis*, só haverá uma derrogação à regra geral na medida em que a lei que rege uma matéria específica contenha uma regra especial.¹³⁴

Ou seja, os fatos do caso devem ser cuidadosamente analisados para descobrir até que ponto a derrogação se estende, especialmente, nos casos em que os dados pessoais sofram diversos tipos de processamento.¹³⁵ Explicitando a abordagem do Comitê, o Tribunal de Justiça da União Europeia indicou que o consentimento para o uso de cookies e outros métodos e técnicas de rastreamento online (por exemplo, *cookies flash, tags, scripts, pixels*, impressão digital do dispositivo), apesar de ser atualmente regido por normas legais especiais da Diretiva de Privacidade Eletrônica, não escapa dos requisitos de consentimento, conforme estabelecido na GDPR.¹³⁶ O Tribunal ainda ressalta que o objetivo da Diretiva Privacidade Eletrônica é proteger os utilizadores contra qualquer interferência na sua vida privada, independentemente de essa interferência dizer respeito ou não a dados pessoais. Além disso, a

coordenadas electrónicas de contacto para fins de comercialização directa dos seus próprios produtos ou serviços análogos, desde que aos clientes tenha sido dada clara e distintamente a possibilidade de recusarem, de forma gratuita e fácil, a utilização dessas coordenadas electrónicas de contacto quando são recolhidos e por ocasião de cada mensagem, quando o cliente não tenha inicialmente recusado essa utilização.”

¹³² VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 4.

¹³³ O European Data Protection Board (EDPB) foi criado, a partir da entrada em vigor da GDPR e é o organismo europeu que contribui para a aplicação das regras de proteção de dados em toda a União Europeia e promove a cooperação entre as autoridades de proteção de dados pessoais da União. Para consulta sobre o Comitê, ver: EUROPEAN Data Protection Board. Disponível em: https://edpb.europa.eu/edpb_pt. Acesso em: 18 jan. 2021.

¹³⁴ EUROPEAN Data Protection Board. *Parecer 5/2019 sobre a interação entre a Diretiva Privacidade Eletrônica e o RGPD, particularmente em matéria de competência, atribuições e poderes das autoridades de proteção de dados*. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/styrelsensytrande-art-64/opinion-52019-interplay-between-eprivacy_pt. Acesso em: 18 jan. 2021.

¹³⁵ WIEDEMANN, Klaus. *The ECJ's decision in “Planet49” (Case C-673/17): a cookie monster or much ado about nothing?* IIC – International Review of Intellectual Property and Competition Law, 2020. p. 2.

¹³⁶ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 68.

Diretiva Privacidade Eletrônica refere-se ao “armazenamento de informações” e “à obtenção de acesso a informações já armazenadas”, sem qualificar essas informações como dados pessoais.

Com fundamento nesta orientação, não faz diferença se as informações (ou *cookies*) armazenadas ou acessadas constituem dados pessoais para efeitos da Diretiva e-Privacy.¹³⁷ Na prática, isso quer dizer que, ao usar cookies, o site que se exija o consentimento deve revisar o mecanismo de consentimento e, especificamente, revisar o mecanismo sobre o uso de caixas pré-marcadas (*opt-in/opt-out*). Deve, ainda, observar que o uso de caixas de consentimento pré-marcadas não leva a um consentimento de cookie válido. Por fim, a política de cookies deve apresentar aos usuários informações claras e precisas, entre outras, sobre a duração da operação de cookies, bem como se terceiros têm ou não acesso a esses cookies.¹³⁸

Finalmente, o Tribunal lembrou que o direito da União deve receber uma interpretação uniforme. Com esta declaração, o Tribunal reconheceu, ainda que implicitamente, que as diferentes transposições da Diretiva Privacidade Eletrônica e as orientações divergentes das autoridades nacionais de proteção de dados, presentes nos vários Estados-Membros, podem causar incertezas jurídicas, sobretudo quando as operações de tratamento ocorrem em mais de um Estado-Membro.¹³⁹

Por isso, o projeto de confecção de um Regulamento de e-Privacy foi apresentado pela primeira vez pela Comissão Europeia em 2017, o que tem o objetivo de reforçar a confiança e segurança no mercado único digital. O regulamento foi concebido para substituir a Diretiva de Privacidade e Comunicações Eletrônicas (Diretiva 2002/58/CE) e tem o intuito de constituir uma parte fundamental da modernização da União do quadro da regulação da privacidade.¹⁴⁰ O projeto inclui propostas para harmonizar as regras de privacidade eletrônica em todo o mercado único, o que tem o intuito de fornecer maior proteção para o conteúdo das comunicações eletrônicas e garantir que serviços “over-the-top”¹⁴¹ (como WhatsApp, Skype e Facebook Messenger) sigam os mesmos padrões dos provedores de telecomunicações

¹³⁷ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 77.

¹³⁸ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019.

¹³⁹ WIEDEMANN, Klaus. *The ECJ's decision in “Planet49” (Case C-673/17): a cookie monster or much ado about nothing?* IIC – International Review of Intellectual Property and Competition Law, 2020. p. 2.

¹⁴⁰ POLČÁK, Radim; KASL, František; MÍŠEK, Jakub. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *National report: Czech Republic. Ius Comparatum – Global Studies in Comparative Law*. Suíça: Springer, 2020. p. 115-158. p. 120.

¹⁴¹ POLČÁK, Radim; KASL, František; MÍŠEK, Jakub. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *National report: Czech Republic. Ius Comparatum – Global Studies in Comparative Law*. Suíça: Springer, 2020. p. 115-158. p. 122.

tradicionais. Tudo isso com a finalidade de proteger os cidadãos contra comunicações eletrônicas não solicitadas.¹⁴²

1.8 Tribunal de Justiça da União Europeia e Tribunal Europeu de Direitos Humanos

Criado pelo Tratado de Paris no ano de 1952 como órgão jurisdicional integrante da Comunidade Europeia do Carvão e do Aço, o Tribunal de Justiça da União Europeia (Tribunal) foi inicialmente denominado de Tribunal de Justiça da Comunidade Europeia. Desde sua instituição, responsabilizou-se por uma segura construção da ordem da União. Suas decisões representaram, ao longo dos anos, um corpo harmônico de construção do direito da União.¹⁴³ Nesta senda, o Tribunal tem por função determinar a interpretação do direito da União (outrora comunitário) como um todo. Através desta prerrogativa, decide disputas entre as instituições da União, entre os Estados-Membros, entre os Estados-Membros e as instituições da União, e finalmente, entre as pessoas privadas e os Estados e as instituições da União.¹⁴⁴ Por isso, Paulo Borba Casella elucida que o “TJCE vem desempenhando papel fundamental não somente enquanto garantidor da uniformidade de interpretação do ordenamento jurídico comunitário, bem como criador desse mesmo direito”.¹⁴⁵

Fato é que, com a entrada em vigor do Tratado de Lisboa, o seu nome foi alterado para Tribunal de Justiça da União Europeia.¹⁴⁶ Isso indica que a relação do direito da União com os direitos nacionais está fundamentada a) na autonomia daquele com relação a este; b) na aplicabilidade direta do direito da União nos ordenamentos jurídicos nacionais, enfim, c) no primado deste sobre os direitos nacionais.¹⁴⁷

Deste modo, os inevitáveis conflitos entre as legislações nacionais e da União devem ser resolvidos pelo Tribunal de Justiça da União Europeia.¹⁴⁸ Deve-se destacar ainda a

¹⁴² POLČÁK, Radim; KASL, František; MÍŠEK, Jakub. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *National report: Czech Republic. Ius Comparatum – Global Studies in Comparative Law*. Suíça: Springer, 2020. p. 115-158. p. 122.

¹⁴³ MANCINI, Federico G. *The making of a Constitution for Europe*. Common Market Law Review, 1989. p. 595-614. p. 601.

¹⁴⁴ STARR-DEELEN, Donna; BART, Deelen. *The European Court of Justice as a Federator*. Publius, v. 26, n. 4, p. 81-97, 1996. p. 83.

¹⁴⁵ CASELLA, Paulo Borba. O papel da Comissão de Comércio do Mercosul: o Tribunal do Mercosul disfarçado? In: MERCADANTE, Araminta de Azevedo; MAGALHÃES, José Carlos de (coord.). *Solução e prevenção de litígios internacionais*. Porto Alegre: Livraria do Advogado, 1999. v. II. p. 495.

¹⁴⁶ GOMES, José Caramelo. *Lições de direito da União Europeia*. Coimbra: Almedina, 2009. p. 161.

¹⁴⁷ STARR-DEELEN, Donna; BART, Deelen. *The European Court of Justice as a Federator*. Publius, v. 26, n. 4, p. 81-97, 1996. p. 85.

¹⁴⁸ Sobre a história dos tribunais da União no Projeto do Tratado da União, ver: SOBRINO HEREDIA, José Manuel. El sistema jurisdiccional el el proyecto de Tratado constitucional de la Unión Europea. *Revista Derecho Comunitario Europeo*, ano 3, v. 16, p. 993-1040, 2003. Sobre a competência do Tribunal, como

inexistência de hierarquia entre as decisões do Tribunal e as jurisdições nacionais. De fato, o Tribunal não reformula as decisões locais. Não é uma instância supervisonal. Isso possibilita que, para proteger a ordem da União, o Tribunal possa censurar as decisões internas, sempre quando necessário para defender as regras da União.¹⁴⁹

Aqui vale uma observação. É frequente que o Tribunal de Justiça da União Europeia seja confundido com o Tribunal Europeu de Direitos Humanos, que tem sede em Estrasburgo.¹⁵⁰ No entanto, enquanto o Tribunal de Justiça da União Europeia é uma das sete Instituições da União Europeia, o Tribunal Europeu dos Direitos Humanos não faz parte da União Europeia, mas sim, do Conselho da Europa.¹⁵¹ Por outro lado, foi apenas com a evolução e desenvolvimento do bloco europeu e com o surgimento de questões sociais e políticas que afetavam direta ou indiretamente o âmbito de atuação da União Europeia, que o Tribunal passou a ter competência sobre matérias não só econômicas. Hoje seus julgamentos tratam também de temas ligados aos direitos humanos, sempre considerando a necessidade de aplicação do direito da União.¹⁵² Por essa razão, atualmente há no continente europeu uma pluralidade de normas e instituições capazes de garantir a salvaguarda dos direitos humanos.¹⁵³

Nessa perspectiva, dada à independência e autonomia dos dois Tribunais, o Tribunal de Justiça da União Europeia deve ser visto como o único órgão jurisdicional supranacional da União. Sua competência quanto se estende à solução de questões referentes à aplicação do Direito da União Europeia, que muitas vezes podem envolver temas de direitos humanos.¹⁵⁴ O

ensina Magnoli: “A atividade do tribunal de Justiça reflete o surgimento de um direito comunitário, que se superpõe aos direitos nacionais e os subordina, no âmbito das questões ligadas aos tratados. O direito comunitário tem força de lei nos países-membros, aplicando-se diretamente a Estados, pessoas jurídicas e particulares” (MAGNOLI, Demétrio. *União Europeia: história e geopolítica*. 3. ed. São Paulo: Moderna, 2007. p. 87).

¹⁴⁹ SCHEPEL, Harm. Reconstructing constitutionalization: law and politics in the European Court of Justice. *Oxford Journal of Legal Studies*, v. 20, n. 3, p. 457-468, 2000. p. 463.

¹⁵⁰ Acerca do debate sobre eventuais conflitos e sobreposições entre o Tribunal de Justiça da União Europeia e Tribunal Europeu dos Direitos Humanos, ver: KARGOPOULOS, Alexandros-Ioannis. *ECHR and the CJEU*. Competing, overlapping, or supplementary competences? *European criminal law and human rights*. Issue 3/2015. 2015. p. 96-100. p. 99.

¹⁵¹ BLANKE, Hermann-Josef. The protection of fundamental rights in Europe. In: BLANKE, Hermann-Josef; MANGIAMELI, Stelio (org.). *The European Union after Lisbon: constitutional basis, economic order and external action*. Berlin: Springer, 2012. p. 159-232 p. 159.

¹⁵² SCHEPEL, Harm. Reconstructing constitutionalization: law and politics in the European Court of Justice. *Oxford Journal of Legal Studies*, v. 20, n. 3, p. 457-468, 2000. p. 465.

¹⁵³ BENEVIDES, Isabella Almeida de Sá e; PEREIRA, Raissa Pose. Os direitos fundamentais: perspectiva da União Europeia. *Revista do Programa de Direito da União Europeia*, Rio de Janeiro, v. 6, p. 49-66, 2016. p. 51.

¹⁵⁴ Corroborando esse entendimento, Benevides e Pereira ressaltaram que “Acompanhando a internacionalização dos direitos humanos, a observância dos direitos humanos vem sendo apreciada por foros não tradicionais, como o Tribunal de Justiça da União Europeia (adiante TJUE, ou Tribunal de Luxemburgo). O TJUE, apesar de ter seu foco principal no direito comunitário, também possui

Tribunal Europeu de Direitos Humanos foi criado, por sua vez, única e exclusivamente para a proteção judicial dos direitos humanos. Isso significa que a competência material da Corte de Estrasburgo está adstrita à interpretação e aplicação da Convenção Europeia de Direitos Humanos.¹⁵⁵ A atuação da Corte de Estrasburgo ou Corte Europeia de Direitos Humanos (CEDH), bem como sua criação, encontram-se positivadas na Convenção Europeia de Direitos Humanos, que é o principal diploma normativo de proteção dos direitos humanos no âmbito do sistema regional europeu.¹⁵⁶

De igual modo, durante muito tempo, a Convenção serviu de parâmetro para proteção dos direitos humanos no âmbito de competência da União Europeia, uma vez que somente em 2009, com o Tratado de Lisboa, a Carta de Direitos Fundamentais da União Europeia passou a ter força vinculante.¹⁵⁷ Dessa maneira, o Tribunal é a autoridade judiciária dentro da organização institucional da União Europeia que, com base no princípio da cooperação junto aos tribunais dos Estados-Membros, garante a interpretação e aplicação uniformes do direito da União. Ele pode ser chamado a se pronunciar quando houver violação dos direitos humanos por parte das instituições, órgãos e organismos da União. Os Estados-Membros só serão indiretamente responsáveis, ou seja, apenas quando aplicarem o direito da União Europeia.¹⁵⁸

Deste modo, o debate sobre as competências do Tribunal de Justiça e do Tribunal Europeu de Direitos Humanos permite que se busquem soluções que, de um lado, mantenham a viabilidade e autonomia da União Europeia e, por outro, assegurem o acesso à justiça, à proteção e à promoção dos direitos humanos, enfim, a reparação para aqueles que sofreram violações desses direitos. Hoje o Tribunal é competente para a solução de conflitos sobre os direitos fundamentais.¹⁵⁹ Neste sentido, o Tratado da União Europeia codifica a importância

jurisprudência acerca de direitos humanos” (BARCELOS, Paulo. Vitangelo Moscarda’s Syndrome. The Charter of Fundamental Rights and European Constitutionalization. In: ANGELIS, Gabriele de; BARCELOS, Paulo (ed.). *The long quest for identity: political identity and fundamental rights protection in the European Union*. Lisbon philosophical studies uses of language in interdisciplinary fields. Pieterlen: Peter Lang, Bern, 2013. v. 4. p. 32).

¹⁵⁵ GRAGL, Paul. The accession of the European Union to the European Convention on Human Rights. *Modern Studies in European Law*, v. 39, 2013. p. 1.

¹⁵⁶ DEITOS, Marc Antoni. A adesão da União Europeia à Convenção Europeia dos Direitos Humanos: rumo a uma quarta camada de proteção dos direitos humanos. *Direitos Fundamentais & Justiça*, ano 7, n. 24, p. 113-133, jul./set. 2013. p. 115.

¹⁵⁷ TRIBUNAL de Justiça da União Europeia. *Opinião 2/13*. Publicada em: 18 dezembro 2014. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140180en.pdf>. Acesso em: 24 mar. 2021.

¹⁵⁸ STARR-DEELEN, Donna; BART, Deelen. *The European Court of Justice as a Federator*. Publius, v. 26, n. 4, p. 81-97, 1996. p. 88.

¹⁵⁹ Em 1969, o Tribunal de Justiça da União Europeia afirmou que “os direitos humanos fundamentais [estão] consagrados nos princípios gerais do direito comunitário e protegidos pelo Tribunal” (Processo C-29/69. *Erich Stauder v. City of Ulm*. Julgamento em: 12 novembro 1969. Parágrafo 7). Ver também: FUSTER,

dos direitos fundamentais.¹⁶⁰ Além disso, em 2000, a Carta dos Direitos Fundamentais da União Europeia foi adotada e nela se enumera os direitos e liberdades fundamentais reconhecidos pela União.¹⁶¹

Desde que a Carta se tornou um instrumento juridicamente vinculativo em 2009, o número de casos em que o Tribunal de Justiça da União Europeia citou este documento aumentou substancialmente.¹⁶² Como grande exemplo, podem ser citados julgamentos relacionados à privacidade e à proteção de dados, como o denominado *Google Spain*.¹⁶³ Mas tendo em vista a ausência de qualquer declaração de direitos efetuada de forma legislativa pela União Europeia até o ano de 2000, a proteção dos direitos fundamentais durante os primeiros 40 anos de integração europeia foi desenvolvida prioritariamente através da jurisprudência do Tribunal.¹⁶⁴ Isso resultou em um sistema no qual o litígio desempenhou um papel importante no desenvolvimento, perfilamento e fiscalização do cumprimento dos direitos fundamentais.¹⁶⁵

A respeito do tema desta dissertação, podemos referendar, com base no que foi exposto, que tanto o direito à privacidade quanto o direito à proteção de dados, insculpidos na Carta dos Direitos Fundamentais da União Europeia, têm aplicação direta aos Estados-Membros da União.¹⁶⁶ Deste modo, é importante analisar, perfunctoriamente, como a União Europeia tratou, normativamente, o direito à proteção de dados pessoais, para, então, entender

Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer. 2014. p. 164.

¹⁶⁰ O artigo 6º, (3), do Tratado, estipula que “Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros”.

¹⁶¹ As expressões 'direitos fundamentais' e 'direitos humanos' são indiferentes. Para maiores explicações: FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer. 2014. p. 164-166.

¹⁶² DE BÚRCA, G. After the EU charter of fundamental rights: the Court of Justice as a human rights adjudicator? *Maastricht Journal of European and Comparative Law*, v. 20, n. 2, p. 168-184, 2013. p. 168.

¹⁶³ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

¹⁶⁴ Em julgamento efetuado no ano de 1970, o Tribunal Europeu considerou que o respeito pelos direitos humanos é parte integrante dos princípios gerais do direito comunitário protegidas pelo Tribunal de Justiça. A proteção de tais direitos, embora inspirada nas tradições constitucionais comuns aos Estados-Membros, devem ser asseguradas no âmbito da estrutura e objetivos da Comunidade (Processo C-11/70. *Internationale Handelsgesellschaft mbH v Einfuhr – und Vorratsstelle für Getreide und Futtermittel*. Julgamento em: 17 dezembro 1970).

¹⁶⁵ ALTER, K. J. Explaining National Court Acceptance of European Court Jurisprudence: a critical evaluation of theories of legal integration. In: SLAUGHTER, A. M.; SWEET, A. S.; WEILER, J. (org.). *The European Court and National Courts – doctrine and jurisprudence: Legal Change in Its Social Context*. London: Hart Publishing, 1998. p. 227-252. p. 230.

¹⁶⁶ HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010. p. 132.

como o Tribunal de Justiça da União Europeia elaborou suas decisões judiciais sobre o assunto.

1.9 Sistema de Reenvio Prejudicial e o Tribunal de Justiça da União Europeia

No contexto apresentado neste capítulo, é importante lembrar que a legislação da União Europeia apresenta vantagens aos litigantes em relação às ações julgadas pelo Tribunal de Estrasburgo. Isso porque, ao contrário do Tribunal Europeu de Direitos Humanos, no qual o requerente deve esgotar todos os remédios jurídicos nacionais para obter êxito no conhecimento de sua matéria, é possível obter uma decisão do Tribunal de Luxemburgo através de um pedido de “reenvio prejudicial”.¹⁶⁷ Isso significa que é possível, com base no artigo 267 do Tratado sobre o Funcionamento da União Europeia, estipular as denominadas “perguntas preliminares”, que podem ou devem (a depender do caso concreto) serem remetidas ao Tribunal de Justiça da União Europeia.¹⁶⁸ Esta determinação contida no Tratado sobre o Funcionamento da União é definida como o “sistema de reenvio prejudicial”, o qual pode ser caracterizado como um mecanismo do direito da União Europeia destinado a fornecer aos órgãos judiciais nacionais a possibilidade da aplicação uniforme dos direitos insculpidos na Carta dos Direitos Fundamentais da União Europeia.¹⁶⁹

A tarefa de criar uma interpretação e uma aplicação uniforme das normas da União é a principal competência do Tribunal de Justiça da União Europeia, sendo sua função trazer uma abordagem transnacional e que deve ser aplicada por todos os entes do bloco.¹⁷⁰ Neste sistema, os órgãos jurisdicionais nacionais submetem ao Tribunal de Justiça as questões relativas à interpretação ou à validade das disposições e, após a tradução do pedido em todas as línguas dos Estados-Membros da União, ocorre a notificação às partes envolvidas no processo

¹⁶⁷ PESCATORE, Pierre. *O recurso prejudicial do artigo 177 do Tratado CEE e a cooperação do tribunal com as jurisdições nacionais*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 1986. p. 28.

¹⁶⁸ PESCATORE, Pierre. *O recurso prejudicial do artigo 177 do Tratado CEE e a cooperação do tribunal com as jurisdições nacionais*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 1986. p. 28.

¹⁶⁹ O recurso em questão é o diferencial do sistema, pois permite a aplicação do Direito da União, diretamente pelos Judiciários locais, sem que haja a necessidade de uma estrutura forense supranacional. (PESCATORE, Pierre. *O recurso prejudicial do artigo 177 do Tratado CEE e a cooperação do tribunal com as jurisdições nacionais*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 1986. p. 27).

¹⁷⁰ BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006. p. 227.

principal, aos Estados-Membros e às instituições da União.¹⁷¹ Realizada a notificação, as partes são convidadas a apresentar observações no âmbito do quadro jurídico definido pela jurisdição que procede ao reenvio.

Após os procedimentos internos, o papel do Tribunal de Justiça consiste em interpretar o direito da União Europeia ou pronunciar-se a respeito de sua validade, devendo a jurisdição nacional discutir os fatos intrínsecos ao caso concreto, razão pela qual o objetivo desta função deve ser registrar uma possível resposta para a resolução do litígio.¹⁷² Em suma, o objetivo do procedimento de reenvio é garantir a interpretação uniforme do direito da União Europeia, desempenhando também um importante papel na proteção dos direitos individuais.¹⁷³

Como consequência, observa-se que o papel do Tribunal de Justiça da União Europeia é dar as balizas ao caso concreto e também determinar as implicações daquele direito da União a todos dentro do espaço da União Europeia (efeito *erga omnes*).

O pedido de decisão prejudicial pode garantir ao cidadão da União o direito de se opor às ações do seu país contrárias à legislação da União Europeia.¹⁷⁴ Vale ainda registrar que se um órgão jurisdicional nacional pretender invocar a invalidade de um ato da União Europeia, ele será obrigado a requisitar um pedido de reenvio prejudicial, uma vez que o Tribunal de Justiça é a única instância que detém competência para dispor sobre questões que violem o direito da União Europeia.¹⁷⁵ Violações das obrigações determinadas pelo reenvio prejudicial representam, simultaneamente, violações dos tratados da União Europeia e, por isso, podem levar à propositura de ação por descumprimento, denominada ação por incumprimento dos tratados.¹⁷⁶ Desta forma, o reenvio prejudicial obriga o órgão jurisdicional nacional que introduziu o pedido, assim como todas as instâncias envolvidas no litígio, a seguirem suas determinações.¹⁷⁷ Os julgamentos dos reenvios funcionam, assim, como precedentes que para

¹⁷¹ SCHWARZE, Jürgen. Judicial review in EC law: some reflections on the origins and the actual legal situation. *The International and Comparative Law Quarterly*, v. 51, n. 1, p. 17-33, 2002. p. 23.

¹⁷² BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006. p. 241.

¹⁷³ BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006. p. 242.

¹⁷⁴ SCHWARZE, Jürgen. Judicial review in EC law: some reflections on the origins and the actual legal situation. *The International and Comparative Law Quarterly*, v. 51, n. 1, p. 17-33, 2002. p. 28.

¹⁷⁵ BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006. p. 243.

¹⁷⁶ MOURA RAMOS, Rui. O sistema jurisdicional da União Europeia. O presente e o futuro. *Revista de Estudos Europeus*, n. 2, 2007. p. 269.

¹⁷⁷ MOURA RAMOS, Rui Manuel de. *Estudos de direito internacional privado e de direito processual civil internacional II*. Coimbra: Coimbra Editora, 2008. v. II. p. 241-273.

processos similares, seja eles oriundos do âmbito nacional, ou continental.¹⁷⁸ Por tudo isso, o reenvio prejudicial não pode ser caracterizado como um recurso judicial, no sentido estrito, vez que as partes prejudicadas na ação principal não têm legitimidade para iniciar este procedimento perante a União.¹⁷⁹

1.10 Conclusão parcial

A União Europeia foi projetada e aprimorada com o intuito de reforçar a integração dos países europeus, com o objetivo inicial de reestruturação daquele continente, frente às graves consequências sofridas pela 2ª Guerra Mundial. Com o decorrer das décadas, a integração foi inovadora a buscar novos meios de aprimorar o mercado comum e evoluir na construção de direitos fundamentais que deveriam ser alcançados por todos os seus entes e cidadãos.

Como meio para este objetivo, o Tribunal de Justiça da União Europeia foi alçado à ente primordial na efetivação dos direitos fundamentais. Sendo certo que foi criado para resolver disputas econômicas e financeiras, viu o seu papel ganhar abrangência, a partir do momento em que a própria União buscou alçar voos a questões sociais e jurídicas fundamentais a uma sociedade moderna.

Com foco para dar seguimento aos objetivos da União, foram criadas normas para estabelecer e direcionar os Estados-Membros e seus cidadãos, com a possibilidade de criação de normas consultivas ou até mesmo normas impositivas, sempre com o intuito de buscar a concretização dos direitos fundamentais na União.

Sobre o direito à proteção de dados pessoais, a União foi inovadora ao buscar a legitimação deste direito e a busca de sua consecução, a partir de regulamentações que datam a década de 1990, as quais foram a base para os Estados-Membros harmonizarem suas normas nacionais. Com o decorrer do tempo, a União deteve a possibilidade de criar um Regulamento Geral, o qual detém aplicação geral e indistinta de regras nacionais, demonstrando que o direito em questão já está equilibrado para a União o tratá-lo de forma harmônica.

¹⁷⁸ MOURA RAMOS, Rui Manuel de. *Estudos de direito internacional privado e de direito processual civil internacional II*. Coimbra: Coimbra Editora, 2008. v. II. p. 241-273.

¹⁷⁹ BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006. p. 245.

Ainda, a Carta de Direitos Fundamentais reforça a construção da União, com o intuito de registrar a proteção dos direitos fundamentais, à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica de todos os seus entes.

Por fim, verifica-se que a União foi criada a partir da necessidade da reconstrução dos países europeus, e com o decorrer do tempo, buscou a criação de um ente transnacional para consolidar o papel dos países europeus na ordem mundial, reforçando a proteção dos direitos fundamentais e o mercado comum existente.

2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE PERANTE O TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA

2.1 Objetivos da pesquisa sobre proteção de dados pessoais

Ao tratar do conceito da proteção de dados, Orla Lynskey adotou um entendimento cético e crítico ao concluir que, com base na argumentação desenvolvida pelo Tribunal, não é possível concluir com clareza o caminho trilhado pelo Tribunal a esse respeito dos fundamentos e contornos deste direito.¹⁸⁰ De fato, a análise jurisprudencial realizada por esta autora indica que a proteção de dados tem fundamentos e aplicações variadas na jurisprudência da União, tendo em vista a aplicação deste direito para a tutela de diferentes direitos fundamentais. Este é o tema central deste trabalho: investigar os fundamentos desta conclusão e avaliar de que forma o conceito do direito fundamental da proteção de dados pessoais foi construído e aplicado no âmbito da União Europeia. Ainda sobre este tema, a coleta da jurisprudência teve a finalidade de verificar se, em meio a variações argumentativas e de concepções distintas, a proteção de dados pessoais foi concebida e tratada pela jurisprudência da Corte da União Europeia apenas como um instrumento para efetivação de outros direitos ou se a este direito foi conferido um tratamento autônomo. Enfim, busca-se neste trabalho identificar os reflexos dogmáticos destas opções conceituais.

Afirma-se que não é objetivo deste trabalho a dissertação sobre conceitos e temas correlatos para com o direito à proteção de dados pessoais, como serão abordados neste capítulo, uma vez que a reflexão a ser trazida é a colisão de direitos e qual o entendimento consolidado pelo Tribunal da União, perfazendo um estudo analítico do caso.

Sob o ângulo dogmático, a análise destes julgamentos será uma oportunidade para revisitar conceitos-chave do regime de proteção de dados pessoais (dentre eles, os problemáticos conceitos de dados de pessoais e operações de tratamento). Fora isso, este exercício serve como antecipação de problemas jurídicos e práticos comuns a todos os órgãos nacionais ou internacionais que se proponham a regular essa matéria. Dentre eles: as relações de tensão entre o conceito de proteção de dados pessoais e os direitos comunicativos em geral, especialmente os direitos a informar e ser informado, as dificuldades decorrentes da aplicação à proteção de dados no âmbito da autonomia privada, enfim, problemas decorrentes de operações de tratamento preditivas (especialmente no âmbito da segurança ou saúde públicas)

¹⁸⁰ Nesse sentido: LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

e automatizadas e seus limites, todos esses temas foram objeto de intenso debate na jurisprudência europeia, que, neste sentido, pode e deve servir como um guia de possíveis caminhos para a solução desses conflitos.

2.2 Metodologia da coleta da jurisprudência do Tribunal de Justiça da União Europeia

Este trabalho busca identificar padrões decisórios e características dogmáticas do direito fundamental¹⁸¹ à proteção de dados pessoais. Ele se insere, portanto, no campo da dogmática jurídica e da pesquisa jurisprudencial empírica do direito. Importa à esta pesquisa delimitar o conteúdo do direito à proteção de dados, tendo em conta a jurisprudência do Tribunal de Justiça da União Europeia. No que tange a esta nomenclatura, vale aqui uma observação. Como já foi aqui salientado, dita denominação do Tribunal surgiu em 2007, com a aprovação do Tratado de Roma (“Reformador”). Apesar dessa alteração de nomenclatura, a base de dados fornecida pelo próprio Tribunal inclui tanto as decisões anteriores como as posteriores a este ano. Por isso não foi necessário seccionar a coleta em dois períodos, tendo em vista que alteração de nomenclatura não teve efeitos diretos sobre a compreensão do Tribunal sobre a matéria aqui pesquisada. Ou seja, os julgados anteriores à alteração do nome do Tribunal estão abarcados nos mesmos sites de pesquisa, como o corpo de julgados analisados identificará.

Em termos procedimentais, para alcançar esse objetivo, a seleção das decisões adotou os seguintes critérios: serão utilizados textos acadêmicos a respeito do direito em questão, que servirão de fundamento para a determinação inicial do conteúdo da privacidade e dados pessoais. Esse material servirá como base teórica para a compreensão da jurisprudência

¹⁸¹ A União Europeia não utiliza o termo “direito constitucional” ou “direito humano” em sua Carta de Direitos, mas tem consistentemente se referido como “direitos fundamentais”. Tem havido discussão considerável sobre a questão de como interpretar este termo. Em geral, existem três posições neste debate. Em primeiro lugar, existem aqueles que veem os direitos fundamentais, principalmente, como direitos constitucionais e posteriormente, a Carta como uma (quase) constituição da União Europeia (HIJMANS, Hielke. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Dissertation. University of Amsterdam, Amsterdam, 2016). Por outro lado, há quem defenda que o termo “direitos fundamentais” deve ser visto como um equivalente aos direitos humanos. Nessa perspectiva, argumenta-se que a Carta, na verdade, contém apenas direitos subjetivos para indivíduos e deveres da União para proteger os interesses dos cidadãos, e não os aspectos processuais que normalmente fazem parte da constituição (VAN DER SLOOT, Bart. *Privacy as personality right: why the ecthr's focus on ulterior interests might prove indispensable in the age of “Big Data”*. *Utrecht Journal of International and European Law*, v. 80, 2015). Por fim, também existem aqueles que adotam uma posição intermediária. Entre outros, estes apontam para o artigo 8º, da Declaração Universal dos Direitos Humanos, onde o termo “direitos fundamentais”, parece se originar (ROBINSON, Nehemiah. *The Universal Declaration of Human Rights: its origin, significance, application, and interpretation*. New York: World Jewish Congress, 1958. p. 111-112). Nesta pesquisa, seguiremos a posição intermediária que pode servir de base para estudos futuros seja qual for a posição a ser levada em consideração.

coletada pela pesquisa. Já as decisões serão selecionadas tendo como fontes primárias de coleta o site da Tribunal¹⁸² e, também, o banco de dados sobre temas ligados à privacidade e proteção de dados, organizado pela Universidade de Columbia.¹⁸³

Neste caso, a utilização de duas fontes de pesquisa se mostra importante para (i) certificar a abrangência da pesquisa realizada, e (ii) evitar a seleção de decisões não relacionadas com o tema da pesquisa. Sabe-se que a base de pesquisa eletrônica pode omitir dados ou julgados no resultado da pesquisa. Contudo, essas bases de dados são amplamente acessíveis e podem ser facilmente verificadas por outros pesquisadores.

Sendo assim, considera-se que tal tais fontes de dados fornecem um padrão confiável de averiguação, o que é suficiente para fundamentar a pesquisa documental. Fora isso, a jurisprudência do Tribunal é composta não só por decisões de casos contenciosos, mas também por manifestações consultivas.¹⁸⁴ Foi necessário, por isso, refinar o objeto da pesquisa. Quanto a esse aspecto, apesar de se reconhecer a importância das manifestações consultivas, foram selecionados os casos contenciosos de sua jurisprudência que tratam especificamente da matéria privacidade e/ou proteção de dados. Mas isso não foi o bastante. Foram também aplicados os seguintes critérios específicos de busca.

No banco de dados da Corte Europeia, foram aplicados filtros contidos no próprio site. Primeiramente, delimitou-se o “Estado dos processos” como “Processos encerrados”, com o intuito de averiguar casos já finalizados para garantir a segurança do julgado. Foi, então, aplicado um novo filtro limitador que seleciona para casos julgados pelo “Tribunal Geral” e “Tribunal de Justiça”, de acordo com a composição do Tribunal de Justiça, disposta em seu próprio site.¹⁸⁵

Já no campo “Documentos”, incluiu-se o tipo “Acórdão”, excluindo manifestações consultivas da Corte. Já no campo “Palavras do texto”, os itens “privacidade” e “dados pessoais” foram inseridos, isso para delimitar o tema a ser estudado. No tópico, “Matéria” indicou-se o tema “Proteção de Dados”; ainda, no ponto “Período ou data”, indicou-se em “todos os tipos de datas”, com as datas de 01/01/1989 a 31/12/2019, com o intuito de delimitar o período temporal aos últimos 30 (trinta) anos.

No tópico “Plano de classificação sistemática”, indicou-se “todos os valores selecionados”, para a coleta de dados indicar casos pré e pós Tratado de Lisboa. Já na questão

¹⁸² Disponível em: <http://curia.europa.eu/juris/recherche.jsf?language=pt>. Acesso em: 10 out. 2021.

¹⁸³ Disponível em: <https://globalfreedomofexpression.columbia.edu/>. Acesso em: 10 out. 2021.

¹⁸⁴ Para uma definição sobre as normativas referidas como Decisão; Recomendação e Parecer, verificar o capítulo 1 desta dissertação.

¹⁸⁵ Disponível em: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_pt. Acesso em: 10 out. 2021.

“Língua que faz fê”, foram indicadas todas as línguas, quais sejam, “alemão”, “Búlgaro”, “checo”, “Croácia”, “dinamarquês”, “Eslovaco”, “Esloveno”, “espanhol”, “estónio”, “finlandês”, “francês”, “grego”, “húngaro”, “inglês”, “Irlandês”, “italiano”, “letão”, “lituano”, “Maltês”, “neerlandês”, “Polaco”, “português”, “Romeno”, “sueco”. Da aplicação destes critérios resultou a identificação de 20 (vinte) documentos.

Foi ainda utilizado como contraprova o mecanismo disponibilizado pela Universidade de Columbia.¹⁸⁶ Nesse mecanismo de busca, a escolha dos casos se deu, basicamente, selecionando os filtros disponibilizados pelo próprio site. Primeiramente, foi delimitado o período temporal a ser analisado: também de trinta anos, ou seja, do ano 1989 ao 2019. Além disto, selecionou-se o modo de expressão a ser analisado “privacy, data protection and retention”, isto é, privacidade, proteção e retenção de dados, com a indicação do Tribunal de Justiça da União Europeia, qual seja, “Court of Justice of the European Union (CJEU)”, atingindo um total de 13 (treze) casos. Enfim, do cruzamento destas pesquisas, foram identificados 27 (vinte e sete) casos, sendo que 6 (seis) casos eram idênticos. No mais, foram incluídos 03 (três) casos que são considerados pela literatura como paradigmáticos da jurisprudência do Tribunal de Justiça acerca do direito à proteção de dados pessoais. Estes casos foram incluídos nesta pesquisa diante da relevância dos temas neles analisados.¹⁸⁷ Como resultado final, serão analisados 30 (trinta) casos julgados pelo Tribunal.

Os 03 (três) primeiros casos analisados tratam especificadamente sobre a transposição das normas do Direito da União para as legislações nacionais, tema que merece destaque diante da dificuldade apresentada pelos países para a criação da legislação específica. Estes julgados não adentram especificamente no mérito da proteção de dados pessoais, mas merecem reflexão por neles ser debatido o tema da supremacia do Direito da União. Diante da natureza e extensão do problema apresentado, bem como da metodologia e da perspectiva

¹⁸⁶ Disponível em: <https://globalfreedomofexpression.columbia.edu/>. Acesso em: 10 out. 2021.

¹⁸⁷ Os casos incluídos são 1) Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003; 2) Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003, e; 3) Processo C-73/07. *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008. Estes processos são analisados por: LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015; LYNSKEY, Orla. From market-making tool to fundamental right: the role of the Court of Justice in data protection’s identity crisis. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 59-84; RALLO, Artemi; MARTÍNES, Ricard. Data protection, social networks and online mass media. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 407-430; TZANOU, Maria. Personal data protection and legal developments in the European Union. Hershey, PA: IGI Global, 2019; CLASSEN, Claus Dieter. *Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk*. Common Market Law Review, Issue 5, 2004. v. 41. p. 1377-1385; FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2014. v. 16.

escolhida para enfrentá-lo, a pesquisa pretende descrever e analisar as jurisprudências do Tribunal de Justiça da União Europeia sobre privacidade e dados pessoais.

2.3 Categorização de direitos abarcados na jurisprudência sobre direito à proteção de dados pessoais do Tribunal de Justiça da União Europeia

A análise da jurisprudência coletada pressupõe algumas distinções prévias. Primeiro é preciso observar que em pelo menos metade dos casos a serem identificados,¹⁸⁸ o precedente não cita explicitamente o artigo 8º da Carta como um direito fundamental autônomo.¹⁸⁹ Ao contrário, os julgados tratam a proteção de dados em conjunto com o artigo 7º (dispositivo que trata da privacidade), assim como um conjunto dos demais direitos previstos na própria Carta.¹⁹⁰ Inclusive, o direito à proteção de dados pessoais é analisado diante de variados direitos existentes no ordenamento da União Europeia, devendo-se investigar desde a inclusão de normativas da União às legislações nacionais, perpassando por direitos sobre a propriedade intelectual, privacidade, liberdade de expressão, dignidade humana, devido processo legal.

Com profundidade de análise, o Tribunal pôde se debruçar sobre o conceito de controlador de dados (Encarregados de dados, no caso da União Europeia), o direito ao esquecimento, acesso à dados pessoais, responsabilização de prestadores de serviço de Internet, acesso aos dados por terceiros, transferência internacional de dados, além do próprio conceito de dados pessoais. Em todas essas situações, o Tribunal destacou a importância da razoabilidade (proporcionalidade) nas medidas impetradas pelos tribunais locais, sempre visando a garantia dos direitos previstos na Carta.¹⁹¹ As consequências dessa orientação jurisprudencial atravessaram o Atlântico e influenciaram a elaboração de diversas normas do direito brasileiro. Como exemplo, a Lei que trata da responsabilização de provedor de

¹⁸⁸ Dos casos elencados na introdução, ao menos, 15 dos 30 casos indicam a coexistência de direitos. Orla Lynskey indica que, até a promulgação da GDPR, o Tribunal indicava que a diretiva da UE visava garantir a proteção dos direitos fundamentais, em particular a privacidade (LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015).

¹⁸⁹ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011.

¹⁹⁰ Exemplos destes direitos podem ser encontrados em: 1) Direito de Proteção de Dados e Direito à Propriedade (Processo C 275/09. *Promusicae*. Julgamento: 17 março 2011); 2) Direito de Proteção de Dados e Direito à Liberdade De Expressão (Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014); 3) Direito de Proteção de Dados e Direito ao Esquecimento (Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricultura di Lecce v. Salvatore Manni. Relator M. Ilešič*. Julgamento em: 09 março 2017).

¹⁹¹ POLAKIEWICZ, Jörg. Profiling – the Council of Europe’s Contribution. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 367-377. p. 372.

serviços de Internet por conteúdo de terceiros (Lei nº 12.965, de 23 de abril de 2014, conhecida como o Marco Civil da Internet – MCI), utilizou de fundamentos semelhantes ao do Tribunal da União.¹⁹² Isso mostra que essas decisões podem ser consideradas um ato de equilíbrio do Tribunal na tentativa de reconciliar os muitos divergentes direitos e interesses dos sujeitos envolvidos, principalmente à custa do direito à proteção de dados pessoais.

A divisão dos direitos abarcados pela pesquisa sempre estará com o pano de fundo do direito à proteção de dados pessoais, portanto, não serão desenvolvidos estes demais direitos para facilidade da leitura e análise.

2.2.1 *Transposição do direito da União à legislação nacional*

Os três casos agrupados neste item tratam de matérias semelhantes e indicam situações em que houve a falta de transposição de medidas da União sobre o tratamento de dados pessoais e à proteção da privacidade às legislações nacionais.¹⁹³ Eles não tratam do conceito da proteção de dados, mas indicam a importância da jurisdição exercida pelo Tribunal, assim como apresentam o esforço desta Corte no sentido de tornar a matéria (proteção de dados) vinculante e uniforme em todo o continente Europeu.

2.2.1.1 *Commission of the European Communities v. Kingdom of the Netherlands*

No ano de 2004 o Tribunal de Justiça apreciou o Processo C-350/02 (*Commission of the European Communities v. Kingdom of the Netherlands*).¹⁹⁴ Nele a Comissão das Comunidades Europeias intentou a ação, por descumprimento, contra o Reino dos Países Baixos, por entender que este último não adotou as disposições legislativas, regulamentares e administrativas necessárias para transpor integral e corretamente para o seu direito nacional. Como fundamento, foram indicados os artigos 6º e 9º da Diretiva 97/66/CE, que exigem a definição de prazo específico para o a implementação das medidas ali descritas em nível nacional.¹⁹⁵ Salientou-se nos casos que, para que a referida disposição nacional seja conforme

¹⁹² SOUZA, Carlos Affonso Pereira. Responsabilidade civil dos provedores de acesso e aplicações de internet: evolução jurisprudencial e os impactos da Lei n. 12.965/2014 (Marco Civil da Internet). In: LEITE, George Salomão; LEMOS, Ronaldo (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 791-816. p. 812.

¹⁹³ KUNER, Christopher. Beyond Safe Harbor: European data Protection Law and Electronic Commerce. *The International Lawyer*, n. 1, p. 79-88, 2001. p. 80.

¹⁹⁴ Processo C-350/02. *Commission of the European Communities v. Kingdom of the Netherlands*. Julgamento em: 29 janeiro 2004.

¹⁹⁵ “Artigo 15º Execução da directiva. 1. Os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente directiva o mais tardar em 24

a esta diretiva, a medida geral da Administração da União deve comportar uma lista exaustiva de dados pessoais.¹⁹⁶ Desta forma, a legislação nacional não teria assegurado os direitos previstos pelo Direito da União, ao tratamento de dados pessoais.

Neste ponto, verifica-se a dificuldade de transposição das Diretivas para as legislações nacionais, as quais encontram desafios próprios e singulares para a construção legislativa interna. Inclusive, o próprio Reino dos Países Baixos sustentou não ter realizado a transposição necessária, mas que estava em processo de adequação da legislação nacional, o que ocorreu a partir da promulgação de Diretiva posterior, criada com o intuito de efetivar seu papel como Estado-Membro. Contudo, o Tribunal entendeu que o país não cumpriu com o prazo legal devido. Verifica-se, portanto, que a União determinava a plena segurança aos dados pessoais no campo das telecomunicações, desde o final da década de 1990. Por outro lado, é preciso observar que Diretiva estabelece uma conexão entre dados pessoais e a privacidade e que apesar deste julgamento não adentrar sobre os direitos em si, há a clara determinação de que estes direitos devem ser regulados pela legislação nacional, trazendo ao arcabouço jurídico seu tratamento.¹⁹⁷

2.2.1.2 Commission of the European Communities v. Grand Duchy of Luxemburg

No ano de 2003 o Tribunal de Justiça analisou processo semelhante ao anterior (Caso C-211/02 – *Commission of the European Communities v. Grand Duchy of Luxemburg*). Nele, a Comissão Europeia intentou ação declaratória para que se reconhecesse que, ao não criar a legislação nacional e ao não comunicar à Comissão Europeia das medidas nacionais de transposição sobre a Diretiva 97/66/CE, o Estado de Luxemburgo estaria violando normas da União.¹⁹⁸ Novamente, o Tribunal enfrentou a dificuldade da implementação da Diretiva em países da União. Inclusive, o governo de Luxemburgo afirmou que ainda não havia sido realizada a transposição, pois tiveram de ser feitos importantes estudos preliminares para determinar as formas adequadas de transposição.¹⁹⁹ Contudo, o Tribunal identificou que o não cumprimento deveria ser apreciado em função da situação de não haver sido cumprido o

de Outubro de 1998. Em derrogação do primeiro parágrafo, os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento ao disposto no artigo 5º da presente directiva, o mais tardar, até 24 de Outubro de 2000.”

¹⁹⁶ Processo C-350/02. *Commission of the European Communities v. Kingdom of the Netherlands*. Julgamento em: 29 janeiro 2004. Parágrafo 33.

¹⁹⁷ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

¹⁹⁸ Processo C-211/02. *Commission of the European Communities v. Grand Duchy of Luxemburg*. Julgamento em: 03 março 2003.

¹⁹⁹ Processo C-211/02. *Commission of the European Communities v. Grand Duchy of Luxemburg*. Julgamento em: 03 março 2003. Parágrafo 5.

prazo fixado.²⁰⁰ Além disso, a decisão foi fundamentada no fato de que um Estado-Membro não pode invocar práticas ou situações da sua ordem jurídica interna para justificar a inobservância das obrigações e dos prazos fixados numa Diretiva.²⁰¹ Esta decisão está, portanto, intrinsicamente ligada à doutrina da supremacia da norma da União, segundo a qual:

As disposições do Tratado e os actos das instituições directamente aplicáveis têm por efeito, nas suas relações com o direito interno dos Estados-membros, não apenas tornar inaplicável de pleno direito, desde o momento da sua entrada em vigor, qualquer norma de direito interno que lhes seja contrária, mas também – e dado que tais disposições e actos integram, com posição de precedência, a ordem jurídica aplicável no território de cada um dos Estados-membros – impedir a formação válida de novos actos legislativos nacionais, na medida em que seriam incompatíveis com normas do direito comunitário.²⁰²

Assim, proíbe-se as autoridades públicas de invocarem o direito e fatos nacionais para justificar o não cumprimento do direito da União.²⁰³

2.2.1.3 *Commission of the European Communities v. French Republic*

O Tribunal se debruçou sobre o tema ao analisar o caso C-151/00 (*Commission of the European Communities v. French Republic*). Novamente, a ação pedia que o Tribunal declarasse que, ao não pôr em vigor e ao não comunicar à Comissão Europeia, no prazo previsto, a República Francesa não cumpriu com as obrigações que lhe incumbia, para a transposição da Diretiva 97/66/CE.²⁰⁴ Como nos outros casos, o governo francês não contestou sua obrigação de transpor às disposições para o direito interno e admitiu o seu atraso. Disse somente que a Diretiva 97/66/CE implicaria na revisão de sua legislação e que o processo legislativo já havia sido iniciado e chegaria ao seu termo em curto prazo.²⁰⁵ Em sua decisão, o Tribunal reconheceu que o processo político nacional decisório tem suas variantes

²⁰⁰ Processo C-211/02. *Commission of the European Communities v. Grand Duchy of Luxemburg*. Julgamento em: 03 março 2003. Parágrafo 6.

²⁰¹ Processo C-211/02. *Commission of the European Communities v. Grand Duchy of Luxemburg*. Julgamento em: 03 março 2003. Parágrafo 7.

²⁰² Processo C-106/77. *Amministrazione delle Finanze dello Stato v Simmenthal SpA*. Julgamento em: 9 março 1978. Parágrafo 17.

²⁰³ SWEET, Alec Stone. Constitutional dialogues in the european community. In: SLAUGHTER, Anne-Marie; SWEET, Alec Stone; WEILER, J. H. H. (org.). *The European Court and National Courts – doctrine and jurisprudence. Legal Change in Its Social Context*. Oxford: Hart Publishing, 1998. p. 305-330. p. 307.

²⁰⁴ Processo C-151/00. *Commission of the European Communities v French Republic*. Julgamento: 18 janeiro 2001.

²⁰⁵ Processo C-151/00. *Commission of the European Communities v French Republic*. Julgamento: 18 janeiro 2001. Parágrafo 4.

locais e costumes que merecem destaque para a transposição indicada.²⁰⁶ Neste sentido, o julgado cita a quantidade de alterações legislativas que deveriam ter ocorridos no prazo indicado pela União:

Por carta de 12 de abril de 1999, a Representação Permanente da França junto da União Europeia comunicou à Comissão que a Directiva 97/66 tinha já sido parcialmente transposta para o direito francês. As autoridades francesas esclareciam que os artigos da Directiva 97/66 ainda não transpostos o seriam através de um decreto que alterava o artigo D.98-1 do code des postes et télécommunications (Código dos Correios e Telecomunicações), cuja adopção era anunciada para finais do primeiro semestre de 1999. As mesmas autoridades acrescentavam ainda que o artigo 12º da Directiva 97/66 seria transposto ao mesmo tempo que a Directiva 97/7/CE do Parlamento Europeu e do Conselho, de 20 de Maio de 1997, relativa à protecção dos consumidores em matéria de contratos à distância (JO L 144, p. 19), e que estava a ser analisada a necessidade de invocar as disposições do artigo 3.º, n.º 3, da Directiva 97/66.²⁰⁷

De todo modo, o Tribunal entendeu que a transposição da Directiva 97/66/CE não foi realizada no prazo nela fixado e a ação proposta pela Comissão deveria ser julgada procedente.

2.2.2 Transferência internacional de dados pessoais, segurança nacional

2.2.2.1 Ireland v. European Parliament and Council of the European Union

Em avença judicial acerca de matéria de segurança nacional, a Irlanda requisitou ao Tribunal que anulasse a Directiva 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas disponíveis publicamente ou em redes públicas de comunicações.²⁰⁸ Aqui o Tribunal asseverou que a Directiva 2006/24/CE foi necessária para prever um nível harmonizado de conservação de dados relativos às comunicações eletrônicas a todos os membros da União, vez que as

²⁰⁶ Sobre uma análise mais perfunctória sobre o efeito prático das teorias do efeito direto, efeito indireto e responsabilidade governamental, ver: SWEET, Alec Stone. Constitutional dialogues in the european community. In: SLAUGHTER, Anne-Marie; SWEET, Alec Stone; WEILER, J. H. H. (org.). *The European Court and National Courts – doctrine and jurisprudence. Legal Change in Its Social Context*. Oxford: Hart Publishing, 1998. p. 305-330.

²⁰⁷ Processo C-151/00. *Commission of the European Communities v French Republic*. Julgamento: 18 janeiro 2001. Parágrafo 4.

²⁰⁸ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009.

medidas nacionais anteriores à esta Diretriz apresentavam divergências no que diz respeito à natureza dos dados conservados e ao período da sua conservação.²⁰⁹

Foi ainda esclarecido pelo julgamento que o caso incide unicamente sobre a escolha da base jurídica, não sobre uma eventual violação dos direitos fundamentais decorrentes de ingerências no exercício do direito ao respeito da vida privada consagrado na Diretiva 2006/24. Não analisada, por isso, a matéria de fundo acerca da privacidade e proteção de dados em si.²¹⁰ Afirmou-se também que o objetivo da Diretiva era a convergência das legislações nacionais relativas à obrigação de conservação de dados, às categorias de dados a serem conservados, ao período de conservação, à proteção e à segurança dos sistemas de conservação dados, bem como aos requisitos para a sua armazenagem.²¹¹

Deste modo, no entender do Tribunal, a Diretiva não trazia alusão ao acesso aos dados pessoais, nem à sua exploração pelas autoridades dos Estados-Membros, ou à cooperação entre os Estados, o que significa que a legislação regula o modo de tratamento dos dados e não o seu compartilhamento.²¹² Com base nessas premissas, o Tribunal concluiu que o conteúdo substantivo da Diretiva 2006/24 se dirigia, essencialmente, às atividades dos prestadores de serviços no mercado interno, com exclusão das atividades do Estado que necessitam de tratados internacionais ou comunitários, mantendo a validade da Diretiva.²¹³

Este acórdão do Tribunal de Justiça é de importância crucial, tendo em vista que ele serviu de paradigma para as futuras ações da União Europeia no domínio da privacidade e da proteção de dados. Ele também confirmou que o Tribunal utilizaria, nas demais decisões, de uma avaliação da proporcionalidade e da necessidade de medidas que configurem sérias restrições aos direitos fundamentais, salvo situações que envolvam valores como a segurança nacional.²¹⁴ O julgamento indica, por fim, que as exceções aos direitos fundamentais deverão

²⁰⁹ “Artigo 4º: Os Estados Membros devem tomar medidas para assegurar que os dados conservados em conformidade com a Diretiva só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. Os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado Membro no respectivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem.”

²¹⁰ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 57.

²¹¹ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 63.

²¹² Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 83.

²¹³ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 53.

²¹⁴ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 64.

vir acompanhadas por salvaguardas adequadas, o que tem o fim de garantir que qualquer restrição grave aos direitos fundamentais deve ser circunscrita ao estritamente necessário. Essas garantias fazem parte da legislação da União e não podem ser afastadas pela legislação dos Estados-Membros.²¹⁵

2.2.2.2 *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeia*

No ano de 2004 o Tribunal se debruçou sobre processo de relevância diplomática. No julgamento dos casos C-317/04 e C-318/04 (*European Parliament v. European Data Protection Supervisor (EDPS) and Council of the European Union*), o Parlamento Europeu intentou ação para discutir acordo internacional entre a Comunidade Europeia e os Estados Unidos da América. Este acordo abordava o tratamento e a transferência de dados pessoais contidos nos Registos de Identificação dos Passageiros (PNR), documentos elaborados por transportadoras aéreas e utilizados no Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos da América.²¹⁶ Na demanda solicitou-se que o Tribunal identificasse se o nível de proteção do Acordo era adequado para a transferência de dados para esta agência interna dos Estados Unidos.²¹⁷

O caso trata de questões intrinsicamente ligadas à proteção de dados pessoais, quais sejam: (i) finalidade do tratamento; e (ii) transferência à terceiros.²¹⁸ Em seu julgamento, o Tribunal utilizou como fundamentos jurídicos a Diretiva n.º 97/66/CE e o artigo 8º, da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.²¹⁹ Com isso, definiu que os dados pessoais contidos nos Registos de Identificação dos Passageiros (PNR), que em um primeiro momento são transferidos com

²¹⁵ Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009. Parágrafo 88.

²¹⁶ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006.

²¹⁷ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 2.

²¹⁸ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 63.

²¹⁹ Artigo 8º: “1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”.

base em atividades econômicas realizadas pelas companhias aéreas, deveriam ser tratados de acordo com o uso e o objetivo do processamento, não pelo objetivo dado pelo Acordo.²²⁰

O Tribunal parte da premissa de que a transferência de dados dos passageiros constitui operações de processamento relativas à segurança pública e às atividades do Estado na área criminal.²²¹ Com base nisso, o julgamento se limita a analisar em suas fundamentações o tema da base jurídica do processamento do PNR e evitou a questão da implicação da proteção de dados do Acordo sobre os direitos dos indivíduos.²²² Em sua conclusão, o Tribunal entendeu que o tratamento de dados pessoais deve ser justificado pelo seu uso e objetivo final, não sobre sua justificação primária ou econômica.²²³ E, por isso mesmo, as transferências de dados do PNR foram consideradas como processamento de dados relacionado à segurança e, assim, o acordo foi anulado.²²⁴

Importante aspecto sobre o tema do tratamento dos dados pessoais, neste caso, foi o fundamento adotado pela Corte ao indicar que o fato de os dados pessoais terem sido recolhidos por operadores privados para fins comerciais e de serem eles os agentes que organizam a sua transferência para um Estado terceiro não implica em violação das medidas de proteção em vigor à época. Isso porque essa transferência de dados integra-se num quadro instituído pelos poderes públicos tem em vista a tutela da segurança pública e, por isso mesmo, não é necessária à prestação de serviços dos referidos operadores.²²⁵

Ressalta-se, por fim, que este aspecto da justificação das medidas de controle de dados relacionadas com o tema da segurança pública e de atividades do Estado no campo criminal tem nexos causal com a sequência dos ataques terroristas de 11 de setembro de 2001, o que, inclusive, foi rememorado no julgamento em questão.²²⁶

²²⁰ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 57.

²²¹ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 65.

²²² Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 67.

²²³ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 58.

²²⁴ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 70.

²²⁵ Para discussões aprofundadas sobre as ações da União em relação à segurança ver CARRERA, S.; MITSILEGAS, V. (org.). *Constitutionalising the Security Union: effectiveness, rule of law and rights in countering terrorism and crime*. Brussels: Centre For European Policy Studies, 2017.

²²⁶ Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006. Parágrafo 33.

2.2.2.3 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources*

O julgamento dos casos C-293/12 e C-594/12 (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources*) tratou do equilíbrio de direitos no contexto da coleta e retenção de dados, a partir de medidas dos Estados-Membros.²²⁷ Este precedente é paradigmático e importante para a consolidação deste direito no âmbito da União e, por isso, merece uma análise cuidadosa. A controvérsia envolve a Diretiva 2006/24/CE, que obrigava os Estados-Membros a adotarem leis que exijam dos provedores de acesso à internet e telecomunicações a retenção de metadados de todos os seus clientes por um período de até dois anos. A retenção tem como objetivo e aplicação da lei e de medidas de ordem pública.²²⁸ Os dados conservados em conformidade esta Diretiva 2006/24/CE poderia revelar a identidade da pessoa, hora, local e frequência da comunicação e permitem conclusões bastante precisas sobre a vida privada das pessoas, incluindo residência, movimento, círculos sociais, entre outros.²²⁹

Foi solicitado, assim, que o Tribunal examinasse a validade da Diretiva 2006/24/CE, à luz dos artigos 7º, 8º e 11 da Carta Europeia. Esses direitos dizem respeito a privacidade, proteção de dados e liberdade de expressão.²³⁰ Em sua decisão, o Tribunal salientou que a essência do direito à privacidade foi respeitada, uma vez que a Diretiva não permitia adquirir conhecimento do conteúdo das comunicações.²³¹ Disse também que esta norma não afetava a essência do direito à proteção de dados pessoais, pois a Diretiva determinava certos princípios de proteção e segurança de dados, como medidas técnicas e organizacionais contra a destruição acidental ou ilegal, perda acidental ou alteração dos dados.²³²

Porém, apesar de identificar uma ingerência potencial no conteúdo do artigo 11, da Carta Europeia, dispositivo que garante a liberdade de expressão, o Tribunal entendeu não ser necessária a análise do caso com relação a este direito, uma vez que somente a identificação dos direitos abarcados pelos artigos 7º e 8º, também da Carta, já satisfariam a análise da

²²⁷ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014.

²²⁸ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 2.

²²⁹ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 16.

²³⁰ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 28.

²³¹ BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

²³² BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

controvérsia.²³³ Após constatar que a Diretiva tinha o objetivo de interesse geral de salvaguardar a segurança pública, o Tribunal desenvolve um teste de proporcionalidade em duas camadas.²³⁴ Em um primeiro momento, analisa a adequação da Diretiva para alcançar o objetivo por ela era perseguindo.²³⁵ Quanto a este ponto, o Tribunal concluiu que os dados conservados auxiliavam as autoridades com a investigação de crimes graves e eram uma ferramenta valiosa para procedimentos criminais. Em um segundo momento, o Tribunal considerou a necessidade das medidas.²³⁶ E aqui o julgamento afirma que, mesmo que intacta a essência do direito, as limitações da Diretiva aos direitos da Carta poderiam ser consideradas desproporcionais e também desnecessária. Por isso, a Diretiva em questão foi invalidada.²³⁷

Para chegar a esta conclusão, o Tribunal afirma que os indivíduos devem ser efetivamente protegidos contra uso indevido e abusivo de seus dados pessoais por meio de regras claras e precisas que imponham salvaguardas mínimas nos processos de tratamento.²³⁸ Além disso, como a Diretiva Retenção de Dados se aplica a todos os meios de comunicação eletrônica, cuja utilização é comum e de crescente importância no cotidiano das pessoas, os efeitos adversos da retenção generalizada eram potencializados com o crescimento e ampliação de sistemas eletrônicos comunicações.²³⁹ No limite, com o desenvolvimento tecnológico, poderia ocorrer a coleta massiva de dados pessoais.

Outro aspecto incompatível com o requisito de necessidade do tratamento é a falta de limites para que as autoridades nacionais acessem e usem posteriormente os dados.²⁴⁰ Isso porque o termo “crime grave” permanecia indefinido na Diretiva, que apenas se referia a esta expressão de maneira geral.²⁴¹ Além disso, a Diretiva não previa regras substanciais ou

²³³ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 70.

²³⁴ ARNBAK, Axel M. *Securing private communications: protecting private communications security in EU law: fundamental rights, functional value chains and market incentives*. Wolters Kluwer. Kluwer Law International, 2016.

²³⁵ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 38.

²³⁶ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 41.

²³⁷ BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

²³⁸ BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. SSRN Electronic Journal, 2018.

²³⁹ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 60.

²⁴⁰ BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. SSRN Electronic Journal, 2018.

²⁴¹ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 61.

processuais para reger o acesso e a utilização dos dados, nem exigia que os Estados-Membros estabelecessem limites.²⁴² Enfim, o terceiro problema é o período de retenção dos dados, que, de acordo com a Diretiva, ficaria entre o mínimo de 06 (seis) e máximo de 24 (vinte e quatro) meses. Não havia ainda distinção entre reter diferentes categorias de dados, nem existiam critérios objetivos para a determinação de qual o período exato de retenção.²⁴³

Com base nessas premissas, o Tribunal considerou que a Diretiva Retenção de Dados não cumpria a proteção dos dados prescrita na Diretiva Proteção de Dados (95/46/CE) e na Diretiva Privacidade e Proteção Eletrônica das Comunicações Eletrônicas (2002/58/CE). Estes diplomas garantiam a confidencialidade dos dados de comunicação e também obrigavam os controladores (Encarregados de dados, no caso da União Europeia) a apagar ou a anonimizar dados, sempre quando estes não se revelassem mais necessários para a sua finalidade primária.²⁴⁴ E, assim, o Tribunal não apenas estabeleceu um direito positivo à segurança técnica das comunicações, mas também desenvolveu elementos novos e concretos do direito à proteção de dados pessoais, tanto de uma perspectiva substancial quanto procedimental.

Em conclusão de grande importância para a disciplina da proteção de dados, o Tribunal afirma que garantir a segurança dos metadados retidos deve ser um papel importante quando da retenção de dados pessoais.²⁴⁵ Isso porque o Tribunal estabeleceu que a retenção obrigatória de metadados equivale a uma interferência grave no direito à privacidade e à proteção de dados, consagrados nos artigos 7º e 8º, da Carta da União.²⁴⁶ Isso significa que retenção ou o acesso aos dados pelas autoridades pode afetar diretamente a vida privada das pessoas e se enquadra no escopo do artigo 7º, da Carta. Além disso, essas atividades constituem tratamento de dados pessoais e, portanto, devem necessariamente se enquadrar no escopo do artigo 8º, da Carta. Por fim, importante passagem deste julgado traz definições claras sobre o processamento de dados pessoais realizado com o fim de salvaguardar a segurança pública:

²⁴² BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

²⁴³ BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. SSRN Electronic Journal, 2018.

²⁴⁴ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 62.

²⁴⁵ ARNBAK, Axel M. *Securing private communications: protecting private communications security in EU law: fundamental rights, functional value chains and market incentives*. Wolters Kluwer. Kluwer Law International, 2016.

²⁴⁶ BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

[A] regulamentação da União em causa deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e imponham exigências mínimas, de modo a que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos²⁴⁷

O Tribunal decidiu, portanto, que o legislador da União excedeu os limites impostos pelos artigos 7º e 8º da Carta e, por isso, invalidou a Diretiva 2006/24/CE. Esta foi a primeira vez que o Tribunal invalidou norma europeia com base no direito fundamental à proteção de dados pessoais.²⁴⁸ Para os fins deste trabalho, é preciso observar ainda que Tribunal associa a proteção de dados não só à privacidade, mas também à liberdade de expressão, o que indica que, na concepção do Tribunal, a proteção de dados não é sinônimo de privacidade e sua incidência pode ocorrer em conjunto com outro direito fundamental.²⁴⁹

No mais, dois pontos foram considerados fundamentais para o Tribunal anular a diretiva: (i) falta de especificidade da legislação para garantir a integridade e a confidencialidade dos dados, e (ii) a falha da legislação em garantir supervisão independente.²⁵⁰ Mas há críticas a serem tecidas a este julgado, devido à sua importância e amplitude. Como foi exposto, o Tribunal encontrou uma interferência particularmente grave aos direitos abarcado nos artigos 7º e 8º, da Carta.²⁵¹ No entanto, certas conclusões do Tribunal são contestadas pela literatura especializada. Em primeiro lugar, o Tribunal entendeu que a interferência no direito à proteção de dados é estabelecida apenas porque os dados são processados.²⁵² Isso significa que qualquer processamento dados pessoais interfere diretamente insculpido no artigo 8º, da Carta, conclusão que torna a violação da proteção de dados um fato permanente e até mesmo dificulta a existência deste direito, uma vez que ele estaria em risco constantemente.²⁵³

²⁴⁷ Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014. Parágrafo 54.

²⁴⁸ BRKAN, Maja. The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's Constitutional Reasoning. *German Law Journal*, v. 20, n. 6, p. 864-883, 2018. p. 865.

²⁴⁹ LYNSKEY, Orla. *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*. *International and Comparative Law, Quarterly*, 2014. p. 569-597.

²⁵⁰ BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. *SSRN Electronic Journal*, 2018.

²⁵¹ BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. *SSRN Electronic Journal*, 2018.

²⁵² VRIES, Katja de; BELLANOVA, Rocco; HART, Paul de; GUTWIRTH, Serge. The German Constitutional court judgment on data retention: proportionality overrides unlimited surveillance (doesn't it?). In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; LEENES, Ronald. *Computers, privacy and data protection: an element of choice*. Springer Dordrecht Heidelberg London, 2011. p. 29-50.

²⁵³ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

Isso indica que o julgamento em questão opera uma inversão, pois em regra o processamento de dados deve ser permitido, mas este ato deve estar sujeito a várias regras que protegem o titular dos dados contra abusos. Não é qualquer processamento que interfere com o direito, mas somente aquele que ultrapassa as regras que regem a proteção de dados pessoais.²⁵⁴

2.2.2.4 Maximillian Schrems v. Data Protection Commissioner (Safe Harbor)

Em julgamento posterior, conhecido como *Safe Harbor (Maximillian Schrems v. Data Protection Commissioner – C-362/14)*, o Tribunal declarou a nulidade do Acordo Transatlântico firmado entre a União e os EUA, que permitia às empresas transferirem dados pessoais da Europa para os Estados Unidos.²⁵⁵ Trata-se, novamente, de um caso com grande repercussão e importância para o tema em questão, merecendo maior destaque na pesquisa. A demanda foi apresentada no âmbito de litígio que opôs o cidadão austríaco M. *Schrems* e o *Data Protection Commissioner* irlandês, que se recusou a investigar uma queixa fundamentada no fato de o *Facebook Ireland Ltd* transferir, para os Estados Unidos, dados pessoais dos seus usuários e os conservar em servidores situados naquele país.

O Acordo Transatlântico firmado entre a União e os Estados Unidos da América foi criado para que empresas norte-americanas se certifiquem a transferência de dados de cidadãos europeus para os Estados Unidos obedecem aos padrões de proteção de dados da União. Com este objetivo, uma empresa sediada nos Estados Unidos da América pode aderir ao acordo *Safe Harbor*, desde que garanta os seguintes princípios: (i) aviso ao usuário de que os dados pessoais foram coletados; (ii) oferecer a escolha aos indivíduos que optarem em não participar da coleta de dados; (iii) garantirem que nenhuma transferência de dados coletados deve ser realizada, a menos que explicitamente consentido pelo indivíduo; (iv) criar um sistema de segurança da coleta dos dados; (v) garantir a integridade dos dados coletados; (vi) enfim, assegurar aos indivíduos o direito de acessar dados mantidos.²⁵⁶

A razão determinante para a assinatura desse Acordo é a obrigatoriedade de os Estados-Membros garantirem um nível de proteção para a transferência de dados pessoais

²⁵⁴ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

²⁵⁵ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015.

²⁵⁶ RUITER, Joep; WARNIER, Martijn. Privacy regulations for cloud computing: compliance and implementation in theory and practice. In: *Computers, privacy and data protection: an element of choice*. London: Springer Dordrecht Heidelberg, 2011. p. 387-402.

para países terceiros – proteção em nível igualitário, nos termos da Diretiva 95/46/CE.²⁵⁷ A União Europeia exige esta equivalência de proteção nas operações de transferência internacional de dados pessoais, em razão da limitação jurisdicional de cada país em legislar e atuar dentro do seu espaço territorial. Por isso, a regra criada pela União não poderia criar determinações vinculantes à países estrangeiros à União Europeia. Em compensação, o sistema exige que as operações de transferência sejam acompanhadas de salvaguardas suficientes para a proteção de dados pessoais no exterior.²⁵⁸

Contudo, há um gama de relações conflituosas que decorrem da maior intensidade e complexidade da transnacionalidade das relações sociais e econômicas.²⁵⁹ Para que a segurança dessas operações não seja comprometida, é necessário criar um canal de diálogo entre os Estados para o estabelecimento de regras claras no que tange à recepção e à aplicação de normas no contexto internacional.²⁶⁰ É o que ocorre com a crescente demanda para o alinhamento transnacional de regulações sobre a privacidade e proteção de dados, tema que tem como principal meta a criação de regras equânimes em um mundo cada vez mais globalizado. A esse respeito, apesar da vigência da Convenção 108 do Conselho da Europa, sua adesão é facultativa.²⁶¹ Não existe, portanto, tratado internacional vinculante sobre esta matéria, que se dirija de forma específica requisitos e procedimentos para a proteção de dados pessoais nas operações de transferência internacional. Foi por isso que a União Europeia criou o mecanismo (*Safe Harbor*) contestado neste processo.²⁶²

²⁵⁷ Artigo 25.º, n.º 6, da Diretiva 95/46 e artigo 46, do Regulamento (UE) 2016/679.

²⁵⁸ Para alguns autores, a palavra competência exprime melhor o fenômeno em questão neste julgado. É o caso de Charles Rousseau, para quem competência territorial significa “a competência do estado em relação aos homens que vivem em seu território, às coisas que nele se encontram e aos fatos que aí ocorrem” (ROUSSEAU, Charles. *Principes généraux du droit international public*. Paris: Pédone, 1958. v. I. p. 370. Tradução livre).

²⁵⁹ “O fenômeno da transnacionalidade, nos dizeres de Marcos Leite Garcia, dá-se a partir das chamadas demandas transnacionais, que por sua vez estão relacionadas com a questão da efetividade dos chamados direitos difusos e transfronteiriços. Desta maneira, as demandas transnacionais são questões fundamentais para o ser humano e que vem sendo classificadas pela doutrina como ‘novos direitos’” (FERNANDES, Rodrigo; SANTOS, Rafael Padilha dos. Transnacionalidade e os novos rumos do Estado e do Direito. *Revista Eletrônica Direito e Política*, Itajaí, v. 9, n. 1, 1º quadrimestre 2014. p. 648).

²⁶⁰ Segundo Joana Stelzer, transnacionalidade pode ser definido como: “o fenômeno da transnacionalização representa o novo contexto mundial, surgido principalmente a partir da intensificação das operações de natureza econômico-comercial no período de pós-guerra, caracterizado especialmente – pela desterritorialização, expansão capitalista, enfraquecimento da soberania e emergência de ordenamento jurídico gerado à margem do monopólio estatal” (STELZER, Joana. O fenômeno da transnacionalização da dimensão jurídica. In: CRUZ, Paulo Márcio; STELZER, Joana (org.). *Direito e transnacionalidade*. Curitiba: Juruá, 2009. p. 15-54. p. 16).

²⁶¹ Há 55 (cinquenta e cinco) países que aderiram à Convenção (Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=1bxwWyOt. Acesso em: 26 abril 2021).

²⁶² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 197.

Retornando os fatos, no julgamento o Tribunal averiguou que todas os residentes do território da União que pretendem utilizar o Facebook são obrigados, no momento da sua inscrição, a celebrar um contrato com a *Facebook Ireland*.²⁶³ Assim, os dados pessoais dos usuários do *Facebook*, residentes no território da União são transferidos para servidores pertencentes à *Facebook Inc.* (matriz da empresa), todos eles situados em território dos Estados Unidos, onde são objeto de tratamento.²⁶⁴ Constatando esses fatos, em 25 de junho de 2013, M. Schrems apresentou ao *Commissioner* uma queixa em que pedia que fosse determinada a proibição da *Facebook Ireland* de transferir os seus dados pessoais para os Estados Unidos. Alegava que o direito e as práticas em vigor neste país não asseguravam uma proteção suficiente dos dados pessoais conservados no seu território, sobretudo em razão da realização de atividades de vigilância (*surveillance*) pelas autoridades norte-americanas.²⁶⁵

Referindo-se à precedentes do Tribunal, o autor afirma que a Diretiva 95/46/CE foi redigida com o objetivo de salvaguardar a privacidade dos habitantes da União Europeia e de harmonizar diferentes legislações de privacidade aos Estados-Membros.²⁶⁶ Nesse mesmo sentido, o Tribunal salientou que, para garantir a proteção acima indicada, as autoridades de controle deveriam assegurar o equilíbrio entre o respeito do direito à vida privada e os interesses que regem a livre circulação de dados pessoais.²⁶⁷ Com essas premissas, o Tribunal constatou que os dados dos cidadãos europeus não estavam suficientemente protegidos nos Estados Unidos e invalidou a decisão que criou o acordo.²⁶⁸

O ponto sensível sobre esta anulação é que o Tribunal entendeu que, apesar da existência de Acordo, as autoridades nacionais de controle e proteção de dados poderiam examinar, com total independência, se a transferência desses dados respeita as exigências estabelecidas pela referida Diretiva. Isso porque, diz o Tribunal, essas autoridades são os órgãos perante os quais um cidadão pode apresentar pedido relativo à proteção dos seus

²⁶³ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015. Parágrafo 27.

²⁶⁴ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015. Parágrafo 27.

²⁶⁵ Neste ponto, o argumento do autor aborda as revelações feitas por Edward Snowden sobre as atividades dos serviços de vigilância dos Estados Unidos da América, nomeadamente as da National Security Agency. A esse respeito, ver: POSCHER, Ralf. The right to data protection. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 129-142.

²⁶⁶ Como exemplo dos precedentes citados, podemos indicar o caso acima discutido, qual seja, Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

²⁶⁷ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 189.

²⁶⁸ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015. Parágrafo 106.

direitos e liberdades.²⁶⁹ Com isso, a declaração da invalidade do Acordo não obsta que uma autoridade nacional examine o pedido relativo à proteção de dados pessoais que foram transferidos de um Estado-Membro para o país terceiro. Enfim, o julgamento termina por manter as operações de transferência internacional de dados e, ao mesmo tempo, assegura o direito de o titular contestar essa operação perante as autoridades nacionais.

Para chegar a essa conclusão, o Tribunal considerou que, mesmo que as empresas americanas envolvidas estivessem tomando medidas de proteção adequadas, as autoridades públicas dos Estados Unidos da América não estão sujeitas às diretrizes de *Safe Harbor*. Portanto, os dados pessoais e a privacidade dos cidadãos europeus estavam em risco, tendo em vista a constante vigilância do governo dos Estados Unidos da América.²⁷⁰ Sobre isso, o Tribunal afirma que o Acordo não continha nenhuma referência à normas ou regras dos Estados Unidos da América destinadas a limitar ingerências nos direitos fundamentais das pessoas cujos dados fossem transferidos. Salientou, inclusive, que as ações de vigilância tornariam possível o acesso aos dados pessoais pelo governo dos Estados Unidos, que, com fulcro na proteção da segurança nacional, ainda poderia conferir aos dados coletados finalidades diversas daquela que fundamentou a sua transferência.²⁷¹ Finalmente, o Tribunal afirma que os titulares dos dados pessoais não dispunham de vias administrativas ou judiciais nos EUA que lhes permitissem acessar os dados que lhes dizem respeito, o que afasta qualquer possibilidade de retificação ou supressão de dados coletados.

Como resultado, o Acordo que permita às autoridades públicas acesso, de modo generalizado, ao conteúdo das comunicações eletrônicas foi considerado lesivo do conteúdo essencial do direito ao respeito da vida privada, tal como é garantido pelo artigo 7º da Carta. Fora isso, a falta de regulamentação do acesso do titular aos dados foi considerada como uma ofensa ao artigo 8º da Carta. Neste ponto, o Tribunal destaca que o direito à proteção de dados pessoais é uma ferramenta voltada a salvaguardar o sigilo e o direito à privacidade. Deste modo, o Tribunal conferiu eficácia direta aos direitos à privacidade e à proteção de dados pessoais, incumbindo, não só aos Estados-Membros, mas também à União Europeia o dever de criar normas com eficácia interna e externa para que, assim, os objetivos da segurança e da transparência das informações pessoais dos titulares sejam devidamente aplicados.

²⁶⁹ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015. Parágrafo 65.

²⁷⁰ Como exemplo dos precedentes citados, podemos indicar o caso acima discutido, qual seja, Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014.

²⁷¹ Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015. Parágrafo 90.

2.2.2.5 *Tele2 (Netherlands) BV e o. v. Autoriteit Consument en Markt (ACM)*

Em março de 2017, o Tribunal decidiu o Caso C-536/15 (*Tele2 – Netherlands – BV e o. v. Autoriteit Consument en Markt – ACM*).²⁷² A questão analisada dizia respeito ao pedido de empresa belga (*Tele2*) que prestava serviços de informações telefônicas e, para isso, criava listas telefônicas acessíveis a partir do território belga. A empresa havia solicitado às empresas que atribuem números de telefone a assinantes nos Países Baixos que lhe disponibilizassem os dados relativos de seus assinantes. Com a recusa deste pedido, a *Tele2* submeteu pedido revisão judicial.²⁷³ O pedido invocava uma obrigação de compartilhamento, fundada nos termos do Diretiva de Serviço Universal (Diretiva 2002/22/CE), que exigia das empresas que atribuem números telefônicos aos titulares a obrigação de disponibilizassem esses dados a quem os solicitar, caso os assinantes consentam em publicá-los.²⁷⁴ Ocorre que as empresas holandesas se recusaram a realizar essa transferência de dados, afirmando que eles não eram obrigados a fornecer essas informações a uma empresa estabelecida em outro Estado-Membro.²⁷⁵

Confrontado com essa questão, o Tribunal considerou que a Diretiva de Serviço Universal abrange todos os pedidos, independentemente do Estado-Membro em que estão estabelecidos. Indicou, ainda, que a Diretiva impunha que a disponibilização de informações seja feita em condições não discriminatórias, sem que exista qualquer proibição de transferência de dados para outro Estado-Membro.²⁷⁶ A decisão afirma também que a Diretiva tinha como objetivo garantir serviços de boa qualidade e acessíveis ao público, através da concorrência e da possibilidade de escolha efetivas, objetivo que é refletido na denominação da Diretiva.²⁷⁷ Sendo assim, a transmissão de dados para empresa sediada em outro Estado-Membro, que pretendia publicar e disponibilizar a lista, não necessita do consentimento explícito que informe para qual país os dados serão transmitidos. Basta o simples

²⁷² Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017.

²⁷³ Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017. Parágrafo 15.

²⁷⁴ Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017. Parágrafo 7.

²⁷⁵ Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017. Parágrafo 29.

²⁷⁶ Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017. Parágrafo 30.

²⁷⁷ Como precedente utilizado para esta fundamentação, utilizou-se do julgado relativo Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011.

consentimento de que poderá haver sua publicação, com fulcro no princípio da não-discriminação.²⁷⁸

Isso significa que o direito à proteção de dados pessoais determina que o titular dos dados autorize o consentimento prévio para publicação dos dados. Contudo, não é necessário que o consentimento seja fornecido para cada Estado-Membro em que o dado será transferido, uma vez que as Diretivas da União garantem a segurança e transparência para todos os Estados-Membros, desde que haja similitude de condições e garantias aos titulares dos dados.²⁷⁹ Este julgamento reforça a ideia da União entre todos os Estados-Membros no objetivo de uniformizar as regras de tratamento e proteção de dados pessoais. Sua conclusão diz que a transferência interna (entre países membros) deve conter regras básicas, que em nenhuma hipótese devem impedir as negociações realizadas no mercado interno europeu. Com isso, o julgamento tem o intuito de reforçar o papel do mercado único.²⁸⁰

De fato, não há razão que justifique uma diferença de tratamento consoante o operador que esteja estabelecido no território nacional de cada Estado-Membro. A partir do momento em que esse agente realize o tratamento dados pessoais para fins idênticos àqueles para que foram coletados, com fulcro no princípio da livre prestação de serviços (garantido no artigo 56, do Tratado de Funcionamento), não há vício da operação de tratamento, independente de onde (em qual país do bloco europeu) o operador mantenha sua sede.²⁸¹ Essa é uma garantia inerente à plena realização do mercado comum (artigo 25 da Diretiva) e, por isso mesmo, o legislador da União indica sua intenção de possibilitar o serviço de informações telefônicas de forma transfronteiriça.²⁸² Há, portanto, uma clara ligação dos aspectos fundamentais da

²⁷⁸ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

²⁷⁹ Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017. Parágrafo 35.

²⁸⁰ TRIBUNAL de Justiça da União Europeia. *Press Release n° 31/17*. Luxemburgo, 2017. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170031en.pdf>. Acesso em: 11 jan. 2021.

²⁸¹ “Art. 56. No âmbito das disposições seguintes, as restrições à livre prestação de serviços na União serão proibidas em relação aos nacionais dos Estados-Membros estabelecidos num Estado-Membro que não seja o do destinatário da prestação”.

²⁸² De acordo com este disposto: “(25) Os mercados das comunicações continuam a evoluir em termos dos serviços utilizados e dos meios técnicos empregues para os fornecer aos utilizadores. As obrigações de serviço universal, que se encontram definidas a nível comunitário, devem ser revistas periodicamente com vista à apresentação de propostas de alteração ou à redefinição do seu âmbito. Essa revisão deve ter em conta a evolução das condições sociais, comerciais e tecnológicas e o facto de qualquer alteração do âmbito dessas obrigações dever estar sujeita à dupla prova dos serviços que passam a estar disponíveis para uma maioria substancial da população, com o risco consequente de exclusão social para aqueles que não os podem pagar. Ao introduzir qualquer alteração no âmbito das obrigações de serviço universal devem tomar-se precauções para garantir que determinadas opções tecnológicas não sejam artificialmente promovidas em desfavor de outras, que não seja imposto um encargo financeiro desproporcionado às empresas do sector (pondo assim em perigo a evolução do mercado e a inovação) e que os consumidores ou utilizadores com

criação da União Europeia – mercado comum – com o respeito às regras relativas à privacidade e proteção de dados pessoais – consentimento.²⁸³ É justamente por isso as regras da União analisadas neste julgamento respeitaram a regra básica de transparência junto ao titular dos dados privados, com a possibilidade de as empresas proporcionarem seus serviços de forma comum a todos os países da União.

2.2.2.6 *Ministério Fiscal*

No julgamento do Caso C-207/16 (*Ministério Fiscal*), o Tribunal proferiu decisão sobre acesso a dados retidos por provedores de serviços de comunicações eletrônicas, no âmbito da Diretiva e-Privacy.²⁸⁴ Mais uma vez, trata-se de caso de importância para o tema da proteção de dados, tendo em vista, principalmente, a consolidação do entendimento a respeito da aplicação da Diretiva e-Privacy. O caso trata da atividade de investigação criminal. Ao investigar o roubo de um telefone celular, a polícia espanhola requisitou que o juiz nacional ordenasse a provedores de serviços de comunicações eletrônicas que divulgassem os números de telefone que foram ativados durante um período de doze dias com o *International Mobile Equipment Identity* (IMEI) do dispositivo móvel roubado, bem como que fossem identificados os nomes e endereços dos assinantes usados para esta ativação.²⁸⁵

O pedido foi negado pelo magistrado nacional, que decidiu com base no fato de que o crime não cumpria os requisitos da lei nacional sobre retenção de dados relativos às comunicações eletrônicas e redes de comunicação pública. Em sede de recurso, o Tribunal de justiça espanhol remeteu o caso ao Tribunal de Justiça da União Europeia. Em sua decisão, o Tribunal da União identificou que o acesso aos dados retidos, com o objetivo de encontrar os proprietários de um dispositivo móvel, implicaria uma interferência nos direitos fundamentais dos proprietários à privacidade e à proteção de dados pessoais.²⁸⁶ No entanto, esclareceu que se o objetivo do acesso é apenas obter a identidade do assinante, a Diretiva 2002/58/CE

baixos rendimentos não sejam injustamente sobrecarregados do ponto de vista financeiro. Qualquer alteração do âmbito das obrigações significa automaticamente que qualquer custo líquido pode ser financiado pelos métodos permitidos pela presente directiva. Os Estados-Membros não estão autorizados a impor aos agentes do mercado contribuições financeiras relativas a medidas que não façam parte das obrigações de serviço universal. Cada Estado-Membro continua a ser livre de impor medidas especiais (fora do âmbito das obrigações de serviço universal) e de financiá-las em conformidade com o direito comunitário, mas não através de contribuições dos agentes do mercado”.

²⁸³ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

²⁸⁴ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018.

²⁸⁵ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018. Parágrafo 20.

²⁸⁶ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018. Parágrafo 48.

permitia restrições aos direitos previstos para prevenção, investigação, detecção e repressão de crimes – não apenas crimes graves.²⁸⁷

Essa decisão destoa dos precedentes do Tribunal, que já havia entendido que o acesso a dados pessoais retidos se limitava aos casos que envolvam crimes graves.²⁸⁸ Para conciliar esses posicionamentos, o Tribunal afirma que, na avaliação da interferência do direito fundamental, o objetivo prosseguido pelo acesso deveria ser proporcional à seriedade da interferência no conteúdo do direito.²⁸⁹ Por outro lado, se o acesso aos dados representasse uma interferência menos onerosa no direito, como ocorre no presente caso, a transferência poderia ser justificada com base no objetivo de combater ofensas criminais em geral.²⁹⁰

No entanto, a decisão do Tribunal confirmou que o acesso aos dados retidos que revelem a data, hora, duração e destinatários das comunicações ou os locais onde as comunicações ocorreram, deve ser considerado uma interferência séria no conteúdo do direito, pois esses dados permitem inferir conclusões precisas sobre a vida privada das pessoas. Nessas situações, o acesso aos dados retidos deve ser limitado a casos que envolvam crimes graves.²⁹¹ Contudo, vale frisar que o julgado não definiu o que pode constituir um “crime grave”, o que gera insegurança quanto aos seus efeitos. Da mesma forma, a decisão não esclarece se a finalidade da coleta inicial dos dados deve afetar as condições de acesso aos dados retidos, o que dificulta a análise fática do caso e suas consequências.²⁹²

No que diz respeito à interpretação da Diretiva e-Privacy, ao se referir ao direito à proteção de dados, o julgado identificou que os dados de tráfego incluem o nome do assinante e o endereço IMEI do dispositivo móvel, o que significa que o acesso a esses dados se enquadra no escopo e nas salvaguardas da Diretiva, abrangendo os tipos de dados pessoais abarcados pela legislação da União.²⁹³ Em contexto mais amplo, a discussão de fundo do julgado trata da relação tensa entre segurança e liberdades, que sempre existirá

²⁸⁷ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018. Parágrafo 52.

²⁸⁸ O precedente utilizado pelo Tribunal é relativo ao julgado do Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016.

²⁸⁹ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018. Parágrafo 56.

²⁹⁰ HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010. p. 206.

²⁹¹ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018. Parágrafo 60.

²⁹² HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010. p. 207.

²⁹³ HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010. p. 207.

quando medidas investigatórias infringirem direitos humanos, como privacidade ou liberdade de expressão.²⁹⁴

A esse respeito, o julgamento reitera que os artigos 7º e 8º, da Carta incidem em conflitos envolvendo a segurança pública, quer a interferência estatal seja considerada séria ou não.

Com base neste pressuposto, o Tribunal exige condições e requisitos substantivos, que devem ser baseados em critérios objetivos, para se autorizar o acesso aos dados retidos por operadoras de serviços de telecomunicação. Diz inclusive que esse acesso deve estar sujeito a revisão prévia de tribunal ou órgão administrativo independente. Deste modo, podemos verificar que o Tribunal tem mantido e desenvolvido sua abordagem ampla para o escopo da proteção dos direitos fundamentais garantidos ao abrigo da Carta e da Diretiva e-Privacy em dois importantes aspectos: (i) o amplo escopo dos tipos de dados pessoais protegidos, e (ii) o escopo material do quadro de proteção de dados pessoais da União.²⁹⁵

2.2.2.7 *Digital Rights Ireland Ltd v. Comissão Europeia*

No Recurso T-670/16 (*Digital Rights Ireland Ltd v. Comissão Europeia*), o Tribunal teve de se debruçar sobre os requisitos intrínsecos ao direito à proteção de dados pessoais, analisando a sua extensão e aplicação para a proteção de pessoas jurídicas.²⁹⁶ A controvérsia inicia em outubro de 2015, quando o Tribunal declarou inválida a Decisão 2000/520/CE, que trata da adequação da proteção oferecida pelos princípios de privacidade do (*Safe Harbor*).²⁹⁷ Após essa decisão, a Comissão Europeia iniciou negociações com os Estados Unidos da América, com vistas a fortalecer a proteção dos dados pessoais transferidos da União Europeia. Tendo analisado e examinado as questões técnicas ligadas ao tema, a Comissão Europeia aprovou a Decisão de Execução UE 2016/1250, relativa à adequação da proteção fornecida pelo Escudo de Privacidade UE-EUA. Nela se concluiu que os Estados Unidos da América asseguravam um nível adequado de proteção para transferência de dados pessoais da União Europeia para organizações sediadas nos Estados Unidos.²⁹⁸ O objetivo direto desta

²⁹⁴ WEINRIB, Lorena E. The Supreme Court of Canada and section one of the charter. *Supreme Court Law Review*, v. 10, p. 469-513, 1986.

²⁹⁵ HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010. p. 207.

²⁹⁶ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017.

²⁹⁷ Para maiores informações sobre o caso, verificar as questões indicadas no Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015.

²⁹⁸ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 5.

Decisão era autorizar a transferência para os Estados Unidos de dados pessoais em processamento ou destinados a serem processados para organizações com sede neste país.

Em setembro de 2016, a recorrente, *Digital Rights Ireland*, interpôs recurso para ser invalidada a Decisão de Execução/UE 2016/1250. A *Digital Rights Ireland* é uma empresa sem fins lucrativos que tem como objeto essencial a defesa das liberdades individuais na internet. Ao analisar a possibilidade de a *Digital Rights Ireland* interpor este recurso, o Tribunal expôs o requisito básico da proteção de dados pessoais no direito europeu.

A Diretiva 95/46/CE, que regulava a matéria até a entrada em vigor da GDPR, previa a incidência do direito à proteção de dados pessoais apenas para pessoas físicas.²⁹⁹ Deste modo, as entidades coletivas só poderiam reivindicar a proteção de dados de indivíduos, na medida em que a razão social da entidade identificasse uma ou mais pessoas físicas como titulares dos dados processados indevidamente. No caso, isso não ocorreu.³⁰⁰ Procurando afastar essa dificuldade, a recorrente alegou que o Acordo afetava a sua situação de controladora dos dados pessoais. Isso porque, ao coletar dados pessoais e transmiti-los por correio eletrônico, a entidade atuaria como responsável pelo tratamento desses dados.³⁰¹

Em sua decisão, o Tribunal indicou que o Acordo de transferência em questão (também denominado como *Privacy Shield*) se aplicava às organizações americanas, independentemente de atuarem como encarregadas ou como processadoras de dados pessoais. Concluiu, assim, que o Escudo não afeta a aplicação da legislação da União que rege o tratamento de dados pessoais nos Estados-Membros.³⁰² Como consequência, essa decisão teve o efeito de permitir a realização de transferências em determinadas condições e não restringe os direitos nem impõe obrigações a quem se encontra na União.³⁰³

Alegou-se ainda que existiria o risco de a utilização de serviços de comunicações eletrônicas para processar os dados resultar na sua transferência de dados para os Estados Unidos por um prestador desses serviços, o que seria uma ilegal que compromete a sua obrigação do encarregado perante o Direito da União. Contudo, o Tribunal indicou que a execução do Acordo não resultaria necessariamente em tal violação das obrigações do

²⁹⁹ VAN DROOGHENBROECK, Sébastien; PICOD, Fabrice; RIZCALLAH, Cécilia. *Charte des droits fondamentaux de l'Union européenne*. Commentaire article par article. 2. ed. Bruxelles: Bruylant, 2019.

³⁰⁰ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 25.

³⁰¹ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 30.

³⁰² Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 34.

³⁰³ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 37.

encarregado, uma vez que as regras atinentes a este *Privacy Shield* não são colidentes com as regras internas. Assim, a anulação deste acordo seria igualmente incapaz de obter vantagens a esse respeito.³⁰⁴ Neste sentido, o Tribunal entendeu que a recorrente não detinha interesse em agir e não poderia ter requerido a anulação do Acordo em questão.

Por fim, o Tribunal teve de analisar se a *Digital Rights Ireland* poderia ter interposto este recurso em nome de seus membros, apoiadores e do público em geral.³⁰⁵ A este respeito, a recorrente alegou representar os interesses dos seus membros e apoiadores e que também atuava no interesse público, pois sua demanda foi elaborada com base em disposições do direito da União que abriram a possibilidade de interpor uma ação popular para o interesse público.³⁰⁶ Quanto a este aspecto foi decidido que pessoas jurídicas podem representar os interesses de pessoas que dela fazem parte, como em uma associação. Isso ocorre principalmente quando a posição de “negociador” da pessoa jurídica for afetada pela determinação normativa cuja anulação é solicitada, ou quando uma disposição legal lhes concede expressamente os poderes de impetrar processo.³⁰⁷

No entanto, o Tribunal observou que não foi demonstrada a autorização dos membros da recorrente para a distribuição da ação judicial destinada a proteger os seus dados pessoais. Novamente, isso afastou a legitimidade da recorrente.³⁰⁸ Além disso, entendeu-se que a participação da recorrente em processos judiciais não permite inferir a sua posição de “negociadora”. No entender do Tribunal, essa participação só pode ser admitida quando a entidade tiver relação direta com a lide, ou seja, a pessoa jurídica deve estar intrinsecamente ligada ao prejuízo, ou ganho, daquela discussão, para ter a sua participação admitida no processo.³⁰⁹ Por conseguinte, a recorrente não detinha legitimidade para agir em nome dos seus membros ou em nome do público em geral. Por isso o processo extinto, sem análise do mérito.

Além de o Tribunal estabelecer regras para que pessoas físicas ou pessoas jurídicas possam buscar análise de eventuais divergências sobre o direito à proteção de dados pessoais frente

³⁰⁴ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 42.

³⁰⁵ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 45.

³⁰⁶ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 47.

³⁰⁷ Como precedente, o Tribunal indicou o Processo T-670/14. *Milchindustrie-Verband eV e Deutscher Raiffeisenverband eV v. European Commission*. Julgamento em: 23 novembro 2015.

³⁰⁸ VAN DROOGHENBROECK, Sébastien; PICOD, Fabrice; RIZCALLAH, Cécilia. *Charte des droits fondamentaux de l'Union européenne*. Commentaire article par article. 2. ed. Bruxelles: Bruylant, 2019.

³⁰⁹ Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017. Parágrafo 49.

aos tribunais, o precedente indica que, na compreensão desta Corte, pessoas jurídicas não são titulares do direito à proteção de dados pessoais.

2.2.3 Privacidade e direito ao esquecimento

2.2.3.1 Google Spain SL v. Agencia Española de Protección de Datos

Interpretando os artigos 7º e 8º da Carta Europeia, no Caso C-131/12 (*Google Spain SL v. Agencia Española de Protección de Datos – AEPD* 2014), o Tribunal decidiu um dos casos mais conhecidos e debatidos na literatura jurídica mundial. A Agência espanhola de proteção de dados havia determinado que o *Google* deveria excluir uma lista de links que levavam o usuário da ferramenta de busca para um anúncio do Jornal *La Vanguardia*, meio de comunicação digital que havia veiculado os processos fiscais de penhora e buscas de bens realizados contra o Mario Corteza González. Esta desvinculação deveria ocorrer mesmo que o site da publicação eletrônica seja mantido.³¹⁰

Os detalhes do caso são conhecidos. O requerente em âmbito nacional (Mario Corteza González) teve contra ele proposta ação fiscal e seus bens foram sujeitos a leilão imobiliário para a recuperação de suas dívidas. Os anúncios do leilão foram publicados em jornal de grande circulação no país (*La Vanguardia*), que publicou a notícia em sua versão eletrônica. Assim, ao inserir o nome e sobrenome do requerente, a pesquisa realizada no mecanismo de busca do *Google* reproduzia essa informação e indicava o link para o site do jornal no topo de sua lista de resultados. Isso mesmo tendo passado 16 anos do fato.

O Tribunal foi instigado a decidir, analisando a situação com base no direito da União. Sua decisão considerou que as páginas do Jornal *La Vanguardia* continham dados pessoais, os quais, de acordo com a Diretiva 95/46/CE, são definidos como quaisquer informações relativas a uma pessoa identificada ou identificável. O *Google* foi considerado como encarregado dos dados ao incluir as páginas do *La Vanguardia* na lista de resultados de pesquisa.³¹¹ Deste modo e considerando que a Diretiva definia o encarregado como o agente responsável pelo tratamento, o *Google* foi identificado como “co-controlador” de dados pessoais em questão.

³¹⁰ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

³¹¹ MASING, Johannes. Assessing the CJEU’s “Google Decision”. A tentative first approach. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 435-456.

A decisão foi elaborada com base nos artigos 7º e 8º, da Carta Europeia e tratou dos seguintes pontos.³¹² Avaliando o âmbito territorial das normas de proteção de dados europeias, o Tribunal afirma que o objetivo da Diretiva impedia uma restrição na interpretação de suas disposições. Concluiu, assim, que o âmbito territorial da Diretiva se aplicava ao *Google*, pois, mesmo com sede em país terceiro, a empresa possuía um estabelecimento em Estado-Membro.³¹³ O Tribunal considerou ainda que o direito de remover certas informações do resultado pesquisa decorria da Diretiva, seja porque essa informação poderia prejudicial o titular dos dados, ou porque o titular simplesmente desejava que ser esquecido.³¹⁴ A decisão afirma ainda que parecia não haver interesse público nas informações divulgadas no site, do que se conclui que o requerente tem o direito de ter a informação excluída do resultado da busca. Não obstante, a decisão indica que cabe ao órgão jurisdicional nacional decidir a respeito da incidência definitiva deste “direito a ser esquecido” no caso em exame.³¹⁵

A dificuldade da decisão está na situação de tensão entre o direito à liberdade de expressão e a proteção de dados. Sobre esse tema, com fulcro nas conclusões do advogado-geral *Jääskinen*, o Tribunal argumenta que o escopo de aplicação das regras da União em matéria de proteção de dados é amplo e genérico. Na compreensão do Tribunal, o direito à proteção de dados afeta toda e qualquer comunicação humana, sobretudo aquelas divulgadas em meios eletrônicos.³¹⁶ A esse respeito, a Diretiva de Proteção de Dados busca equilibrar a proteção de dados e a liberdade de expressão. Prevê, por exemplo, uma exceção para dados que são processados para “fins jornalísticos ou expressão artística e literária, se necessário para conciliar o direito à privacidade com as regras que regem a liberdade de expressão”.³¹⁷ Mas o Tribunal afirmou que um operador de mecanismo de pesquisa não pode contar com a exceção da Diretiva para o processamento de dados com finalidade jornalística.³¹⁸

³¹² MASING, Johannes. Assessing the CJEU’s “Google Decision”. A tentative first approach. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 435-456.

³¹³ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014. Parágrafo 46.

³¹⁴ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014. Parágrafo 74.

³¹⁵ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014. Parágrafo 76.

³¹⁶ POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

³¹⁷ Ver artigo 9º, Diretiva de Proteção de Dados. Ver também o artigo 85, do Regulamento Geral de Proteção de Dados.

³¹⁸ A versão em inglês do julgamento diz que o Google “não parece” ser capaz de se beneficiar de a exceção da mídia. No entanto, no idioma autêntico do julgamento, espanhol, o TJ-UE diz que o Google não pode beneficiar-se da exceção da mídia. (ERDROS, David. *From the scylla of restriction to the charybdis of*

Um dos pressupostos desta conclusão está na identificação da proteção de dados pessoais com a autodeterminação informacional. Disso decorre que, embora o termo não seja mencionado explicitamente na Carta, é de significado central para o artigo 8º. O direito à proteção de dados pessoais abrange, por isso, os direitos dos titulares de dados de acessar dados e retificá-los, além de estabelecer a necessidade de consentimento com o processamento.³¹⁹ Esses direitos ajudam os indivíduos a acompanhar como seus dados são processados e também os capacita com um certo grau de tomada de decisão sobre esse processamento.³²⁰ Assim, quem publica uma questão relativa à vida privada está sujeito à responsabilidade por invasão da privacidade. Isso ocorre se o assunto divulgado ofender a honra da pessoa e não for uma preocupação legítima para o público.³²¹ Considerando que os motores de busca são, assim, capazes de divulgar informações detalhadas e estruturadas sobre os titulares dos dados,³²² assim como as consequências do conceito de autodeterminação informacional,³²³ a conclusão a que chega o Tribunal é a importância do tratamento justo de dados pessoais e sua junção, ao menos parcial, com o direito à vida privada.

Fora isso, esse o julgamento é um precedente importante sobre a responsabilidade corporativa por interferir em direitos fundamentais.³²⁴ Nele se registra que, em caso de um conflito entre direitos fundamentais, corporações devem assumir a responsabilidade pela divulgação de notícias ou fatos que degradem, humilhem ou afetem indivíduos.³²⁵ Cabe a elas o dever de criar sistemas de prevenção dessas consequências. Por outro lado, o fato de o Tribunal responsabilizar o *Google* pela difusão de informações que perdeu importância e notoriedade, mas permitir que o jornal mantinha as mesmas informações em seu próprio site, dificulta em muito a análise do caso.³²⁶ Afinal, se a proteção de dados e o

license? exploring the present and future scope of the ‘special purposes’ freedom of expression shield in european data protection. Cambridge: Faculty of Law Research Paper, 2015. v. 20. p. 119-154. p. 120).

³¹⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

³²⁰ POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

³²¹ POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

³²² MASING, Johannes. Assessing the CJEU’s “Google Decision”. A tentative first approach. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 435-456.

³²³ LYNKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

³²⁴ POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

³²⁵ WERRO, Franz. The right to be forgotten: the general report – Congress of the International Society of Comparative Law. Fukuoka, July 2018. In: WERRO, Franz (org.). *The right to be forgotten. A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2018. p. 1-35. p. 11.

³²⁶ POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

autodesenvolvimento informacional da personalidade são realmente direitos fundamentais, como afirma o Tribunal, não tem sentido afirmar que somente o *Google* deve ser responsabilizado pela lesão desses direitos. Direitos fundamentais valem contra todos, não só contra grandes empresas. Mas, de fato, uma vez que se atribua efeitos gerais à conclusão desta decisão, as consequências serão catastróficas em relação à liberdade de expressão: nenhum fato ou notícia que indique um dado pessoal será passível de publicação sem a autorização do titular.

Fato é que, após o julgamento do caso, o *Google* criou um formulário online que permite que as pessoas solicitem a remoção de resultados específicos para pesquisas em seu nome.³²⁷ Realizada tal solicitação, o *Google* irá “equilibrar os direitos de privacidade do indivíduo com o interesse público de saber e o direito para distribuir informações”.³²⁸ Ou seja, o resultado prático da decisão é transferir ao *Google* o controle sobre o equilíbrio de direitos e o poder de determinar, em última instância, se notícias ou afirmações têm relevância para o público.

Atualmente, o art. 17 do Regulamento Europeu de proteção de dados trata deste direito “ao esquecimento”, mais corretamente denominado de “direito de apagar” ou referido como o “direito para desreferenciar”.³²⁹ Com isso, o titular dos dados pode solicitar que um mecanismo de pesquisa remova (desreferenciar) dos resultados da pesquisa que levam a sites que contêm dados pessoais, quando, por exemplo, os dados são inadequados, irrelevantes ou não são mais relevante, à luz dos fins para os quais foram coletados e processados.³³⁰ Contudo, mesmo que as informações sejam desreferenciadas da pesquisa, elas ainda estarão visíveis na página da web foram publicadas inicialmente.³³¹

É interessante notar que o Tribunal não faz referência ao artigo 11, da Carta, e descreveu o acesso à informação pelos utilizadores da Internet como um “interesse” e não um “direito”.³³² Esta classificação abre caminho para a conclusão do Tribunal de que o direito do

³²⁷ GOOGLE. *Removing Content from Google*, Google. Disponível em: <https://developers.google.com/search/docs/advanced/crawling/remove-information>. Acesso em: 26 mar. 2021.

³²⁸ GOOGLE. *Search removal request under data protection law in Europe*. Disponível em: https://support.google.com/legal/contact/lr_eudpa?product=websearch. Acesso em: 26 mar. 2021.

³²⁹ IGLEZAKIS, Ioannis. *The right to be forgotten in the Google Spain Case (Case C-131/12): a clear victory for data protection or an obstacle for the internet?*. Aristotle University of Thessaloniki-Law, Economic and Political Sciences, 2014.

³³⁰ POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

³³¹ POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

³³² Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014. Parágrafo 51.

titular dos dados à privacidade e à proteção de dados se sobrepõe o interesse dos internautas em ter acesso à informação.³³³ O Tribunal, no entanto, condicionou esta conclusão às circunstâncias do caso, pois acrescenta que o equilíbrio entre esses direitos pode “depende, em determinados casos particulares, da natureza da informação em questão e da sua sensibilidade para a vida privada da pessoa em causa, bem como do interesse do público em dispor dessa informação”.³³⁴

2.2.3.2 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*

No julgamento do Caso C-398/15 (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), o Tribunal tratou dos aspectos relacionados à proteção de dados pessoais com vínculo à exclusão de dados e à autodeterminação informacional.³³⁵ Em âmbito nacional, o autor (*Salvatore Manni*) argumentou que as informações a seu respeito disponibilizadas na internet prejudicavam sua reputação e causaram prejuízos aos seus negócios, requisitando a eliminação de tais dados.³³⁶ Seu objetivo era que as informações sobre ele fossem removidas do registro de empresas na Itália. As informações diziam respeito ao período que ele foi diretor e administrador de uma empresa que ficou insolvente e posteriormente liquidada.³³⁷ Não obstante o argumento de propósito público que justificaria o tratamento permanente de dados pessoais, o Tribunal local reconheceu a relevância do direito de exclusão de dados como um instrumento fundamental para proteger a identidade pessoal.³³⁸

Como consequência, afirmou que esse direito precisava ser equilibrado com a necessidade de garantir segurança jurídica, por meio das informações publicadas no registro das empresas.³³⁹

³³³ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 148.

³³⁴ Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014. Parágrafo 81.

³³⁵ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017.

³³⁶ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 26.

³³⁷ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 25.

³³⁸ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 28.

³³⁹ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 29.

Ao enfrentar essa questão, o Supremo Tribunal italiano solicitou ao Tribunal da União que informasse se, na ausência de uma regra explícita, a proteção de dados pessoais concedia ao titular dos dados o direito de obter o cancelamento ou o anonimato de seus dados publicados nas empresas após um certo período. Fundamentou-se o pedido de reenvio na Diretiva 95/46, ao indicar que o processamento de dados, principalmente quando afeta o direito ao respeito pela vida privada, deveria ser avaliado em relação à Carta dos Direitos Fundamentais.³⁴⁰

Em sua decisão, o Tribunal concluiu que havia interesse público em disponibilizar informações a terceiros sobre a constituição de empresas e os poderes das pessoas autorizadas a representá-las. No entanto, a decisão confirma que pode haver situações específicas que justifiquem a limitação do acesso.³⁴¹ Porém, neste caso o Tribunal entendeu que as justificativas do autor para requerer a exclusão de seus dados pessoais não eram legítimas para que justificasse a exclusão do acesso aos dados públicos.³⁴²

Para chegar a essa conclusão, o Tribunal considerou que esta interpretação não resultava em uma interferência desproporcional nos direitos do indivíduo, cujos dados foram retidos. Isso porque: (i) o registro da empresa continha apenas uma quantidade restrita de dados pessoais; e (ii) os indivíduos que optarem por participar do comércio por meio de uma empresa de responsabilidade limitada deveriam ser obrigados a se identificar e indicar o seu papel dentro da empresa. Isso para proteger o interesse de terceiros.³⁴³ A decisão recorda, inclusive, que o Direito da União ou dos Estados-Membros poderiam impor restrições à exclusão de dados pessoais, na medida em que isso for necessário e proporcional à sociedade e para salvaguardar a segurança pública ou outros objetivos importantes de interesse público geral. No caso, havia interesse público na manutenção de registros públicos de interesse do público geral.³⁴⁴

Com base nesses argumentos, foi decidido que as normas nacionais podem conter autorizações para que as pessoas tenham o direito de solicitar tal limitação de acesso aos dados pessoais que lhes digam respeito. Mas este direito também pode ser negado, e neste

³⁴⁰ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 39.

³⁴¹ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 51.

³⁴² Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 50.

³⁴³ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 48.

³⁴⁴ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 61.

caso caberia à jurisdição nacional a avaliação da restrição do conteúdo do direito.³⁴⁵ Na prática, o Tribunal reconheceu a existência do direito à autodeterminação funcional, direito que a depender da situação pode gerar a exclusão de dados pessoais pelo seu titular.³⁴⁶

2.2.3.3 *GC e outros v. Commission nationale de l'informatique et des libertés – CNIL*

Os próximos dois casos podem ser lidos em conjunto, uma vez que foram julgados no mesmo dia pelo Tribunal e eles contêm matérias similares que auxiliam a compreensão do direito ao esquecimento no Direito da União. No julgamento do Caso C-136/17 (*GC e outros v. Commission nationale de l'informatique et des libertés – CNIL*), o Tribunal decidiu que o Direito da União protege o direito à privacidade no que diz respeito ao processamento de dados pessoais sensíveis. A decisão repete a conclusão de que este direito deve ser aplicado aos operadores de mecanismos de busca.³⁴⁷ A controvérsia teve início quando quatro cidadãos franceses apresentaram queixas perante a Autoridade Francesa de Proteção de Dados (CNIL, sigla em francês) nas quais requisitavam a exclusão de links exibidos no *Google*, após pesquisas de seus nomes. Estas informações incluíam dados sobre condenações penais, inquéritos judiciais e opiniões religiosas e políticas.³⁴⁸ Entre 2015 e 2016, a CNIL indeferiu os pedidos e os recorrentes interpuseram recurso ao *Conseil d'État* (Conselho de Estado) da França, que constatou que os pedidos suscitavam dúvidas interpretativas das Diretiva da União. O caso foi, então, submetido ao Tribunal de Justiça Europeu.³⁴⁹

A Corte da União considerou que o tratamento de dados pessoais pelos mecanismos de busca afetou, de forma significativa, os direitos de privacidade dos interessados.³⁵⁰ Por isso, os titulares poderiam solicitar a exclusão de seus dados pessoais e, ao avaliar esses requerimentos, os operadores dos mecanismos de busca precisariam encontrar um equilíbrio entre os direitos de privacidade dos titulares de dados e os direitos dos usuários da Internet

³⁴⁵ Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricultura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017. Parágrafo 61.

³⁴⁶ WERRO, Franz. The right to be forgotten: the general report – Congress of the International Society of Comparative Law. Fukuoka, July 2018. In: WERRO, Franz (org.). *The right to be forgotten*. A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia. Springer, 2018. p. 1-35.

³⁴⁷ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019.

³⁴⁸ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafos 24-28.

³⁴⁹ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 29.

³⁵⁰ PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502. p. 497.

potencialmente interessados nessas informações.³⁵¹ Para chegar a esta conclusão, argumentou-se que a Diretiva da União proibia o processamento de dados pessoais sem o consentimento do titular dos dados pessoais, salvo em casos com base no interesse público.³⁵²

Por outro lado, o julgamento considera que a atividade de um mecanismo de pesquisa que inclui informações em ambiente online, realiza a indexação automática desses dados, as armazena e disponibiliza aos usuários da Internet constitui “processamento de dados pessoais” na acepção da legislação europeia.³⁵³ Por isso, baseando no julgamento no caso *Google Spain*, o Tribunal reiterou que um mecanismo de pesquisa online deve ser considerado responsável pelo tratamento de dados pessoais que surjam nos resultados da busca.³⁵⁴ O Tribunal observou ainda que o processamento de dados pessoais pelos mecanismos de pesquisa desempenha papel decisivo na disseminação de dados e torna os sites mais acessíveis ao usuário da internet.³⁵⁵ Fora isso, os mecanismos de pesquisa permitem que seja criado um perfil detalhado do titular dos dados. Consequentemente, os mecanismos de pesquisa afetaram significativamente o direito fundamental à privacidade e, portanto, suas atividades se enquadravam no domínio da Diretiva da União.³⁵⁶

Finalmente, o Tribunal lembrou que a Comissão Europeia enfatizou que o operador de um mecanismo de busca é responsável pela exibição de *hiperlink* que conduza a uma lista de resultados exibida após a pesquisa do nome de uma pessoa. Isso ocorre quando tal resultado afetar significativamente a vida privada e a proteção dos dados pessoais.³⁵⁷ E como os mecanismos de busca foram considerados como controladores/encarregados de dados, o Tribunal avalia se o operador é obrigado a desassociar links para páginas da web que contenham determinadas categorias de dados pessoais.³⁵⁸ Para isso, observa que, de acordo com o artigo 17, da GDPR, o titular dos dados tem o direito de ser esquecido ou de obter do

³⁵¹ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey, PA: IGI Global, 2019.

³⁵² PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502.

³⁵³ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

³⁵⁴ Para maiores informações sobre o precedente, verificar o Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

³⁵⁵ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

³⁵⁶ PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502.

³⁵⁷ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 46.

³⁵⁸ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

responsável pelo tratamento a exclusão dos dados pessoais, sem demora injustificada.³⁵⁹ Os motivos para a exclusão de dados pessoais são: (i) os dados pessoais não são mais necessários em relação aos propósitos para os quais foram processados; (ii) o titular dos dados retira o consentimento e não há outro fundamento legal para o processamento; (iii) o titular dos dados opõe-se ao tratamento; (iv) os dados foram processados ilegalmente; (v) os dados devem ser apagados para cumprimento de uma obrigação legal; enfim, (vi) os dados foram coletados com base na oferta de serviços da sociedade da informação para crianças.³⁶⁰

No entanto, o Tribunal também observa em sua decisão que o direito ao esquecimento do titular dos dados não é absoluto e deve ser equilibrado com relação ao direito à informação, garantido pelo artigo 11, da Carta Europeia.³⁶¹ O direito à privacidade e o direito à proteção de dados pessoais, garantidos respectivamente pelos artigos 7º e 8º, da Carta Europeia, podem assim ser restritos com base em objetivos de interesse geral da União Europeia ou na necessidade de proteger os direitos e liberdades de terceiros. Desde que as limitações sejam previstas por lei, que a essência destes direitos e liberdades seja respeitada e se sujeitem ao teste da proporcionalidade, as restrições são admitidas pelo Tribunal.³⁶² Sendo assim, à luz dessas exceções, o Tribunal teve que determinar as condições em que o operador de um mecanismo de busca era obrigado a aderir a um pedido de exclusão de dados.

No caso, o Tribunal observou que a proibição de tratamento de dados pessoais não se aplicava quando o titular dos dados tivesse consentido de forma explícita a favor desta operação, a menos que o Estado-Membro proíba esse consentimento.³⁶³ Quanto a isso, o Tribunal reitera que o consentimento deve ser específico e, portanto, deve se relacionar especificamente à finalidade do processamento realizado. No entanto, o julgamento admitiu que, na prática, os operadores de mecanismos de busca não exigem o consentimento expresso dos titulares dos dados para processar seus dados pessoais e, por isso, destacou que o pedido e exclusão de dados é um dos motivos que justificam a aplicação do direito de exclusão.³⁶⁴ Mas, como já se observou, este direito não pode ser ilimitado, do que se infere que o operador de

³⁵⁹ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 54.

³⁶⁰ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

³⁶¹ PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502.

³⁶² Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 58.

³⁶³ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 62.

³⁶⁴ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 62.

um mecanismo de busca deve verificar, em concreto, se o direito à liberdade de informação dos usuários da internet prevalece sobre o direito à privacidade do titular dos dados. Para conduzir essa avaliação, o operador do mecanismo de busca deve considerar *i)* a natureza das informações e sua sensibilidade para a vida privada do titular dos dados e *ii)* o interesse do público em obter essas informações. Além disso, nos casos em que se trata de dados sensíveis, a interferência nos direitos fundamentais à privacidade e proteção dos titulares de dados acarreta particular seriedade.³⁶⁵ Ademais, ainda que o operador decidisse não excluir os links em questão, ele é obrigado a ajustar a lista de resultados de modo que a imagem do usuário reflita a sua situação atual.³⁶⁶ Como resultado, cada um desses interesses pode sofrer variações, de acordo com o papel desempenhado pelo titular dos dados na vida pública.³⁶⁷

Por conseguinte, o Tribunal concluiu que os operadores dos motores de busca devem processar pedidos de exclusão de links para páginas da web que contenham dados pessoais abrangidos pelo Direito da União, salvo exceções. No caso em concreto, observou-se que as informações relativas a processos judiciais movidos contra indivíduo, como as relativas à investigação judicial, são dados pessoais sensíveis, independentemente de o titular dos dados ter sido eventualmente condenado.³⁶⁸ Sendo assim, ao avaliar solicitações de cancelamento de referência de dados relacionados a crimes e condenações criminais, os operadores de mecanismos de busca devem encontrar um equilíbrio entre o direito ao respeito pela vida privada e, entre outros direitos, a liberdade de informação do público.³⁶⁹

Na avaliação da literatura especializada, este julgamento expande a orientação do Tribunal nos precedentes, pois confere aos operadores de mecanismos de busca a autoridade e a prerrogativa de decidir quais links devem ser excluídos e quais não.³⁷⁰ Além disso, a decisão exige que seja criado um sistema de aviso e retirada, permitindo que os mecanismos de pesquisa respondam às solicitações dos usuários, o que afasta a necessidade de criação de um

³⁶⁵ PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502.

³⁶⁶ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 78.

³⁶⁷ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

³⁶⁸ Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 77.

³⁶⁹ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

³⁷⁰ YAMAGUCHI, Itsuko. A japanese equivalent of the “right to be forgotten”: unveiling judicial proactiveness to curb algorithmic determinism. In: WERRO, Franz (org.). *The right to be forgotten. a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2018. p. 1-310. p. 292.

sistema de monitoramento constante e proativo, destinado a desindexar os dados confidenciais de maneira autônoma e independente.³⁷¹

2.2.3.4 *Google LLC v. Commission nationale de l'informatique et des libertés – CNIL*

Concomitante ao julgamento anterior, o Tribunal debruçou-se sobre o caso C-507/17 (*Google LLC v. Commission nationale de l'informatique et des libertés – CNIL*).³⁷² Nele, decidiu-se que o direito à exclusão de dados, ou o “direito ao esquecimento”, tem uma aplicação territorial limitada. Em particular, quando exercido contra um encarregado com operações multinacionais, ou globais, o direito de ser esquecido se aplica apenas às operações realizadas nos Estados-Membros da União Europeia. O caso foi remetido ao Tribunal pelo CNIL após a recusa do *Google* em pagar uma multa de €100.000,00, imposta no ano de 2016, pelo órgão regulador francês.³⁷³ A penalidade foi aplicada porque o *Google* se recusou a excluir links de pesquisa, contendo dados pessoais que eram prejudiciais a um indivíduo. Os domínios do *Google* em que se situavam as informações estavam fora da União Europeia.³⁷⁴ Apesar de ter recebido um aviso formal da CNIL, o *Google* se recusou a remover os dados pessoais de todas as versões de seus mecanismos de pesquisa em todo o mundo.

Como o operador de mecanismo de pesquisa, o *Google* tem atuação em diversos países e versões específicas deste instrumento são criados em função das especificidades linguísticas dos vários Estados em que a empresa exerce suas atividades.³⁷⁵ Aqui a questão relacionada à remoção do domínio é ainda mais controverso.³⁷⁶ Por isso, tendo em vista as especificidades regulatórias europeias, o *Google* remove resultados de pesquisa apenas em seus domínios europeus (por exemplo, “google.de” ou “google.fr”). Não remove resultados de pesquisa em seu domínio “google.com”, por exemplo.³⁷⁷ Embora os usuários da Internet não

³⁷¹ FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer. 2014. p. 170.

³⁷² Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019.

³⁷³ Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 33.

³⁷⁴ Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 32.

³⁷⁵ ZALNIERIUTE, Monika. *Google LLC v. Commission Nationale de l'informatique et des Libertés (CNIL)*. *American Journal of International Law*, Forthcoming, v. 114, p. 1-13, 2020.

³⁷⁶ Para posições sobre o tema analisar: (1) ALSENOY, Brendan; KOEKKOEK, Marieke. *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'*. *International Data Privacy Law*, 2015; (2) KUNER, Christopher. *The Court of Justice of the EU judgment on data protection and internet search engines: current issues and future challenges*. *SSRN Electronic Journal*, 2014.

³⁷⁷ POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

possam acessar versões estrangeiras do *Google*, em regra, ainda é possível acessar versões estrangeiras do *Google*, alterando as configurações de pesquisa, o que pode ser ocorrer quando o usuário utiliza uma rede privada (VPN), que permite aos usuários alterar a versão do *Google*.³⁷⁸

Ao tomar sua decisão, o Tribunal examinou o artigo 17 do GDPR, assim como os artigos 12 e 14 da Diretiva Proteção de Dados. Fora isso, o precedente *Google Spain* serviu de paradigma para a análise do julgamento.³⁷⁹ Com fundamento neste conjunto normativo, o julgamento trata, em primeiro lugar, da questão do território de aplicabilidade da proteção de dados, tema que está disciplinado no artigo 4º, (1), alínea “a”, da antiga Diretiva de Proteção de Dados, que corresponde ao conteúdo do artigo 3º, (1), da GDPR.³⁸⁰ Essa legislação é aplicável ao tratamento de dados efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento no território da União.³⁸¹ Mas se o fator territorial for o único para a definição da aplicação deste direito, um mecanismo de pesquisa poderia facilmente escapar da aplicação das leis nacionais ao optar por um determinado domínio.³⁸² O *Google*, por exemplo, é uma empresa sediada nos Estados Unidos da América que não remove os resultados da pesquisa em seu domínio “.com”, e, por isso, argumentou no processo que direciona os usuários da Europa para seus domínios locais, por exemplo “Google.fr”, para França, e “Google.de”, para a Alemanha,³⁸³ nos quais a legislação da união tem aplicação.

³⁷⁸ JACQUES, Sabine; HEMPEL, Felix. The right to be forgotten in the UK: a fragile balance? In: WERRO, Franz (org.). *The right to be forgotten. a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2020. p. 195-222.

³⁷⁹ Para maiores informações sobre o precedente, verificar o Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

³⁸⁰ Diretiva 95/46/CE: “Artigo 4º. Direito nacional aplicável. 1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente directiva ao tratamento de dados pessoais quando: a) O tratamento for efectuado no contexto das actividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável”.

GDPR: “Artigo 3º. Âmbito de aplicação territorial. 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das actividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União”.

³⁸¹ POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

³⁸² FOUAD, Y. *Reikwijdte van het Europese dataproctectierecht na Google Spanje: wat is de territoriale werkingssfeer en wordt eenieder beschermd?* 2015. Dissertação (Mestrado) – Institute for Information Law. University of Amsterdam, 2015 (Âmbito da lei europeia de proteção de dados após Google Espanha: qual é o território escopo e todos estão protegidos?).

³⁸³ FLEISCHER, P. *Reflecting on the right to be forgotten*. Blog do Google na Europa. Disponível em: <https://blog.google/around-the-globe/google-europe/reflecting-right-be-forgotten/>. Acesso em: 7 jan. 2021.

Em sua decisão, mais uma vez o Tribunal enfatizou que o direito à proteção de dados pessoais não é absoluto e deve ser analisado em relação à sua função na sociedade e precisa ser equilibrado com outros direitos fundamentais.³⁸⁴ Com base neste pressuposto, esta decisão adota uma abordagem pragmática em relação à questão da aplicação extraterritorial do Direito da União, reconhecendo as limitações técnicas do direito a ser esquecido nas jurisdições. Isso quer dizer que cabe, em primeira linha, ao Estado-Membro determinar se as medidas técnicas adotadas pelo mecanismo de busca atenderam a esses requisitos.³⁸⁵ Neste ponto, o Tribunal indicou que, em diversos Estados terceiros à União, o direito à supressão de referências pessoais na internet pode não existir ou pode ser objeto de uma abordagem diferente. Nessas situações, não caberia ao Tribunal impor sua legislação a terceiros.³⁸⁶ Inclusive, caso a exclusão de dados de forma mundial fosse permitida, as autoridades da União não seriam capazes de equilibrá-la com os outros direitos fundamentais.³⁸⁷ Por isso, a Corte sublinhou que o Estado-Membro continua a ser a instância competente para efetuar, à luz dos padrões nacionais de proteção, uma ponderação entre, de um lado, os direitos à vida privada e à proteção dos seus dados pessoais e, por outro, o direito à liberdade de informação.³⁸⁸

Outro tópico importante da decisão é se o Direito da União e as normativas de proteção à dados pessoais poderiam ser analisados diante de uma empresa com sede em Estado terceiro. Quanto a isso, o Tribunal afirma que a condução da pesquisa de dados é processada pela empresa sede, localizada em um terceiro Estado (ou seja, Google Inc., com sede em os Estados Unidos da América), enquanto a sucursal local espanhola apenas promove o meio de pesquisa e vende anúncios. De todo modo, o Tribunal identificou uma ligação intrínseca entre essas atividades (manutenção do mecanismo de pesquisa e marketing).³⁸⁹ Afinal, diz o julgamento, a atividade publicitária da realizada filial torna o mecanismo de pesquisa lucrativo.³⁹⁰ Com este fundamento, o Tribunal concluiu que os dados são processados no contexto das atividades da subsidiária espanhola do Google, concluindo pela

³⁸⁴ Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 60.

³⁸⁵ Para maiores informações sobre a transacionalidade, verificar a discussão sobre o Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015.

³⁸⁶ Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 63.

³⁸⁷ JACQUES, Sabine; HEMPEL, Felix. The right to be forgotten in the UK: a fragile balance? In: WERRO, Franz (org.). *The right to be forgotten. a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2020. p. 195-222. p. 209.

³⁸⁸ Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019. Parágrafo 72.

³⁸⁹ KUNER, Christopher. *The Court of Justice of the EU judgment on data protection and internet search engines: current issues and future challenges*. SSRN Electronic Journal, 2014.

³⁹⁰ POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

aplicabilidade da Diretiva 95/46/CE.³⁹¹ Se interpretado de forma mais restritiva, o processamento de dados pessoais de titulares de dados localizados na União, para as finalidades do seu mecanismo de pesquisa pela Google Inc. estaria fora do escopo da Diretiva, um resultado que não se mostra compatível com os objetivos da legislação da União em matéria de proteção de dados.³⁹²

Diante desse cenário e solucionar este problema, a GDPR adotou em seu artigo 3º, (2), alínea “a”,³⁹³ a doutrina *Marktortprinzip*,³⁹⁴ de acordo com a qual a aplicabilidade do Regulamento Europeu deve ser expandida para o processamento de dados pessoais de sujeitos localizados na União por um encarregado não estabelecido na União. Assim, no caso das atividades de processamento que estiverem relacionadas com a transferência de bens ou serviços aos titulares de dados, independentemente de saber se um pagamento do titular dos dados foi requerido, há aplicação do Direito da União.³⁹⁵

Com isso, o Regulamento somente será aplicável se os dados forem processados “no contexto das atividades” de um estabelecimento de um encarregado na União. Se, por exemplo, em um determinado Estado-Membro, o mecanismo de pesquisa anunciava seus serviços por meio de um estabelecimento disposto em um Estado terceiro, a aplicabilidade do Regulamento ocorrerá nos termos do artigo 3º, (2), alínea “a”, a fim de garantir a proteção do direito à proteção de dados pessoais. Esse resultado também acontecerá durante o exercício o direito de ser esquecido de acordo com o artigo 17, do Regulamento.³⁹⁶

Nestes termos, de acordo com o julgamento, ao avaliar se uma determinada informação deve ser desreferenciada dos resultados da pesquisa, deve-se realizar um teste de três etapas.³⁹⁷ Primeiro, o encarregado deve avaliar se os dados são confidenciais no sentido

³⁹¹ KUNER, Christopher. *The Court of Justice of the EU judgment on data protection and internet search engines: current issues and future challenges*. SSRN Electronic Journal, 2014.

³⁹² FOUAD, Y. *Reikwijdte van het Europese dataproctierecht na Google Spanje: wat is de territoriale werkingssfeer en wordt eenieder beschermd?* 2015. Dissertação (Mestrado) – Institute for Information Law. University of Amsterdam, 2015 (Âmbito da lei europeia de proteção de dados após Google Espanha: qual é o território escopo e todos estão protegidos?).

³⁹³ “Artigo 3º: Âmbito de aplicação territorial (...) 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento”.

³⁹⁴ Em tradução livre, podemos defini-lo como “princípio do mercado local”. GLOBOCNIK, Jure. *The right to be forgotten is taking shape: CJEU judgments in GC and others (C-136/17) and Google v CNIL (C-507/17)*. Oxford: GRUR International, 2020. v. 69. p. 380-388. p. 381.

³⁹⁵ Para maior debate sobre o *Marktortprinzip*, ver: FILGUEIRAS, Sofia Pereira. Aspectos legais do *marketing* em mundos virtuais. *Revista da FDUP*, p. 461-525, 2008.

³⁹⁶ GLOBOCNIK, Jure. *The right to be forgotten is taking shape: CJEU judgments in GC and others (C-136/17) and Google v CNIL (C-507/17)*. Oxford: GRUR International, 2020. v. 69. p. 380-388. p. 382.

³⁹⁷ GLOBOCNIK, Jure. *The right to be forgotten is taking shape: CJEU judgments in GC and others (C-136/17) and Google v CNIL (C-507/17)*. Oxford: GRUR International, 2020. v. 69. p. 380-388. p. 384.

do artigo 9º, (1), do Regulamento. Se for este o caso, o encarregado deve, em princípio, aceitar o pedido de anulação da referência. Segundo, o encarregado deve verificar se se aplica alguma exceção prevista no artigo 9º, (2), do Regulamento. Se for esse o caso, o encarregado de dados pode recusar o pedido de cancelamento de referência. No entanto, mesmo nesta hipótese, o mecanismo de busca terá que remover a referência dos links se o titular dos dados for incluído nas situações do artigo 17, alíneas “a” e “c”, do GDPR.³⁹⁸ Enfim, o processador de dados deve determinar, com base no artigo 9, (2), alínea “g”, da GDPR, se a inclusão do link nos resultados da pesquisa é estritamente necessária para proteger o interesse público em disponibilizar informações a terceiros. Se este for o caso, o operador do mecanismo de pesquisa deve rejeitar o pedido de cancelamento de referência.³⁹⁹ Aqui, novamente, o Tribunal se utiliza de uma espécie teste que busca o equilíbrio de direitos para aplicar (ou não) o direito de ser esquecido, na medida em que o processamento é necessário para exercer o direito de liberdade de expressão e informação a terceiros.

2.2.4 *Direitos autorais*

2.2.4.1 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*

A *SABAM*, entidade composta por representantes de músicos e empresas que protege obras garantidas por direitos autorais, entrou com uma ação perante o Tribunal Belga contra a *Netlog*, uma rede social, exigindo a criação de um sistema de filtragem que impeça a disponibilização de trabalho de seus clientes sem permissão.⁴⁰⁰ A *Netlog* era uma plataforma online, na qual os membros podiam criar sua própria página como um blog, nos quais ocorria a inserção de fotos, listas de reprodução, vídeos. Trata-se de uma rede social e um provedor

³⁹⁸ “Artigo 17º Direito ao apagamento dos dados («direito a ser esquecido»)

1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; (...) c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevaletentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;”

³⁹⁹ Veja-se que esta disposição foi utilizada no julgamento do caso Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricultura di Lecce v. Salvatore Manni*. Relator M. Ilešič. Julgamento em: 09 março 2017.

⁴⁰⁰ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012.

de hospedagem.⁴⁰¹ O judiciário nacional submeteu uma questão preliminar ao Tribunal: seria o mecanismo de filtragem proposto era compatível com o Direito da União?⁴⁰²

A esse respeito, a Diretiva nº 2001/29/EC, relativa aos direitos autorais, determinava que os detentores de direitos autorais poderiam obter liminares contra serviços utilizados para violar direitos autorais. Mas isso era limitado pelas demais matérias da União, incluindo a proteção aos direitos fundamentais à liberdade de informação e expressão.⁴⁰³ O julgado trata do artigo 15 da Diretiva n.º 2000/31/CE, sobre Comércio Eletrônico da União, que proíbe os Estados-Membros de imporem uma obrigação geral aos serviços de hospedagem para monitorar informações por eles transmitida ou armazenada.⁴⁰⁴ Por isso, decidiu-se que as redes sociais não podem ser obrigadas a monitorar e filtrar as comunicações de seus usuários para impedir a violação de direitos autorais de músicas e filmes.⁴⁰⁵

Quanto a este tema, o Tribunal considerou inclusive seu precedente de 2008 (*Promusicae v. Telefonica* – C-275/06) que determinou que os Estados e tribunais membros da União devem encontrar um equilíbrio entre a proteção dos direitos autorais e a proteção dos direitos fundamentais dos direitos autorais.⁴⁰⁶ Por isso, o Tribunal concluiu que a imposição de uma ampla obrigação de filtragem nas redes sociais exigiria um monitoramento ativo dos arquivos dos usuários, em violação à legislação da União, o que poderia prejudicar a liberdade de expressão dos cidadãos e o direito à proteção dos dados pessoais, garantidos nos termos dos artigos 8º e 11, da Carta.⁴⁰⁷

Já os direitos relativos à propriedade intelectual são absorvidos pelo direito fundamental da propriedade privada.⁴⁰⁸ Frente a este conflito de direitos, novamente, o Tribunal utilizou do teste da proporcionalidade, buscando com isso alcançar um ponto de equilíbrio entre os direitos em colisão: de um lado, os direitos de propriedade sobre obras

⁴⁰¹ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 16.

⁴⁰² Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 25.

⁴⁰³ PEREIRA, Alexandre L. D. The influence of human rights and basic rights in other fields of private law: intellectual property. In: TRSTENJAK, Verica; WEINGERL, Petra (org.). *The influence of human rights and basic rights in private law*. Springer, 2015. p. 523-533. p. 530.

⁴⁰⁴ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 33.

⁴⁰⁵ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 49.

⁴⁰⁶ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 42.

⁴⁰⁷ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 48.

⁴⁰⁸ PEREIRA, Alexandre L. D. The influence of human rights and basic rights in other fields of private law: intellectual property. In: TRSTENJAK, Verica; WEINGERL, Petra (org.). *The influence of human rights and basic rights in private law*. Springer, 2015. p. 523-533. p. 530.

intelectuais e a proteção de dados pessoais, de outro a liberdade de expressão e também a liberdade de as empresas prestarem serviços de armazenamento de informações.⁴⁰⁹ No caso, a solução de equilíbrio alcançada pelo Tribunal que seja imposta ao servidor de hospedagem (*Netlog*) uma obrigação de atuação preventiva, destinada a monitorizar e a filtrar, de forma sistemática e indiscriminada, todas as informações inseridas pelos usuários.⁴¹⁰ Neste sentido, a conclusão do julgamento salienta que a Diretiva 2004/48 é clara ao determinar que as medidas para assegurar o respeito dos direitos de propriedade intelectual não podem ser desnecessariamente complexas ou onerosas.⁴¹¹ Enfim, novamente se verificar no caso que o direito à proteção de dados pessoais não é o único direito protegido no ordenamento europeu, do que resulta a necessidade de compatibilizar a proteção de dados pessoais com os demais direitos fundamentais.

⁴⁰⁹ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 44.

⁴¹⁰ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 45.

⁴¹¹ Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012. Parágrafo 46.

2.2.4.2 *Digital Promusicae v. Telefónica de España SAU*

Na decisão conhecida como *Promusicae*, o Tribunal teve a oportunidade de considerar o equilíbrio entre os direitos de propriedade intelectual e proteção de dados pessoais.⁴¹² Em 2008, uma associação de detentores de direitos autorais (*Promusicae*) solicitou que uma operadora de telecomunicações (*Telefonica*) fornecesse a identidade e endereços físicos dos assinantes que eles suspeitavam terem infringido seus direitos autorais. Essa transferência de dados ocorreria por meio de um serviço de compartilhamento de arquivos “peer-to-peer” (sistema de filtragem eletrônica comunicações que utiliza software de compartilhamento de arquivos).⁴¹³ Nestes termos, o julgamento analisou se o direito da União Europeia exigia que os Estados-Membros adotassem regras nacionais que no sentido de impor aos prestadores de servidores de Internet o fornecimento de dados pessoais de supostos infratores de direitos autorais a seus titulares. Isso com a finalidade de facilitar a responsabilização pela violação das obras. Aqui o Tribunal buscou, mais uma vez, equilibrar o direito de propriedade com os direitos à privacidade e à proteção de dados.⁴¹⁴

O caso exigia a reconciliação do direito ao respeito pela vida privada e os direitos à proteção da propriedade e à reparação efetiva.⁴¹⁵ Analisando o tema, o Tribunal concluiu (i) que as operadoras de telecomunicações não podem ser obrigadas a comunicar dados pessoais como os solicitados, mas (ii) que os Estados-membros podem impor tal obrigação, levando em consideração a Diretiva de Comércio Eletrônico, a Diretiva de Direitos Autorais, a Diretiva e-Privacy e a Diretiva de Proteção de Dados, tudo com base no equilíbrio exigido pelo teste da proporcionalidade.⁴¹⁶

Vale lembrar que Diretiva e-Privacy é bastante clara ao garantir a confidencialidade do sistema eletrônico comunicações em redes públicas.⁴¹⁷ No entanto, o artigo 15, (1), desta mesma Diretiva permite que os Estados-Membros imponham restrições à obrigação de

⁴¹² KOSTA, Vasiliki. *Fundamental rights in EU internal market legislation*. Oregon: Oxford and Portland, 2018.

⁴¹³ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008.

⁴¹⁴ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

⁴¹⁵ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

⁴¹⁶ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008. Parágrafo 70.

⁴¹⁷ KOSTA, Vasiliki. *Fundamental rights in EU internal market legislation*. Oregon: Oxford and Portland, 2018.

confidencialidade quando estes “constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional, a defesa, a segurança pública”.⁴¹⁸ Porém, o Tribunal considerou que esta disposição dizia respeito ao julgamento de atividades criminosas ou atividades do Estado não relacionadas com o campo de atividade dos indivíduos. Não incluía, portanto, processos cíveis.⁴¹⁹ Por outro lado, o Tribunal observou também que o artigo 13 (1), da Diretiva Proteção de Dados, dispositivo que é referido no artigo 15 (1) da Diretiva e-Privacy, permite aos Estados-Membros restringir a obrigação de confidencialidade, quando necessário para “proteção dos direitos e liberdades de outrem”.⁴²⁰

Concluiu-se no julgamento, portanto, que a Diretiva da Privacidade Eletrônica não impede os Estados-Membros de estabelecerem uma obrigação de divulgação de dados pessoais no âmbito de processos cíveis; nem obriga os Estados-Membros a impor tal obrigação.⁴²¹ Disso resulta que os níveis de proteção dos direitos de propriedade intelectual e de proteção de dados variem entre os Estados-Membros, consoante o modo como o teste de equilíbrio é alcançado.⁴²²

No que tange à fundamentação, a referência do Tribunal ao artigo 8º, da Carta, pode ser vista como um passo adiante no reconhecimento autônomo do direito à proteção de dados pessoais em âmbito europeu. Mas a escolha das palavras do Tribunal e a linha de argumentação sugerem que a proteção de dados e privacidade ainda foram percebidos como sinônimos. Isso é evidenciado pela conclusão do Tribunal de que direitos fundamentais à propriedade e proteção judicial efetiva deveriam ser equilibradas com o direito à privacidade.⁴²³ Considerada como paradigma interpretativo, esta decisão indica que, até a promulgação da GDPR, o Tribunal indicava que a Diretiva da União visava garantir a proteção dos direitos fundamentais, com particular atenção à privacidade, como nos indica

⁴¹⁸ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008. Parágrafo 49.

⁴¹⁹ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008. Parágrafo 52.

⁴²⁰ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008. Parágrafo 53.

⁴²¹ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

⁴²² Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008. Parágrafo 57.

⁴²³ Como referência, podemos citar os casos C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*; C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. C-314/12; *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*; C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016.

Lynskey.⁴²⁴ Foram, inclusive, as disparidades verificadas em casos como esse que serviram de base para a constituição do Regulamento Europeu de Proteção de Dados e para a proposta de Regulamento Europeu de Privacidade Eletrônica.⁴²⁵

2.2.4.3 *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*

O caso C-70/10 (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*) teve origem em uma disputa entre a *Scarlet Extended SA*, um provedor de serviços de Internet, e a *SABAM*, empresa de administração belga responsável por autorizar o uso por terceiros das obras musicais de autores, compositores e editores.⁴²⁶ *Scarlet* havia sido obrigada, pelo tribunal belga de primeira instância, a instalar um sistema de filtragem eletrônica de comunicações que utiliza um software de compartilhamento de arquivos (“peer-to-peer”). Isso foi feito com o objetivo de prevenir o compartilhamento de arquivos que infrinjam direitos autorais de terceiros. O Tribunal foi instado a avaliar se esta liminar não desrespeitava a exigência de que um justo equilíbrio entre a proteção do direito de propriedade intelectual e a liberdade de conduzir negócios, o direito à proteção de dados pessoais, enfim, a liberdade de receber ou transmitir informações.⁴²⁷

A decisão parte do princípio de que os endereços de IP são dados pessoais protegidos porque permitem que os usuários sejam precisamente identificados.⁴²⁸ A fundamentação do Tribunal para chegar a esta conclusão diz que as Diretivas 95/46/CE e 2002/58/CE devem ser interpretadas tendo em conta os artigos 7º e 8 da Carta, o que denota a ascensão do direito à proteção de dados pessoais como direito fundamental para a União Europeia, apesar da sua ligação intrínseca com o direito à privacidade.⁴²⁹ Assim, conclusão de que o direito à proteção de dados pessoais foi afetado baseia-se no fato de liminar questionada obrigar a empresa a

⁴²⁴ LYNKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

⁴²⁵ KOSTA, Vasiliki. *Fundamental rights in EU internal market legislation*. Oregon: Oxford and Portland, 2018.

⁴²⁶ Processo C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*. Julgamento em: 24 novembro 2011.

⁴²⁷ PEREIRA, Alexandre L. D. The influence of human rights and basic rights in other fields of private law: intellectual property. In: TRSTENJAK, Verica; WEINGERL, Petra (org.). *The influence of human rights and basic rights in private law*. Springer, 2015. p. 523-533. p. 528.

⁴²⁸ Processo C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*. Julgamento em: 24 novembro 2011. Parágrafo 51.

⁴²⁹ Processo C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*. Julgamento em: 24 novembro 2011. Parágrafo 50.

realizar um tratamento amplo e sistemático dos endereço de IP. E estes endereços foram indicados como constituintes de dados pessoais.⁴³⁰

Sendo assim, o Tribunal concluiu que a medida implicaria a coleta e o tratamento sistemático de informações relacionadas com os perfis dos utilizadores, perfis que também devem ser considerados dados pessoais. Disso se deduziu que, ao adotar uma liminar exigindo que a *Netlog* instalasse o sistema de filtragem, o judiciário nacional não respeitou a exigência de que seja alcançado um justo equilíbrio entre o direito à propriedade intelectual e a correta proteção de dados pessoais.⁴³¹

2.2.5 Direito do consumidor

2.2.5.1 *Josef Probst v. mr.nexnet GmbH*

Neste caso (*Josef Probst v. mr.nexnet GmbH - C-119/12*), o Tribunal debruçou-se sobre a proteção de dados pessoais e os requisitos necessários para a transferência de dados entre empresas, especialmente aquelas que atuam no ramo da telefonia. Trata-se de importante julgado sobre as bases legais para a cessão de dados.⁴³² Nele, o Tribunal teve de decidir se, e em que circunstâncias, é permitido que uma empresa do ramo da telefonia transmita dados pessoais (relativos ao tráfego de navegação) para o cessionário de pagamento. Isso para que este último possa processar esses dados e realizar a cobrança.

O ponto de partida da decisão foram os artigos 6º, (2) e (5), da Diretiva 2002/58, que no entender do Tribunal eram exceções do princípio geral de confidencialidade, sobretudo no que diz respeito aos dados de tráfego da Internet. O artigo 6º, (2), da Diretiva 2002/58, prevê uma exceção à confidencialidade de comunicações, informando que os dados de tráfego necessários para fins de faturamento do assinante e os pagamentos de interconexão podem ser processados “apenas até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado”.⁴³³ A Diretiva reconhece, assim, a legitimidade do processamento de dados necessário para garantir o pagamento de obrigações, incluindo a cobrança de dívidas.⁴³⁴

⁴³⁰ Processo C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM*. Julgamento em: 24 novembro 2011. Parágrafo 26.

⁴³¹ FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer. 2014. p. 240.

⁴³² Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012.

⁴³³ Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012. Parágrafo 17.

⁴³⁴ IRION, Kristina. A special regard: the Court of Justice and the fundamental rights to privacy and data protection. In: FABER, Ulrich; FELDHOFF Kerstin; NEBE, Katja; SCHMIDT, Kristina; WAßER, Ursula

Já o artigo 6º, (5), da Diretiva, estabelece que o processamento de dados de tráfego é autorizado e “será limitado ao pessoal que trabalha para os fornecedores (...) encarregado da faturação” e “[deve] ser limitado ao necessário”, ou seja, ao único propósito da atividade contratada.⁴³⁵ Dessa forma, o cessionário da cobrança está autorizado a processar os dados, sob a condição de agir “sob a autoridade” do prestador de serviços e que ele ainda receba apenas os dados de tráfego que são necessários para efeitos de recuperação desses créditos.⁴³⁶ Essa disposição visa garantir que a transferência da cobrança de dívidas não afete o nível de proteção dos dados pessoais desfrutado pelo usuário.⁴³⁷

Por tudo isso, o termo “sob a autoridade” deve ser interpretado estritamente, assumindo o significado de que o cessionário age apenas sob as instruções e sob o controle do provedor de serviços.⁴³⁸ Disso resulta que o contrato firmado entre o prestador de serviço e o cessionário deve conter disposições que garantam o processamento lícito de dados devem prever meios para que o prestador de serviços garanta que essas disposições estão sendo cumpridas.⁴³⁹

Por fim, conclui o Tribunal no sentido de que caberia ao tribunal nacional verificar se o prestador de serviço (encarregado de dados) tem poder de controle efetivo que lhe permita verificar se o cessionário dos créditos (operador de dados) cumpre os requisitos que a regulamentação exige para que se realize o correto processamento dos dados pessoais. Em suma, o Tribunal indicou que a legislação da União permite esta transferência de dados pessoais ocorra, mas desde que sejam cumpridas todas as obrigações e requisitos pelo encarregado e operador, para que assim o direito à proteção de dados pessoais seja protegido de forma clara e transparente. Essa conclusão se coaduna, inclusive, com sua missão de realização do progresso económico e social da União.⁴⁴⁰

3.2.5.2 *Maximilian Schrems v. Facebook Ireland Limited*

(org.). *Gesellschaftliche Bewegungen – Recht unter Beobachtung und in Aktion*. Baden-Baden: Nomos, 2016. p. 873-890.

⁴³⁵ Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012. Parágrafo 18.

⁴³⁶ Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012. Parágrafo 3.

⁴³⁷ IRION, Kristina. A special regard: the Court of Justice and the fundamental rights to privacy and data protection. In: FABER, Ulrich; FELDHOFF Kerstin; NEBE, Katja; SCHMIDT, Kristina; WAßER, Ursula (org.). *Gesellschaftliche Bewegungen – Recht unter Beobachtung und in Aktion*. Baden-Baden: Nomos, 2016. p. 873-890.

⁴³⁸ Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012. Parágrafo 28.

⁴³⁹ Processo C-119/12. *Josef Probst v. mr.nexnet GmbH*. Julgamento em: 22 novembro 2012. Parágrafo 27.

⁴⁴⁰ Ver Considerando 1, da GDPR.

O próximo caso traz interessantes pontos de reflexão e debate acerca do direito ao acesso à justiça, o direito do consumidor e o direito à cessão de direitos, todos vinculados ao Caso C-498/16 (*Maximilian Schrems v. Facebook Ireland Limited*).⁴⁴¹ Diante da relevância do julgado e dos temas por ele tratados, será necessário desenvolver de forma mais atenta os argumentos do Tribunal no julgamento deste importante precedente. O personagem central é, mais uma vez, *Maximilian*, cidadão austríaco que utiliza a rede social *Facebook* desde 2008. Inicialmente, ele utilizou esta rede social apenas para fins pessoais; utilizava a conta para atividades privadas, como a troca de fotografias, conversas e publicação de conteúdo.⁴⁴² Seu nome era escrito em caracteres cirílicos, de modo a impedir qualquer busca a seu respeito. Fora isso, desde 2011 *Schrems* abriu uma página Facebook, por ele registrada e criada para informar os internautas sobre as suas medidas contra a *Facebook Ireland*. Lá *Schrems* inseriu as suas conferências, a sua participação em debates e suas aparições na mídia. Até mesmo campanhas de angariação de fundos e a fazer publicidade aos seus livros foram divulgadas.⁴⁴³

Lembre-se que, desde 2011, *Schrems* apresentou à Comissão Irlandesa para a Proteção de Dados 23 (vinte e três) queixas contra a *Facebook Ireland*, tendo uma delas dado origem a um pedido de reenvio prejudicial ao Tribunal Europeu.⁴⁴⁴ *Schrems* também publicou livros relativos à suas ações contra as alegadas violações da proteção de dados, proferiu conferências, registou numerosos sítios, tudo para custear as ações contra a *Facebook Ireland*.⁴⁴⁵ Enfim, *Schrems* chegou a constituir uma associação destinada a assegurar o respeito do direito fundamental à proteção de dados, recebeu diversas cessões de direitos: mais de 25.000 pessoas de todo o mundo enviaram autorizações para a *Schrems* apresente queixas no processo em comento. O julgado sintetiza a situação nos seguintes termos:

A associação constituída por M. Schrems destinada a assegurar o respeito do direito fundamental à proteção de dados não tem fins lucrativos e tem por objeto fazer respeitar o direito fundamental à proteção dos dados, realizar o trabalho necessário de acompanhamento em matéria de informação e junto dos *media*, bem como de esclarecimento político. O seu objetivo consiste em apoiar financeiramente processos modelo de interesse geral contra empresas que possam ameaçar este direito fundamental. Pretende-se igualmente

⁴⁴¹ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019.

⁴⁴² Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 10.

⁴⁴³ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 11.

⁴⁴⁴ O caso em questão foi analisado acima. Veja-se o Processo C-362/14. *Maximilian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015.

⁴⁴⁵ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 12.

financiar as despesas necessárias e, para o efeito, recolher, gerir e aplicar os donativos.⁴⁴⁶

O autor apresentou ao Tribunal Regional Cível de Viena uma ação com o intuito de obter a declaração relativamente de que *Schrems* atuava na qualidade de mero prestador de serviços da *Facebook Ireland*. Como consequência, solicitou a sujeição desta empresa às instruções por ele apresentadas na qualidade de mandante, quando o tratamento é efetuado em proveito próprio. Exigiu ainda que fosse declarada a invalidade de cláusulas contratuais relativas às condições de utilização do serviço prestado pelo *Facebook*.⁴⁴⁷ Fora isso, *Schrems* requereu que fosse cessada a utilização, para fins próprios ou de terceiros, de seus dados e ainda requisitou a prestação de informações sobre a utilização dos seus dados pessoais. Por fim, exigiu a prestação de contas relativamente ao ajustamento das condições contratuais e a reparação dos danos, devido ao enriquecimento sem causa da empresa. A ação tinha como autores não só *Schrems* outros consumidores residentes na Áustria, Alemanha e Índia, que cederam seus direitos contra a *Facebook Ireland*.⁴⁴⁸ Diante de tudo isso, o tribunal nacional abriu questionamento sobre o status de consumidor do autor da ação e sobre a possibilidade de cessão de direitos e o foro competente para julgar estas ações.⁴⁴⁹

Sobre o primeiro aspecto, de acordo com os precedentes do Tribunal de Justiça (processos C-269/95⁴⁵⁰ e C-464/01⁴⁵¹), a avaliação a respeito da qualidade da parte como consumidor não envolve suas qualidades subjetivas, mas sim sua posição da pessoa envolvida em um contrato específico, o qual deve ter sido confeccionado com o objetivo de satisfazer as necessidades de cada indivíduo.⁴⁵² Nesses termos, quando um contrato for celebrado com um objetivo parcialmente privado e parcialmente profissional, o aspecto profissional dele deve ser marginal para que o contrato ainda se enquadre como contrato de consumo.⁴⁵³

No presente caso, essa definição levantou duas questões. O Tribunal, primeiro, teve que decidir se a avaliação deveria ser feita apenas levando em conta a data em que o contrato

⁴⁴⁶ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 13.

⁴⁴⁷ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 15.

⁴⁴⁸ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 16.

⁴⁴⁹ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 24.

⁴⁵⁰ Processo C-269/95. *Francesco Benincasa v Dentalkit Srl*. Julgamento em: 03 julho 1997.

⁴⁵¹ Processo C-464/01. *Johann Gruber v Bay Wa AG*. Julgamento em: 20 janeiro 2005.

⁴⁵² Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 29.

⁴⁵³ GUIMARÃES, Guilherme Cintra. *Global technology and legal theory: transnational constitutionalism. Google and the European Union*. New York: Routledge, 2019.

foi originalmente celebrado ou se mudanças subsequentes também devem ser levadas em consideração.⁴⁵⁴ Quanto a este ponto, diz o julgamento que mudanças contratuais posteriores devem ser objeto de análise se e na medida em que o uso do contrato for, posteriormente, tornado como predominantemente profissional.⁴⁵⁵ Em segundo lugar, o Tribunal teve que decidir se esse era o caso de autor, que originalmente havia firmado um contrato com o *Facebook* para fins particulares, mas posteriormente, desenvolveu uma atividade profissional envolvendo litígios contra o *Facebook*.⁴⁵⁶

De acordo com o Tribunal, uma interpretação da noção de consumidor que exclua a representação dos direitos e interesses dos usuários teria o efeito de impedir a defesa efetiva dos direitos que os consumidores gozam em relação aos seus parceiros contratuais que atuem como profissionais, incluindo os direitos que se relacionam à proteção de seus dados pessoais.⁴⁵⁷ Esta conclusão encontra fundamento no Regulamento/CE n.º 44/2001, que define a competência judiciária sobre matérias cíveis e comerciais. De fato, de acordo com o artigo 2º deste Regulamento, os demandantes apenas podem apresentar processos judiciais no Estado-Membro em que o requerido esteja domiciliado.⁴⁵⁸ No entanto, para proteger as partes hipossuficientes, como consumidores ou funcionários, o Regulamento/CE n.º 44/2001 inclui regras de jurisdição especial, que estão insculpidas nos artigos 15 e 16, normas que determinam que domicílio do consumidor define a competência para julgar a demanda.⁴⁵⁹ Neste sentido, o autor poderia processar o *Facebook Ireland* e a jurisdição competente para julgar a causa seria aquela de seu próprio domicílio. Porém, em sua decisão, o Tribunal também proibiu que as ações coletivas sejam julgadas com base nesta regra de jurisdição especial. Isso porque, no entender do Tribunal, a jurisdição especial seria uma exceção à regra geral de divisão de competências e deveria, por isso, ser interpretada restritivamente.⁴⁶⁰ Em

⁴⁵⁴ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 30.

⁴⁵⁵ PATO, Alexia. *Jurisdiction and cross-border collective redress: a european private international law perspective*. Oxford: Hart Publishing, 2019.

⁴⁵⁶ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 31.

⁴⁵⁷ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 39.

⁴⁵⁸ “Artigo 2.º

1. Sem prejuízo do disposto no presente regulamento, as pessoas domiciliadas no território de um Estado-Membro devem ser demandadas, independentemente da sua nacionalidade, perante os tribunais desse Estado.”

⁴⁵⁹ “Artigo 16.º

1. O consumidor pode intentar uma acção contra a outra parte no contrato, quer perante os tribunais do Estado-Membro em cujo território estiver domiciliada essa parte, quer perante o tribunal do lugar onde o consumidor tiver domicílio.”

⁴⁶⁰ PATO, Alexia. *Jurisdiction and cross-border collective redress: a european private international law perspective*. Oxford: Hart Publishing, 2019.

outras palavras, decidiu-se que a jurisdição especial se aplicava apenas à pessoa que celebrou o contrato original com a empresa; não às ações coletivas, como pretendia o autor.⁴⁶¹

Esta decisão trouxe ao cidadão europeu a prevalência de seu status de consumidor. Contudo, interrompeu a possibilidade de haver reparações coletivas em situações de violações transfronteiriças dos direitos dos consumidores.⁴⁶² De fato, em sua decisão, o Tribunal indicou que o conceito de consumidor deve ter interpretação estrita, restringindo-se à oposição dele ao conceito de “operador econômico”. Assim, o conceito de consumidor independe da reputação ou da atuação profissional do sujeito, bastando analisar a parte oposta da lide.⁴⁶³ Nessa linha, o Tribunal considerou que *Schrems* não poderia processar o *Facebook* na Áustria em nome de consumidores que não são parte no contrato. Por isso, foi impossibilitada a interposição de ação coletiva, por ferir a cláusula de estrita relação entre o autor e o cessionário dos serviços.⁴⁶⁴

Frise-se que o próprio Tribunal indicou que esta foi uma opção do legislador europeu, não havendo a possibilidade de o Poder Judiciário modificar esta determinação legislativa.⁴⁶⁵ Por fim, é preciso registrar que a GDPR, que não se encontrava em vigor na data deste processo, estendeu a jurisdição especial aos titulares de dados pessoais, considerados como uma classe independente de demandantes vulneráveis (artigo 79). Isso reverte a orientação do Tribunal deste julgamento e reconhece o direito de uma classe de indivíduos apresentar uma ação no Estado-Membro em que tiverem residência habitual.⁴⁶⁶ No entanto, para isso, a entidade representativa necessita de mandato expresso do consumidor, sendo que tal demanda pode ser voltada a obter a indenização tanto por danos materiais como imateriais (artigo 82, da GDPR).

⁴⁶¹ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 48.

⁴⁶² GUIMARÃES, Guilherme Cintra. *Global technology and legal theory: transnational constitutionalism. Google and the European Union*. New York: Routledge, 2019.

⁴⁶³ Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019. Parágrafo 39.

⁴⁶⁴ Veja-se que este é um exemplo de restrição à possibilidade de interposição de ação coletiva, no âmbito da União Europeia, cerceando a intenção de ações coletivas abarcarem o direito à proteção de dados pessoais dos consumidores. Para um maior aprofundamento sobre Ações Coletivas e a Economia Global, ver: BUXBAUM, Hannah L. Class actions, conflict and the global economy. *Indiana Journal of Global Legal Studies*, v. 21, n. 2, p. 585-597, 2014.

⁴⁶⁵ PATO, Alexia. *Jurisdiction and cross-border collective redress: a european private international law perspective*. Oxford: Hart Publishing, 2019.

⁴⁶⁶ PATO, Alexia. *Jurisdiction and cross-border collective redress: a european private international law perspective*. Oxford: Hart Publishing, 2019.

Neste mesmo sentido, a União caminha para expandir a discussão sobre o papel do consumidor no continente, definindo quais de ações são asseguradas para sua proteção.⁴⁶⁷ A nova Diretiva 2020/1828, que entrou em vigor em 24 de dezembro de 2020, foi especialmente elaborada para tratar das ações coletivas para proteção dos interesses coletivos dos consumidores.⁴⁶⁸ O objetivo desta nova Diretiva é assegurar que exista ao menos algum meio processual que permita a propositura de uma ação coletiva eficaz e eficiente para obtenção de medidas inibitórias e de reparação à disposição dos consumidores em todos os Estados-Membros.⁴⁶⁹ Este meio processual aumentaria a confiança dos consumidores, os capacitaria para exercerem os seus direitos, contribuiria para uma concorrência mais justa e criaria condições equitativas para os profissionais que operam no mercado interno. Porém, como já foi observado, a Diretiva deve ser transposta à legislação nacional e os Estados-Membros têm o prazo de 24 (vinte e quatro) meses para tanto.

2.2.5.3 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*

O julgamento do Caso C-40/17 (*Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*) lançou luzes sobre as implicações do direito à proteção de dados pessoais que a ferramenta comumente utilizada na rede social, denominada “Like”, tem para os operadores de sites que incorporam este *plug-in* social em suas páginas na web.⁴⁷⁰ A *Verbraucherzentrale NRW*, uma associação de proteção dos consumidores, interpôs uma ação contra o *Fashion ID* exigindo que abandonasse a prática em seu website.⁴⁷¹ O *Fashion ID* havia colocado um botão “like” em seu site, que estava conectado ao *Facebook*. Assim, independente de os clientes da *Fashion ID* utilizarem do botão, as informações a respeito delas estavam eram transmitidas ao *Facebook*.⁴⁷² Assim, a questão precípua a ser discutida no julgado era saber se o *Fashion ID* detinha alguma obrigação em relação ao processamento de dados, incluindo o dever de informar os consumidores de que seus dados eram coletados e se, para realizar esta

⁴⁶⁷ Sobre a revisão da legislação do consumidor da União Europeia, verificar: UNIÃO EUROPEIA. *New deal for consumers*. Disponível em: https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en. Acesso em: 25 jan. 2021.

⁴⁶⁸ UNIÃO EUROPEIA. *Diretiva (EU) 2020/1828 do Parlamento europeu*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020L1828&from=EN>. Acesso em: 25 jan. 2021.

⁴⁶⁹ Considerando 7, da Diretiva 2020/1828.

⁴⁷⁰ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019.

⁴⁷¹ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 28.

⁴⁷² Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 25.

operação, a empresa era obrigada a obter o consentimento dos consumidores.⁴⁷³ Desta feita, foi realizado pedido de reenvio prejudicial ao Tribunal.

Em sua resposta, o Tribunal diz que o operador do site atua como encarregado de dados e, por isso, ele é responsável por informar o consumidor a respeito da coleta e deve obter seu consentimento no que diz respeito à coleta de informações e transmissão ao *Facebook*.⁴⁷⁴ Em particular, acerca da obtenção do consentimento do usuário, o Tribunal destacou que a legislação não estaria de acordo com o critério da proteção eficiente ao não oferecer a garantia eficiente e oportuna dos direitos do sujeito. Isso ocorreria caso o consentimento fosse exigido apenas do segundo responsável pelo tratamento.⁴⁷⁵ Contudo, o operador do site não é responsável perante os titulares dos dados por quaisquer outros usos que o próprio Facebook fará dos dados, nem por coletar seu consentimento a esse respeito.⁴⁷⁶ E embora o site não tenha controle sobre o uso dos dados transmitidos, o objetivo de tal coleta está em parte relacionado aos benefícios do site, pois permite uma melhor promoção de seus produtos.⁴⁷⁷

No que diz respeito à coleta de dados sem o consentimento do sujeito, o Tribunal esclareceu que, como o site e o provedor do *plug-in* social são considerados encarregados de dados, ambos devem buscar um legítimo interesse do processamento a ser aplicado.⁴⁷⁸ Nesse sentido, é importante frisar que o Tribunal aplicou a GDPR neste julgamento, uma vez que a antiga Diretiva 95/46 foi revogada a partir de 25 de maio de 2018. Como resultado, a função de controlador atribuída ao operador do site implica que ele seja considerado responsável pelo cumprimento das tarefas que normalmente dependem dos encarregados, particularmente (a) o dever de informar os titulares dos dados sobre o processamento, e (b) as obrigações relativas à base jurídica do em processamento.⁴⁷⁹

O operador do site deve, portanto, informar os titulares sobre o processamento de dados e deve coletar o seu consentimento a esse respeito, quando necessário. Deve,

⁴⁷³ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 26.

⁴⁷⁴ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 45.

⁴⁷⁵ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 74.

⁴⁷⁶ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 98.

⁴⁷⁷ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 101.

⁴⁷⁸ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 94.

⁴⁷⁹ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020. p. 74.

principalmente, verificar se o processamento de dados autoriza o acesso do operador do site às informações armazenadas no equipamento terminal dos titulares de dados através do uso de cookies e tecnologias similares.⁴⁸⁰ No entanto, essa responsabilidade é limitada às atividades de coleta e divulgação em decorrência da transmissão ao *Facebook* dos dados pessoais dos visitantes.⁴⁸¹

Nestes termos, o Tribunal adotou um amplo conceito de controle conjunto de dados, situação que pode existir para fases específicas do processamento de dados – no caso, a coleta inicial dos dados e sua transmissão ao *Facebook*. Disso decorre que a função de controladoria dos dados pode ser atribuída a apenas uma das partes nas fases subsequentes. O Tribunal ainda relegou ao órgão jurisdicional nacional a função de investigação, cabendo a ele avaliar se o provedor do *plug-in* obteve acesso do operador do site às informações armazenadas no equipamento terminal dos usuários, o que implicaria a necessidade de obter também o consentimento dos usuários nos termos da Diretiva 2002/58/CE.⁴⁸² Independentemente disso, o Tribunal esclareceu que o escopo de qualquer consentimento que o operador do site tenha que solicitar é limitado à coleta e comunicação de dados transferidos ao fornecedor do *plug-in*.⁴⁸³

Esta decisão também abordou a questão relativa à base jurídica do conceito de “interesse legítimo”. Isso porque, a Corte considerou que é necessário que o operador do site e o fornecedor busquem um interesse legítimo através das operações de processamento para que, assim, essas operações sejam justificadas.⁴⁸⁴

Por fim, este caso também trata da questão de ações coletivas propostas perante a União Europeia. Sobre isso, o Tribunal foi questionado se a legislação nacional pode (ou não) prever a possibilidade de ações transindividuais sobre a proteção de dados pessoais ou se a legislação da União Europeia deve ser seguida em estrito raciocínio. Quanto a este ponto, o Tribunal salientou que a Diretiva 95/46 dispõe que os Estados-Membros devem adotar as “medidas adequadas” para assegurar a plena aplicação das disposições da Diretiva. Contudo, a Diretiva não proíbe que cada Estado-Membro incorpore à sua legislação as possibilidades de

⁴⁸⁰ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 100.

⁴⁸¹ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1. p. 162.

⁴⁸² COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

⁴⁸³ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

⁴⁸⁴ TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

apresentação de ação administrativa ou judicial.⁴⁸⁵ Aplicando este princípio, o Tribunal entendeu que, caso o Estado-Membro possibilite a apresentação de ação coletiva, não há como a legislação da União negar sua existência, tendo em vista a independência dos Estados.⁴⁸⁶

Como resultado, define-se que o operador do site é encarregado de dados pessoais, em conjunto com o *Facebook*, quando há a utilização do *plug-in* social “Like”, em seu site. Deve-se, nesta hipótese, buscar o consentimento prévio do usuário para o uso deste fim ou o seu interesse legítimo. Contudo, é somente para este fim que o operador tem responsabilidade, sendo certo que demais uso e finalidades, utilizadas pelo *Facebook*, são de sua inteira responsabilidade.⁴⁸⁷

2.2.5.4 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*

Ainda em relação aos direitos dos consumidores, o caso C-673/17 (*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*) trata de importante figura nas páginas da web.⁴⁸⁸ Nesta decisão, conhecida pela literatura como *Planet49*, o Tribunal determinou que uma caixa de seleção pré-selecionada em um site (que o usuário deve desmarcar ativamente para recusar o consentimento – *opt-out*) não constitui consentimento válido sob a lei de proteção de dados. O assunto em disputa dizia respeito a um jogo promocional on-line organizado pela *Planet49 GmbH*. Para participar os usuários precisavam fornecer seu nome e endereço.

Os internautas que pretendiam participar nesse jogo tinham de comunicar o respectivo código postal e o aplicativo os encaminhava para uma página web em que deviam inscrever os nomes e endereços. Sob os campos a preencher com o endereço encontravam-se duas menções, antecedidas de quadrículas de seleção.⁴⁸⁹ A primeira menção, cuja quadrícula⁴⁹⁰ não

⁴⁸⁵ Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*. Julgamento em: 29 julho 2019. Parágrafo 59.

⁴⁸⁶ BARATTA, R. Complexity of EU law in the domestic implementing process. *Theory Pract Legis*, n. 3, v. 2, p. 293-308, 2014.

⁴⁸⁷ Para um maior debate sobre consentimento e legítimo interesse, ver: BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

⁴⁸⁸ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019.

⁴⁸⁹ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 26.

⁴⁹⁰ Sua redação era a seguinte: “Concordo que alguns *patrocinadores e parceiros de cooperação* me informem por via postal ou telefônica ou por correio eletrônico/SMS sobre ofertas dos seus ramos de negócio. Posso

estava pré-validada, questionava se os usuários concordavam em serem contatados, para fins de marketing, por empresas terceirizadas. Já a segunda menção, cuja quadrícula⁴⁹¹ estava pré-validada, solicitava consentimento para a instalação de cookies nos navegadores dos usuários. A participação no jogo só era possível depois de selecionada, pelo menos, a primeira quadrícula de seleção.

Antes de adentrar a análise do tema, o Tribunal afirmou que o consentimento válido não pode ser obtido através de uma caixa de verificação pré-marcada (*opt-out*), que o utilizador deve desmarcar seu não consentimento. Isso porque o Direito da União se refere aos requisitos para o consentimento como “específicos” e “inequívocos”, requisitos que não teriam sido observados no caso. Verifica-se, portanto, que o consentimento válido pressupõe o comportamento ativo do usuário (*opt-out*), e não passivo (*opt-in*). Quanto a isso, foi inclusive constatado que a GDPR encerrou este debate, exigindo expressamente consentimento ativo e impedindo que o silêncio e as “caixas de inatividade pré-marcadas” constituam consentimento válido do titular dos dados pessoais.⁴⁹²

O Tribunal observou que o consentimento deve estar relacionado ao processamento dos dados e não pode ser deduzido dos desejos do titular dos dados. Portanto, o fato de um usuário selecionar o botão para participar do jogo promocional não é suficiente para concluir que o usuário concedeu seu consentimento para o armazenamento de cookies ou então para o compartilhamento de seus dados com parceiros comerciais. E mais, o Tribunal também salientou que a Diretiva Privacidade Eletrônica se refere apenas às informações, sem indicar que estas informações devem ser caracterizadas como dados pessoais ou não. Portanto, é

aqui indicá-los pessoalmente; se não o fizer, a escolha dos mesmos é feita pelo organizador. Posso revogar o meu consentimento a qualquer momento. *Mais informações aqui.*” (Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 26).

⁴⁹¹ Com redação da seguinte forma: “Concordo que o serviço de análise Web Remintrex seja instalado no meu terminal, o que implica que o organizador do jogo promocional, a [Planet49], instalará *cookies* depois da inscrição no jogo, o que permitirá à Planet49 uma avaliação dos meus hábitos de navegação e utilização de sítios Web de parceiros publicitários, possibilitando assim uma publicidade orientada para os meus interesses por parte da Remintrex. Posso bloquear de novo os *cookies* a qualquer momento. Leia mais pormenores *aqui.*” (Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 27).

⁴⁹² Verifica o Considerando 32, do Regulamento 2016/679: “(32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. (...)”

irrelevante se os dados acessados por cookies constituam ou não dados pessoais, denotando que os requisitos sobre o consentimento se aplicam independentemente deste fato.⁴⁹³

Em síntese, o Tribunal esclareceu que as informações fornecidas devem permitir ao usuário determinar as consequências do consentimento. As informações fornecidas ao usuário devem ser suficientemente detalhadas para permitir ao usuário entender o funcionamento dos cookies empregados. Dentre estas informações devem ser relatadas a duração dos cookies e se terceiros podem ou não ter acesso a esses cookies.⁴⁹⁴

Ainda a este respeito, é importante ressaltar que o Tribunal não detalhou as exigências para que o consentimento deva ser considerado como “concedido livremente”. Isso porque esta pergunta não havia sido feita pelo órgão jurisdicional que elaborou o reenvio.⁴⁹⁵ De toda forma, o julgamento do caso *Planet49* fortalece a proteção da privacidade na esfera digital, não apenas dos consumidores, mas dos usuários da Internet em geral. Além disso, o Tribunal confirmou que o padrão de “proteção de cookies” não depende de envolver ou não os dados pessoais do usuário. A proteção da privacidade, de acordo com esta leitura, refere-se à inserção de cookies no website.⁴⁹⁶ Nessas circunstâncias, informar aos usuários, em nota de rodapé ou impressão, sobre o uso de cookies não é mais suficiente. O usuário deve concordar ativamente com o uso de cookies. E mesmo as caixas pré-selecionadas de consentimento não são consideradas como um consentimento suficientemente ativo, uma vez que o usuário pode ignorá-los e não fornecer nenhuma informação sobre sua vontade.⁴⁹⁷ Quanto a isso, o Tribunal foi claro ao afirmar que “a manifestação de vontade (...) deve, nomeadamente, ser ‘específica’, no sentido de que deve incidir precisamente sobre o tratamento de dados pessoais em causa”.⁴⁹⁸ Ou seja, a manifestação da vontade em aceitar os cookies não deve ser confundida com a manifestação utilizar o serviço ou produto.

Assim, o serviço ou produto oferecido deve ser desvinculado do cookie, não podendo ter entrelaçamento entre as duas vontades do consumidor. Em suma, verifica-se que a proteção de dados pessoais está abarcada neste julgado, apesar de os dados pessoais não

⁴⁹³ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

⁴⁹⁴ WIEDEMANN, Klaus. *The ECJ's decision in “Planet49” (Case C-673/17): a cookie monster or much ado about nothing?* IIC – International Review of Intellectual Property and Competition Law, 2020. p. 543-553.

⁴⁹⁵ COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

⁴⁹⁶ KOKOTT, Juliane; SOBOTTA, Christoph. *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*. International Data Privacy Law, 2013. p. 222-228.

⁴⁹⁷ WIEDEMANN, Klaus. *The ECJ's decision in “Planet49” (Case C-673/17): a cookie monster or much ado about nothing?* IIC – International Review of Intellectual Property and Competition Law, 2020. p. 543-553.

⁴⁹⁸ Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019. Parágrafo 58.

serem necessariamente incluídos na Diretiva e-privacy. Isso significa que o direito à privacidade está abrangido os objetos aqui discutidos, perfazendo o direito à proteção de dados pessoais quando da sua utilização no caso em concreto.

2.2.5.5 *Bavarian Lager*

A disputa no caso em *Bavarian Lager* centrou-se na interação dos direitos à proteção de dados pessoais e o acesso à informação, sendo certo que aqui trataremos do recurso impetrado.⁴⁹⁹ A *Bavarian Lager* foi criada para importar cerveja engarrafada para bares no Reino Unido.⁵⁰⁰ O produto não podia ser vendido facilmente, porque a maioria desses estabelecimentos estava vinculada a contratos de compra exclusiva com determinadas cervejarias. Além disso, os regulamentos do Reino Unido exigiam que as cervejarias britânicas permitissem que os gerentes de bares comprassem cerveja de outra cervejaria, desde que a cerveja fosse condicionada em barril. No entanto, a maioria das cervejas produzidas fora do Reino Unido, como a do requerente, era vendida em garrafas.

Deste modo, a *Bavarian Lager* apresentou uma queixa à Comissão Europeia no que diz respeito à restrição às importações, sendo que no decorrer do processo contra o Reino Unido foi realizada uma reunião privada com a Comissão e o Reino Unido. Após a reunião, o Reino Unido informou que as normas internas seriam alteradas para permitir a venda de cerveja em garrafa, o que indicaria a suspensão do processo. No entanto, a cervejaria fez diversos pedidos à Comissão Europeia para acessar os documentos das reuniões, incluindo as atas completas com os nomes dos participantes. A Comissão concordou em divulgar a ata, mas restringiu acesso a cinco nomes, uma vez que dois dos participantes se recusaram, especificamente, a divulgar seus nomes e os outros três não puderam ser contactados.⁵⁰¹

Sobre o tema, alegou-se que o requerente não tinha estabelecido uma finalidade ou necessidade expressa e legítima de divulgação, tal qual se exige no artigo 8º, do Regulamento nº 1045/2001 (Regulamento Relativo à Proteção de Dados) e, por conseguinte, o artigo 4º, do Regulamento nº 1049/2001 (Regulamento Relativo ao Acesso a Documentos).⁵⁰²

O referido Regulamento de Acesso a Documentos estabelece que o público pode acessar documentos das instituições da União Europeia, direito que está sujeito a certas

⁴⁹⁹ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010.

⁵⁰⁰ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 19.

⁵⁰¹ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 22.

⁵⁰² Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 37.

exceções.⁵⁰³ A exceção incidente no caso ocorre quando a divulgação comprometeria a privacidade e a integridade dos indivíduos. Nestes casos, o Regulamento exige que o destinatário estabeleça a necessidade de divulgação e que o sujeito a ser exposto tenha o direito de se opor.⁵⁰⁴

Deste modo, o Tribunal examinou se a divulgação dos nomes dos participantes da reunião violaria o direito à privacidade do artigo 8º, da Carta Europeia. Sua conclusão foi que a divulgação da lista de participantes não resultaria em violação do direito à privacidade. Nesses termos, o Tribunal considerou que a necessidade de consentimento do titular dos dados seria contrária ao conteúdo do Regulamento 1049/2001 e não violaria a proteção de dados pessoais do sujeito.⁵⁰⁵ Em consequência, o Tribunal anulou a decisão da Comissão.

O raciocínio do Tribunal neste caso parece claro: na ausência de uma violação do direito à privacidade como resultado da divulgação de um documento, as regras de proteção de dados não se aplicam.⁵⁰⁶ Embora, à primeira vista, isso possa ser confundido com outro exemplo da fusão dos direitos à proteção e privacidade de dados, a conclusão correta é oposta.⁵⁰⁷ O Tribunal interpretou a redação do artigo 4º, do Regulamento 1049/2001, considerando que, em casos de conflito entre proteção de dados e liberdade de informação, as regras de proteção de dados prevalecem apenas quando a privacidade é comprometida.⁵⁰⁸ Em sentido oposto, quando a privacidade não é prejudicada, as regras de liberdade de informação prevalecem sobre as regras de proteção de dados.⁵⁰⁹ Por conseguinte, a interpretação do artigo 4º, do Regulamento 1049/2001, apresentada pelo Tribunal reconhece que nem todo o tratamento de dados afeta negativamente o direito à privacidade e, por conseguinte, que a proteção de dados se aplica a uma variedade mais ampla de dados pessoais do que à privacidade.⁵¹⁰

Em outras palavras, o escopo material da aplicação dos dois direitos é distinto.⁵¹¹ Essa conclusão enfrenta uma série de críticas. Hert e Gutwirth, por exemplo,⁵¹² sugerem que o

⁵⁰³ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 21.

⁵⁰⁴ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 43.

⁵⁰⁵ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 49.

⁵⁰⁶ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 51.

⁵⁰⁷ JAECKEL, Liv. *The duty to protect fundamental rights in the european community*. United Kingdom: Oxford Studies in European Law Review, 2003.

⁵⁰⁸ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

⁵⁰⁹ LYNKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

⁵¹⁰ Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager*. Julgamento em: 28 junho 2010. Parágrafo 57.

⁵¹¹ JAECKEL, Liv. *The duty to protect fundamental rights in the european community*. United Kingdom: Oxford Studies in European Law Review, 2003.

Tribunal distinguiu entre dois tipos de dados pessoais – aqueles protegidos pelo direito à privacidade e aqueles que não o são. Na opinião destes autores, esta distinção não se encaixa na codificação da União.⁵¹³ E ao reconhecer que as regras de proteção de dados poderiam ser aplicadas mesmo na ausência de violação da privacidade, o Tribunal expandiu o âmbito de aplicação das regras de proteção de dados do direito, abrindo caminho para o surgimento de um direito verdadeiramente autônomo à proteção de dados na ordem jurídica da União.⁵¹⁴ Se, de um lado isso pode parecer positivo, de outro gera problemas. Afinal, a maior amplitude do direito à proteção de dados é acompanhada da multiplicação dos casos em que o Tribunal admite a limitação deste direito, resultado que gera insegurança e incertezas.

De toda forma, é preciso reter que, de acordo com esta decisão, o escopo material da proteção de dados pessoais é diverso do conteúdo do direito à privacidade. Na compreensão apresentada pelo Tribunal, os dados pessoais podem (ou não) ter nexos com a privacidade. No caso em comento, não há tal nexo, visto que a exposição de nomes dos participantes das reuniões não expunha de forma negativa a privacidade dos cidadãos. Por tudo isso, a divulgação estava em consonância com as regras de exposição e proteção de dados pessoais.

2.2.5.6 *Deutsche Telekom AG v. Bundesrepublik Deutschland*

Na sequência, há o caso C-543/09 (*Deutsche Telekom AG v. Bundesrepublik Deutschland*), no Tribunal, novamente, analisou o direito à proteção de dados pessoais de forma autônoma.⁵¹⁵

A *Deutsche Telekom* – sociedade empresária que explora uma rede de telecomunicações na Alemanha – atribuiu números de telefone aos seus assinantes e, além disso, publicou listas impressas e eletrônicas com informações relativas não só aos seus próprios assinantes, mas também aos assinantes de empresas terceiras.⁵¹⁶ A *Deutsche Telekom* obteve os dados junto à fornecedores de serviços telefônicos que atribuíram os números de telefone aos assinantes e celebrou cerca de 100 (cem) contratos, tendo por objeto a aquisição

⁵¹⁴ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

⁵¹⁴ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

⁵¹⁵ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011.

⁵¹⁶ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 19.

de dados pessoais, relativos aos assinantes.⁵¹⁷ Já as sociedades empresárias *GoYellow GmbH* e *Telix AG*, intervenientes no processo principal, exploravam, respectivamente, o serviço de informações pela Internet e o serviço de informações telefônicas. Ambas utilizavam dados colocados à sua disposição pela *Deutsche Telekom*, mediante o pagamento de remuneração.⁵¹⁸ Na sequência de um desacordo quanto à amplitude dos dados que a *Deutsche Telekom* deveria colocar à disposição das intervenientes, estas últimas submeteram a questão à jurisdição alemã.⁵¹⁹

⁵¹⁷ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 19.

⁵¹⁸ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 20.

⁵¹⁹ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 21.

Após transcurso do processo nacional, houve o reenvio da matéria ao Tribunal da União para se verificar se a obrigação de fornecer dados a terceiros imposta pelo direito nacional à *Deutsche Telekom*, está em conformidade com o direito da União.⁵²⁰ A primeira questão prejudicial indicada no processo tem correlação com a Diretiva 2002/22/CE,⁵²¹ mais especificamente, com o artigo 25 (2). Foi questionado se este dispositivo deve ser interpretado no sentido de que ele impede a criação de uma legislação nacional que impõe às empresas que atribuem números de telefone a utilizadores finais a obrigação de colocar esses dados à disposição de empresas que fornecem informações telefónicas ao público.⁵²² Esta medida tem como intuito primário assegurar o cumprimento da obrigação enunciada no artigo 5º, (1), de tal Diretiva, disposição que prevê que os Estados-Membros assegurarão que ao menos uma lista completa ou um serviço de informações telefónicas seja colocado à disposição dos usuários.⁵²³

Com esses fundamentos, o Tribunal entendeu que a *Deutsche Telekom* deve comunicar as informações às empresas que assim requererem, de acordo com o Direito da União. Eventuais informações adicionais devem ser verificadas de acordo com legislação nacional.⁵²⁴ Já em relação ao tema da proteção de dados pessoais, o Tribunal analisou a matéria a partir da Diretiva 2002/58/CE, mais precisamente, o artigo 12.⁵²⁵ Em sua fundamentação, o Tribunal

⁵²⁰ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 28.

⁵²¹ “Artigo 25.º

Serviços com a assistência de telefonista e serviços de informações de listas (...)

2. Os Estados-Membros garantirão que todas as empresas que atribuam números de telefone a assinantes satisfaçam todos os pedidos razoáveis no sentido de fornecerem, para efeitos de oferta de serviços de informações de listas e de listas acessíveis ao público, informações pertinentes num formato acordado, em condições justas, objectivas, baseadas nos custos e não discriminatórias.”

⁵²² Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 32.

⁵²³ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 33.

⁵²⁴ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 36.

⁵²⁵ “Artigo 12º. Listas de assinantes. 1. Os Estados-Membros assegurarão que os assinantes sejam informados, gratuitamente e antes de serem incluídos nas listas, dos fins a que se destinam as listas de assinantes impressas ou electrónicas publicamente disponíveis ou que podem ser obtidas através de serviços de informações de listas, nas quais os seus dados pessoais podem ser incluídos, bem como de quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões electrónicas da lista. 2. Os Estados-Membros assegurarão que os assinantes disponham da possibilidade de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, de quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, como estipulado pelo fornecedor das listas, bem como de verificar, corrigir ou retirar esses dados. A não inclusão numa lista pública de assinantes, a verificação, a correcção e a retirada de dados pessoais da mesma devem ser gratuitas. 3. Os Estados-Membros poderão exigir que o consentimento adicional dos assinantes seja solicitado para qualquer utilização de uma lista pública que não a busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação. 4. Os n. 1 e 2 aplicam-se aos assinantes

indicou que a Diretiva determinava que é possível a transmissão dos dados à terceiros, desde que o assinante seja informado anteriormente a respeito desta possibilidade e dos possíveis destinatários.⁵²⁶

Deste modo, o Tribunal entendeu que os Estados-Membros podem legislar sobre a transmissão de dados de lista telefônica à terceiros desde que (i) estes usuários tenham sido informados, antes da primeira inclusão dos seus dados na lista pública, da finalidade desta operação e do fato de que esses dados poderiam ser comunicados a outro fornecedor de serviços telefônicos e (ii) que garanta que os dados não serão, após a respectiva transmissão, utilizados para fins diferentes daqueles para os quais foram recolhidos.⁵²⁷

Da análise deste julgado, principalmente com base na segunda parte da fundamentação, há a clara indicação de que o Tribunal entende que o direito à proteção de dados é um direito autônomo e que pode ser utilizado como fundamento único e próprio para a proteção do indivíduo e das diretrizes fixadas pela própria União.⁵²⁸ Mais precisamente, a própria Diretiva de impõe que a transmissão de dados de carácter pessoal dos assinantes à terceiros deve obedecer à condição de que os dados não possam ser utilizados para outros fins além dos que motivaram a sua concessão, condição que tem correlação com o princípio da finalidade.⁵²⁹

No mais, é possível verificar que a Corte possibilitou aos Estados-Membros exigirem o consentimento adicional dos assinantes para qualquer utilização de lista pública que não envolva a busca de informações das pessoas relacionadas com o nome.⁵³⁰ Deste modo, verifica-se que o caso envolve a aplicação do direito à proteção de dados de forma autônoma, sem qualquer necessidade de verificação de outros direitos fundamentais. Porém, percebe-se que se trata no caso de situação de rasa importância à vida pessoal, não havendo uma clara e grave ameaça aos direitos de seus titulares.

que sejam pessoas singulares. Os Estados-Membros assegurarão igualmente, no âmbito do direito comunitário e das legislações nacionais aplicáveis, que os interesses legítimos dos assinantes que não sejam pessoas singulares sejam suficientemente protegidos no que se refere à sua inclusão em listas públicas.”

⁵²⁶ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 35.

⁵²⁷ Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011. Parágrafo 65.

⁵²⁸ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 255.

⁵²⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

⁵³⁰ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

2.2.6 Direito ao acesso dos dados pessoais

2.2.6.1 Patrick Kelly v. National University of Ireland

O Tribunal debruçou-se sobre o Caso C-104/10 (*Patrick Kelly v. National University of Ireland*), no qual aludiu ao fato de que a proteção de dados pessoais está prevista no artigo 8º, da Carta, sobre acesso a documentos e ônus da prova em casos de discriminação.⁵³¹ Neste caso, o Tribunal afirmou que as Diretivas 95/46/EC e 2002/58/EC, como regras do direito da União, “relativas à confidencialidade”, podem afetar o direito ao acesso a documentos. Inclusive, este caso é um importante julgamento sobre o ônus da prova em casos de discriminação.⁵³² Ademais, veja-se que este caso se soma aos julgados em que Corte que se refere ao direito previsto no artigo 8º, da Carta (proteção de dados), sem mencionar o direito à privacidade.⁵³³

No caso, o requerente se candidatou a um programa vocacional no *National University of Ireland*, mas sua inscrição foi recusada.⁵³⁴ Contudo, o requerente acreditava que ele era mais qualificado do candidato a quem havia sido oferecida a vaga e, por isso, sustentou que não havia recebido o treinamento em virtude de discriminação sexual. Demandou, assim, a divulgação de dados dos outros candidatos para apurar os fatos.⁵³⁵ Como a *National University of Ireland* divulgou apenas uma versão editada dos dados requeridos, o candidato preterido solicitou a análise judicial da situação.⁵³⁶

Por conseguinte, coloca-se a questão de saber se os litigantes em processos de discriminação têm o direito de exigir a divulgação de certas informações retidas pelo respondente.⁵³⁷ Uma questão adicional é se a recusa em fornecer as informações solicitadas pode ser levada em consideração para estabelecer uma presunção de discriminação.⁵³⁸ Em sua decisão, o Tribunal afirma que nem a Diretiva Sobre o Ônus da Prova nos casos de Discriminação Sexual (97/80/CE), nem a Diretiva de Igualdade de Tratamento (76/207/EEC), autorizavam um candidato a acessar informações sobre as qualificações dos outros

⁵³¹ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011.

⁵³² TZANOU, Maria. *The fundamental right to data protection: normative value in the context of Counter-Terrorism Surveillance*. Oregon: Oxford and Portland, 2017. p. 57.

⁵³³ TZANOU, Maria. *The fundamental right to data protection: normative value in the context of Counter-Terrorism Surveillance*. Oregon: Oxford and Portland, 2017. p. 57

⁵³⁴ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 19.

⁵³⁵ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 20.

⁵³⁶ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 2.

⁵³⁷ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 26.

⁵³⁸ RINGE, Julie. *The burden of proof in anti-discrimination proceedings*. A focus on Belgium, France and Ireland. *European Equality Law Review*, 2019. n. 2.p. 61.

requerentes. Mesmo com base na suspeita de discriminação, qualquer divulgação estaria sujeita às regras sobre confidencialidade de dados pessoais.⁵³⁹

Por outro lado, o Tribunal observa que as regras processuais nacionais não devem tornar impossível ou excessivamente difícil o exercício dos direitos conferidos pela União.⁵⁴⁰ Assim, não se deve impor em âmbito nacional regras que possam comprometer os efeitos objetivos de uma Diretiva.⁵⁴¹ Nessa linha, o Tribunal indicou que caberia ao órgão jurisdicional nacional decidir se o objetivo da Diretiva 97/80/CE exigia a divulgação de tais fatos. Não caberia ao Tribunal a análise do caso naquele momento e, também, caberia ao órgão jurisdicional nacional analisar se as regras processuais internas tornaram impossível ou excessivamente difícil exercer os direitos conferidos pelo direito da União.⁵⁴²

Como resultado, este julgamento indica que o direito à proteção de dados pessoais pode se tornar um óbice à direitos fundamentais do cidadão; no caso, o direito ao devido processo legal. De toda forma, considerando que o Tribunal simplesmente indica o panorama geral da situação e não adentrou ao mérito do tema do concreto, permanece o questionamento de qual seria a decisão do Tribunal em um teste que envolva o equilíbrio entre o direito à proteção de dados e o direito ao acesso à documentos para obtenção de provas judiciais.

2.2.6.2 *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert*

Ao analisar o caso C-473/12 (*Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert*), o Tribunal deteve-se na análise sobre quais medidas da União a respeito do direito à proteção de dados pessoais devem ser obrigatoriamente repassadas à legislação nacional.⁵⁴³ O Instituto Belga de Agentes Imobiliários (IPI) utilizou detetives particulares para verificar se a atividade de *Englebert* e outros estava em conformidade com a prática adequada da profissão de agentes imobiliários.⁵⁴⁴ O IPI constatou que os indicados haviam agido contra essas regras e requisitou ao tribunal local que ordenasse a interrupção de suas atividades de agência imobiliária.⁵⁴⁵ Nessas circunstâncias, o Tribunal foi confrontado com a questão de se

⁵³⁹ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafos 44-48.

⁵⁴⁰ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 53.

⁵⁴¹ Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 39.

⁵⁴² Processo C-104/10. *Patrick Kelly v. National University of Ireland*. Julgamento em: 21 julho 2011. Parágrafo 50.

⁵⁴³ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013.

⁵⁴⁴ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013. Parágrafo 14.

⁵⁴⁵ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013. Parágrafo 15.

o processamento direto e indireto de dados pessoais dos acusados constituía uma violação à Diretiva 95/46/CE, ou se essa atividade foi abrangida pela exceção do art. 13, (1), alínea “d”.⁵⁴⁶

Em sua decisão, o Tribunal indicou que os dados coletados por detetives particulares relacionados às pessoas que atuam como agentes imobiliários dizem respeito às pessoas físicas identificadas ou identificáveis. São, portanto, dados pessoais.⁵⁴⁷ Ocorre que a exceção do art. 13, (1) indica que o Estado-Membro *pode* e não *deve* transpor a medida à legislação interna.⁵⁴⁸ Deste modo, o Estado-Membro tem a liberdade de decidir se, e para que fins, tomará medidas legislativas destinadas a limitar o alcance das obrigações de informar o titular dos dados de prevenção, investigação, detecção e repressão de infracções penais e também das violações das funções das profissões regulamentadas.⁵⁴⁹

Com base nesses fundamentos, o Tribunal observa que Instituto Belga de Agentes Imobiliários corresponde a um organismo profissional responsável por garantir o cumprimento das regras que regem a profissão de agente imobiliário, que é uma profissão regulamentada na Bélgica. Ao IPI se reconhece, portanto, a prerrogativa de realizar a investigação e receber denúncias de violações das regras atinentes à profissão regulamentadas. E, para tanto, ele é capaz de se enquadrar nessa exceção. Em suma, isso quer dizer que a Diretiva não impede que esse organismo profissional recorra a investigadores particulares.

Assim, se um Estado-Membro optar por aplicar a exceção, o organismo profissional e os detetives particulares estarão abrangidos por esta norma e não estão sujeitos à obrigação de informar o titular dos dados.⁵⁵⁰ Por tudo isso, o Tribunal concluiu que a proteção do direito fundamental à privacidade exige que derrogações e limitações à legislação interna de proteção de dados pessoais sejam aplicadas apenas na medida que entender necessário.

2.2.6.3 *Nils Svensson e outros v. Retriever Sverige AB*

⁵⁴⁶ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013. Parágrafo 27.

⁵⁴⁷ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013. Parágrafo 29.

⁵⁴⁸ Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 7 novembro 2013. Parágrafo 32.

⁵⁴⁹ HIJMANS, Hielke. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Dissertation. University of Amsterdam, Amsterdam, 2016. p. 63.

⁵⁵⁰ HIJMANS, Hielke. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Dissertation. University of Amsterdam, Amsterdam, 2016. p. 63.

No julgamento do caso C-466/12 (*Nils Svensson e outros v. Retriever Sverige AB*), o Tribunal dedicou-se à análise de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação⁵⁵¹ A disputa inicia com um pedido de reenvio prejudicial relativo à interpretação do artigo 3º (1), da Diretiva 2001/29/CE, que traz soluções à problemáticas envolvida com a vida privada e o acesso à informação na World Wide Web.⁵⁵² Inclusive, é interessante notar que o caso é tratado sob o aspecto da vida privada em si, não havendo, propriamente, a defesa e o debate a respeito do conceito de dados pessoais.⁵⁵³ Fato que, mais uma vez, indica que na concepção do Tribunal, estes direitos são autônomos.

O processo havia sido instaurado em decorrência de pedido de *Svensson* e outros (todos jornalistas) proposto frente ao grupo de mídia *Retriever Sverige AB*. A questão debatida no processo trata de pedidos indenizações por danos que os autores consideraram ter sofrido em decorrência da divulgação no site da empresa *Retriever* de links de Internet (*hiperlinks*), os quais redirecionavam os usuários a artigos sobre os quais os requerentes detinham direitos autorais.⁵⁵⁴ De fato, os jornalistas escreveram os artigos para o *Jornal Göteborgs-Posten* e exclusivamente para o site da *Göteborgs-Posten*, mas o seu conteúdo podia ser acessados de forma gratuita na *Retriever*, que operava como um site que fornecia a seus clientes listas de links na Internet a artigos disponibilizados em outros sites.⁵⁵⁵

Deste modo, a questão precípua a ser analisada pelo Tribunal foi se o fornecimento de listas de links da Internet para artigos expostos em outros sites constituía ato suscetível de afetar os direitos autorais dessas obras.⁵⁵⁶ Debateu-se ainda se a indicação de um hiperlink constituiu uma transmissão do trabalho ou apenas uma indicação dos sites.⁵⁵⁷ Para realizar esta análise foi trazido aos autos a Diretiva 2001/29/CE, relativa à proteção de direitos autorais, que em seu artigo 3º dispõe que o ato de comunicação de obra ao público deve ter sido autorizado pelo titular do direito.⁵⁵⁸ Para interpretar este dispositivo, o Tribunal parte de

⁵⁵¹ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014.

⁵⁵² Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 14.

⁵⁵³ HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. *Communication to a new public? Three reasons why EU copyright law can do without a 'new public'*. *International Review of Intellectual Property and Competition*, 2016. p. 797-816. p. 813.

⁵⁵⁴ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 2.

⁵⁵⁵ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 8.

⁵⁵⁶ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 13.

⁵⁵⁷ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 20.

⁵⁵⁸ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 15.

algumas definições. No que se refere à noção de ato de comunicação,⁵⁵⁹ o Tribunal entendeu que este termo deve ser interpretado em termos gerais, a fim de garantir um alto nível de proteção aos detentores de direitos autorais.⁵⁶⁰ Assim, para haver um ato de comunicação, basta que um trabalho seja disponibilizado ao público.⁵⁶¹ O Tribunal observou, portanto, que o fornecimento de links (hiperlinks) para obras protegidas deveria ser, em regra, considerado como um ato de comunicação.⁵⁶²

Ocorre que, no caso em comento, o Tribunal referendou que a “comunicação ao público” deve ser dirigida a um público novo. Isto é, um público que não tenha sido levado em consideração pelos titulares primários, quando autorizaram a comunicação inicial.⁵⁶³ Deste modo e considerando que a primeira inserção dos artigos no Jornal *Göteborgs-Posten* detinha acesso ao público em geral, o fornecimento de links (hiperlinks) pela *Retriever* não violou o item da comunicação ao público, uma vez que não haveria público novo para acesso dos artigos.

Por isso, foi definido que o ato discutido não constituiu um ato de comunicação ao público, na acepção da Diretiva.

Por fim, o Tribunal firmou entendimento de que cabe à Corte Europeia o entendimento final sobre os aspectos das Diretivas da União. Assim, não caberia à jurisprudência nacional o analisar os termos e conceitos utilizados por estas normas, como o conceito de “ato de comunicação ao público”. As instâncias decisórias nacionais devem, portanto, respeitar e aplicar os entendimentos da jurisprudência do Tribunal a respeito das normas da União.

2.2.6.4 *Tele2 Sverige AB v. Post-och telestyrelsen e Secretary of State for the Home Department v. Watson*

No julgamento de processos apensos C-203/15 e C-698/15 (*Tele2 Sverige AB v. Post-och telestyrelsen e Secretary of State for the Home Department v. Watson*), foi definido que o

⁵⁵⁹ O precedente do Tribunal esclarece que a “comunicação ao público” requer um ato de intervenção da pessoa (Processo C-306/05. *SGAE contra Rafael Hoteles*. Julgamento em: 07 dezembro 2006).

⁵⁶⁰ Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014. Parágrafo 17.

⁵⁶¹ Tanya Aplin afirma que “Parece equivocado dizer que (...) [links] (...) constituem disponibilização (...) tudo o que eles fizeram é encaminhar outros usuários para onde os arquivos podem ser facilmente encontrados. Em outras palavras, eles forneceram uma forma de citação para as obras protegidas por direitos autorais” (APLIN, Tanya. *Copyright law in the digital society*. Oxford: Hart, 2005. p. 151. Tradução livre).

⁵⁶² AXHAMN, Johan. *Hyperlinking: Case C-466/12 Svensson and Others and Its Impact On Swedish Copyright Law*. *Europarättslig Tidskrift*, 2015. p. 847-865. p. 849.

⁵⁶³ O Tribunal utilizou-se da jurisprudência do próprio Tribunal para fundamentar este ponto, inclusive utilizando como parâmetro o Processo C-136/09. *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v Divani Akropolis Anonimi Xenodocheiaki kai Touristiki Etaireai*. Julgamento em: 18 março 2010.

acesso à dados pessoais constituí, necessariamente, uma interferência na privacidade dos usuários de comunicações eletrônicas.⁵⁶⁴ O conflito teve início no dia 9 de abril de 2014, quando a *Tele2 Sverige*, fornecedora sueca de serviços de comunicação eletrônica, informou a *Post-och Telestyrelsen* (Autoridade Sueca de Correios e Telecomunicações) que, tendo em conta a decisão europeia no processo *Digital Rights Ireland e outros* (C- 293/12 e C-594/12), na qual foi invalidada a Diretiva 2006/24/CE, deixaria de armazenar dados de comunicações eletrônicas.⁵⁶⁵ Nesta decisão, a *Tele2* considerou que a lei nacional sobre este armazenamento de dados foi constituída sobre o prisma da Diretiva 2006/24/CE e, sendo esta Diretiva anulada, a lei nacional seguiria o mesmo caminho.⁵⁶⁶

Contudo, em 29 de abril de 2014, o Ministro da Justiça Sueco nomeou um representante para examinar a legislação sueca em questão, à luz do julgamento europeu dos casos C- 293/12 e C-594/12. A conclusão do relatório foi que a legislação nacional não era incompatível com o direito da União ou com a Convenção Europeia de Direitos Humanos. Sendo assim, a legislação nacional não deveria ser invalidada.⁵⁶⁷ Como consequência desta decisão, a Autoridade Sueca de Correios e Telecomunicações determinou que a fornecedora voltasse a reter as informações. Diante deste imbróglio, a *Tele2 Sverige* interpôs recurso ao tribunal nacional.

Já no caso *Secretário de Estado do Departamento do Interior v. Tom Watson e outros*, os recorrentes apresentaram pedidos de revisão judicial da legalidade do regime de retenção de dados da Seção 1, da *Data Retention and Investigatory Powers Act* (a sigla, em inglês, DRIPA) de 2014.⁵⁶⁸ O Tribunal nacional havia declarado que tal Seção da DRIPA não é compatível com os artigos 7º e 8º da Carta, pois não indicava como obter acesso e usar os dados retidos. Na sequência, o Secretário de Estado do Departamento do Interior interpôs recurso contra esta sentença ao órgão jurisdicional local, o que ocasionou o reenvio prejudicial ao Tribunal.

Em seu julgamento, o Tribunal da União considerou que não há legislação da União que impeça um Estado-Membro de adotar legislação que permita a retenção direcionada de

⁵⁶⁴ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016.

⁵⁶⁵ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 44.

⁵⁶⁶ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 53.

⁵⁶⁷ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 46.

⁵⁶⁸ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 2.

dados de tráfego e localização. Isso pode ocorrer, diz o Tribunal, com o objetivo de combater crimes graves, desde que a retenção de dados seja limitada ao estritamente necessário.⁵⁶⁹ Nessa linha, ao analisar esse requisito, o Tribunal declarou que a legislação nacional deve estabelecer regras claras e precisas a respeito desta modalidade de coleta e impor salvaguardas mínimas para garantir a proteção efetiva dos dados retidos.⁵⁷⁰ Diz, inclusive, que a legislação nacional deve a possibilidade de revisão prévia por um tribunal ou autoridade administrativa, independente da concessão do acesso aos dados.⁵⁷¹ Além disso, as autoridades nacionais, que obtêm acesso os dados, devem fornecer informações ao interessado, contanto que essa notificação não possa mais comprometer a investigação.⁵⁷²

Este entendimento pode ser considerado como um avanço na defesa de grupos marginalizados pelo Estado, uma vez que a relação entre os dados e a ameaça deve ser devidamente notificada ao titular.⁵⁷³ De fato, as questões éticas e sociais relacionadas ao perfil dos investigados poderiam exigir uma análise mais aprofundada dos dados coletados e, por isso, a resposta do Tribunal foi no sentido de que esse perfil precisaria ser estritamente baseado em evidências. Caso as medidas de retenção sejam generalizadas e atinjam indivíduos indeterminados, elas devem ser substituídas por medidas de retenção *ad hoc*, baseadas na localização dos titulares dos dados pessoais.⁵⁷⁴

Com este julgamento, o Tribunal demonstra sua preocupação em garantir o respeito à Carta, em particular os direitos ao respeito à vida privada e à proteção de dados pessoais.⁵⁷⁵ Contudo, o julgamento busca também preservar a soberania nacional de cada Estado-Membro em possibilitar a regulamentação de matérias sensíveis, que devem ficar sob sua jurisdição, desde que as salvaguardas mínimas e os requisitos identificados no direito da União sejam preservados. Inclusive, de acordo com o precedente dos casos C- 293/12 e C-594/12, foi reafirmado que a vigilância generalizada e indiscriminada não é permitida pela legislação da

⁵⁶⁹ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 71.

⁵⁷⁰ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 90.

⁵⁷¹ Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 86.

⁵⁷² Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016. Parágrafo 102.

⁵⁷³ CAMERON, Iain. *Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Law, Department of Law*. Common market law review. v. 54, n. 5, p. 1467-1495, 2017. p. 1476.

⁵⁷⁴ CAMERON, Iain. *Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Law, Department of Law*. Common market law review. v. 54, n. 5, p. 1467-1495, 2017.

⁵⁷⁵ BRKAN, Maja. The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's Constitutional Reasoning. *German Law Journal*, v. 20, n. 6, p. 864-883, 2018.

União. Mas, de forma mais detalhada, o Tribunal destacou e detalhou um ponto focal a respeito da coleta indiscriminada de dados.

O ponto realçado pelo Tribunal diz que, com base nesta modalidade de coleta, podem ser retiradas conclusões bastante precisas em relação à vida privada da pessoa cujos dados foram retidos. Isso significa que estes dados podem ser retirados de cada ligação telefônica, de textos ou da conexão com a internet, os quais exibem informações sobre o local, horário e duração da comunicação.⁵⁷⁶ Apesar disso, foi declarado que cabe aos tribunais nacionais averiguarem se as legislações nacionais respeitam estes parâmetros.

⁵⁷⁶ CAMERON, Iain. *Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Law, Department of Law*. Common market law review. v. 54, n. 5, p. 1467-1495, 2017.

2.2.6.5 *Bodil Lindqvist*

Este julgamento merece destaque, pois foi um dos primeiros casos em que o Tribunal tratou do mérito da proteção de dados pessoais com base no Direito da União.⁵⁷⁷ A senhora Lindqvist trabalhava como catequista voluntária para uma igreja na Suécia e, em 1998, criou um sítio eletrônico para apresentar 18 (dezoito) colegas da sua paróquia. Neste sítio, seus colegas de trabalho foram identificados em detalhes, com descrições de suas situações familiares e suas atividades. Foram fornecidos até mesmo os seus números de telefone.⁵⁷⁸ Fora isso, foi mencionado que uma das colegas estava trabalhando em meio à uma lesão sofrida física.⁵⁷⁹ Após receber objeções de seus colegas, Lindqvist removeu o site e todas as informações.⁵⁸⁰ No entanto, ela foi processada pela Autoridade Sueca de proteção de dados devido à transferência de dados pessoais para países terceiros e processamento de dados sensíveis, tudo sem a devida anuência dos titulares.

Em decisão de primeira instância, Lindqvist foi condenada ao pagamento de multa no valor de 4.000,00 SEK. Apresentou recurso, ao qual foi deferido efeito suspensivo até a decisão do Tribunal.⁵⁸¹ Em sua argumentação, a recorrente diz que a Diretiva apenas abrangia o tratamento de dados pessoais no âmbito de uma atividade econômica, sendo que a operação de tratamento por ela realizada foi gratuita.⁵⁸² Neste mesmo sentido, o advogado-geral (Antonio Tizzano) afirmou em suas conclusões sobre o caso que o tratamento em causa não era abrangido pelo âmbito de aplicação do direito da União. Caberia ao Tribunal reverter a condenação, portanto.⁵⁸³ Porém, não foi esta a decisão do Tribunal.

Em sua fundamentação, o Tribunal identificou que o artigo 3º, da Directiva 95/46/CE, exclui do seu âmbito de aplicação somente o tratamento de dados “efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário”.⁵⁸⁴ Por isso e para reforçar a sua conclusão de que o tratamento era abrangido pelo âmbito de aplicação do direito da União, o Tribunal constatou que os exemplos das “atividades não sujeitas à aplicação do direito

⁵⁷⁷ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003.

⁵⁷⁸ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafos 12-13.

⁵⁷⁹ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafos 12-13.

⁵⁸⁰ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 14.

⁵⁸¹ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 18.

⁵⁸² Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 18.

⁵⁸³ Processo C-101/01. *Conclusões do advogado-geral Tizzano*. Apresentado em: 19 setembro 2002. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62001CC0101&from=EN>. Acesso em: 17 mar. 2021.

⁵⁸⁴ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 39.

comunitário”, mencionadas no artigo 3º (2), são atividades do Estado ou de Autoridades Estatais.⁵⁸⁵ Disso deduziu-se que a exceção apenas se aplica às atividades que podem ser classificados na mesma categoria (atividades estatais) e que as atividades de caridade ou religiosas, como as realizadas pela senhora Lindqvist, não se enquadravam nesta categoria.⁵⁸⁶

Em relação ao segundo ponto do artigo 3º, (2), que considera uma exceção o tratamento “efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas”, o Tribunal não correlacionou esta hipótese com a atividade da senhora Lindqvist. Isso porque tal exceção está vinculada exclusivamente à vida privada ou familiar do titular, não se aplicando no caso da inserção de dados de terceiros, como ocorre em relação às atividades ligadas à igreja.⁵⁸⁷ Assim, entendeu-se que a inserção de dados pessoais de terceiros – como efetuado pela senhora Lindqvist – deve ser entendido como tratamento de dados pessoais, conforme Diretiva 95/46/CE. Essa operação foi, inclusive, identificada como tratamento de dados pessoais por meio automatizados, o que mereceu maior proteção pelo direito da União.⁵⁸⁸

De fato, em sua fundamentação, o Tribunal identificou que a publicação em páginas da web sempre será um tratamento por meios automatizados, uma vez que “segundo os procedimentos técnicos e informáticos aplicados atualmente”, os carregamentos de informações em servidores necessariamente “são efectuadas, pelo menos em parte, de maneira automatizada”.⁵⁸⁹ E não é tudo, pois a indicação da lesão física da colega da senhora Lindqvist foi considerada como dado pessoal sensível, o que também mereceu maior proteção do legislador da União.⁵⁹⁰ Por outro lado, o Tribunal entendeu que a simples inserção de dados pessoais em página na web não pode ser caracterizada como transferência internacional de dados, mesmo que a página da web seja estabelecida em Estado terceiro,⁵⁹¹ o que pode ser considerado como precedente para a decisão do Processo C-136/17.⁵⁹²

Do exposto, podemos concluir que, para o Tribunal, qualquer inserção de dados pessoais em página da web (a título gratuito ou não) deve ser enquadrada como tratamento de dados pessoais, o que gera a incidência das regulações do Direito da União. Como resultado, verifica-se pela análise deste caso que o direito à proteção de dados pessoais foi alçado à

⁵⁸⁵ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 39.

⁵⁸⁶ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 40.

⁵⁸⁷ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 47.

⁵⁸⁸ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Conclusão 1.

⁵⁸⁹ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 26.

⁵⁹⁰ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Conclusão 3.

⁵⁹¹ Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Conclusão 4.

⁵⁹² Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019.

protetor da privacidade, em detrimento da liberdade de expressão. Porém, no caso em questão, este último direito não foi negado. Foi apenas salientado que a divulgação de dados deverá ser protegida pelas normas da União sobre dados pessoais, as quais são consideradas de maior importância para o titular do dado pessoal do que a liberdade de expressão.⁵⁹³

2.2.6.6 *Rundfunk*

Este caso diz respeito ao âmbito de proteção da Diretiva de Proteção de Dados da União e à relação entre as regras da União com a proteção do direito à privacidade. Por sua importância, o julgamento pode ser comparado com o acórdão do Tribunal proferido poucos meses depois, que dizia respeito ao tratamento de dados pessoais efetuado na Internet (*Lindqvist*).⁵⁹⁴ O pedido de reenvio prejudicial foi apresentado a pedido de dois tribunais austríacos. Ambos abordavam questões relativas à compatibilidade de uma disposição do direito austríaco com o direito da União. De acordo com esta disposição, as entidades sujeitas ao controle do Tribunal de Contas austríaco devem informá-lo sobre os vencimentos anuais elevados de seus empregados. Essas informações deveriam ser publicadas em relatório público.⁵⁹⁵ Argumentou-se no reenvio que a publicação desta listagem interfere na livre circulação de trabalhadores e prejudicaria as empresas pela desvantagem competitiva que a publicação acarreta. Fora isso, questionou-se se a publicação destas listas visava objetivos de interesse unicamente nacional, o que não se admite na legislação da União.⁵⁹⁶

Em seu julgamento, o Tribunal afirma que o registro dos dados pessoais pelo órgão público pode não interferir na privacidade. Mas este ato deve ser considerado como processamento de dados e, como tal, deve ser avaliado em relação às regras de proteção de dados.⁵⁹⁷ Na fundamentação, o Tribunal sustentou que, não havendo interferência em si sobre a vida privada das pessoas, as regras de proteção de dados pessoais deveriam prevalecer sobre as regras de privacidade para tutelar o registro e publicação de dados pessoais.⁵⁹⁸

⁵⁹³ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 68.

⁵⁹⁴ Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003.

⁵⁹⁵ Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003. Parágrafo 57.

⁵⁹⁶ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 52.

⁵⁹⁷ Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003. Parágrafo 65.

⁵⁹⁸ CLASSEN, Claus Dieter. *Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk*. *Common Market Law Review*, Issue 5, 2004. v. 41. p. 1377-1385.

Contudo, o Tribunal entendeu que, ao registrar os dados pessoais relativos ao vencimento de seus trabalhadores, não ocorre qualquer ingerência sobre a vida privada.⁵⁹⁹ Nesse sentido, foi ponderado ainda que a legislação nacional observa a “boa gestão dos fundos públicos prosseguido pelo legislador”, e que no presente caso deveria prevalecer pelo interesse público em torno da transparência dos atos governamentais.⁶⁰⁰ Justamente por isso, Hert e Gutwirth afirmaram que o legado deste julgamento está na vinculação entre o sistema europeu de proteção de dados (à época regulado pela Diretiva) e a garantia do direito fundamental à privacidade. De forma lapidar, esses autores afirmaram, portanto, que na visão do Tribunal a “proteção de dados é privacidade, nem mais, nem menos”.⁶⁰¹

2.2.6.7 *Satamedia*

No processo conhecido como *Satamedia*,⁶⁰² decisão proferida antes da entrada em vigor do Tratado de Lisboa, o Tribunal teve de se pronunciar sobre a derrogação, para fins jornalísticos, do sistema europeu de proteção de dados. O julgamento está relacionado com a interpretação do artigo 9º, da Diretiva 95/46.⁶⁰³ A controvérsia surgiu no contexto de um processo judicial entre duas empresas finlandesas e o Conselho de Proteção de Dados da Finlândia. As empresas publicaram dados relacionados à situação fiscal de cidadãos finlandeses, incluindo detalhes sobre sua renda. Tais dados foram disponibilizados via telecomunicações móveis com a ajuda de um serviço de mensagens de texto (SMS).

Assim, as questões dirigidas ao Tribunal abordavam a possível qualificação de tais informações como dados pessoais, considerando que esses dados eram do domínio público. Questionava-se, assim, se era possível considerar as atividades das empresas como “fins jornalísticos”, o que excluiria a ilegalidade do processamento. Em sua resposta, o Tribunal do Luxemburgo parte do pressuposto de que as atividades das empresas constituem o tratamento de dados na acepção da Diretiva de Proteção de Dados.⁶⁰⁴ Em seguida, o julgamento analisa se essas atividades devem ser consideradas processamento de dados exclusivamente para fins

⁵⁹⁹ Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003. Parágrafo 74.

⁶⁰⁰ Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003. Parágrafo 94.

⁶⁰¹ HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44. p. 33.

⁶⁰² Processo C-73/07. *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008.

⁶⁰³ Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008.

⁶⁰⁴ Processo C-73/07. *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008. Parágrafo 37.

jornalísticos, nos termos do artigo 9º da diretiva.⁶⁰⁵ Esta exceção permite derrogações às regras de processamento de dados, desde que elas sejam necessárias para conciliar os direitos à privacidade e à liberdade de expressão.⁶⁰⁶

Assim, entendeu-se que essas derrogações não se aplicam apenas às empresas de mídia, mas a todas as entidades que se dedicam ao jornalismo, uma vez que não é possível que o Poder judiciário conceitue, de forma abstrata, o jornalismo.⁶⁰⁷ Desta forma, as atividades jornalísticas devem ser abrangidas pelo âmbito de proteção da liberdade de imprensa, excluindo a incidência da Diretiva, desde que seja a “única finalidade a divulgação ao público de informações, de opiniões ou de ideias, o que compete ao órgão jurisdicional nacional apreciar”.⁶⁰⁸

Como consequência, conclui-se que cabe ao tribunal nacional decidir se, no caso, a *Satamedia* se enquadraria no conceito de “fins jornalísticos”, o que faz incidir a exceção ao processamento de dados pessoais e possibilita o processamento. Diante do exposto, verifica-se que, mais uma vez, o Tribunal analisou o direito à proteção de dados pessoais em conjunto com o princípio da liberdade de expressão, sem citações ou indicações do direito à privacidade e o artigo 7º da Carta Europeia.

2.3 Conclusão parcial

O Tribunal reafirma a sua posição suprema em assuntos da União, enquanto se configura como fiador do respeito aos Direitos Fundamentos da União, no campo da aplicação aos entes da União e a todos os Estados-Membros, com clara consequência aos cidadãos particulares. Com a análise perfunctória de 30 (trinta) decisões do Tribunal, é possível traçar os aspectos macros e micros do Direito à Proteção de Dados Pessoais na União Europeia.

⁶⁰⁵ Processo C-73/07. *Tietosuojavaluutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008. Parágrafos 49-50.

⁶⁰⁶ HIJMANS, Hielke. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Dissertation. University of Amsterdam, Amsterdam, 2016. p. 234.

⁶⁰⁷ Processo C-73/07. *Tietosuojavaluutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008. Parágrafo 54.

⁶⁰⁸ Processo C-73/07. *Tietosuojavaluutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*. Julgamento em: 16 dezembro 2008. Parágrafo 62.

Ponto importante a registrar é que o Tribunal utiliza da ponderação entre os direitos para a busca da solução que considera correta, a partir da colisão de diversos direitos e princípios existentes na Carta de Direitos Fundamentais.⁶⁰⁹

A conclusão macro mais clara é que, aplicando uma espécie de ponderação de direitos em várias situações, o Tribunal gera uma compreensão abrangente e instável da proteção de dados, que às vezes cede perante outros direitos, mesmo que na maioria dos casos prevaleça.

O Tratado de Lisboa é o marco de mudança na abordagem do Tribunal. Por um lado, o Tribunal está claramente determinado a julgar com base na Carta e salvaguardar os direitos dos titulares dos dados, seja através do direito à vida privada, proteção de dados pessoais ou um híbrido de ambos. Por outro lado, concede a proteção de direitos diversos – tais como liberdade de informação e expressão – através das regras positivadas sobre a proteção de dados pessoais.

Claramente, os direitos à privacidade e proteção de dados serão direitos que sempre terão uma ligação intrínseca; porém, com o decorrer da utilização deste direito na realidade e com a evolução da percepção pessoal sobre o direito à proteção de dados, a tendência é ocorrer um desgarramento das posições a serem adotadas em casos que envolverem a matéria.

Ao investigar as conclusões micro, podemos indicar que a proteção de dados pessoais é regra a ser analisada por todos, principalmente a partir da presença das redes de informação e comunicação nos ambientes sociais – as quais serão mais bem analisadas no capítulo 3 – com aplicação em casos cotidianos como a inserção de nomes em página da web, perpassando a casos de média complexidade, como a transferência de dados pessoais a empresas de cobranças de serviços, até a chegar em casos de grande complexidade, como a transferência internacional para países como Estados Unidos da América.

Nessa perspectiva, a normatização do direito à proteção de dados pessoais na Carta pode ser encarada como uma evolução positiva, pois a proteção de dados tem objetivo nesta nova era da sociedade e que detém princípios diferentes do direito à privacidade, visando regulamentar o processamento justo de dados por atores públicos e privados.

Veja-se, portanto, que o Tribunal utiliza o direito à proteção de dados pessoais para a proteção de direitos fundamentais, o que demonstra que este direito pode ser definido como um mecanismo normativo para que as pessoas físicas tenham o poder de se opor às invasões de sua liberdade, de sua dignidade, de sua privacidade.

⁶⁰⁹ Para um debate mais aprimorado sobre a ponderação e o Tribunal, ver: SCACIA, Gino. Proportionality and the balancing of rights in the Case-law of European Courts. *Rivista di Diritto Pubblico Italiano*, Comparato, Europeo, fev. 2019.

3 NOVAS PERSPECTIVAS PARA A PROTEÇÃO DE DADOS PESSOAIS

3.1 Globalização, dados pessoais e transferência internacional

A presença das redes de informação e comunicação nos ambientes sociais, jurídicos, políticos tem determinado a tomada de consciência e a necessidade de se conceber os valores e os direitos da pessoa como garantias universais ao seu desenvolvimento integral em virtude de sua essencial dignidade.⁶¹⁰ Neste contexto, a realidade da transferência de uma gama de informações pessoais em rede digital culminou na difusão da vida privada e na exposição da intimidade, eis que todos os atos da vida humana e em sociedades são virtualizados e praticados na rede sem sigilo.⁶¹¹ Nas palavras de Victor Gonçalves:

Outra desconfiança aberta neste trabalho, seguindo a trilha aberta por Foucault, é a da forma da lei como apaziguadora e solução para os questionamentos trazidos pela inclusão digital. No percurso de discussão das formas da construção da inclusão digital como um direito fundamental na forma da lei inviabilizaria a sua capacidade transformadora. Enrijeceria duplamente a teoria e a prática. Não que a inclusão digital não possa ser absorvida pela lei, mas ela não pode ser pensada como restrita a ela. A inclusão digital tem sempre de ser ampliada para além, para os lugares e o tempo que as lutas e combates são travados e vividos. Lá onde o valor nasce da necessidade. Por isso, a forma da lei não deve ser tomada como princípio nem fim da inclusão digital como direito fundamental.⁶¹²

Deste modo, cabe relatar que a prática tem revelado o vigilantíssimo virtual crescente, principalmente do Estado e de empresas, que negociam, trocam e armazenam informações para obterem lucros, persecuções criminais satisfatórias, acessos a sigilos bancários, padrões de consumo, enfim, uma série de práticas que frustram os direitos humanos daqueles que utilizam das tecnologias de informação⁶¹³ e comunicação.⁶¹⁴

⁶¹⁰ Como definição dos termos aqui descritos, utilizaremos a definição de SILVA: “A rede e serviços telemáticos são em si mesmos híbridos enquanto linguagem porque acolhem simultaneamente escrita, imagem, som, vídeo unidos pela estrutura do laço (link) e da interactividade, que faz com que se designe como hipermedia. Estas novas mídias apresentam uma estrutura triádica (Nunes, 1996a), ou seja, estética, tecnológica e social. A vida social é um construto que tem a sua génese e metamorfose nas tecnologias da informação e da comunicação, são essas tecnologias que geram novas dinâmicas fazendo surgir o que usualmente se designa de tecnocultura que gera uma nova ecologia cognitiva marcada pelo hibridismo e pela globalização” (SILVA, Lídia Loureiro da. *Globalização das redes de comunicação: uma reflexão sobre as implicações cognitivas e sociais*. Biblioteca online de ciência da comunicação. 1999. Disponível em: <http://www.bocc.ubi.pt/esp/autor.php?codautor=63>. Acesso em: 22 fev. 2021. p. 5).

⁶¹¹ LÉVY, Pierre. *As tecnologias da inteligência: o futuro do pensamento na era informática*. Lisboa: Instituto Piaget, 1994. p. 79.

⁶¹² GONÇALVES, Victor Hugo Pereira. *Inclusão digital como direito fundamental*. São Paulo: Delfos, 2012. p. 14.

⁶¹³ Sobre este assunto, nos elucidava Roberto Senise Lisboa, “A sociedade da informação resulta desses acontecimentos, viabilizando-se a comunicação mais rápida e a obtenção adequada de dados. Verifica-se a

O direito à liberdade de informação, previsto art. 5º, XIV e XXXIII e art. 220, § 1º, todos da Constituição Federal, assume especial importância em uma sociedade democrática, pois é essencial à participação na vida pública.⁶¹⁵ De outro lado, há que se considerar a proteção aos direitos da personalidade,⁶¹⁶ principalmente o direito à intimidade.⁶¹⁷

Tendo em vista o desenvolvimento dos meios de comunicação de massa, notadamente a internet, vêm à mente a reflexão de Milan Kundera em “A Insustentável Leveza do Ser”: partindo da ideia nietzschiana do “eterno retorno”, o autor desenvolve as questões existenciais sobre efemeridade da vida em contraposição com o peso de uma história condenada à eterna repetição.⁶¹⁸ De forma similar, a internet tem a aptidão para o registro permanente das informações, o que pode se revelar avassalador sobre o indivíduo, que poderá sofrer diversas vezes as consequências do “eterno retorno” de acontecimentos passados.⁶¹⁹ Tal situação é infensa ao regime jurídico dos efeitos do tempo no Direito que, em prol da segurança jurídica, faz desaparecer situações em razão da passagem do tempo, como no caso da prescrição.

Colocado o problema, com base na teoria dos princípios formulada por Robert Alexy, se afirma que tais conflitos principiológicos se resolvem segundo a ponderação do peso de cada um deles em um caso concreto, ou seja, “quanto maior é o grau de satisfação ou de não satisfação ou de afetação de um princípio, tanto maior deve ser a importância da satisfação do

concentração de empresas mundiais de dados. Busca-se o acesso a todo tipo de obra ou de informação disponível, inclusive em rede de telecomunicações, por meio de uma base de dados obtida em obras multimídia e em trabalhos desenvolvidos pela internet” (LISBOA, Roberto Senise. A inviolabilidade de correspondência na Internet. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto. *Direito & Internet: aspectos jurídicos relevantes*. Bauru: Edipro, 2001).

⁶¹⁴ LANGHEINRICH, Marc; FINN, Rachel; COROAMA, Vlad; WRIGHT, David. Quo vadis smart surveillance? How smart technologies combine and challenge democratic oversight. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul (org.). *Reloading data protection*. Inglaterra: Springer, 2014. p. 151-182.

p. 154.

⁶¹⁵ FISS, Owen M. *A ironia da liberdade de expressão: estado, regulação e diversidade na esfera pública*. Tradução e prefácio de Gustavo Binenbojm e Caio Mário da Silva Pereira Neto. Rio de Janeiro: Renovar, 2015.

⁶¹⁶ Nesse sentido, observa Marcel Leonardi, “No entanto, parte da doutrina enfatiza que a Constituição de 1988 foi redundante, não havendo a necessidade de distinguir entre o direito à intimidade e o direito à vida privada: ‘Embora seja princípio de hermenêutica de que a lei não deve abrigar expressões inúteis, de todo dispensável a menção, feita pela Constituição de 1988, à inviolabilidade da vida privada.’” (LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2011. p. 49).

⁶¹⁷ STOCO, Rui. Proteção da imagem *versus* liberdade de informação. *Revista da Escola da Magistratura Federal da 2ª Região – EMARF – TRF 2ª Região*, Rio de Janeiro, v. 8, n. 1, mar. 2007.

⁶¹⁸ Segundo o autor, “Se cada segundo de nossa vida deve se repetir um número infinito de vezes, estamos pregados na eternidade como Cristo na cruz. Essa ideia é atroz. No mundo do eterno retorno, cada gesto carrega o peso de uma responsabilidade insustentável. É isso que levava Nietzsche a dizer que a ideia do eterno retorno é o mais pesado dos fardos” (KUNDERA, Milan. *A insustentável leveza do ser*. São Paulo: Companhia das Letras, 2008. p. 10).

⁶¹⁹ LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2011.

outro”.⁶²⁰ Seguindo essa lógica, a regulamentação da proteção de dados pessoais no âmbito nacional fez parte de uma estratégia global, visando a proteção aos dados pessoais e dados sensíveis à população. Nessa linha, a legislação nacional brasileira estabelece bases legais para legitimação do tratamento de dados pessoais e garante direitos aos titulares dos dados como: acesso, correção, eliminação, portabilidade e revogação do consentimento.⁶²¹

Neste contexto, a inovação tecnológica também é e será um dos componentes importantes para as organizações estatais e empresariais, uma vez que a LGPD traz desafios de gestão e governança de privacidade tais como: a gestão de consentimentos (e respectivas revogações), gestão das petições abertas por titulares (que, em alguns casos, devem ser respondidas imediatamente), gestão do ciclo de vida dos dados pessoais (*data mapping & data discovery*) e implementação de técnicas de anonimização (os dados anonimizados não serão considerados dados pessoais desde que o processo de ocultação não seja reversível).⁶²²

Tópico relevante sobre o assunto é o regime regulatório da transferência internacional de dados, que tem como objetivo regular transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. A razão precípua da criação desta regra está no fato de que, no âmbito de proteção de dados, a localização da informação pessoal não deveria diminuir as garantias para tutelar os respectivos titulares, ou seja, a proteção dos dados deve acompanhar o trânsito do dado pessoal, independentemente da sua localização física.⁶²³ Contudo, em razão da limitação jurisdicional/competência de cada país em legislar e atuar dentro do seu espaço territorial, esta regra não poderia criar determinações diretas à países estrangeiros, em decorrência da jurisdição de cada sociedade nacional, sendo que alguns autores consideram que a noção de competência exprime melhor o fenômeno.⁶²⁴

Fato é que a jurisdição representa a limitação do exercício de poder, o que em termos processuais ocorre com o intuito de desenvolver a atividade que visa a solução imparcial de conflitos dentro de determinada competência.⁶²⁵ Todavia, notadamente em virtude de processos de adaptação do sistema capitalista – como o fenômeno da Globalização – esta

⁶²⁰ ALEXY, Robert. *Teoria dos derechos fundamentales*. Tradução de Ernésto Garzón Valdés. Madrid: Centro de Estudios Constitucionales, 1997. p. 161. Tradução livre.

⁶²¹ LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2011.

⁶²² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

⁶²³ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

⁶²⁴ É o caso de Charles Rousseau, para quem competência territorial significa “a competência do estado em relação aos homens que vivem em seu território, às coisas que nele se encontram e aos fatos que aí ocorrem”. ROUSSEAU, Charles. *Principes de droit international public*. RCADI, 1958. p. 370. Tradução livre.

⁶²⁵ CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido R. *Teoria geral do processo*. 31. ed. São Paulo: Malheiros, 2015.

noção, que tem origem processual, não mais se comporta de forma suficiente acerca da relação jurisdicional de característica internacional.⁶²⁶

Deste modo, a forte e crescente demanda para o alinhamento transnacional de regulações sobre a privacidade e proteção de dados tem como principal meta a criação de regras equânimes em um mundo cada vez mais globalizado, com a intenção de abster os indivíduos dos possíveis “paraísos dos dados”, locais em que não haveria a disciplina dos direitos de proteção, o que possibilitaria o comércio sem regulação.⁶²⁷ Isso fez com que a União Europeia criasse o mecanismo previsto no artigo 45, da Regulação Geral de Proteção de Dados Europeia, que tem o intuito de criar regras e parâmetros dentro do contexto da União Europeia e do Espaço Econômico Europeu, e cria regras internacionais para a proteção da transferência internacional de dados a países terceiros.⁶²⁸

Neste sentido, a criação de regras internacionais, e, até mesmo, a criação de organismo internacional para regulação da privacidade e proteção de dados ensejaria um melhor nível de segurança jurídica a todos os partícipes, o que se comprova pelo fato de a criação de órgãos transnacionais tem contribuído para a melhor humanização do direito internacional.⁶²⁹

Fato típico a respeito da discussão sobre a transferência internacional de dados pessoais e as regras internas de cada jurisdição pode ser exemplificado pelo caso do governo dos Estados Unidos da América, que, através de seu Departamento de Comércio, anunciou no mês de setembro de 2020 que os downloads do aplicativo TikTok seriam proibidos, tornando ilegal o tráfego de dados deste aplicativo.⁶³⁰ Essa decisão teve por base a segurança nacional dos seus cidadãos, pois, de acordo com o porta-voz do governo, “Partido Comunista Chinês demonstrou os meios e motivos para usar esses aplicativos para ameaçar a segurança nacional, a política externa e a economia dos EUA”.⁶³¹ Em ação judicial, a rede social TikTok relatou que armazena informações dos usuários dos EUA fora da China e garantiu a criação de softwares que auxiliariam o armazenamento os dados de usuário nos EUA separadamente

⁶²⁶ GAIO JÚNIOR, Antônio Pereira. *O consumidor e sua proteção na União Europeia e Mercosul: pesquisa conjuntural como contribuição à política desenvolvimentista de proteção consumerista nos blocos*. Curitiba: Juruá, 2014.

⁶²⁷ BENNETT, Colin. *Regulating privacy, data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992. p. 116-152.

⁶²⁸ HENRY, Michael. *International privacy publicity & personality laws*. London: Butterworths, 2001. p. 5.

⁶²⁹ SHAW, Malcolm N. *International law*. 17. ed. Cambridge: Cambridge University Press, 2017.

⁶³⁰ A determinação passou a valer a partir de 20 de setembro foi alterada em 27 de setembro de 2020. Outras restrições entrariam em vigor em 12 de novembro. UNITED STATES GOVERNMENT. *Executive Order 13943*. Disponível em: <https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency>. Acesso em: 22 fev. 2021.

⁶³¹ U.S. DEPARTMENT OF COMMERCE. *Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States*. Disponível em: <https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect>. Acesso em: 22 fev. 2021.

dos dados de usuário de outros produtos da empresa. Com isso, a Justiça Federal dos Estados Unidos da América emitiu ordem para suspender a eficácia das medidas do governo daquela país, liberando o acesso ao aplicativo, em todo o território.⁶³²

Em sua fundamentação, indica a decisão que a Ordem Executiva utiliza a Lei de Poderes Econômicos de Emergência Internacional (IEEPA) como base legal. Esta Lei permite que o Presidente promulgue regulamentos de emergência relativos ao comércio internacional após declarar uma emergência nacional. Foi o que Donald Trump fez.⁶³³ No entanto, existem duas limitações no próprio IEEPA. Primeiro, a lei não concede ao Presidente a autoridade para regulamentar ou proibir a troca de informações ou materiais informativos ou comunicações pessoais, sendo que o juiz federal entendeu que o conteúdo do aplicativo se qualifica como tal.

É fato que o magistrado indicou que o governo federal forneceu ampla evidência de que a China representa uma ameaça significativa à segurança nacional, mas a evidência específica da ameaça representada pelo aplicativo, bem como de que as proibições seriam a única forma eficaz de lidar com essa ameaça. Como resultado, o TikTok confeccionou acordo judicial em mais de 21 (vinte e uma) ações coletivas sediadas nos Estados Unidos da América, no qual consta a necessidade de se evitar comportamentos que possam comprometer a privacidade do usuário, a menos que divulgue, especificamente, esses comportamentos em sua política de privacidade. Estes comportamentos incluem o armazenamento de informações biométricas, a coleta de dados de GPS e o envio de dados pessoais de usuários dos Estados Unidos da América para fora do país.⁶³⁴

Há informações de processos judiciais similares aos verificados nos Estados Unidos da América no Reino Unido e na Coreia do Sul.⁶³⁵ Em todos eles a questão central diz respeito à transferência de dados com operações de processamento relativas à segurança pública e às atividades de Estado estrangeiro. A esse respeito, conforme como foi verificado no capítulo 2 desta dissertação, a União Europeia identificou que a transferência internacional de dados pessoais aos Estados Unidos da América não detinha a segurança necessária e adequada aos

⁶³² UNITED States District Court. *Civil Action No. 1:20-cv-02658 (CJN)*. Disponível em: https://www.pacermonitor.com/view/W23REIQ/TIKTOK_INC_et_al_v_TRUMP_et_al_dcdce-20-02658_0029.0.pdf?mcid=tGE3TEOA. Acesso em: 22 fev. 2021.

⁶³³ UNITED States Government. *50 U.S. Code CHAPTER 35 – International emergency economic powers*. Disponível em: <https://www.law.cornell.edu/uscode/text/50/chapter-35>. Acesso em: 22 fev. 2021.

⁶³⁴ REUTERS. *ByteDance agrees to \$92 million privacy settlement with U.S. TikTok users*. Disponível em: https://www.reuters.com/article/us-bytedance-tiktok-lawsuit-idUSKBN2AP2O5?utm_campaign=newsletter_-_10032021&utm_medium=email&utm_source=RD+Station. Acesso em: 10 mar. 2021.

⁶³⁵ LEXLATIN. *Os impactos jurídicos no Brasil do processo contra o TikTok no Reino Unido*. Disponível em: <https://br.lexlatin.com/reportagens/os-impactos-juridicos-no-brasil-do-processo-contra-o-tiktok-no-reino-unido>. Acesso em: 23 abr. 2021.

padrões da União.⁶³⁶ De fato, com base nesta análise, é possível concluir que a transferência internacional de dados pessoais aos Estados Unidos da América não cumpria os requisitos básicos de segurança da informação que exigidos pelas normas europeias

E, tendo em conta que também os Estados Unidos da América já entenderam que a transferência internacional de dados merece maior detalhamento e cuidado, é possível identificar que a próxima barreira negocial transfronteiriça esbarará no direito à proteção de dados pessoais de cada país, visto a singularidade e soberania que cada Estado exerce sobre seu território. Cumprirá aos organismos internacionais a pacificação da matéria, identificando uma regulamentação transfronteiriça com os requisitos mínimos para a segurança e transparência que os titulares de dados têm direito.

3.2 Tendências das futuras atuações do Tribunal de Justiça da União Europeia

Com base no que foi até aqui exposto, é possível verificar que a atuação do Tribunal junto às questões relativas à proteção de dados pessoais estará em voga, principalmente, na próxima década. De fato, há diversas questões em aberto que tocam o conceito deste direito, a sua abrangência e quais os requisitos legais e fáticos para sua proteção. No ano de 2020, o Tribunal teve uma vasta discussão sobre o tema. Questões relacionadas sobre o uso de dados pessoais e a segurança nacional dos países ou de comunidades de países serão sempre um tema em voga que merecerá melhor debate na academia e na jurisprudência. Nos itens seguintes, as tendências contemporâneas da jurisprudência do tribunal serão esquematicamente apresentadas e analisadas.

3.2.1 *Privacy International e la Quadrature du Net e outros*

Julgamentos como o do caso C-623/17 (*Privacy International*)⁶³⁷ e C-511/18 (*La Quadrature du Net e outros*)⁶³⁸ reafirmam que o direito da União Europeia proíbe que as legislações nacionais estabeleçam uma obrigação para os fornecedores de serviços de comunicação no sentido de encaminharem dados de localização dos usuários para uma

⁶³⁶ Para melhor análise ver o tópico 3.2.1.3 (Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015) e 3.2.1.6 (Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017) desta Tese.

⁶³⁷ Processo C-623/17. *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e outros*. Julgamento em: 06 outubro 2020.

⁶³⁸ Processo C-511/18. *La Quadrature du Net and Others v Premier ministre e outros*. Julgamento em: 06 outubro 2020.

autoridade pública, que os retenha de forma geral ou indiscriminada, mesmo que esta medida seja fundamentada na finalidade de combate ao crime em geral ou de salvaguarda da segurança nacional. No entanto, em situações em que um Estado-Membro enfrenta uma ameaça grave à segurança nacional e prove ser esta uma razão genuína e presente, poderá ele derogar a obrigação de garantir a confidencialidade dos dados relativos às comunicações eletrônicas, exigindo, por vias legislativas, a conservação geral e indiscriminada desses dados, mesmo que isso ocorra por um período limitado. Tal interferência nos direitos fundamentais deve sempre ser acompanhada por salvaguardas eficazes e ser revisada por um tribunal ou por uma autoridade administrativa independente.

3.2.2 *Processo C-311/18 (Comissário de Proteção de Dados v. Facebook Ireland Ltd e Maximillian Schrems)*

Isso mostra que a segurança nacional e a transferência internacional de dados pessoais serão um tema recorrente nos próximos debates do Tribunal, tendo em vista a recente declaração de nulidade do Acordo Transatlântico, instrumento que autorizava a transferência de dados pessoais de Europa para um país terceiro.⁶³⁹ Essa decisão levantou duas questões. A primeira diz respeito à validade do acordo UE-EUA (*Privacy Shield*), que autorizou a transferência de dados pessoais de indivíduos localizados na União Europeia para os Estados Unidos.

Questionou-se se este instrumento atenderia, de fato, aos requisitos do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), tendo em vista sobretudo os programas de vigilância do governo dos EUA que autorizam as autoridades de segurança pública do país a acessarem e utilizarem dados pessoais importados da Europa União. A segunda questão versa sobre a validade da disposição contratual das “cláusulas-tipo”, aprovadas pela Comissão Europeia como instrumentos adequados e suficientes para a transferência internacional de dados pessoais. Tais cláusulas são aplicadas nos casos em que não haja decisão de adequação emitida pela Comissão da União Europeia em relação ao país que receberá esses dados.

Fato é que, no ano de 2016, o Departamento de Comércio dos Estados Unidos e a Comissão Europeia celebraram o acordo denominado *Privacy Shield* (em português, “Escudo de Segurança”), que estabelecia um conjunto de princípios e salvaguardas a serem garantidos

⁶³⁹ Processo C-311/18. *Comissário de Proteção de Dados v. Facebook Ireland Ltd e Maximillian Schrems*. Julgamento em: 16 julho 2020.

pelas empresas aderentes ao acordo no sentido de possibilitar a transferência de dados pessoais de pessoas físicas localizadas na União Europeia para empresas localizadas nos Estados Unidos.

No entanto, no caso conhecido como *Schrems II*, esse instrumento foi declarado nulo, por não se ter reconhecido a adequação do *Privacy Shield* como base legal idônea para a transferência internacional de dados. Isso porque, de acordo com o entendimento do Tribunal, os programas de vigilância implementados pelo governo dos Estados Unidos representam uma violação desproporcional dos direitos à privacidade e proteção de dados garantidos pelo GDPR. Com efeito, ao não preverem de forma clara as limitações das competências atribuídas aos serviços de informação, os programas de vigilância acabam por permitir aos poderes públicos a realização de excessos, que não se limitam ao estritamente necessário para garantir a segurança nacional, previsto no GDPR.⁶⁴⁰

Em paralelo, o Tribunal analisou quais os elementos devem ser tidos em conta para determinar o caráter adequado do nível de proteção no contexto de uma transferência de dados pessoais para um país terceiro, tudo com base nas cláusulas-padrão de proteção de dados adotadas sob o GDPR. Desde 1987, tais cláusulas são reconhecidas pela Comissão Europeia como um mecanismo válido e adequado para autorizar transferências internacionais de dados, conforme estabelecido na decisão 2010/87.

De acordo com a decisão, as salvaguardas adequadas, os direitos executórios e as medidas judiciais corretivas eficazes devem garantir que os direitos dos titulares, cujos dados pessoais são transferidos para um país terceiro com base em cláusulas de proteção de dados padrão, beneficiem-se de um nível de proteção equivalente ao garantido na União, à luz da Carta Europeia dos Direitos do Homem. Assim, para o efeito da avaliação do nível de proteção proporcionado no contexto dessa transferência, deve-se ter em conta as disposições contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecido na União e o destinatário da transferência estabelecido no país terceiro. Isso no que diz respeito ao possível acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos.

A decisão destaca inclusive a importância de as leis e práticas de um país serem compatíveis com o nível de proteção garantido pela GDPR, uma vez que a não adequação pode resultar em um aumento de custos de transferência de dados (devido a salvaguardas)

⁶⁴⁰ BIGNAMI, Francesca. *Schrems II*: o direito à privacidade e o novo iliberalismo. *VerfBlog*, 2020/7/29.

adicionais a serem adotadas pelo controlador/encarregado) ou, ainda, na impossibilidade de transferência.

Tudo isso mostra que, além de a proteção de dados ter sido gradualmente desconectada do direito de privacidade, tal direito também foi regulamentado em um nível cada vez mais denso e por meio de regimes mais detalhados de proteção. Isso se deve, entre outros fatores, à evolução que o Tribunal efetuou sobre o entendimento das regras de proteção de dados pessoais.

De resto, vale registrar a decisão do Reenvio Prejudicial C-61/19, na qual se dispôs sobre o ônus da prova em casos de discussão sobre o consentimento efetuado por pessoa física, frente à regulação da proteção de dados pessoais.⁶⁴¹ Neste caso, o Tribunal decidiu que (i) o responsável pelo tratamento deve demonstrar que a pessoa em causa consentiu, com um comportamento ativo, no tratamento dos seus dados; (ii) o responsável pelo tratamento deve demonstrar que a pessoa em causa foi informada sobre todas as circunstâncias que envolveram o tratamento, de forma inteligível e facilmente acessível, utilizando uma linguagem clara e simples; e (iii) o método de prestação de informações utilizado pelo responsável pelo tratamento deve permitir que essa pessoa compreenda facilmente as consequências do consentimento, de modo a que seja dado com pleno conhecimento dos factos.⁶⁴²

Veja-se que o Tribunal vai além das definições trazidas ao julgamento do Processo C-40/17 (*Planet49*) e traz luz sobre o conceito de consentimento. A esse respeito, o julgamento afirma que o consentimento não é válido se a caixa de seleção em anexo tiver sido marcada pelo controlador/encarregado de dados antes da assinatura do contrato.⁶⁴³ Já no que se refere ao caráter livre e informado do consentimento, ele não será válido quando os termos do contrato são suscetíveis de induzir o titular dos dados ao erro quanto à possibilidade de celebrar o contrato em causa, mesmo que ele ou ela se recusa a consentir com o tratamento de seus dados.⁶⁴⁴ Assim, a inclusão de condições adicionais (neste caso, o preenchimento de um formulário adicional para recusa do consentimento) conduz à invalidade do consentimento.⁶⁴⁵

⁶⁴¹ Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020.

⁶⁴² Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020. Parágrafo 53.

⁶⁴³ Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020. Parágrafo 52.

⁶⁴⁴ Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020. Parágrafo 41.

⁶⁴⁵ Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020. Parágrafo 45.

O Tribunal atribui, assim, um valor absoluto ao consentimento, quando usado como base legal para o processamento e, conseqüentemente, qualquer restrição ou formalidade pode levar à invalidade deste ato.⁶⁴⁶

Outra situação que merece destaque e será, muito provavelmente, analisada pelo Tribunal nos próximos anos é a saída do Reino Unido da União Europeia, o que ocorreu de forma definitiva e plena em 01 de janeiro de 2021. A Autoridade Nacional de Proteção de Dados Pessoais do Reino Unido publicou guia para elucidar dúvidas e questionamentos sobre a questão, com o intuito de iniciar o processo de separação do Reino Unido.⁶⁴⁷ Na prática, as normas regulatórias da União Europeia não terão mais vigência no território do Reino Unido, inclusive o Regulamento Geral de Proteção de Dados (GDPR). Assim, em solo do Reino Unido, a norma que vigerá sobre o tema em voga será a Data Protection Act de 2018.⁶⁴⁸

O ato intitulado *Data Protection Act* de 2018 (DPA 2018), que complementava e adaptava o Regulamento Europeu ao no Reino Unido, será a principal norma sobre o tópico.⁶⁴⁹

Ao final de 2020, o governo do Reino Unido anunciou a assinatura de Tratado Internacional com a União Europeia, o qual permitirá que os dados pessoais tenham livre fluxo no país, até que sejam adotadas decisões de adequação sobre o assunto. O Tratado em questão tem validade por período não superior a seis meses.⁶⁵⁰ Isso permitirá que empresas e organismos públicos de todos os setores continuem a transitar dados pessoais para e da União Europeia, incluindo agências públicas.

Posteriormente, a União Europeia e o Reino Unido formalizaram o Acordo de Comércio e Cooperação entre a União Europeia e a Comunidade Europeia da Energia Atômica, o Reino Unido da Grã-Bretanha e a Irlanda do Norte.⁶⁵¹ Neste documento, as Partes reconhecem o direito à proteção dos dados pessoais à privacidade, considerando que normas

⁶⁴⁶ Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*. Julgamento em: 11 novembro 2020. Parágrafo 39.

⁶⁴⁷ REINO UNIDO. *UK-EU Trade And Cooperation Agreement*. 2020. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-statement-in-response-to-uk-governments-announcement-on-the-extended-period-for-personal-data-flows-that-will-allow-time-to-complete-the-adequacy-process/>. Acesso em: 19 jan. 2021.

⁶⁴⁸ REINO UNIDO. *Data Protection Act 2018*. Disponível em: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. Acesso em: 19 jan. 2021.

⁶⁴⁹ ISLAM, Sardar M. N. Data protection. In: SHAPIRO, Lauren R.; MARAS, Marie-Helen (org.). *Encyclopedia of Security and Emergency Management*. Springer International Publishing AG. Switzerland, 2019.

⁶⁵⁰ ISLAM, Sardar M. N. Data protection. In: SHAPIRO, Lauren R.; MARAS, Marie-Helen (org.). *Encyclopedia of Security and Emergency Management*. Springer International Publishing AG. Switzerland, 2019.

⁶⁵¹ UNIÃO EUROPEIA. *Documento 22020A1231 (01)*. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01.0014.01.ENG. Acesso em: 03 maio 2021.

sobre esta matéria contribuem para a confiança na economia digital e para o desenvolvimento do comércio. Porém, não se adentra neste tratado sobre conceitos e termos para esta proteção de dados efetiva, o que merecerá Acordo específico sobre o tema.

Isso indica que este o assunto merecerá melhor debate na academia e na jurisprudência para entender os termos desta transferência de dados de forma internacional e quais serão as bases normativas que regerão a matéria.

3.2.3 *Processo 620/19 (Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG)*

No mês de dezembro de 2020, o Tribunal de Justiça publicou importante julgamento sobre a definição de dados pessoais.⁶⁵² No caso, um tribunal nacional alemão considerou que o direito de acesso à informação, exercido com base na lei da liberdade de informação, não era excluído por regras específicas sobre matéria fiscal.

Assim, embora as informações solicitadas estivessem abrangidas pelo sigilo fiscal, o requerente (*D.-HT*) tinha o direito, na qualidade de mandatário da falência, de solicitar à requerida (*J&S Service*) quaisquer informações relativas ao processo de insolvência. Em sua fundamentação, o tribunal alemão observou que o Regulamento Geral de Proteção de Dados não é aplicável no caso em que o processo não diga respeito à dados pessoais relativos a uma pessoa singular, nem ao direito de acesso conferido ao titular dos dados.

No entanto, diante das disposições da União sobre acesso à dados e da possibilidade de inserção no âmbito da GDPR, apresentou-se um questionamento ao sistema europeu no que diz respeito às questões relativas à interpretação do artigo 23, do GDPR. A este respeito, o Tribunal observou que o conceito de informação relativa a pessoas coletivas é distinto do conceito de dados pessoais. O GDPR estabelece regras relativas à proteção de pessoas singulares, mas não abrange os dados relativos a pessoas coletivas. Portanto, a lei alemã se refere, na verdade, não à proteção de dados pessoais de pessoas físicas, mas ao conceito, específico da legislação nacional, de proteção de dados pessoais de pessoas jurídicas.

Nestas condições, as questões prejudiciais não diziam respeito à interpretação de uma disposição do direito da União, mas sim a um conceito de direito nacional sem equivalente na legislação da União. No que diz respeito ao artigo 23, que procura encontrar um equilíbrio justo entre o respeito pelos direitos fundamentais das pessoas singulares afetadas pelo

⁶⁵² Processo 620/19. *Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG*. Julgamento em: 10 dezembro 2020.

processamento de dados e a necessidade de salvaguardar outros interesses legítimos numa sociedade democrática, o Tribunal esclareceu que esta disposição não pode ser lida ignorando o fato de se destinar especificamente a garantir os direitos fundamentais das pessoas singulares. Assim, para o Tribunal uma interpretação das disposições do GDPR, em particular do seu artigo 23, não pode ser realizada da mesma forma no que diz respeito às pessoas singulares e às pessoas coletivas cujo direito à proteção de dados não foi definido pela União.

O Tribunal, assim, concluiu que não era possível considerar que as disposições do GDPR seriam aplicáveis como tal pelo direito nacional, mesmo fora do âmbito deste regulamento, e que, portanto, não havia nenhum interesse manifesto no Tribunal em interpretar essas disposições, a fim de assegurar a sua uniformidade de interpretação.

3.2.4 European Commission v. Kingdom of Spain

Ademais a transposição das Diretivas da União à legislação nacional ainda encontrará discussões a serem analisadas pelo Tribunal. Exemplo disso ocorreu em 25 de fevereiro de 2021, o Tribunal entendeu que a Espanha deveria ser penalizada pela falta de transposição e informação à Comissão da União, tendo em vista a determinação contida na Diretiva 2016/680.⁶⁵³ No processo, o Reino da Espanha informou que estava em curso um processo legislativo para formular as medidas nacionais para cumprimento das obrigações relativas à Diretiva 2016/680, porém não apresentou as medidas no prazo correto.⁶⁵⁴

O Tribunal buscou elastecer o prazo por falta de transposição, vez que advertiu que somente haverá sanções pecuniárias quando o descumprimento persistir até o momento do exame dos fatos pelo Tribunal.⁶⁵⁵ Salientando que, até o momento do julgamento, a Espanha não detinha com suas obrigações como Estado-Membro, o Tribunal fundamentou que a imposição de multa pecuniária é a medida dissuasiva para o cumprimento do Direito da União.⁶⁵⁶

⁶⁵³ A Diretiva 2016/680 refere-se sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

⁶⁵⁴ Processo 658/19. *European Commission v. Kingdom of Spain*. Julgamento em: 25 fevereiro 2021.

⁶⁵⁵ Processo 658/19. *European Commission v. Kingdom of Spain*. Julgamento em: 25 fevereiro 2021. Parágrafo 16 e 17.

⁶⁵⁶ Processo 658/19. *European Commission v. Kingdom of Spain*. Julgamento em: 25 fevereiro 2021. Parágrafo 70.

3.2.5 *Facebook Ireland Limited e outros v. Gegevensbeschermingsautoriteit*

Em 11 de setembro de 2015, o Presidente da Comissão de Privacidade da Bélgica, iniciou um processo contra Facebook Inc., perante o Tribunal nacional da Bélgica. Esse processo diz respeito a alegadas violações das leis de proteção de dados que consistem, nomeadamente, na recolha e utilização ilegais de informações sobre o comportamento de navegação privada dos utilizadores da internet na Bélgica, operação que é realizada através de tecnologias como 'cookies', 'plugins sociais' e pixels.⁶⁵⁷

Em essência, a Autoridade Belga alegou que o Facebook utilizava dessas tecnologias para monitorar e rastrear indivíduos para, então, usar as informações coletadas para traçar o perfil de seu comportamento de navegação e, com base nisso, mostrar aos usuários uma publicidade direcionada, sem informar adequadamente as pessoas em causa ou obter o seu consentimento válido.⁶⁵⁸ Por determinação de 9 de novembro de 2015, o presidente do Tribunal de Primeira Instância de Bruxelas considerou que era competente para conhecer do processo e que o recurso era admissível. Este tribunal também condenou provisoriamente os demandados a cessarem certas atividades relativas aos utilizadores da Internet situados no território belga.⁶⁵⁹

Com a entrada em vigor do GDPR, os réus do processo alegaram que a Autoridade belga havia perdido a competência para intentar a ação, recorrendo ao mecanismo denominado “balcão único” previsto no art. 56 e seguintes, da GDPR.⁶⁶⁰ Após a tramitação de recursos internos, houve a submissão ao Tribunal de Justiça da União Europeia de questões prejudiciais.

Assim, o Tribunal entendeu, à luz do Regulamento Geral de Proteção de Dados, que é permitido que uma autoridade de supervisão de um Estado-Membro intente um processo perante um tribunal nacional por uma alegada violação desse regulamento no que diz respeito ao processamento de dados transfronteiras, mesmo quando a autoridade não é a autoridade supervisora principal no que diz respeito a esse processamento. Basta que os procedimentos de cooperação e consistência do Regulamento sejam devidamente assegurados e que a

⁶⁵⁷ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021.

⁶⁵⁸ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 30.

⁶⁵⁹ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 32.

⁶⁶⁰ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 35.

reclamação principal atinja, primariamente, uma questão local (ou seja do país membro em questão).⁶⁶¹

Foi, assim, assegurado o alinhamento à jurisprudência do Tribunal ao se observar os fundamentos do Processo C-210/16.⁶⁶² Porém, como este caso tratava prioritariamente da Diretiva 95/46, era necessário analisar a nova situação com base no Regulamento 2016/679 – o qual revogou a dita Diretiva.⁶⁶³ Enfim, observou-se na decisão que não é condição prévia para o exercício do poder de uma autoridade nacional de controle que o responsável pelo tratamento tenha um estabelecimento principal ou outro estabelecimento no território do Estado-Membro da autoridade de controle.⁶⁶⁴

Esta decisão traz contornos importantes para as Autoridades Nacionais de Proteção de Dados possam dar seguimento a investigações e ações judiciais contra atos atentatórios à proteção de dados pessoais, principalmente quando se tratar de atividades de tratamento de dados em seus países, possibilitando a efetivação do art. 56 e seguintes, da GDPR.

3.2.6 Conclusão parcial

Com base no exposto, é possível observar que o tema da proteção de dados pessoais merecerá e será analisado pelo Tribunal de Justiça da União Europeia em novas demandas, as quais deverão esclarecer aspectos fundamentais para o melhor entendimento deste direito tão em voga no momento. Verifica-se ainda que o Tribunal foi o principal órgão de manutenção e solidificação dos termos da Diretiva da União e, no momento, se encontra em plena consolidação da GDPR, com o intuito de elucidar, especialmente, as modificações da Regulamentação para a antiga Diretiva.

Cuida-se, portanto, de importante órgão para a temática da proteção de Dados Pessoais, ainda que haja divergências culturais e literárias para outros países, como o caso do Brasil, que poderemos observar no próximo subtópico.

3.3 Ubiquidade do processamento de dados pessoais e as novas fronteiras

⁶⁶¹ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 47.

⁶⁶² Processo 210/16. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contra Wirtschaftsakademie Schleswig-Holstein GmbH*. Julgamento em: 05 junho 2018.

⁶⁶³ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 39.

⁶⁶⁴ Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021. Parágrafo 87.

Marc Langheinrich acredita que a rápida evolução da vigilância inteligente seja impulsionada por cinco principais tendências: (i) uma ampliação qualitativa dos tipos de dados que podem ser coletados, (ii) o aumento quantitativo para a maioria desses tipos de fonte de dados, impulsionado por maior automação, (iii) mais e melhores ferramentas analíticas e de processamento, (iv) a crescente ubiquidade da vigilância como uma ferramenta cotidiana, e (v) a convergência dos sistemas de vigilância.⁶⁶⁵

De fato, tecnologia de vigilância foi muito além das gravações de vídeo e áudio. Os tipos de fontes de dados podem incluir: dados de posicionamento da triangulação de dispositivos móveis telefones entre torres de celular ou da relação vizinha para acesso de pontos Wi-Fi; leituras remotas de temperatura de câmeras infravermelhas; dados sobre localização de veículos, coletados a partir de câmeras de tráfego ou sistemas eletrônicos de cobrança de pedágio; a conteúdo de e-mails e mensagens instantâneas de redes sociais, além dos chamados programas de “controle dos pais”.⁶⁶⁶

Todo este acervo de vigilância e controle de dados pessoais serve de fundamento para se questionar a respeito da real efetividade da legislação para controle do acesso, uso e transferência de dados pessoais. Afinal, com a ubiquidade do processamento de dados pessoais pelo globo e a crescente e veloz eficácia que a internet detém sobre as vidas pessoais torna-se difícil – senão impossível – de se analisar quem, quando, quais e como o controlador/encarregado de dados pessoais tem sobre a vida de alguém.⁶⁶⁷

Exemplo desta situação pode ser observado na impossibilidade de identificação a respeito da qual a origem, quais dados pessoais e de quais pessoas foram afetados no maior vazamento de dados pessoais registrados do Brasil.⁶⁶⁸ Neste caso, identificado em 2021, uma empresa de segurança da informação (PSafe) verificou a venda de dados pessoais de mais de

⁶⁶⁵ LANGHEINRICH, Marc; FINN, Rachel; COROAMA, Vlad; WRIGHT, David. Quo vadis smart surveillance? How smart technologies combine and challenge democratic oversight. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul (org.). *Reloading data protection*. Inglaterra: Springer, 2014. p. 151-182.
p. 154.

⁶⁶⁶ MCDERMOTT, Yvonne. *Conceptualising the right to data protection in an era of Big Data*. Big Data & Society, jun. 2017.

⁶⁶⁷ LANGHEINRICH, Marc; FINN, Rachel; COROAMA, Vlad; WRIGHT, David. Quo vadis smart surveillance? How smart technologies combine and challenge democratic oversight. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul (org.). *Reloading data protection*. Inglaterra: Springer, 2014. p. 151-182.
p. 155.

⁶⁶⁸ Para maiores informações ver: TECMUNDO. *Tudo sobre o vazamento de dados de 223 milhões de brasileiros*. Disponível em: <https://www.tecmundo.com.br/software/210168-tudo-vazamento-dados-223-milhoes-de-brasileiros.htm>. Acesso em: 17 fev. 2021.

223 milhões de pessoas residentes no Brasil.⁶⁶⁹ Inicialmente, foi relatado o vazamento de dados pessoais como nome, sexo, data de nascimento; posteriormente, anunciou-se que o vazamento também atingia questões ligadas a dados sensíveis e completos do cidadão, tais como endereços, números de telefones, dados de veículos (placa, número de chassi), detalhes sobre imposto de renda de pessoas físicas, fotos de rosto, benefícios sociais, escolaridade e dados financeiros (tais como score de crédito, cheques sem fundo e renda). Até o momento, as autoridades nacionais nem mesmo encontraram os responsáveis por este vazamento, quanto menos identificaram qual(is) a(s) origem(ns) deste vazamento, o que impossibilita a correta remediação da situação e da aplicação de penas e a reparação dos danos dos prejudicados.⁶⁷⁰

O próprio direito ao esquecimento, tratado nos casos *Google Spain* e *Salvatore Manni*, se consubstancia em uma tentativa de se frear a hiperexposição da pessoa natural frente ao processamento em massa de dados pessoais e a perduração das notícias e fatos na internet. Consubstanciado no julgado pelo Tribunal da União, tal direito não foi recepcionado no direito brasileiro, tendo em vista o precedente do Supremo Tribunal Federal, no qual se firmou a seguinte tese:

Tema 786, da Repercussão Geral: ‘É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais – especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral – e as expressas e específicas previsões legais nos âmbitos penal e cível.’⁶⁷¹

Esta decisão do Supremo Tribunal Federal já nasce com atraso dogmático, vez que a própria Lei Geral de Proteção de Dados permite solicitar a exclusão de dados pessoais ao controlador de dados⁶⁷², direito que inclusive consta do Regulamento Europeu de Proteção de

⁶⁶⁹ CNN BRASIL. *'O estrago está feito', diz diretor de empresa que detectou vazamentos de dados*. Disponível em: <https://www.cnnbrasil.com.br/business/2021/02/20/o-estrago-esta-feito-diz-diretor-de-empresa-que-detectou-vazamentos-de-dados>. Acesso em: 22 fev. 2021.

⁶⁷⁰ Para maiores informações ver: PROCONSP. *Vazamento de dados pessoais*. Disponível em: <https://www.procon.sp.gov.br/vazamento-de-dados-pessoais/>. Acesso em: 17 fev. 2021.

⁶⁷¹ SUPREMO TRIBUNAL FEDERAL. *RE 1010606/RJ*. Ministro Relator: Dias Toffoli. Sessão realizada por videoconferência – Resolução 672/2020/STF). Disponível em: <http://stf.jus.br/portal/jurisprudencia/Repercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>. Acesso em: 18 fev. 2021.

⁶⁷² Para a União Europeia, o direito ao “apagamento de dados” é sinônimo de “direito a ser esquecido”, conforme artigo 17º, da GDPR. Porém, há divergências na academia sobre a vinculação do direito à desindexação e o direito ao esquecimento. Para este autor, o direito ao esquecimento é englobado pelo direito a ser esquecido e o direito à desindexação. Para maior debate sobre o tema, ver: SARTOR, G. *The right to be forgotten: balancing interests in the flux of time*. International Journal of Law and Information Technology. Spring 2016. V. 24. P. 72–98.

Dados.⁶⁷³ Ressalte-se ainda que esta mesma Corte reconheceu a existência do direito fundamental à proteção de dados em conhecido precedente (ADI 6390). Assim, considerando que o julgamento da Corte Constitucional brasileira trata da impossibilidade de haver a aplicação do direito ao esquecimento – seja qual ele for – quando houver publicação em meios de comunicação social analógicos ou digitais, seria mais coerente se a Corte houvesse restringido a impossibilidade de oposição do direito ao esquecimento quando o fim desta publicação for, exclusivamente, para fins jornalísticos – o que inclusive consta na LGPD. Não foi isso o que ocorreu e agora cabe aos operadores do direito entenderem e interpretarem esta Repercussão Geral ao caso concreto.

Desta feita, verifica-se que o processamento de dados pessoais na rede da informação possui diversos aspectos e interessantes debates a respeito do alcance e das possibilidades de interação com diversos outros direitos já existentes na sociedade atual.⁶⁷⁴ Nesse sentido, um aspecto interessante acerca do processamento de dados pessoais que merece destaque é a chamado coleta de dados “voluntários”, que ocorre por meio do aumento de dispositivos móveis e das redes de mídia social, por meio dos quais, embora não tenham ciência inequívoca, os usuários concedem seu consentimento para a coleta massiva, inclusive de dados de terceiros.⁶⁷⁵

Conforme foi observado por diversos casos julgados pelo Tribunal e pelas revelações trazidas dos vazamentos de dados por Eduard Snowden, a vigilância em massa é vista como um meio de prevenir crimes, entre eles, ataques terroristas e ciberataques, e a segurança nacional é alçada a finalidade máxima do Estado para a vigilância de dados, a vigilância online e a vigilância de comunicações.⁶⁷⁶

Esta gama de ações pode ser categorizada por meio da noção de “vigilância líquida”, de acordo com a qual a vigilância está se tornando cada vez mais difundida na sociedade, do que se conclui que o mundo está entrando em uma era de inteligência ambiental, na qual todas as coisas fabricadas poderão ser conectadas para comunicar e contribuir para a onipresença da

⁶⁷³ Para maior debate sobre o fato de que apesar da existência legal do direito ao esquecimento (ou exclusão), há críticas sobre as diversas possibilidades de exceções e perdurações dos dados pessoais pelos controladores, diante da dificuldade e abrangência dos termos da GDPR. Ver: KOOPS, Bert-Jaap. *The trouble with european data protection law*. International Data Privacy Law. Forthcoming, Tilburg Law School Research Paper, 2015. v. 4.

⁶⁷⁴ MCDERMOTT, Yvonne. *Conceptualising the right to data protection in an era of Big Data*. Big Data & Society, jun. 2017.

⁶⁷⁵ LYON, David. *Surveillance, Snowden, and big data: capacities, consequences, critique*. Big Data & Society, jul. 2014.

⁶⁷⁶ MCDERMOTT, Yvonne. *Conceptualising the right to data protection in an era of Big Data*. Big Data & Society, jun. 2017.

vigilância.⁶⁷⁷ No âmbito do tratamento de dados pessoais na internet, o caso *Lindqvist* identificou que a exposição de dados pessoais de terceiros em páginas da Web deve ser concebido como tratamento de dados pessoais, o que pode trazer consequências para as redes sociais, mundialmente utilizadas.⁶⁷⁸ Com base neste pressuposto, a transmissão, disseminação ou disponibilização de dados pessoais em páginas da web devem ser considerados como operações de tratamento. Assim, a exposição de fotos com nome e a data de nascimento de terceiro, o que é corriqueiramente utilizado nas redes sociais, deve ser considerado como uma operação de tratamento de dados pessoais.

O Tribunal inclusive considerou que a publicação na internet desses dados faz com que eles sejam acessíveis a um número indefinido de pessoas, e por isso essa operação não pode ser considerada como uma exceção do tratamento a atividades exercida no âmbito da vida privada ou familiar.⁶⁷⁹ Contudo, uma questão que não foi respondida pela jurisprudência da União Europeia diz respeito à responsabilidade sobre a exposição de dados pessoais em redes sociais: essa responsabilidade é apenas daquele que a transmitiu ou a empresa que organiza e coordena a rede social também é responsável na qualidade de controlador/encarregado?⁶⁸⁰

No Brasil, o julgamento do REsp nº 1859665 serviu como paradigma acerca do tema da obrigação das redes sociais em fornecer dados pessoais de todos os usuários que compartilharam conteúdo falso.⁶⁸¹ No caso, o Superior Tribunal de Justiça, deu provimento ao Recurso Especial do *Facebook Brasil*, afastando assim a obrigação desta empresa em fornecer os dados de todos os usuários que compartilharam um vídeo com informação considerada falsa – nela, um homem afirma ter comprado um salgado repleto de larvas em uma padaria de

⁶⁷⁷ LANGHEINRICH, Marc; FINN, Rachel; COROAMA, Vlad; WRIGHT, David. Quo vadis smart surveillance? How smart technologies combine and challenge democratic oversight. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul (org.). *Reloading data protection*. Inglaterra: Springer, 2014. p. 151-182.

p. 154.

⁶⁷⁸ LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015. p. 68.

⁶⁷⁹ RALLO, Artemi; MARTÍNES, Ricard. Data protection, social networks and online mass media. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 407-430. p. 416.

⁶⁸⁰ Neste tópico, importante trazer à luz a Opinião 5/2009 do *Article 29 Working Party* que em seu posicionamento dispõe que a exceção da vida privada só será aplicável quando o espaço na rede social for configurado de forma que seja visível apenas para um grupo de amigos expressamente autorizado. Caso contrário, as circunstâncias do caso em voga ocorreriam por completo. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf. Acesso em: 17 mar. 2021.

⁶⁸¹ SUPERIOR TRIBUNAL DE JUSTIÇA. *REsp 1859665*. Julgamento em: 09 março 2021. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201859665>. Acesso em: 11 mar. 2021.

Santa Catarina. Os Ministros do STJ consideraram que, apesar de o artigo 22, do Marco Civil da Internet, dispor que a parte interessada poderá, com o propósito de reunir provas em processo, requerer judicialmente o fornecimento de registros de conexão ou de registros de acesso a aplicações da internet, esta mesma legislação traz especiais salvaguardas à privacidade e aos dados pessoais de usuários da internet. Nas palavras do Relator:

Se é certo afirmar que o usuário das redes sociais pode livremente reivindicar seu direito fundamental de expressão, também é correto sustentar que a sua liberdade encontrará limites nos direitos da personalidade de outrem, sob pena de abuso em sua autonomia, já que nenhum direito é absoluto, por maior que seja a sua posição de preferência, especialmente se se tratar de danos a outros direitos de elevada importância.⁶⁸²

Desta forma, a quebra de sigilo de todos os usuários que compartilharam o vídeo não seria proporcional em relação ao dano sofrido pelo requerente. Salientou-se, ainda, no julgamento que não houve provas da ilicitude da conduta dos usuários por simplesmente compartilharem o vídeo.⁶⁸³ É possível identificar, assim, que o STJ está conduzindo sua jurisprudência para a identificação da proteção de dados pessoais como meio para a proteção da privacidade e da liberdade de expressão do indivíduo. Caminho este similar ao identificado no STF, com o julgamento da Repercussão Geral Tema 786. Neste mesmo sentido, observa-se que tanto o STJ quanto o STF têm conduzido seus julgamentos em situações de colisão entre a liberdade de expressão e a privacidade, ou a proteção de dados pessoais, fazendo prevalecer o primeiro direito, sobretudo em destaque sobre o direito à memória coletiva.⁶⁸⁴

A próxima “fronteira” que a academia e a jurisprudência terão de enfrentar diz respeito à aplicabilidade das legislações de proteção da privacidade aos danos concretos relacionados à proteção de dados pessoais, o que pode definir a real exigibilidade e exequibilidade.⁶⁸⁵ Há aqui uma real dificuldade em se estabelecer a relação direta entre os danos à proteção de dados pessoais e a produção de danos financeiros ou físicos tangíveis.

⁶⁸² SUPERIOR TRIBUNAL DE JUSTIÇA. *REsp 1859665*. Julgamento em: 09 março 2021. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201859665>. Acesso em: 11 mar. 2021.

⁶⁸³ Verifica-se uma relação direta com o julgamento do caso *Ministério Fiscal* pelo Tribunal da União, conforme verificado no capítulo 2, desta tese.

⁶⁸⁴ A Ministra Carmen Lucia trouxe ao debate o “direito de lembrar, como adverso ao direito ao esquecimento em seu voto: “Num país de triste desmemória como o nosso, discutir o direito ao esquecimento como direito fundamental, de alguém poder impor silêncio ou segredo de fato ou ato que pode ser de interesse público, seria um desaforo jurídico para a minha geração. A minha geração lutou pelo direito de lembrar” (SUPREMO TRIBUNAL FEDERAL. *RE 1010606/RJ*. Ministro Relator: Dias Toffoli. Sessão realizada por videoconferência – Resolução 672/2020/STF). Disponível em: <http://stf.jus.br/portal/jurisprudencia/Repercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>. Acesso em: 18 fev. 2021).

⁶⁸⁵ CITRON, Danielle Keats; SOLOVE, Daniel J. *Privacy harms*. GWU Legal Studies Research Paper, 2021. v. 11.

Quanto a isso, em solo americano, a Suprema Corte dos Estados Unidos da América teve de enfrentar a questão ao julgar o caso conhecido como *Spokeo v. Robins*, no qual concluiu que os tribunais americanos poderiam exigir do demandante que provasse o seu dano real e efetivo para a concessão de uma indenização.⁶⁸⁶ Isso porque a violação à proteção de dados pessoais detém características especulativas e hipotéticas, em sua grande maioria de casos, baseado em questões subjetivas, visto que muitas violações envolvem promessas quebradas ou expectativas frustradas sobre como os dados das pessoas são coletados, usados, divulgados, ou tratados.⁶⁸⁷

As consequências posteriores dessas práticas são frequentemente difíceis de determinar. Pessoas podem ser inundadas com publicidade indesejada ou spam de e-mail; suas expectativas podem ser traídas, resultando no compartilhamento de seus dados com terceiros que podem usá-los em formas prejudiciais.⁶⁸⁸ É inclusive possível que a lesão decorrente destes atos seja caracterizada como mero dissabor do cotidiano quando vista isoladamente. Porém, quando se considera a multiplicação dessas ações por centenas ou milhares de empresas, o dano se torna deveras relevante.⁶⁸⁹ Danielle Citron e Daniel Solove resumiram as fundamentações dos tribunais americanos para negar as indenizações relativas à danos à privacidade e proteção de dados pessoais, quais sejam:

(1) adicionar a exigência de dano físico ou concreto para legitimar a ação judicial; (2) exigir prova real e efetiva do dano para obter indenizações, minando assim o objetivo das disposições legais; (3) exigir danos reais e efetivos, mesmo quando a legislação não dispõe deste requisito; e (4) adoção de concepções restritivas sobre o dano para excluir diversos tipos de indenizações.⁶⁹⁰

⁶⁸⁶ “Isso não significa, entretanto, que o risco de dano real não possa satisfazer esse requisito. Ver, por exemplo, *Clapper v. Amnesty Int’l USA*, 568 U. S. _____. A violação de um direito processual concedido por lei pode ser suficiente em algumas circunstâncias para constituir um dano de fato; em tal caso, o querelante não precisa alegar nenhum dano adicional além do identificado pelo Congresso, ver *Federal Election Comm’n v. Akins*, 524 U. S. 11-25. Este Tribunal não toma posição sobre a exatidão da conclusão final do Nono Circuito, mas esses princípios gerais demonstram duas coisas: que o Congresso claramente procurou conter a disseminação de informações falsas, adotando procedimentos concebidos para diminuir esse risco e que *Robins* não pode satisfazer as demandas de Artigo III, alegando uma violação processual pura” (US SUPREME COURT. *Spokeo, Inc. v. Robins*, 578 U.S. (2016). Julgamento em: 16 maio 2016. Disponível em: <https://supreme.justia.com/cases/federal/us/578/13-1339/>. Acesso em: 26 fev. 2021. Tradução livre).

⁶⁸⁷ CITRON, Danielle Keats. *The privacy policymaking of state attorneys general*. Notre Dame L., 2016. v. 2. p. 747-816.

⁶⁸⁸ CITRON, Danielle Keats; SOLOVE, Daniel J. *Privacy harms*. GWU Legal Studies Research Paper, 2021. v. 11. p. 3.

⁶⁸⁹ Para um melhor debate sobre danos à dados pessoais e a capacidade de exigibilidade destes, ver: CITRON, Danielle Keats; SOLOVE, Daniel J. *Privacy harms*. GWU Legal Studies Research Paper, 2021. v. 11.

⁶⁹⁰ CITRON, Danielle Keats; SOLOVE, Daniel J. *Privacy harms*. GWU Legal Studies Research Paper, 2021. v. 11. p. 16. Tradução livre.

Disto decorre que será necessária uma maior atuação das autoridades nacionais e dos institutos de proteção de dados pessoais privados para a segurança deste direito de forma difusa, coletiva e, até mesmo, individual homogênea, possibilitando demonstrar aos Tribunais a capacidade difundida que esta violação pode tomar para a sociedade. Por isso mesmo, outro aspecto que merecerá debate na academia diz respeito a se a legislação sobre proteção de dados pessoais será de fato um direito concreto ao cidadão, o qual poderá utilizá-lo na prática e nas Cortes. Como exemplo, há uma possibilidade de “vazamento” de dados pessoais através de um mecanismo denominado “data scraping”,⁶⁹¹ qual seja, uma maneira eficaz de obter dados (pessoais ou não) de páginas da internet, aplicativos e redes sociais, sem, necessariamente, haver uma violação da segurança desta página, uma vez que a medida pode apenas compilar dados que estejam disponíveis ao público em geral.

No ano de 2021, duas redes sociais tiveram dados pessoais de seus usuários expostos de forma ilegal,⁶⁹² sendo que seus relatórios de segurança informaram que não se tratava de vazamento de dados pessoais a ocasionar um incidente de segurança.⁶⁹³ Contudo, os casos estão em análise pelas Autoridades de Proteção de Dados.⁶⁹⁴ As empresas relatam que não se trata de uma violação ao direito de proteção de dados pessoais e da privacidade de seus usuários, uma vez que os dados pessoais retirados estavam disponíveis de forma pública. Haveria, neste sentido, eventual responsabilidade do ator que colocou os dados em circulação, não da plataforma. Aqui novamente adentra-se na questão da exequibilidade deste direito,

⁶⁹¹ Podemos identificar “data scraping” como uma técnica computacional, na qual extrai-se dados de uma saída, legível somente para humanos, proveniente de um serviço ou aplicativo (HIRSCHEY, Jeffrey Kenneth. Symbiotic relationships: pragmatic acceptance of data scraping. *Berkeley Technology Law Journal*, v. 29, p. 897-927, 2014).

⁶⁹² THE HACK. *Vazamento' do Clubhouse é só mais uma raspagem de dados públicos*. 2021. Disponível em: <https://olhardigital.com.br/2021/04/07/seguranca/facebook-atribui-recente-vazamento-de-dados-de-usuarios-a-scraping/>. Acesso em: 16 abr. 2021; OLHAR Digital. *Facebook atribui recente vazamento de dados de usuários a “scraping”*. 2021. Disponível em: <https://olhardigital.com.br/2021/04/07/seguranca/facebook-atribui-recente-vazamento-de-dados-de-usuarios-a-scraping/>. Acesso em: 16 abr. 2021.

⁶⁹³ ANPD. *Comunicação de incidentes de segurança*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em: 16 abr. 2021.

⁶⁹⁴ Veja-se que 03 (três) órgãos estatais abriram investigação contra este fato: 1) Irlanda: DATA Protection Commission. *DPC launches inquiry into Facebook in relation to a collated dataset of Facebook user personal data made available on the internet*. 2021. Disponível em: <https://www.dataprotection.ie/en/news-media/press-releases/dpc-launches-inquiry-facebook-relation-collated-dataset-facebook-user-personal-data-made-available>. Acesso em: 20 abr. 2021; 2) Colômbia: INDUSTRIA y Comercio. *Superindustria inicia investigación contra Facebook ante posibles fallas de seguridad*. 2021. Disponível em: https://www.sic.gov.co/slider/superindustria-inicia-investigaci%C3%B3n-contra-facebook-ante-posibles-fallas-de-seguridad?utm_campaign=newsletter_-_20042021&utm_medium=email&utm_source=RD+Station. Acesso em: 20 abr. 2021; 3) Itália: GARANTE per la Protezione dei Dati Personali. *Furto di dati da Facebook: il garante chiede al social network di adottare misure per limitare i rischi e avverte che l'utilizzo dei dati provenienti dalla violazione è illecito. Utenti invitati a prestare particolare attenzione a possibili anomalie sui propri cellulari*. 2021. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9572143?utm_campaign=newsletter_-_20042021&utm_medium=email&utm_source=RD+Station. Acesso em: 20 abr. 2021.

sendo certo que há capacidades técnicas além do imaginável do ser humano médio, os quais podem facilitar ou dificultar o acesso ao direito à proteção de dados pessoais.⁶⁹⁵

É questionável se o direito à proteção de dados pessoais será, de fato, um direito exequível em situações como as narradas, tendo em vista a exposição universal dos dados pessoais e a capacidade imensurável de processamento dos dados pessoais pela era da Big Data. Caberá à dogmática e à jurisprudência estabelecer as possibilidades e balizas da proteção deste direito. Certo é que, hoje, nem mesmo a jurisprudência do Tribunal de Justiça da União Europeia, objeto da análise exaustiva deste trabalho, oferece esses parâmetros para a avaliação e solução deste problema.

3.4 Proteção de dados pessoais um direito fundamental?

Ao confundir o exercício do direito à privacidade (art. 7º) com o direito à proteção de dados pessoais (art. 8º) em diversos julgados analisados neste trabalho, a jurisprudência do Tribunal de Justiça pouco facilitou a interpretação deste tópico. É fato, porém, que em casos de extrema preocupação para a população daquela União, a Corte identificou o direito à proteção de dados pessoais como base para a liberdade dos cidadãos.⁶⁹⁶ Por outro lado, também existem regras de proteção de dados e casos que parecem candidatos menos óbvios para a proteção dos direitos fundamentais, pois protegem mais interesses comuns a outros direitos. Por exemplo, em algumas ocasiões, o Tribunal analisou a pertinência do direito à proteção de dados com direitos à propriedade privada e o acesso a obras protegidas por direitos autorais.⁶⁹⁷ Ocorre, portanto, uma colisão com os demais direitos insculpidos na Carta, os quais detêm caráter de direito fundamental junto à União Europeia, destacando o papel fundamental deste direito.

De fato, existem pelo menos certas disposições dos instrumentos de proteção de dados pessoais e certos casos que intuitivamente não se qualificam como (parte de) um direito

⁶⁹⁵ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

⁶⁹⁶ Como referência, podemos identificar os julgados dos casos: Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e.o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014; Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015; e Processo C-311/18. *Comissário de Proteção de Dados v. Facebook Ireland Ltd e Maximillian Schrems*. Julgamento em: 16 julho 2020.

⁶⁹⁷ Como referência, podemos identificar os julgados dos casos: Como referência, podemos identificar os julgados dos casos; e Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012.

fundamental.⁶⁹⁸ Nessa linha, Bart Van der Sloot afirma que, embora algumas regras de proteção de dados pessoais e alguns casos pareçam se adequar à ideia de direitos humanos fundamentais, há casos de proteção de dados que não.⁶⁹⁹ O autor afirma que são registradas três abordagens para a questão de saber se o direito à proteção de dados pessoais é um direito fundamental.⁷⁰⁰ Em primeiro lugar, pode-se argumentar que, embora a proteção de dados não se encaixe no âmbito clássico dos direitos fundamentais, uma interpretação mais moderna deve ser adotada, disso decorrendo que a proteção de dados seria vista como um direito fundamental autônomo.⁷⁰¹

Em uma segunda abordagem pode-se tentar distinguir entre diferentes aspectos das regras de proteção de dados e atividades de processamento de dados, do que resulta que certas regras e casos seriam tratados sob o manto do direito fundamental, enquanto outros podem ser tratados como parte das regras orientadas para a regulação do mercado e como proteção dos direitos do consumidor.⁷⁰² Enfim, terceiro, pode-se argumentar que as regras de proteção de dados, como um todo, não devem ser tratadas como parte de um direito fundamental autônomo. Na visão de Van der Sloot, a terceira opção é a mais plausível:

a proteção de dados não é realmente um direito fundamental. Isto parece que é a resposta mais lógica para a questão de saber se a proteção de dados é um direito fundamental propriamente dito. Como argumentado, o escopo de 'dados pessoais' não se encaixa no clássico âmbito dos direitos humanos; o tipo de regras que facilitam o processamento de dados em vez de restringir ou proibir, parece divergir da finalidade típica dos instrumentos de direitos humanos; e o papel das Autoridades de Proteção de Dados e a regulamentação detalhada de quase todos os aspectos de as atividades de processamento de dados em um regulamento em toda a União Europeia parecem mais semelhantes à ideia de regulamentação de mercado do que a proteção dos direitos humanos. Mas, pode-se perguntar, e as regras de proteção de dados e casos que parecem proteger aspectos fundamentais,

⁶⁹⁸ Vale registrar que sob o direito à privacidade, uma série de interesses triviais também são fornecidos proteção. Veja neste ponto. VAN DER SLOOT, Bart. The practical and theoretical problems with 'balancing': Delfi, Coty and the redundancy of the human rights framework. *Maastricht Journal of European and Comparative Law*, v. 3, 2016.

⁶⁹⁹ VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30.

⁷⁰⁰ VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30.

⁷⁰¹ VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30. p. 27.

⁷⁰² VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30. p. 28.

como o caso *Digital Rights Ireland* e as regras sobre o processamento de dados sensíveis? Como foi enfatizado, processar dados pessoais confidenciais e outros dados que tenham um impacto significativo sobre o interesse do indivíduo já estão protegidos no âmbito dos direitos humanos, nomeadamente sob o direito à privacidade. O mesmo pode ser dito sobre vigilância em massa, retenção de dados de escutas de fio em grande escala; eles geralmente constituem uma violação de ambos o sigilo de comunicação e direito à vida privada do cidadão. Portanto, omitindo o direito de a proteção de dados do quadro de direitos fundamentais não deixaria esses interesses desprotegido.⁷⁰³

Sob este aspecto, podemos concluir que o direito à proteção de dados pessoais merece destaque na legislação, principalmente, da União Europeia. Ademais, em virtude de sua potencial colisão com os demais direitos insculpidos na Carta, este direito mereceu destaque ao lado de direitos fundamentais, como a liberdade de ir e vir, a liberdade religiosa e a liberdade de expressão. Por exemplo, o escopo do conceito de “dados pessoais” não se baseia na questão de saber se interesses pessoais significativos estão em jogo, mas simplesmente no critério objetivo de se alguém pode ser identificado ou individualizado com base nos dados. Sob este aspecto a proteção incide sobre o dado bruto (tratamento), não sobre a pessoa. Vale aqui inclusive frisar que a LGPD define dados pessoais sensíveis de forma taxativa (art. 5º, inc. II). Porém, a própria lei dispõe que dados não sensíveis devem ser tratados com base nas salvaguardas de um dado sensível se este tratamento causar dano ao titular (“§ 1º aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica”).⁷⁰⁴ Isso não só mostra que o principal aspecto que a lei deveria tratar é a segurança do tratamento do dado pessoal, não se o dado é sensível ou não, mas também indica que o tema principal do direito e da regulação deve ser o prejuízo para o titular decorrente do uso (tratamento) do dado pelo controlador/operador, não qual tipo de dado está em jogo.

Isso não quer dizer que a proteção de dados não seja um direito. Trata-se, de fato, de um direito sensível da pessoa física ter o conhecimento e a possibilidade de autodispor seus dados pessoais da forma que melhor lhe convier. E aqui verificamos que, de acordo com o histórico definido no Capítulo 2 desta dissertação, o direito à proteção de dados pessoais

⁷⁰³ VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30. p. 29. Tradução livre.

⁷⁰⁴ Veja-se que a GDPR (Considerando 51) não estabelece conceito estático sobre “dados sensíveis”, inclusive o Tribunal da União assim se pronunciou: “À luz da finalidade da diretiva, a expressão «dados relativos à saúde», constante do seu artigo 8.º, n.º 1, deve ser interpretada de forma ampla, de modo a incluir informações relativas a todos os aspetos, tanto físicos como mentais, da saúde de um Individual” (Processo C-101/01. *Bodil Lindqvist*. Julgamento em: 06 novembro 2003. Parágrafo 50).

surge como meio da pessoa física utilizar-se de meios legais para a proteger seus bens pessoais contra a invasão do Estado e do privado em sua privacidade, o que alcançou níveis globais e hipersensíveis com a consolidação da sociedade da informação. Fato é, o tempo fez com que a configuração deste direito seja alterada e, da mesma forma, o futuro indicará qual será o verdadeiro papel deste direito na sociedade contemporânea.

Hoje é possível prever que, tendo em vista a ligação precípua deste direito com a automação da vida humana, a partir da retenção de dados de forma abrangente e da utilização de técnicas de difícil compressão à sociedade, o direito à proteção de dados pessoais ainda não alcançou o seu devido espaço na era moderna.⁷⁰⁵ O tempo e a reflexão servirão de processo de ajustamento do direito na sociedade do século XXI.⁷⁰⁶ Processo que foi iniciado no continente europeu, sobretudo com a atuação do Tribunal de Justiça da União Europeia, mas que hoje é desenvolvido mundo afora, por tribunais (como o STF) e estudos (como o aqui desenvolvido) que procuram aprofundar a compreensão e a análise de um tema que moldará nosso futuro, assim como a jurisprudência do Tribunal moldou, em grande parte, o nosso presente.

⁷⁰⁵ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

⁷⁰⁶ OST, François. *O tempo do direito*. Lisboa: Piaget, 1999.

CONCLUSÃO

Esta pesquisa surgiu com o objetivo investigar de que forma o conceito do direito fundamental da proteção de dados pessoais foi construído e aplicado no âmbito da União Europeia. Ao acompanhar cronologicamente o desenvolvimento do direito, conforme disposto no capítulo 2, torna-se evidente que seu relacionamento com o direito à privacidade não está totalmente claro. A interpretação demonstra que embora os conceitos de privacidade e proteção de dados estejam intimamente ligados, suas finalidades são diversas, ocasionando a possibilidade de se agregar valor a estes direitos quando relacionados no caso concreto. Mas não só. O direito à proteção de dados não é derivado apenas da privacidade e não se relaciona apenas com este direito. Três fatores distintivos foram indicados para apoiar o argumento.

Em primeiro lugar, nem todo processamento de dados é capaz de interferir com privacidade, mesmo que ele possa ser concebido de maneira a violar as regras de proteção de dados contidas no artigo 8º, da Carta.⁷⁰⁷ Em segundo lugar, o direito à proteção de dados serve a vários interesses que vão além da privacidade, incluindo direitos sobre a propriedade intelectual, privacidade, liberdade de expressão, dignidade humana, devido processo legal.⁷⁰⁸ Em terceiro lugar, o artigo 8º, da Carta prevê expressamente direitos relacionados à autodeterminação informacional, como acesso a dados, sua retificação e consentimento com o processamento. **Embora esses direitos possam ser incidentalmente derivados do direito à vida privada, seu reconhecimento dependeria no contexto da situação sem qualquer garantia explícita na legislação.**⁷⁰⁹ Finalmente, o modelo de opacidade-transparência fornece uma resposta abrangente quanto à coexistência dos artigos 7º e 8º, da Carta. Privacidade pode ser entendida como uma ferramenta de opacidade, visando a não interferência na vida privada. A proteção de dados pessoais, como ferramenta de transparência, visa canalizar o uso legítimo de poder. A proteção de dados pessoais é, portanto, percebida como uma ferramenta

⁷⁰⁷ Como exemplo, podemos indicar o Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019, refere-se a importante jurisprudência acerca do direito ao esquecimento e a regulamentação acerca da proteção de dados pessoais.

⁷⁰⁸ Exemplos destes direitos podem ser encontrados em: 1) Direito de Proteção de Dados e Direito à Propriedade (Processo C 275/09. *Promusicae*. Julgamento: 17 março 2011); 2) Direito de Proteção de Dados e Direito à Liberdade de Expressão (Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014); 3) Direito de Proteção de Dados e Direito ao Esquecimento (Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricultura di Lecce v. Salvatore Manni. Relator M. Ilešič*. Julgamento em: 09 março 2017).

⁷⁰⁹ O caso paradigmático *Google Spain* traz a clareza sobre a vinculação a autodeterminação informacional como principal função da proteção de dados pessoais, com a consequente análise da quebra da privacidade dos cidadãos (Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014).

processual que permite o processamento como meio, mas estabelece suas limitações através de medidas de proteção de dados pessoais.⁷¹⁰

A evolução legislativa na área de proteção de dados também sugere uma mudança no sentido entender o artigo 8º, como um direito autônomo. O pacote de reforma preparado para proteção de dados, composto pelo RGPD e pela proposta de Regulamento relativo à Privacidade e Comunicações Eletrônicas, garante o direito à proteção de dados pessoais em particular, implicando seu status autônomo.⁷¹¹ O artigo 8º, da Carta Europeia, desempenha, portanto, um papel indispensável na execução deste direito.

E incluir um direito autônomo à proteção de dados pessoais na Carta parece ser uma decisão fundamentada por parte dos legisladores da União Europeia, considerando a extensão do processamento de dados pessoais no mundo moderno.⁷¹² Mas para utilizar a proteção oferecida por um direito autônomo a dados pessoais proteção, as conclusões anteriores teriam que ser implementadas na prática. Descobrir se esse era o caso é o objetivo desta pesquisa, a qual enfoca as perspectivas sobre o direito à proteção de dados pessoais e se o Tribunal permite que ele permaneça autônomo à privacidade.

Verificou-se, a esse respeito, que a jurisprudência do Tribunal varia no que diz respeito ao valor agregado da proteção de dados pessoais a depender do caso analisado. Porém, essa jurisprudência indica uma linha contínua: a essência da proteção de dados pessoais não pode ser limitada a apenas um único interesse de liberdade ou igualdade; em vez disso, envolve potencialmente todos os outros direitos fundamentais. Em sentido similar, Daniel J. Solove desenvolveu a classificação de danos potenciais que podem ser causados pelo tratamento de dados pessoais. Esta classificação inclui a perda de vida, a perda da liberdade de expressão, infrações à propriedade, violações de privacidade e negação do devido processo legal.⁷¹³ A jurisprudência do Tribunal se alinha com à estas conclusões. Como podemos analisar pela leitura do capítulo 2, a proteção de dados pessoais serve como meio para infrações aos demais direitos fundamentais serem protegidos pelo Poder Judiciário.

⁷¹⁰ POSCHER, Ralf. *Artificial intelligence and the right to data protection*. Max Planck Institute for the Study of Crime, Security and Law, n. 2021/03, 2021.

⁷¹¹ VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. *In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44. p. 3.

⁷¹² MANERO SALVADOR, A. El valor jurídico de la Carta de derechos fundamentales. De Niza a Lisboa. *In: FERNANDEZ LIESA, C.; DIAZ BARRADO, C. El tratado de Lisboa*. Análisis y perspectivas. Instituto universitario de estudios internacionales y europeos Francisco de Vitoria, Dykinson, 2009. p. 113-133.

⁷¹³ SOLOVE, Daniel J. *Nothing to hide: the false tradeoff between privacy and security*. Yale University Press, 2011. p. 158.

De fato, foi demonstrado que a proteção de dados pessoais deve servir como base para que o cidadão da União Europeia tenha acesso a este direito e o mercado-comum possa realizar o tratamento de dados pessoais de forma regular. Neste contexto, a transposição internacional de dados pessoais é tema de importância extrema ao verificar que é a União Europeia que deve garantir as bases mínimas de segurança aos seus cidadãos às interferências estrangeiras, seja de países externos, seja de empresas situadas em países terceiros, o que demonstra que a proteção de dados pessoais é tema primordial para a garantia da democracia e liberdade dos cidadãos da União. A esse respeito, o Tribunal foi inovador ao garantir a possibilidade de utilização do direito ao esquecimento pelos cidadãos, o que é um dos objetos centrais da autodeterminação informacional. Ainda em consonância com a autodeterminação informacional, foi possível observar o cuidado do Tribunal com o acesso aos dados pessoais, perfazendo julgados importantes para análise dos requisitos básicos deste direito.

Outrossim, foi possível observar a utilização da proteção de dados pessoais para a consecução de direitos patrimoniais, como direitos autorais, direitos do consumidor, direito à acesso a informações públicas. Quanto a este ponto, parece que o Tribunal de Justiça não aceita a compreensão do direito à proteção de dados pessoais como um direito autônomo. Independentemente da ênfase colocada na proteção de dados, o artigo 8º dificilmente pode ser percebido como um direito autônomo sem que o Tribunal confirme seu escopo. De fato, na abordagem do Tribunal parece a proteção de dados um direito-meio (instrumento), o qual serve como requisito analítico e prático para a consecução dos demais direitos fundamentais descritos na Carta.

Nessa toada, concluiu-se que a constitucionalização do direito à proteção de dados na Carta da União representa uma evolução positiva, pois a proteção de dados tem um objetivo preciso bastante diferente de questões ligadas exclusivamente à privacidade. A proteção de dados se apresenta como um direito formal, que visa organizar o processamento justo de dados por atores públicos e privados. Nesse sentido, o Tribunal utiliza o direito à proteção de dados pessoais para a proteção de direitos fundamentais, o que demonstra que este direito pode ser definido como um mecanismo normativo para que as pessoas naturais tenham o poder de se opor às invasões de sua liberdade, de sua dignidade, de sua privacidade.

Neste sentido, no julgamento do caso *Ministerio Fiscal*, o Tribunal enfatizou, prioritariamente, que ao verificar uma potencial infração ao direito à proteção de dados pessoais, a jurisdição deve utilizar-se do teste de proporcionalidade, para verificar se a intervenção no direito é suficiente a proporcionar a recusa ao ato ocorrido, ou se a infração é

proporcional ao ato interventivo.⁷¹⁴ Atráves da interpretação da Carta, especialmente após a introdução do artigo 8.º, o Tribunal criou a possibilidade do aperfeiçoamento da proteção de dados para o direito capaz de conduzir a sociedade para uma maior transparência e cuidado, especialmente, no meio tecnológico.

Nessa linha, ao utilizar o direito à proteção de dados como um direito-meio (instrumento), não apenas para a consecução do direito à privacidade, o Tribunal reforça o papel inovador e primordial deste direito. Uma conceituação consistente do direito à proteção de dados serve ao propósito de justificar a dicotomia formal entre privacidade e proteção de dados introduzida pela Carta, que ainda são muitas vezes confundidos. Justamente por isso, através da jurisprudência do Tribunal, podemos identificar o aumento da legitimidade do quadro de proteção de dados na União Europeia, ao definir explicitamente este direito como um direito fundamental à União. Mais importante ainda, isso leva ao reconhecimento da autonomia conceitual da proteção de dados pessoais e seus vínculos com o avanço da tecnologia de computação e, portanto, com a sociedade moderna poderia promover o desenvolvimento do Artigo 8º em todo o seu potencial.

Por tudo isso, o trabalho cumpre seu papel em identificar as bases utilizadas na jurisprudência do Tribunal de Justiça da União Europeia sobre o direito à proteção de dados pessoais, assim como sua ligação para com o direito à privacidade, a qual não constitui o cerne deste direito, mas um importante aliado na busca por sua consecução.

⁷¹⁴ Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018.

REFERÊNCIAS

AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy: the new landscape*. Massachusetts; Cambridge: MIT Press, 2001.

ALEXY, Robert. Direitos fundamentais no estado constitucional democrático. Para a relação entre direitos do homem, direitos fundamentais, democracia e jurisdição constitucional. *Revista da Faculdade de Direito da UFRGS*, v. 16, p. 203-214, 1999.

ALEXY, Robert. *Teoría dos derechos fundamentales*. Tradução de Ernésto Garzón Valdés. Madrid: Centro de Estudios Constitucionales, 1997.

ALMEIDA, J. C. M de. *Direito comunitário. A ordem jurídica comunitária. As liberdades fundamentais na CEE*. Lisboa: Centro de Publicações do Ministério da Justiça, 1985.

ALSENOY, Brendan; KOEKKOEK, Marieke. *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'*. International Data Privacy Law, 2015.

ALTER, K. J. Explaining National Court Acceptance of European Court Jurisprudence: a critical evaluation of theories of legal integration. In: SLAUGHTER, A. M.; SWEET, A. S.; WEILER, J. (org.). *The European Court and National Courts – doctrine and jurisprudence: Legal Change in Its Social Context*. London: Hart Publishing, 1998. p. 227-252.

ANDRADE, Norberto Nuno Gomes de. Right to personal identity: the challenges of ambient intelligence and the need for a new legal conceptualization. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; LEENES, Ronald. *Computers, privacy and data protection: an element of choice*. London: Springer Dordrecht Heidelberg, 2011. p. 65-100.

APLIN, Tanya. *Copyright law in the digital society*. Oxford: Hart, 2005.

ARNBAK, Axel M. *Securing private communications: protecting private communications security in EU law: fundamental rights, functional value chains and market incentives*. Wolters Kluwer. Kluwer Law International, 2016.

AXHAMN, Johan. *Hyperlinking: Case C-466/12 Svensson and Others and Its Impact On Swedish Copyright Law*. Europarättslig Tidskrift, 2015. p. 847-865.

BARATTA, R. Complexity of EU law in the domestic implementing process. *Theory Pract Legis*, n. 3, v. 2, p. 293-308, 2014.

BARBIER DE LA SERRE, Eric. Procedural justice in the European Community case law concerning the rights of the defence: essentialist and instrumental trends. *European Public Law*, v. 12, n. 2, p. 225-250, 2006.

BARCELOS, Paulo. Vitangelo Moscarda's Syndrome. The Charter of Fundamental Rights and European Constitutionalization. In: ANGELIS, Gabriele de; BARCELOS, Paulo (ed.). *The long quest for identity: political identity and fundamental rights protection in the European Union*. Lisbon philosophical studies uses of language in interdisciplinary fields. Pieterlen: Peter Lang, Bern, 2013. v. 4.

BENEVIDES, Isabella Almeida de Sá e; PEREIRA, Raissa Pose. Os direitos fundamentais: perspectiva da União Europeia. *Revista do Programa de Direito da União Europeia*, Rio de Janeiro, v. 6, p. 49-66, 2016.

BENNETT, Colin. *Regulating privacy, data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992. p. 116-152.

BERGKAMP, Lucas. *EU data protection policy: the privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy*. *Computer Law & Security Review*, 2002. v. 18. p. 31-47.

BIGNAMI, Francesca. *Schrems II: o direito à privacidade e o novo iliberalismo*. VerfBlog, 2020/7/29.

BIGNAMI, Francesca. *The case for tolerant constitutional patriotism: the right to privacy before the European Courts*. *Cornell International Law Journal*, 2008.

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

BLANKE, Hermann-Josef. The protection of fundamental rights in Europe. In: BLANKE, Hermann-Josef; MANGIAMELI, Stelio (org.). *The European Union after Lisbon: constitutional basis, economic order and external action*. Berlin: Springer, 2012. p. 159-232.

BLUME, Peter. The myths pertaining to the proposed general data protection regulation. *International Data Privacy Law*, v. 4, n. 4, p. 269-273, 2014.

BOEHM, F. *Information sharing and data protection in the area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU-level*. Springer Science & Business Media, 2011.

BOEHM, Franziska; COLE, Mark D. *Data retention after the judgement of the Court of Justice of the European Union*. Wayback Machine, 2014.

BONAVIDES, Paulo. *Curso de direito constitucional*. 4. ed. São Paulo: Malheiros, 1993.

BORGESIUS, Frederik; STEENBRUGGEN, Wilfred. *The right to communications confidentiality in Europe: protecting trust, privacy, and freedom of expression*. SSRN Electronic Journal, 2018.

BRKAN, Maja. The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's Constitutional Reasoning. *German Law Journal*, v. 20, n. 6, p. 864-883, 2018.

BUXBAUM, Hannah L. Class actions, conflict and the global economy. *Indiana Journal of Global Legal Studies*, v. 21, n. 2, p. 585-597, 2014.

CAMERON, Iain. *Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Law, Department of Law*. Common market law review. v. 54, n. 5, p. 1467-1495, 2017.

CARRERA, S.; MITSILEGAS, V. (org.). *Constitutionalising the Security Union: effectiveness, rule of law and rights in countering terrorism and crime*. Brussels: Centre For European Policy Studies, 2017.

CASELLA, Paulo Borba. O papel da Comissão de Comércio do Mercosul: o Tribunal do Mercosul disfarçado? In: MERCADANTE, Araminta de Azevedo; MAGALHÃES, José Carlos de (coord.). *Solução e prevenção de litígios internacionais*. Porto Alegre: Livraria do Advogado, 1999. v. II.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido R. *Teoria geral do processo*. 31. ed. São Paulo: Malheiros, 2015.

CITRON, Danielle Keats. *The privacy policymaking of state attorneys general*. Notre Dame L., 2016. v. 2. p. 747-816.

CITRON, Danielle Keats; SOLOVE, Daniel J. *Privacy harms*. GWU Legal Studies Research Paper, 2021. v. 11.

CLASSEN, Claus Dieter. *Joined Cases C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk*. Common Market Law Review, Issue 5, 2004. v. 41. p. 1377-1385.

COMISSÃO Europeia. *Recomendação 81/679/CEE de 29 de julho de 1981 relativa à Convenção do Conselho da Europa para a proteção de pessoas no que diz respeito ao tratamento automático de dados pessoais*. 1981. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31981H0679&from=PT>. Acesso em: 19 jan. 2021.

COMMITTEE of Ministers. Resolution (73) 22 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (1973). Disponível em: <http://www.legislationline.org/documents/id/6498>. Acesso em: 24 mar. 2021.

COPPEL, Philip Q. C. *Information rights: a practitioner's guide to data protection, Freedom of Information and other information rights*. 5. ed. Oxford: Hart, 2020. v. 1.

DE BÚRCA, G. After the EU charter of fundamental rights: the Court of Justice as a human rights adjudicator? *Maastricht Journal of European and Comparative Law*, v. 20, n. 2, p. 168-184, 2013.

DEITOS, Marc Antoni. A adesão da União Europeia à Convenção Europeia dos Direitos Humanos: rumo a uma quarta camada de proteção dos direitos humanos. *Direitos Fundamentais & Justiça*, ano 7, n. 24, p. 113-133, jul./set. 2013.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *EJLL*, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ERDROS, David. *From the scylla of restriction to the charybdis of license? exploring the present and future scope of the ‘special purposes’ freedom of expression shield in european data protection*. Cambridge: Faculty of Law Research Paper, 2015. v. 20. p. 119-154.

EUROPEAN Data Protection Board. *Parecer 5/2019 sobre a interação entre a Diretiva Privacidade Eletrónica e o RGPD, particularmente em matéria de competência, atribuições e poderes das autoridades de proteção de dados*. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-privacy_pt. Acesso em: 18 jan. 2021.

EUROPEAN Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2014. p. 16. Disponível em: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. Acesso em 8 jan. 2021.

FERNANDES, Rodrigo; SANTOS, Rafael Padilha dos. Transnacionalidade e os novos rumos do Estado e do Direito. *Revista Eletrônica Direito e Política*, Itajaí, v. 9, n. 1, 1º quadrimestre 2014.

FERNANDES, Victor Oliveira. *Regulação de serviços over-the-top (OTT) e pós-convergência tecnológica: uma análise do regime jurídico setorial de serviços OTT de voz nos EUA e no Brasil*. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2018.

FERRAZ JÚNIOR, Tércio Sampaio. *Introdução ao estudo do direito: técnica, decisão, dominação*. 10. ed. São Paulo: Atlas, 2018.

FILGUEIRAS, Sofia Pereira. Aspectos legais do *marketing* em mundos virtuais. *Revista da FDUP*, p. 461-525, 2008.

FISS, Owen M. *A ironia da liberdade de expressão: estado, regulação e diversidade na esfera pública*. Tradução e prefácio de Gustavo Binenbojm e Caio Mário da Silva Pereira Neto. Rio de Janeiro: Renovar, 2015.

FLEISCHER, P. *Reflecting on the right to be forgotten*. Blog do Google na Europa. Disponível em: <https://blog.google/around-the-globe/google-europe/reflecting-right-be-forgotten/>. Acesso em: 7 jan. 2021.

FOUAD, Y. *Reikwijdte van het Europese dataproctierecht na Google Spanje: wat is de territoriale werkingssfeer en wordt eenieder beschermd?* 2015. Dissertação (Mestrado) – Institute for Information Law. University of Amsterdam, 2015 (Âmbito da lei europeia de proteção de dados após Google Espanha: qual é o território escopo e todos estão protegidos?).

FUSTER, Gloria González. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2014.

GAIO JÚNIOR, Antônio Pereira. *O consumidor e sua proteção na União Europeia e Mercosul: pesquisa conjuntural como contribuição à política desenvolvimentista de proteção consumerista nos blocos*. Curitiba: Juruá, 2014.

GELLMAN, Robert. Fair information practices: a basic history. *SSRN Electronic Journal*, 2017.

GLOBOCNIK, Jure. *The right to be forgotten is taking shape: CJEU judgments in GC and others (C-136/17) and Google v CNIL (C-507/17)*. Oxford: GRUR International, 2020. v. 69. p. 380-388.

GOMES, José Caramelo. *Lições de direito da União Europeia*. Coimbra: Almedina, 2009.

GONÇALVES, Victor Hugo Pereira. *Inclusão digital como direito fundamental*. São Paulo: Delfos, 2012.

GONZÁLEZ FUSTER, Gloria. *The emergence of personal data protection as a fundamental right of the EU*. Springer, 2014. v. 16.

GONZÁLEZ FUSTER, Gloria; GELLERT, Raphaël. *The fundamental right of data protection in the European Union: in search of an uncharted right*. *International Review of Law, Computers & Technology*, 2012. p. 73-82.

GOOGLE. *Removing Content from Google', Google*. Disponível em: <https://developers.google.com/search/docs/advanced/crawling/remove-information>. Acesso em: 26 mar. 2021.

GOOGLE. *Search removal request under data protection law in Europe*. Disponível em: https://support.google.com/legal/contact/lr_eudpa?product=websearch. Acesso em: 26 mar. 2021.

GRAGL, Paul. The accession of the European Union to the European Convention on Human Rights. *Modern Studies in European Law*, v. 39, 2013.

GROS-VERHEYDE, N. Une Charte à valeur juridique variable. *Europolitique*, n. 3407, 2007.

GUIMARÃES, Guilherme Cintra. *Global technology and legal theory: transnational constitutionalism. Google and the European Union*. New York: Routledge, 2019.

HENRY, Michael. *International privacy publicity & personality laws*. London: Butterworths, 2001.

HERT, P. The right to protection of personal data. Incapable of autonomous standing in the basic eu constituting documents?. *Utrecht Journal of International and European Law*, v. 31, n. 80, 2015. p. 1-4.

HERT, P.; GUTWIRTH, S. Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul; NOUWT, Sjaak; TERWANGNE, Cécile de (org.). *Reinventing data protection?*. Springer, 2009. p. 3-44.

HIJMANS, H.; SCIROCCO, A. *Shortcomings in EU Data protection in the third and the second pillars can the Lisbon Treaty be expected to help*. *Common Market Law Review*, 2009. v. 46. n. 5. p. 1485-1525.

HIJMANS, Hielke. *The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU*. Dissertation. University of Amsterdam, Amsterdam, 2016.

HILDEBRANDT, Mireille. *Law for computer scientists and other folk*. United Kingdom: Oxford University Press, 2010.

HIRSCHEY, Jeffrey Kenneth. Symbiotic relationships: pragmatic acceptance of data scraping. *Berkeley Technology Law Journal*, v. 29, p. 897-927, 2014.

HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, p. 65-98, 2019.

HUGENHOLTZ, P. Bernt; VAN VELZE, Sam C. *Communication to a new public? Three reasons why EU copyright law can do without a 'new public'*. *International Review of Intellectual Property and Competition*, 2016. p. 797-816.

IGLEZAKIS, Ioannis. *The right to be forgotten in the Google Spain Case (Case C-131/12): a clear victory for data protection or an obstacle for the internet?.* Aristotle University of Thessaloniki-Law, Economic and Political Sciences, 2014.

IRION, Kristina. A special regard: the Court of Justice and the fundamental rights to privacy and data protection. In: FABER, Ulrich; FELDHOFF Kerstin; NEBE, Katja; SCHMIDT, Kristina; WAßER, Ursula (org.). *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion*. Baden-Baden: Nomos, 2016. p. 873-890.

ISAAK, J.; HANNA, M. J. *User data privacy: Facebook, Cambridge analytica, and privacy protection*. *Computer*, v. 51, n. 8, p. 56-59, Aug. 2018.

ISLAM, Sardar M. N. Data protection. In: SHAPIRO, Lauren R.; MARAS, Marie-Helen (org.). *Encyclopedia of Security and Emergency Management*. Springer International Publishing AG. Switzerland, 2019.

JACQUÉ, Jean Paul. *Droit institutionnel de l'Union Européene*. 4. ed. Paris: Dalloz, 2006.

JACQUES, Sabine; HEMPEL, Felix. The right to be forgotten in the UK: a fragile balance? In: WERRO, Franz (org.). *The right to be forgotten. a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2020. p. 195-222.

JAECKEL, Liv. *The duty to protect fundamental rights in the european community*. United Kingdom: Oxford Studies in European Law Review, 2003.

KARGOPOULOS, Alexandros-Ioannis. *ECHR and the CJEU. Competing, overlapping, or supplementary competences?* European criminal law and human rights. Issue 3/2015. 2015. p. 96-100.

KĘDZIOR, Magdalena. *GDPR and beyond – a year of changes in the data protection landscape of the European Union.* ERA Forum, 2019. v. 19. p. 505-509.

KOKOTT, Juliane; SOBOTTA, Christoph. *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR.* International Data Privacy Law, 2013. p. 222-228.

KOOPS, Bert-Jaap. *The trouble with european data protection law.* International Data Privacy Law. Forthcoming, Tilburg Law School Research Paper, 2015. v. 4.

KOSTA, Vasiliki. *Fundamental rights in EU internal market legislation.* Oregon: Oxford and Portland, 2018.

KOSTELNY JR., Albert J. *Emerging data protection in Europe: community law through the cases.* Fordham International Law Journal, v. 1, Issue 1, p. 71-75, 1997.

KUNDERA, Milan. *A insustentável leveza do ser.* São Paulo: Companhia das Letras, 2008. Edição de bolso.

KUNER, Christopher. *Beyond Safe Harbor: European data Protection Law and Electronic Commerce.* *The International Lawyer*, n. 1, p. 79-88, 2001.

KUNER, Christopher. *The Court of Justice of the EU judgment on data protection and internet search engines: current issues and future challenges.* SSRN Electronic Journal, 2014.

LANGHEINRICH, Marc; FINN, Rachel; COROAMA, Vlad; WRIGHT, David. *Quo vadis smart surveillance? How smart technologies combine and challenge democratic oversight.* In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul (org.). *Reloading data protection.* Inglaterra: Springer, 2014. p. 151-182.

LAURSEN, Finn. *The founding treaties of the European Union and their reform.* Oxford Research Encyclopedia of Politics, 2016. p. 1-28.

LAURSEN, Finn. *The treaty of Nice: the inadequate preparation of enlargement.* In: LAURSEN, Finn. *Designing the European Union From Paris to Lisbon.* Palgrave Studies in European Union Politics, 2012. p. 196-216.

LENAERTS, Koen; GUTIÉRREZ-FONS, José Antonio. *The place of the Charter in the EU constitutional edifice.* In: PEERS, Steve; HERVEY, Tamara; KENNER Jeff; WARD (org.). *The EU Charter of fundamental rights: a commentary.* Hart Publishing, 2014. p. 1559-1594.

LEONARDI, Marcel. *Tutela e privacidade na Internet.* São Paulo: Saraiva, 2011.

LÉVY, Pierre. *As tecnologias da inteligência: o futuro do pensamento na era informática.* Lisboa: Instituto Piaget, 1994.

LISBOA, Roberto Senise. A inviolabilidade de correspondência na Internet. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto. *Direito & Internet: aspectos jurídicos relevantes*. Bauru: Edipro, 2001.

LYNSKEY, Orla. *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*. *International and Comparative Law, Quarterly*, 2014. p. 569-597.

LYNSKEY, Orla. From market-making tool to fundamental right: the role of the Court of Justice in data protection's identity crisis. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 59-84.

LYNSKEY, Orla. *The foundations of EU data protection law*. Oxford: Oxford University Press, 2015.

LYON, David. *Surveillance, Snowden, and big data: capacities, consequences, critique*. *Big Data & Society*, jul. 2014.

MAGNOLI, Demétrio. *União Europeia: história e geopolítica*. 3. ed. São Paulo: Moderna, 2007.

MANCINI, Federico G. *The making of a Constitution for Europe*. *Common Market Law Review*, 1989. p. 595-614.

MANERO SALVADOR, A. El valor jurídico de la Carta de derechos fundamentales. De Niza a Lisboa. In: FERNANDEZ LIESA, C.; DIAZ BARRADO, C. *El tratado de Lisboa. Análisis y perspectivas*. Instituto universitario de estudios internacionales y europeos Francisco de Vitoria, Dykinson, 2009. p. 113-133.

MASING, Johannes. Assessing the CJEU's "Google Decision". A tentative first approach. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 435-456.

MAYER-SCHÖNBERGER, Viktor. *Generational development of data protection in Europe*. *Technology and privacy: the new landscape*, 1997. p. 219-241.

MCDERMOTT, Yvonne. *Conceptualising the right to data protection in an era of Big Data*. *Big Data & Society*, jun. 2017.

MOURA RAMOS, Rui Manuel de. *Estudos de direito internacional privado e de direito processual civil internacional II*. Coimbra: Coimbra Editora, 2008.

MOURA RAMOS, Rui. O sistema jurisdicional da União Europeia. O presente e o futuro. *Revista de Estudos Europeus*, n. 2, 2007.

NADER, Paulo. *Introdução ao estudo do direito*. 15. ed. Rio de Janeiro: Forense, 1997.

NEWMAN, Abraham L. *Protectors of privacy: regulating personal data in the global economy*. Ithaca; London: Cornell University Press, 2008.

OST, François. *O tempo do direito*. Lisboa: Piaget, 1999.

PATO, Alexia. *Jurisdiction and cross-border collective redress: a european private international law perspective*. Oxford: Hart Publishing, 2019.

PEGUERA, Miquel. The right to be forgotten in the European Union. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, 2020. p. 487-502.

PEREIRA, Alexandre L. D. The influence of human rights and basic rights in other fields of private law: intellectual property. In: TRSTENJAK, Verica; WEINGERL, Petra (org.). *The influence of human rights and basic rights in private law*. Springer, 2015. p. 523-533.

PESCATORE, Pierre. *O recurso prejudicial do artigo 177 do Tratado CEE e a cooperação do tribunal com as jurisdições nacionais*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 1986.

PETKOVA, B.; BOEHM, F. Profiling and the essence of the right to data protection. In: SELINGER, E.; POLONETSKY, J.; TENE, O. (org.). *The Cambridge Handbook of Consumer Privacy*. Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2018. p. 285-300.

PIOVESAN, Flávia. *Direitos humanos e justiça internacional: um estudo comparativo dos sistemas regionais europeu, interamericano e africano*. 9. ed. rev., atual. e ampl. São Paulo: Saraiva, 2019.

PLATTEN, N. Background to and history of the directive. In: BAINBRIDGE, D. *EC data protection directive*. London: Butterworths, 1996. p. 13-32.

POLAKIEWICZ, Jörg. Profiling – the Council of Europe’s Contribution. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 367-377.

POLČÁK, Radim; KASL, František; MÍŠEK, Jakub. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *National report: Czech Republic. Ius Comparatum – Global Studies in Comparative Law*. Suíça: Springer, 2020. p. 115-158.

POSCHER, Ralf. *Artificial intelligence and the right to data protection*. Max Planck Institute for the Study of Crime, Security and Law, n. 2021/03, 2021.

POSCHER, Ralf. The right to data protection. In: MILLER, R. (org.). *Privacy and power: a transatlantic dialogue in the shadow of the NSA-Affair*. Cambridge: Cambridge University Press, 2017. p. 129-142.

POST, Robert C. *Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere*. Faculty Scholarship Series, 2018.

POST, Robert C. Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. *Duke Law Journal*, v. 67, p. 981-1072, 2017.

POWLES, Julia. *The case that won't be forgotten*. Chicago: Loyola University Chicago Law Journal, 2015. v. 47. p. 583-615.

QUERMONNE, Jean-Louis. *Le système politique de l'Union Européenne*. France: Montchrestien, 2001.

RALLO, Artemi; MARTÍNES, Ricard. Data protection, social networks and online mass media. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul; POULLET, Yves (org.). *European data protection: coming of age*. London: Springer, 2003. p. 407-430.

REINO UNIDO. *Data Protection Act 2018*. Disponível em: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. Acesso em: 19 jan. 2021.

REUTERS. *ByteDance agrees to \$92 million privacy settlement with U.S. TikTok users*. Disponível em: https://www.reuters.com/article/us-bytedance-tiktok-lawsuit-idUSKBN2AP2O5?utm_campaign=newsletter_-_10032021&utm_medium=email&utm_source=RD+Station. Acesso em: 10 mar. 2021.

RINGE, Julie. *The burden of proof in anti-discrimination proceedings*. A focus on Belgium, France and Ireland. *European Equality Law Review*, 2019. n. 2.

ROBINSON, Nehemiah. *The Universal Declaration of Human Rights: its origin, significance, application, and interpretation*. New York: World Jewish Congress, 1958.

RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÁ, Stefano. *La società sorvegliata*. Milano: Feltrinelli, 2002. Prefácio à edição italiana de David Lyon.

ROUSSEAU, Charles. *Principes de droit international public*. RCADI, 1958.

ROUSSEAU, Charles. *Principes généraux du droit international public*. Paris: Pédone, 1958. v. I.

ROUVROY, A.; POULLET, Y. The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: GUTWIRTH, S.; POULLET, Y.; HERT, P.; TERWANGNE, C.; NOUWT, S. (org.). *Reinventing Data Protection?* Dordrecht: Springer, 2009.

RUBINSTEIN, Ira; LEE, Ronald D.; SCHWARTZ, Paul M. Data mining and internet profiling: emerging regulatory and technological approaches. *University of Chicago Law Review*, v. 75, p. 261, 2008.

RUITER, Joep; WARNIER, Martijn. Privacy regulations for cloud computing: compliance and implementation in theory and practice. In: *Computers, privacy and data protection: an element of choice*. London: Springer Dordrecht Heidelberg, 2011. p. 387-402.

SARTOR, G. *The right to be forgotten: balancing interests in the flux of time*. International Journal of Law and Information Technology. Spring 2016. V. 24. P. 72–98.

SCACIA, Gino. Proportionality and the balancing of rights in the Case-law of European Courts. *Rivista di Diritto Pubblico Italiano, Comparato, Europeo*, fev. 2019.

SCHEPEL, Harm. Reconstructing constitutionalization: law and politics in the European Court of Justice. *Oxford Journal of Legal Studies*, v. 20, n. 3, p. 457-468, 2000.

SCHWARZE, Jürgen. Judicial review in EC law: some reflections on the origins and the actual legal situation. *The International and Comparative Law Quarterly*, v. 51, n. 1, p. 17-33, 2002.

SEGUELA, Ana de Bustos. Métodos de información. *Los documentos del Tribunal de Justicia de la Unión Europea*, Madrid, v. 3, n. 11-12, p. 54-59, maio/jul. 1996.

SHAW, Malcolm N. *International law*. 17. ed. Cambridge: Cambridge University Press, 2017.

SILVA, Lídia Loureiro da. *Globalização das redes de comunicação: uma reflexão sobre as implicações cognitivas e sociais*. Biblioteca online de ciência da comunicação. 1999. Disponível em: http://www.bocc.ubi.pt/_esp/autor.php?codautor=63. Acesso em: 22 fev. 2021.

SOBRINO HEREDIA, José Manuel. El sistema jurisdiccional el el proyecto de Tratado constitucional de la Unión Europea. *Revista Derecho Comunitário Europeo*, ano 3, v. 16, p. 993-1040, 2003.

SOLOVE, Daniel J. *Nothing to hide: the false tradeoff between privacy and security*. Yale University Press, 2011.

SOLOVE, Daniel J. *Understanding privacy*. Cambridge: Harvard University Press, 2008.

SOLOVE, Daniel J.; SCHWARTZ, Paul M. *Information privacy law*. 7. ed. New York: Wolters Kluwer, 2021.

SOUZA, Carlos Affonso Pereira. Responsabilidade civil dos provedores de acesso e aplicações de internet: evolução jurisprudencial e os impactos da Lei nº 12.965/2014 (Marco Civil da Internet). In: LEITE, George Salomão; LEMOS, Ronaldo (org.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 791-816.

STARR-DEELEN, Donna; BART, Deelen. *The European Court of Justice as a Federator*. Publius, v. 26, n. 4, p. 81-97, 1996.

STELZER, Joana. O fenômeno da transnacionalização da dimensão jurídica. In: CRUZ, Paulo Márcio; STELZER, Joana (org.). *Direito e transnacionalidade*. Curitiba: Juruá, 2009. p. 15-54.

STOCO, Rui. Proteção da imagem *versus* liberdade de informação. *Revista da Escola da Magistratura Federal da 2ª Região – EMARF – TRF 2ª Região*, Rio de Janeiro, v. 8, n. 1, mar. 2007.

STORY, Jonathan. The origins, launching and consequences of ‘1992’ and the euro. *In: WEBBER, D.; FORT, B. (org.). Regional integration in Europe and East Asia: convergence or divergence?* London: Routledge, 2006. p. 85-108.

SUPERIOR TRIBUNAL DE JUSTIÇA. *REsp 1859665*. Julgamento em: 09 março 2021. Disponível em:

<https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201859665>. Acesso em: 11 mar. 2021.

SUPREMO TRIBUNAL FEDERAL. *RE 1010606/RJ*. Ministro Relator: Dias Toffoli. Sessão realizada por videoconferência - Resolução 672/2020/STF). Disponível em:

<http://stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>. Acesso em: 18 fev. 2021.

SUPREMO TRIBUNAL FEDERAL. *ADI 6387*. Relatora Min. Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em 04 setembro 202

SWEET, Alec Stone. Constitutional dialogues in the european community. *In: SLAUGHTER, Anne-Marie; SWEET, Alec Stone; WEILER, J. H. H. (org.). The European Court and National Courts – doctrine and jurisprudence. Legal Change in Its Social Context.* Oxford: Hart Publishing, 1998. p. 305-330.

TRIBUNAL de Justiça da União Europeia. *Opinião 2/13*. Publicada em: 18 dezembro 2014. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140180en.pdf>. Acesso em: 24 mar. 2021.

TRIBUNAL de Justiça da União Europeia. *Press Release n° 31/17*. Luxemburgo, 2017. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170031en.pdf>. Acesso em: 11 jan. 2021.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Processo *Costello-Roberts v. the United Kingdom*. Caso n. 13134/87. Julgamento em 25 março 1995.

TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey, PA: IGI Global, 2019.

TZANOU, Maria. *Personal data protection and legal developments in the European Union*. Hershey: Information Science Reference, 2020.

TZANOU, Maria. *The fundamental right to data protection: normative value in the context of Counter-Terrorism Surveillance*. Oregon: Oxford and Portland, 2017.

U.S. SUPREME COURT. *Katz v. United States*, 389 U.S. 347. 1967. Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/>. Acesso em: 01 abr. 2021.

UNIÃO EUROPEIA. Artigo 100º B. *Ato Único Europeu*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:11986U/TXT&from=PT>. Acesso em: 19 fev. 2021.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*. 06/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 30 nov. 2020.

UNIÃO EUROPEIA. *Diretiva (EU) 2020/1828 do Parlamento europeu*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020L1828&from=EN>. Acesso em: 25 jan. 2021.

UNIÃO EUROPEIA. *New deal for consumers*. Disponível em: https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en. Acesso em: 25 jan. 2021.

US SUPREME COURT. *Spokeo, Inc. v. Robins*, 578 U.S. (2016). Julgamento em: 16 maio 2016. Disponível em: <https://supreme.justia.com/cases/federal/us/578/13-1339/>. Acesso em: 26 fev. 2021.

VAN DER SLOOT, Bart. Legal fundamentalism: is data protection really a fundamental right. In: LEENES, R.; VAN BRAKEL, R.; GUTWIRTH, S.; HERT, P. (org.). *Data protection and privacy: (in)visibilities and infrastructures*. Law, Governance and Technology Series, 36. Springer. 2017. p. 3-30.

VAN DER SLOOT, Bart. Privacy as personality right: why the ecthr's focus on ulterior interests might prove indispensable in the age of "Big Data". *Utrecht Journal of International and European Law*, v. 80, 2015.

VAN DER SLOOT, Bart. The practical and theoretical problems with 'balancing': Delfi, Coty and the redundancy of the human rights framework. *Maastricht Journal of European and Comparative Law*, v. 3, 2016.

VAN DROOGHENBROECK, Sébastien; PICOD, Fabrice; RIZCALLAH, Cécilia. *Charte des droits fondamentaux de l'Union européenne*. Commentaire article par article. 2. ed. Bruxelles: Bruylant, 2019.

VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos. Data protection in the internet: general report. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (org.). *Data protection in the internet*. Ius Comparatum – Global Studies in Comparative Law. Suíça: Springer, 2020. p. 4-44.

VRIES, Katja de; BELLANOVA, Rocco; HART, Paul de; GUTWIRTH, Serge. The German Constitutional court judgment on data retention: proportionality overrides unlimited surveillance (doesn't it?). In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paulo; LEENES, Ronald. *Computers, privacy and data protection: an element of choice*. Springer Dordrecht Heidelberg London, 2011. p. 29-50.

WARREN, Samuel; BRENDIS, Louis. The right to privacy. *Harvard Law Review*, v. IV, n. 5, 1890.

WEINRIB, Lorena E. The Supreme Court of Canada and section one of the charter. *Supreme Court Law Review*, v. 10, p. 469-513, 1986.

WENNERSTRÖM, Erik. *EU Accession to the European Convention on Human Rights: the creation of a european legal space for human rights or the last stand for the normative supremacy of the strasbourg system?* *Europarättslig Tidskrift*, 2013. v. 2.

WERRO, Franz. The right to be forgotten: the general report – Congress of the International Society of Comparative Law. Fukuoka, July 2018. In: WERRO, Franz (org.). *The right to be forgotten. A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2018. p. 1-35.

WIEDEMANN, Klaus. *The ECJ's decision in "Planet49" (Case C-673/17): a cookie monster or much ado about nothing?* *IIC – International Review of Intellectual Property and Competition Law*, 2020. p. 543-553.

YAMAGUCHI, Itsuko. A japanese equivalent of the "right to be forgotten": unveiling judicial proactiveness to curb algorithmic determinism. In: WERRO, Franz (org.). *The right to be forgotten. a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer, 2018. p. 1-310.

ZALNIERIUTE, Monika. *Google LLC v. Commission Nationale de l'informatique et des Libertés (CNIL)*. *American Journal of International Law*, Forthcoming, v. 114, p. 1-13, 2020.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

NOTÍCIAS

ANPD. *Comunicação de incidentes de segurança*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em: 16 abr. 2021.

CNN BRASIL. *'O estrago está feito', diz diretor de empresa que detectou vazamentos de dados*. Disponível em: <https://www.cnnbrasil.com.br/business/2021/02/20/o-estrago-esta-feito-diz-diretor-de-empresa-que-detectou-vazamentos-de-dados>. Acesso em: 22 fev. 2021.

DATA Protection Commission. *DPC launches inquiry into Facebook in relation to a collated dataset of Facebook user personal data made available on the internet*. 2021. Disponível em: <https://www.dataprotection.ie/en/news-media/press-releases/dpc-launches-inquiry-facebook-relation-collated-dataset-facebook-user-personal-data-made-available>. Acesso em: 20 abr. 2021.

GARANTE per la Protezione dei Dati Personali. *Furto di dati da Facebook: il garante chiede al social network di adottare misure per limitare i rischi e avverte che l'utilizzo dei dati provenienti dalla violazione è illecito. Utenti invitati a prestare particolare attenzione a possibili anomalie sui propri cellulari*. 2021. Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9572143?utm_campaign=newsletter_-_20042021&utm_medium=email&utm_source=RD+Station. Acesso em: 20 abr. 2021.

INDUSTRIA y Comercio. *Superindustria inicia investigación contra Facebook ante posibles fallas de seguridad*. 2021. Disponível em: https://www.sic.gov.co/slider/superindustria-inicia-investigaci%C3%B3n-contra-facebook-ante-posibles-fallas-de-seguridad?utm_campaign=newsletter_-_20042021&utm_medium=email&utm_source=RD+Station. Acesso em: 20 abr. 2021.

LEXLATIN. *Os impactos jurídicos no Brasil do processo contra o TikTok no Reino Unido*. Disponível em: <https://br.lexlatin.com/reportagens/os-impactos-juridicos-no-brasil-do-processo-contra-o-tiktok-no-reino-unido>. Acesso em: 23 abr. 2021.

OLHAR Digital. *Facebook atribui recente vazamento de dados de usuários a “scraping”*. 2021. Disponível em: <https://olhardigital.com.br/2021/04/07/seguranca/facebook-atribui-recente-vazamento-de-dados-de-usuarios-a-scraping/>. Acesso em: 16 abr. 2021.

PROCONSP. *Vazamento de dados pessoais*. Disponível em: <https://www.procon.sp.gov.br/vazamento-de-dados-pessoais/>. Acesso em: 17 fev. 2021.

REINO UNIDO. *UK-EU Trade And Cooperation Agreement*. 2020. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/ico-statement-in-response-to-uk-governments-announcement-on-the-extended-period-for-personal-data-flows-that-will-allow-time-to-complete-the-adequacy-process/>. Acesso em: 19 jan. 2021.

TECMUNDO. *Tudo sobre o vazamento de dados de 223 milhões de brasileiros*. Disponível em: <https://www.tecmundo.com.br/software/210168-tudo-vazamento-dados-223-milhoes-de-brasileiros.htm>. Acesso em: 17 fev. 2021.

THE HACK. *'Vazamento' do Clubhouse é só mais uma raspagem de dados públicos*. 2021. Disponível em: <https://olhardigital.com.br/2021/04/07/seguranca/facebook-atribui-recente-vazamento-de-dados-de-usuarios-a-scraping/>. Acesso em: 16 abr. 2021.

U.S. DEPARTMENT OF COMMERCE. *Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States*. Disponível em: <https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect>. Acesso em: 22 fev. 2021.

UNIÃO EUROPEIA. *Documento 22020A1231 (01)*. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01.0014.01.ENG. Acesso em: 03 maio 2021.

UNITED States District Court. *Civil Action No. 1:20-cv-02658 (CJN)*. Disponível em: https://www.pacermonitor.com/view/W23REIQ/TIKTOK_INC_et_al_v_TRUMP_et_al__dcdce-20-02658__0029.0.pdf?mcid=tGE3TEOA. Acesso em: 22 fev. 2021.

UNITED States Government. *50 U.S. Code CHAPTER 35 – International emergency economic powers*. Disponível em: <https://www.law.cornell.edu/uscode/text/50/chapter-35>. Acesso em: 22 fev. 2021.

UNITED States Government. *Executive Order 13943*. Disponível em: <https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat>

posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency. Acesso em: 22 fev. 2021.

JULGAMENTOS DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA

Processo 6/64. *Flaminio Costa v E.N.E.L.* Julgamento em: 15 julho 1964.

Processo C-11/70. *Internationale Handelsgesellschaft mbH v Einfuhr – und Vorratsstelle für Getreide und Futtermittel.* Julgamento em: 17 dezembro 1970.

Processo C-17/10. *Toshiba Corporation e outros v. Úřad pro ochranu hospodářské soutěže.* Julgamento em: 14 fevereiro 2012.

Processo C-26/62. *NV Algemene Transport en Expeditie Onderneming Van Gend & Loos contra Administração Fiscal neerlandesa.* Julgamento em: 05 fevereiro 1963.

Processo C-28/08 P. *Comissão Europeia v. Bavarian Lager.* Julgamento em: 28 junho 2010.

Processo C-29/69. *Erich Stauder v. City of Ulm.* Julgamento em: 12 novembro 1969.

Processo C-40/17. *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV.* Julgamento em: 29 julho 2019.

Processo C-61/19. *Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).* Julgamento em: 11 novembro 2020.

Processo C-70/10. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL – SABAM.* Julgamento em: 24 novembro 2011.

Processo C-73/07. *Tietosuojavaluutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy.* Julgamento em: 16 dezembro 2008.

Processo C-101/01. *Bodil Lindqvist.* Julgamento em: 06 novembro 2003.

Processo C-101/01. *Conclusões do advogado-geral Tizzano.* Apresentado em: 19 setembro 2002. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62001CC0101&from=EN>. Acesso em: 17 mar. 2021.

Processo C-104/10. *Patrick Kelly v. National University of Ireland.* Julgamento em: 21 julho 2011.

Processo C-106/77. *Amministrazione delle Finanze dello Stato v Simmenthal SpA.* Julgamento em: 09 março 1978.

Processo C-119/12. *Josef Probst v. mr.nexnet GmbH.* Julgamento em: 22 novembro 2012.

Processo C-120/78. *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein.* Julgamento em: 20 fevereiro 1979.

Processo C-131/12. *Conclusões Gerais do Advogado-Geral Niilo Jääskinen*. Apresentado em: 25 junho 2013.

Processo C-131/12. *Google Spain SL e Google Inc. v. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. Julgamento em: 13 maio 2014.

Processo C-136/09. *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v Divani Akropolis Anonimi Xenodocheiaki kai Touristiki Etaireai*. Julgamento em: 18 março 2010.

Processo C-136/17. *GC e outros v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019.

Processo C-151/00. *Commission of the European Communities v French Republic*. Julgamento: 18 janeiro 2001.

Processo C-176/13. *Conselho da União Europeia v. Bank Mellat*. Julgamento em: 18 fevereiro 2016.

Processo C-203/15 e C-698/15. *Tele2 Sverige AB v. Post-och telestyrelsen e Secretário de Estado do Departamento Interno v. Watson*. Julgamento em: 21 dezembro 2016.

Processo C-207/16. *Ministério Fiscal*. Julgamento em: 02 outubro 2018.

Processo C-211/02. *Commission of the European Communities v. Grand Duchy of Luxemburg*. Julgamento em: 03 março 2003.

Processo C-234/12. *Sky Italia Srl v. Autorità per le Garanzie nelle Comunicazioni*. Julgamento em: 18 julho 2013.

Processo C-269/95. *Francesco Benincasa v Dentalkit Srl*. Julgamento em: 03 julho 1997.

Processo C-275/06. *Digital Promusicae v. Telefónica de España SAU*. Julgamento em: 29 janeiro 2008.

Processo C 275/09. *Promusicae*. Julgamento: 17 março 2011.

Processo C-279/09. *DEB Deutsche Energiehandels – und Beratungsgesellschaft mbH v. Bundesrepublik Deutschland*. Julgamento em: 22 dezembro 2010.

Processo C-291/12. *Michael Schwarz v. Stadt Bochum*. Julgamento em: 17 outubro 2013.

Processo C-293/12 e C-594/12. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e outros*. Julgamento em: 08 abril 2014.

Processo C-301/06. *Ireland v. European Parliament and Council of the European Union*. Julgamento em: 10 fevereiro 2009.

Processo C-306/05. *SGAE contra Rafael Hoteles*. Julgamento em: 07 dezembro 2006.

Processo C-311/18. *Comissário de Proteção de Dados v. Facebook Ireland Ltd e Maximillian Schrems*. Julgamento em: 16 julho 2020.

Processo C-317/04 e C-318/04. *Parlamento Europeu v. Conselho da União Europeia e Comissão das Comunidades Europeias*. Julgamento: 30 maio 2006.

Processo C-350/02. *Commission of the European Communities v. Kingdom of the Netherlands*. Julgamento em: 29 janeiro 2004.

Processo C-360/10. *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*. Julgamento em: 16 fevereiro 2012.

Processo C-362/14. *Maximillian Schrems v. Data Protection Commissioner*. Julgamento em: 06 outubro 2015.

Processo C-390/12. *Robert Pflieger e outros*. Julgamento em: 30 abril 2014.

Processo C-398/15. *Câmara de Comércio, Indústria, Artigianato e Agricultura di Lecce v. Salvatore Manni. Relator M. Ilešič*. Julgamento em: 09 março 2017.

Processo C-401/11. *Blanka Soukupová v. Ministerstvo zemědělství*. Julgamento em: 11 abril 2013.

Processo C-433/93. *Comissão das Comunidades Europeias contra República Federal da Alemanha*. Julgamento em: 11 agosto 1995.

Processo C-464/01. *Johann Gruber v Bay Wa AG*. Julgamento em: 20 janeiro 2005.

Processos C-465/00, C-138/01 e C-139/01. *Rundfunk*. Julgamento em: 20 maio 2003.

Processo C-466/12. *Nils Svensson e outros v. Retriever Sverige AB*. Julgamento em: 13 fevereiro 2014.

Processo C-473/12. *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert e outros*. Julgamento em: 07 novembro 2013.

Processo C-498/16. *Maximilian Schrems v. Facebook Ireland Limited*. Julgamento em: 25 janeiro 2019.

Processo C-507/17. *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*. Julgamento em: 24 setembro 2019.

Processo C-511/18. *La Quadrature du Net and Others v Premier ministre e outros*. Julgamento em: 06 outubro 2020.

Processo C-528/13. *Geoffrey Léger v. Ministre des Affaires sociales, de la Santé et des Droits des femmes e Etablissement français du sang*. Julgamento em: 29 abril 2015.

Processo C-536/15. *Tele2 (Netherlands) BV e o. contra Autoriteit Consument en Markt (ACM)*. Julgamento em: 15 março 2017.

Processo C-543/09. *Deutsche Telekom AG v. República Federal da Alemanha*. Julgamento em: 05 maio 2011.

Processo C-546/09. *Aurubis Bulgaria AD v. Nachalnik na Mitnitsa Stolichna*. Julgamento em: 31 março 2011.

Processo C-617/10. *Åklagaren v. Hans Åkerberg Fransson [GS]*. Julgamento em: 26 fevereiro 2013.

Processo C-623/17. *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e outros*. Julgamento em: 06 outubro 2020.

Processo C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. Julgamento em: 01 outubro 2019.

Processo T-670/14. *Milchindustrie-Verband eV e Deutscher Raiffeisenverband eV v. European Commission*. Julgamento em: 23 novembro 2015.

Processo T-670/16. *Digital Rights Ireland Ltd v. Comissão Europeia*. Julgamento em: 22 novembro 2017.

Processo 210/16. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contra Wirtschaftsakademie Schleswig-Holstein GmbH*. Julgamento em: 05 junho 2018.

Processo 620/19. *Land Nordrhein-Westfalen v D.-H. T. as liquidator of J & S Service UG*. Julgamento em: 10 dezembro 2020.

Processo 645/19. *Facebook Ireland Limited e o. contra Gegevensbeschermingsautoriteit*. Julgamento em: 15 junho 2021.

Processo 658/19. *European Commission v. Kingdom of Spain*. Julgamento em: 25 fevereiro 2021.