



UNIVERSIDADE CATÓLICA PORTUGUESA

A Proteção de Dados Pessoais como Garantia dos Direitos Fundamentais

**As decisões de adequação são mecanismos de tutela efetiva do direito fundamental
no que toca às transferências internacionais para países terceiros?**

Júlia Carrijo de Oliveira

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024



UNIVERSIDADE CATÓLICA PORTUGUESA

A Proteção de Dados Pessoais como Garantia dos Direitos Fundamentais

**As decisões de adequação são mecanismos de tutela efetiva do direito fundamental
no que toca às transferências internacionais para países terceiros?**

Júlia Carrijo de Oliveira

Orientadora: Professora Doutora Maria Benedita Menezes
de Gusmão Peixoto de Queiroz

Mestrado em Direito

Faculdade de Direito | Escola do Porto

2024

“One thing is clear: Close EU – US cooperation, based on our shared values and interests, is key for international peace, security and prosperity”.

Josep Borrell

Agradecimentos.

Aos meus pais, obrigada por terem me ensinado a voar e ir atrás dos meus sonhos. Por me proporcionarem sempre o melhor, incentivando-me mesmo quando eu própria duvidava. Ao meu pai, por ser meu mentor e à minha mãe por ser meu suporte. Vocês são a minha rocha diária.

À minha irmã, obrigada por ser minha parceira e por me motivar a ser uma pessoa melhor todos os dias.

À minha avó, obrigada por sempre orar por mim e pelos meus sonhos. Ao meu falecido avô, obrigada pela herança na busca por conhecimento e pelos ensinamentos da vida, a saudade é eterna. Amo-vos incondicionalmente.

À minha madrinha, pelo inesgotável carinho, por se fazer sempre presente e celebrar cada conquista minha como se fosse sua.

Ao Diogo, por todo o amor, apoio e serenidade nesses anos juntos.

Ao Helder, Fátima, Maria Inês, Ana Rita e Joana Filipa, por terem me acolhido de braços abertos e por terem me incentivado ao longo do processo.

À Maria Clara e Paula, pela constante presença ao longo desses anos; vocês são mais que simples amigas, tornaram-se família.

À Marília e Horácio, por terem me socorrido e orientado quando mais precisei.

À Ana Amélia e Joana, por me acompanharem no desafio do Mestrado.

Ao Prof. Dr. Alexandre por me apresentar o mundo do Direito da Informática ainda na Licenciatura.

À Prof. Dra. Sofia e Prof. Dra. Filipa por impulsionarem meu interesse no Direito da União Europeia e no Direito à Proteção de Dados.

À minha orientadora, pela paciência e incentivo.

Resumo

O direito à proteção de dados foi fortemente estabelecido como Direito Fundamental na perspectiva europeia. No entanto, avanços tecnológicos têm apresentado desafios significativos para a tutela efetiva do direito dos titulares europeus, sobretudo nas transmissões dos dados pessoais para países que possuem padrões de proteção inferiores aos estabelecidos na União. Neste contexto, estudaremos a evolução no direito europeu, em contraponto do direito norte-americano; desafios dos mecanismos para garantir proteção nas transferências para os Estados-Unidos. Não menos importante, as decisões do Tribunal de Justiça da União Europeia, que auxiliam na matéria.

Palavras-chaves: direitos fundamentais; proteção de dados; transferências internacionais; União Europeia; Estados Unidos.

Abstract

The right to data protection has been strongly established as a fundamental right from a European perspective. However, technological advances have presented significant challenges to the effective protection of European data subjects, especially in the transfer of personal data to countries with lower standards of protection than those established in the Union. In this context, we study the evolution of European law, as opposed to US law; the challenges of mechanisms to guarantee protection in transfers to the United States. No less important, the decisions of the Court of Justice of the European Union, that assist in the matter.

Keywords: fundamental rights; data protection; international transfers; European Union; United States.

Índice

Introdução.....	10
Capítulo I.....	12
1. A relevância da proteção de dados na era da globalização.....	12
2. O Direito Fundamental à proteção de dados no contexto europeu.....	15
Capítulo II.....	19
3. Transferências de dados pessoais para países terceiros no RGPD.....	19
4. Mecanismos de garantia de proteção.....	22
4.1. <i>Decisões de adequação.</i>	22
4.2. <i>Garantias adequadas.</i>	24
4.3. <i>Acordos internacionais.</i>	25
4.4. <i>Situações específicas.</i>	26
5. Reflexões intermédias.....	27
Capítulo III.....	28
6. Quadro UE – EUA em matéria de proteção de dados.....	28
6.1. <i>Decisão de Adequação “Porto Seguro”.</i>	29
6.1.1. <i>Acórdão “Schrems I” (C-362/14).</i>	33
6.2. <i>Decisão de Adequação “Escudo de Proteção da Privacidade”.</i>	35
6.2.1. <i>Acórdão Schrems II (C-311/18).</i>	40
6.3. <i>Decisão de Adequação “Quadro de Privacidade de Dados”. Será desta?</i> 41	
6.3.1. <i>Exame crítico da nova Decisão.</i>	43
Conclusão	46
Bibliografia.....	48

Lista de Siglas e Abreviaturas

AEPD – Autoridade Europeia para Proteção de Dados.

AG – Advogado-Geral.

AG Regulation – Attorney General Regulation.

Art. – Artigo.

BCRs – Regras Vinculativas às Empresas.

CCT – Cláusulas Contratuais-Tipo.

CDFUE – Carta dos Direitos Fundamentais da União Europeia.

CEDH – Convenção Europeia dos Direitos do Homem.

CEPD – Comissão Europeia de Proteção de Dados.

CIA – *Central Intelligence Agency.*

CLPO – *Civil Liberties Protection Officer.*

Comissão – Comissão Europeia.

Conselho – Conselho da União Europeia.

Consult. – Consultado.

DOC – Departamento de Comércio dos Estados Unidos.

DOT – *Department of Transportation.*

DPC – Comissão de Proteção de Dados.

DPRC – Tribunal de Fiscalização da Proteção de Dados.

DUDH – Declaração Universal dos Direitos do Humanos.

ECLI: European Case Law Identifier.

EUA – Estados Unidos da América.

FAQ – Questões mais frequentes.

FISC – Tribunal de Vigilância de Inteligência Estrangeira.

FTC – *Federal Trade Commission.*

GT29 – Grupo de Trabalho do artigo 29.º

ITA – International Trade Administration.

n.º - número.

NSA – *National Security Agency*.

OCDE – Organização para a Cooperação e Desenvolvimento Económico ou Económico.

ODNI – *Office of the Director of National Intelligence*.

ONG – Organização Não Governamental.

p. – página/s.

PE – Parlamento Europeu

RGPD ou Regulamento – Regulamento Geral sobre a Proteção de Dados.

TFUE – Tratado de Funcionamento da União Europeia.

TJUE – Tribunal de Justiça da União Europeia.

TUE – Tratado da União Europeia.

UE – União Europeia.

Introdução.

As alterações trazidas pelas tecnologias de informação nos últimos anos vieram revolucionar a forma como as pessoas se relacionam. Os desenvolvimentos para uma Sociedade de Informação, conceção desenvolvida por autores como Marshall McLuhan¹, Fritz Machlup² e Alvin Toffler³, “quebraram” as barreiras físicas e reduziram as distâncias dos seres humanos. De facto, hoje somos capazes de “visitar” uma cidade ou país através da tecnologia de mapeamento e satélite; fazer compras em plataformas digitais; trabalhar, realizar reuniões e encontros sem precisar sair de nossas residências, carecendo apenas de conexão à *Internet*.

Isso deve-se à transição da globalização meramente econômica para a conceção de um mundo virtual completamente interligado. As vantagens que este novo mundo trouxe são inúmeras. Porém, a verdade é que a recolha, armazenamento e partilha de informação (dados) geraram, tanto no setor público como no privado, a necessidade de executar o tratamento de forma veloz. O que abriu margem para violações ao direito à vida privada dos cidadãos, já muito plasmado. Daí a necessidade do Direito, ciência jurídica que regula a sociedade, se adaptar a esta nova realidade dado as consequências à privacidade e intimidade das pessoas.

Com o tema “*A Proteção dos Dados Pessoais como Garantia dos Direitos Fundamentais*” e dividida em três capítulos, iremos questionar se, no âmbito das transferências de dados pessoais para países terceiros, as decisões de adequação são mecanismos de tutela efetiva dos direitos fundamentais, especificamente o direito à proteção de dados.

Iniciamos por retratar a importância dos dados pessoais e a sua proteção na era da globalização digital. Discorreremos sobre a aquisição do *status* de Direito Fundamental autónomo na União face ao direito ao respeito à vida privada e familiar⁴, consagrado desde 1948. E na linha de Menezes Cordeiro (2022), em que “a regulação específica e autónoma surge como uma resposta à utilização de mecanismos automatizados no processamento de informação pessoal”⁵, faremos uma delimitação teleológica da *ratio* deste ramo jurídico. O autor aponta que, o propósito material das produções legislativas

¹ MCLUHAN, Marshall (1964).

² MACHLUP, Fritz (1962).

³ TOFFLER, Alvin (1970)-

⁴ FUSTER, Gloria González (2014), p. 265.

⁵ MENEZES CORDEIRO, A. Barreto (2022), p. 37.

originárias sobre dados pessoais tinha como objetivo principal regular o seu tratamento, não cautelar os interesses individuais dos titulares dos dados⁶. Porém, felizmente, constatamos que hoje não é mais assim.

No Capítulo II, analisamos as transferências internacionais para países terceiros de acordo com o RGPD, ato jurídico de direito derivado da União diretamente aplicável aos Estados-membros, nos termos do art. 288.º §2 TFUE, aqui destacável. Descreveremos os mecanismos de garantia de proteção nas transmissões transatlânticas. E, para a análise da construção regulatória, necessários são elementos que tem por finalidade dar a conhecer as circunstâncias da estruturação⁷. Desse modo, socorremo-nos ao longo do texto aos considerandos do RGPD, para sua melhor aplicação.

Num último momento, urgimos para a apresentação explícita da conturbada relação UE-EUA nas transferências de dados pessoais, trazendo em evidência as decisões de adequação. Decisões essas que nas últimas décadas salientaram a dificuldade da proteção efetiva dos dados dos cidadãos europeus, devido à falha das legislações norte-americanas de garantir direitos fundamentais equivalentes aos da União com sistemas de vigilância em massa.

Em suma, as trocas de dados integram operações diárias, girando a economia da informação que movimenta bilhões. A recolha, análise e armazenamento de dados pessoais de titulares europeus por empresas norte-americanas possuem valor imensurável. Não obstante o impacto económico, é evidente a dificuldade de apresentar ao cidadão comum a razão pela qual seus dados pessoais são tão desejáveis. Desse modo, a escolha da temática justifica-se pela essencial necessidade da proteção dos direitos fundamentais; e considerando a mais recente decisão da Comissão, juntamente com o Governo norte-americano, investigaremos se é possível concluir por uma melhora no sistema.

⁶ Ibidem, p. 33.

⁷ UNIÃO EUROPEIA (2016), p. 31-36.

Capítulo I

1. A relevância da proteção de dados na era da globalização.

Ao encontrarmos-nos numa sociedade que busca o constante progresso tecnológico, é visível a emergência e importância contemporânea dos dados pessoais dada na Era Digital⁸. Uma vez que o Direito está em constante construção, e regularmente é acusado de estar atrás dos acontecimentos da sociedade, aqui não poderia ser diferente. Assim, coube à ciência jurídica acompanhar estes desenvolvimentos, com a tentativa de prognosticar os eventuais desafios que iam surgindo, seus impactos sociais e regulamentá-los.

Na linha de Menezes Cordeiro (2022), “a expressão “*os dados são o novo petróleo*”⁹ exprime a convicção (...) de que os dados representarão na Era Digital um papel análogo ao desempenhado pelo petróleo e demais combustíveis fósseis a partir da Revolução Industrial”¹⁰. Deste entendimento adianta-se que hoje já assim é em matérias como *Marketing*, comércio e saúde.

Apontamos para a insuficiência das ações isoladas de regulamentação dos Estados-membros que encontramos no cenário pré-regulamentação europeia, isto é, sem uma norma mais ou menos uniformizada não era possível obter uma resposta eficaz aos desafios cada vez mais transnacionais colocados pelo aumento dos fluxos transfronteiriços de dados entre cidadãos, empresas e entidades públicas. A repentina evolução tecnológica e multinacionalização criaram desafios novos em matéria de proteção de dados pessoais. Mais especificamente, a recolha e partilha de dados pessoais de forma informatizada e automatizada transformou a vida social e económica numa escala sem precedentes¹¹.

Assim, a insustentabilidade do modelo vigente¹² contribuiu para a reforma do sistema de proteção de dados pessoais. Com objetivo de livre circulação de dados pessoais em território europeu¹³, sua transferência para países terceiros e, paralelamente, assegurar um nível coerente e elevado de proteção desses dados¹⁴, dá-se assim a introdução a um Mercado Único Digital. Destacamos, ainda, a importância da matéria de proteção de

⁸ MENEZES CORDEIRO, A. Barreto (2022), op. cit., p. 27-29.

⁹ Dennis D. Hirsch (2014), p. 374.

¹⁰ MENEZES CORDEIRO, A. Barreto (2022), op. cit., p. 29.

¹¹ Art. 1.º RGPD, Considerandos 6-7.

¹² Na altura, Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.

¹³ Art. 1.º RGPD.

¹⁴ RGPD, Considerandos 2 e 6.

dados dada pelo Tribunal de Justiça da União Europeia (TJUE) em sua jurisprudência, a qual levou o legislador europeu a dar especial atenção ao tema – desde os acórdãos *Lindqvist*, *Scarlet*, *Digital Rights*, *Google Spain e Google*, *Schrems*, *Tele 2 Sverige*, etc.

Numa análise jurisprudencial da matéria, no *Caso Lindqvist* (C-101/01)¹⁵ o Tribunal veio esclarecer quem é considerado responsável pelo tratamento, ou seja, que uma pessoa que opera um site pessoal pode ser considerada responsável pelo tratamento de dados pessoais e que, portanto, está sujeita às obrigações estabelecidas por legislação europeia¹⁶. No *Caso Tele 2 Sverige* (C-203/15)¹⁷ o órgão jurisdicional reafirma a natureza do direito à proteção de dados como um direito fundamental, enfatizando a importância do princípio da proporcionalidade aquando da interferência na privacidade dos indivíduos e estabelece também a proibição da retenção em massa de dados de comunicação telefónica (generalizada e indiferenciada), na qual são incompatíveis com o direito da União¹⁸.

Em um outro prisma, mas reafirmando a relevância das decisões do TJUE, no âmbito da proteção dos direitos do autor na *Internet*, no *Caso Scarlet* (C-70/10)¹⁹ o Tribunal decidiu que, apesar de os provedores de serviços de *internet* não serem responsáveis pela violação dos direitos autorais por parte dos usuários, estes podem ser obrigados a bloquear transferências de ficheiros de sites que infringem os direitos autorais de uma obra, desde que a medida seja proporcional e respeite os direitos fundamentais.

Para o cidadão comum pode não ser compreensível a importância dada para os seus dados pessoais e o impacto na economia cada vez mais globalizada. Tendo agora os dados pessoais como um verdadeiro produto na Era Digital, é passível de representar um verdadeiro perigo para eventuais violações suscetíveis de lesar os interesses e direitos, absolutos e/ou relativos dos titulares dos dados. E mesmo não se tratando de um ramo jurídico novo, apenas nas últimas décadas este assumiu importância indubitável, trazendo concretos desafios no que toca à tutela efetiva dos direitos dos titulares de dados pessoais suscetível de ser imposto às diversas figuras internacionais e o dever destas de adotar uma postura diligente.

¹⁵ Acórdão de 6 novembro 2003, *Caso Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596.

¹⁶ *Ibidem*, n.º 1.

¹⁷ Acórdão de 21 de dezembro de 2016, *Caso Tele2 Sverige*, processos apensos C-203/15 e C-698/15, ECLI:EU:C:2016:970.

¹⁸ *Ibidem*, § 134, ponto 1).

¹⁹ Acórdão de 24 de Novembro de 2011, *Caso Scarlet Extended AS*, C-70/10, ECLI:EU:C:2011:771.

Hoje vemos o nível de proteção adequado exigido pela UE derivado da introdução de instrumentos jurídicos que harmonizam a temática no direito interno dos Estados-membros, sendo expressões do princípio da atribuição, nos termos do art. 4.º Tratado sobre o Funcionamento da União Europeia (TFUE).

O Regulamento de 2016, fonte de direito derivado e dotado de efeito direto, assumiu assim dois grandes propósitos: (i) proteger os direitos e as liberdades fundamentais das pessoas singulares no que toca ao direito à proteção de dados; e (ii) permitir a livre circulação desses dados pessoais²⁰. Como veremos, esse documento normativo prevê, por exemplo, a densificação dos direitos dos titulares; a especificação (e agravamento) dos deveres dos responsáveis pelo tratamento de dados e subcontratantes; a designação do encarregado de proteção de dados (reforço das competências das autoridades de controlo)²¹, e outros. Uma vez mais, não podemos negar o caráter de direito fundamental garantido pela Carta ao direito à proteção de dados, sendo este uma expressão direta da dignidade humana²² intrínseco ao direito à vida privada dos seus titulares.

A atuação das instituições europeia se estendeu à celebração de acordos com países terceiros com o objetivo de estatuir uma base legal comum em que permita o estabelecimento de relações recíprocas na matéria de informações, exemplo disso é os Estados Unidos da América (EUA). Tonificando assim a cooperação internacional e trocas comerciais que muito se alonga no tempo entre os dois parceiros. A materialização destes acordos deu-se nas Decisões da Comissão 2000/520/CE, de 26 de Julho de 2000²³, Decisão 2016/1250/CE de 12 de Julho de 2016²⁴ e mais recentemente na Decisão de 10 de Julho de 2023²⁵.

Dentro do alcance extraterritorial do regime de proteção de dados pessoais da União, surge a questão sobre a extensão da salvaguarda conferida a este direito fundamental. Em outros termos, surge a indagação sobre a capacidade dos países situados fora do território europeu, que necessitam de algum mecanismo para garantir a proteção adequada nas transferências de dados pessoais conforme estabelecido pelo atual Regulamento Geral sobre a Proteção de Dados (RGPD), de efetivamente protegerem os

²⁰ MENEZES CORDEIRO, A. Barreto (2022), op. cit., p. 33.

²¹ *Ibidem*, p. 29-30.

²² CALVÃO, Filipa Urbano (*s.d.*), p. 18.

²³ UNIÃO EUROPEIA, Decisão 2000/520/CE da Comissão, de 26 de Julho de 2000.

²⁴ UNIÃO EUROPEIA, Decisão de Execução (UE) 2016/1250, da Comissão de 12 de julho de 2016.

²⁵ UNIÃO EUROPEIA, Decisão de Execução (UE) 2023/1795 da Comissão de 10 de julho de 2023.

direitos fundamentais, incluindo o acesso à justiça de um titular de dados europeu, quando necessário.

Apesar do discorrido, as decisões do TJUE em matéria de proteção de dados não estão isentas de críticas. Tomando como exemplo empresas que dependem do processamento de grandes quantidades de dados pessoais, há quem pontue que há decisões do Tribunal com interpretações excessivamente restritivas podendo concretamente inibir ou acabar prejudicando a competitividade das empresas europeias em relação aos seus concorrentes globais. Mais, há críticos que argumentam na dificuldade das transferências de dados transfronteiriços podendo prejudicar a colaboração em questões de segurança cibernética e o combate aos crimes de variadas naturezas.

Após uma análise aprofundada sobre a relevância contemporânea dos dados pessoais na economia globalizada, torna-se manifesto que, em virtude de sua natureza como direito fundamental, a potencialidade de risco que sua violação acarreta demanda que tais dados sejam integralmente assegurados e protegidos tanto por entidades públicas quanto privadas²⁶, sem distinção quanto ao sistema jurídico vigente.

2. O Direito Fundamental à proteção de dados no contexto europeu.

Considerando que o conceito de tratamento de dados corresponde à decomposição em três elementos: (i) que seja uma operação ou um conjunto de operações; (ii) que seja efetuada sobre dados pessoais; e (iii) que seja por meios autonomizados ou não autonomizados²⁷, podemos então dizer que o tratamento de dados teve lugar em diversos momentos da história da humanidade antes mesmo de haver qualquer legislação que tratasse do assunto.

É possível, por exemplo, ver o uso deste tratamento de forma abusiva na experiência histórico-trágica da II Guerra²⁸, na medida em que os antigos governos Fascistas e Nazistas acumulavam grandes quantidades de dados pessoais de seus cidadãos e dos cidadãos dos países invadidos, sem o conhecimento ou consentimento dos titulares dos dados²⁹. Nesses registos eram indicados diversos dados, como a filiação em partidos políticos e associações profissionais, a família, os amigos, as moradas privadas e dados

²⁶ MARTINHO, Lúscas Pires (2018), p. 92.

²⁷ MENEZES CORDEIRO, A. Barreto (2022), op. cit., p. 143.

²⁸ ALVES, Joel A. (2021), p. 24.

²⁹ MADSEN, W. (1992), p. 22.

mais íntimos. Os registos de nascimento eram também utilizados para identificar os “arianos puros” dos que tinham uma linhagem não ariana³⁰.

Em consequência da experiência vivida no continente e influenciado pela Declaração Universal dos Direitos do Humanos (DUDH) de 1948, o legislador europeu veio estabelecer em 1950 na Convenção Europeia dos Direitos do Homem (CEDH), no seu art. 8.º, por um lado, “qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”³¹, e por outro,

“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 infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”³².

Assim, com um sentimento ansioso pela volta de uma sociedade democrática, os legisladores europeus lançaram mão do primeiro sistema de proteção do ser humano no que toca ao tratamento de dados pessoais, revestido pelo respeito à vida privada.

Após negociações, em 1981, a Comissão de Ministros do Conselho da Europa adotou a chamada Convenção 108³³. Esta Convenção marcou um passo chave no que toca a normas para o processamento de dados pessoais, por um lado, porque formalmente ligava a proteção de dados com a garantia dos direitos fundamentais e liberdades e, por outro, articulava uma ligação especial da proteção de dados com o direito à privacidade³⁴. Este foi o primeiro documento internacional juridicamente vinculativo a ser adotado na matéria³⁵.

Em 1990, a Comissão apresentou duas diretrizes: uma sobre a proteção das pessoas no tratamento de dados pessoais e outra sobre como as redes públicas digitais de telecomunicações protegem a vida privada e os dados pessoais. O documento final tornar-se-ia na Diretiva 95/46/CE, de 24 de outubro de 1995³⁶, relativa à proteção das pessoas

³⁰Ibidem, p.23.

³¹ Art. 8.º/1 CEDH. Itálico nosso.

³² Art. 8.º/2 CEDH. Itálico nosso.

³³ Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981.

³⁴ FUSTER, Gloria González (2014), op. cit., p. 88-89.

³⁵ MACIEJEWSKI, Mariusz; Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais do Parlamento Europeu (2023).

³⁶ UNIÃO EUROPEIA, Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995.

singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Foi apenas em 2000, com a Carta dos Direitos Fundamentais da União Europeia (CDFUE), que se deu a nova fase do processo de construção dogmática do direito à proteção de dados pessoais de forma autónoma ao direito ao respeito pela vida privada³⁷. Com uma mudança de paradigma a nível da União quanto à cultura de direitos fundamentais de carácter transversal a todos os Estados-membros, foi então criado o catálogo de direitos fundamentais no qual incluía “o direito de todas as pessoas à proteção dos dados pessoais que lhe dissessem respeito”³⁸. E mais, com a entrada em vigor do Tratado de Lisboa (TFUE), em 2009, com carácter juridicamente vinculativo, reconheceu-se alguns direitos, liberdades e princípios, incluindo neste catálogo o direito à proteção de dados pessoais³⁹ juntamente com o valor jurídico equiparado ao dos Tratados⁴⁰.

Neste mesmo sentido e visando aprimoramento, em 2016, tivemos o Regulamento (UE) 2016/679 do Parlamento Europeu (PE) e do Conselho, de 27 de Abril (RGPD), que estabelece as regras relativas à proteção das pessoas singulares no que toca o tratamento de dados pessoais e a livre circulação destes e revoga a Diretiva 95/46/CE. Nos considerandos do RGPD⁴¹ é explicitado que a proteção das pessoas singulares quanto ao tratamento dos seus dados pessoais é, concretamente, um direito fundamental.

Simultaneamente, o TJUE desempenhou papel fundamental para a interpretação do conteúdo relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, densificando este como direito fundamental. *Exempli gratia*, no caso *Google Spain e Google (C-131/12)*⁴² o Tribunal estabeleceu o direito de o indivíduo solicitar a remoção de informações pessoais nos monitores de buscas *online* sob certas circunstâncias, isto é, direito à supressão de referências, conhecido hoje como o direito ao esquecimento⁴³. No caso *Digital Rights Ireland Ltd.* (processos apensos C-293/12 e C-594/12)⁴⁴ o Tribunal invalidou a Diretiva 2006/24/CE a qual exigia a retenção de dados

³⁷ Direitos fundamentais estreitamente relacionados, mas distintos.

³⁸ Art. 8.º/1 CDFUE.

³⁹ Art. 16.º TFUE.

⁴⁰ O TUE, art. 6.º, reconhece os direitos, liberdades e princípios enunciados na Carta e dá-lhes o mesmo valor jurídico que os Tratados.

⁴¹ Art. 1.º do RGPD, Considerandos.

⁴² Acórdão de 13 de maio de 2014, *Google Spain SL, Google Inc.*, C-131/12, ECLI:EU:C:2014:317.

⁴³ *Ibidem*, § (100), ponto 4).

⁴⁴ Acórdão de 8 de abril de 2014, *Digital Rights Ireland*, Processos apensos C-293/12 e C-594/12, ECLI:EU:C:2014:238.

de comunicações eletrónicas, considerou que esta violava os artigos 7.º e 8.º da Carta, designadamente, direitos fundamentais à privacidade e à proteção de dados⁴⁵.

De igual natureza, no Caso *Schrems v. Data Protection Commissioner*, (C-362/14)⁴⁶, o Tribunal invalidou a Decisão 2000/520/CE, acordo de transferências de dados conhecida como *Safe Harbour* (Porto Seguro) entre a UE e os EUA por preocupações com a proteção e privacidade de dados dos cidadãos europeus. Ainda, no caso *Facebook Ireland e Schrems* (C-311/18)⁴⁷ o Tribunal invalidou outro acordo de transferências de dados entre UE e EUA, a Decisão de Execução (UE) 2016/1250 conhecida como *Privacy Shield* (Escudo de Proteção da Privacidade), com as mesmas preocupações. Ambas serão melhor analisadas posteriormente.

Inúmeras são as instâncias de decisões proferidas pelo TJUE que corroboram para a consolidação do direito à proteção de dados como um direito fundamental assegurado pela Carta, com o objetivo de cooperar para a concretização de um espaço de liberdade, segurança e justiça e união económica; princípios, objetivos e valores da União, definidos nos artigos 2.º e 3.º do TFUE e na CDFUE. À vista disso, os princípios e regras nesta matéria deverão ser respeitados em consonância com os direitos e liberdades fundamentais, independentemente da nacionalidade ou do local de residência do titular.

Destarte, e tendo em consideração ao que foi exposto até aqui, cumpre atentar o regime jurídico europeu dos mecanismos que possibilitam a garantia de proteção nas transferências internacionais de dados pessoais.

⁴⁵ *Ibidem*, § (33).

⁴⁶ Acórdão de 6 de outubro de 2015, *Schrems v. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

⁴⁷ Acórdão de 16 de julho de 2020, *Facebook Ireland e Schrems (Schrems II)*, C-311/18, ECLI:EU:C:2020:559.

Capítulo II

3. Transferências de dados pessoais para países terceiros no RGPD.

No que toca às transferências internacionais de dados pessoais para países terceiros, referimo-nos ao processo de movimentação de informações pessoais e/ou sensíveis entre fronteiras para fora da União. Exemplo, no cumprimento de acordos comerciais internacionais, as empresas que operam em um cenário global estão frequentemente a transferir dados de clientes, parceiros comerciais e funcionários para facilitar suas transações comerciais na logística. Análogo a isso, na cooperação internacional, os diversos governos e organizações internacionais partilham dados essenciais para a segurança, combate ao crime internacional, prevenção do terrorismo, entre outras questões. E é por isso que o Capítulo V do RGPD trata da admissibilidade destas transferências, valendo-se de variadas situações-tipo⁴⁸.

No art. 44.º do RGPD temos o princípio geral das transferências. De acordo com Menezes Cordeiro (2022), “a transferência de dados pessoais consubstancia por si só um tratamento de dados, pelo que, para ser feito de forma lícita está diretamente dependente do cumprimento do regulamento e demais legislações aplicáveis”. Isto porque o legislador europeu reconhece a importância na cooperação internacional e no comércio, não proibindo estas transferências, mas restringindo-as⁴⁹.

O regulamento, porém, não definiu explicitamente tal conceito jurídico de transferências. Não obstante, no que se refere ao seu âmbito de aplicação territorial, no art. 3.º é estabelecido critérios:

- O local onde a atividade do responsável pelo tratamento dos dados/subcontratante esteja situada em território da UE, mesmo que este tratamento não ocorra dentro do território em causa (n.º 1);
- O local de residência dos titulares dos dados seja no território da UE, e caso o tratamento seja realizado para fornecer produtos ou serviços na UE ou para monitorar comportamentos (n.º 2); e
- A pessoa responsável pelo tratamento está fora da UE, mas em um lugar onde o direito de um Estado-membro é aplicado por meio do Direito Internacional Público (n.º 3).

⁴⁸ DE JESUS, Inês Oliveira Andrade (2018), p.75.

⁴⁹ MENEZES CORDEIRO, A. Barreto (2022), op. cit., p. 150-151.

Ao n.º 1 do art., implica que se determine o conceito de estabelecimento⁵⁰ de acordo com a Diretiva 95/46/CE, junto com os considerandos do RGPD e a jurisprudência do TJUE⁵¹. O considerando (22) evidencia que “O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa *instalação estável*⁵²”. Na mesma direção, no Acórdão *Google Spain SL e Google Inc.*⁵³ o TJUE decidiu que:

(55) “(...) há que considerar que o tratamento de dados pessoais, (...) é explorado por uma *empresa sediada num Estado terceiro, mas que dispõe de um estabelecimento num Estado-Membro*, é efetuado «no contexto das atividades» desse estabelecimento (...).”⁵⁴

Também no Acórdão *Weltimmo*⁵⁵, o TJUE decidiu que:

(29) “(...) para determinar se uma sociedade, responsável por um tratamento de dados, dispõe de um estabelecimento, na aceção da Diretiva 95/46, num Estado-Membro diferente do Estado-Membro ou do país terceiro em que está registada, *há que avaliar tanto o grau de estabilidade da instalação como a realidade do exercício das atividades nesse outro Estado-Membro* (...).”⁵⁶

Em seguimento, o n.º 2 do mesmo art., na alínea a) e o considerando (23) RGPD refletem que o critério a ter em conta é a presença dos indivíduos em território da UE, “a fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste (...)”; já na alínea b), o considerando (24) coloca em questão o controlo do comportamento de titulares de dados a ser determinado se essas pessoas são seguidas na Internet e a potencial utilização da técnica de definição do perfil de uma pessoa gerando a previsão de suas preferências e atividades *online*.

Em último, o n.º 3, junto com o considerando (25), determinam a aplicação do RGPD onde seja aplicável lei de um Estado-membro fora do seu território e com base no Direito Internacional Público, exemplo, situações de missões diplomáticas ou postos consulares.

Para maior entendimento, o Comité Europeu de Proteção de Dados (CEPD), admitindo que o RGPD não prevê uma definição jurídica da noção de transferência de dados pessoais para um país terceiro, forneceu orientações para clarificar os cenários aos

⁵⁰ EDPB (2019), Guidelines 3/2018.

⁵¹ PINHEIRO, Alexandre Sousa [et. al]; GONÇALVES, Jorge Carlos (2018) p. 109-115.

⁵² Itálico nosso.

⁵³ TJUE, Ac. C-131/12.

⁵⁴ Itálico nosso.

⁵⁵ Acórdão de 1 de outubro de 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

⁵⁶ Itálico nosso.

quais considera que devem ser aplicados⁵⁷. Considerando que o CEPD⁵⁸, tem por missão aconselhar a Comissão sobre questões relacionadas com a matéria de proteção dos dados pessoais da EU e aspetos do regulamento que considere que necessite uma maior clarificação, convidou então a Comissão a prestar especial atenção às mesmas no contexto do relatório sobre avaliação e revisão do RGPD⁵⁹.

O organismo identificou três critérios cumulativos para clarificação de uma operação de tratamento como uma transferência para um país terceiro: (1) “Responsável pelo tratamento ou um subcontratante (“exportador”) está sujeito ao RGPD para o tratamento em causa.”; (2) “O exportador divulga, por transmissão ou por qualquer outra forma, os dados pessoais sujeitos a este tratamento, a outro responsável pelo tratamento, responsável conjunto pelo tratamento ou subcontratante (“importador”).”; e (3) “O importador encontra-se num país terceiro, independentemente de estar ou não sujeito ao RGPD para o tratamento em causa, de acordo com o art. 3.º”.

Considerando o segundo critério delineado pelo CEPD, o *Guidelines 05/2021* fornece como exemplo:

“A empresa X estabelecida na Áustria, agindo como responsável pelo tratamento, fornece dados pessoais dos seus empregados ou clientes à empresa Z num país terceiro, que processa esses dados como subcontratante em nome da empresa X. Neste caso, os dados são fornecidos por um responsável pelo tratamento (...) está sujeito ao RGPD, a um subcontratante num país terceiro. Assim, o fornecimento de dados será considerado como uma transferência de dados pessoais para um país terceiro e, por conseguinte, aplica-se o Capítulo V do RGPD.”⁶⁰

Assim, se todos os critérios da CEPD forem atendidos, acontece a chamada "transferência para um país estrangeiro". Significa que dados pessoais são enviados ou disponibilizados por um responsável pelo tratamento ou subcontratante (“exportador”) que está sujeito às regras do art. 3.º do RGPD, para outra empresa ou organização (“importador”) em um país fora da União, mesmo que este importador não esteja sujeito ao RGPD no tratamento em causa. Neste caso, o “exportador” precisa seguir as regras do Capítulo V do RGPD e se enquadrar num dos mecanismos disponíveis para garantir a proteção dos dados pessoais após a transferência para o país terceiro.

⁵⁷ CEPD (2023), *Guidelines 05/2021*, p.3.

⁵⁸ Art. 70.º, n.º 1, alínea b) do RGPD

⁵⁹ CEPD (2023), *Guidelines 05/2021*, p.7.

⁶⁰ *Ibidem*, p. 6.

Em consonância com o objetivo de livre circulação dos dados pessoais, o aumento desta criou desafios em relação à proteção deste direito fundamental dos cidadãos quando esta transferência tem por origem e destino países não pertencentes à União⁶¹. E, uma vez que vivemos na “Sociedade de Informação”⁶², entende-se o fomento na criação e obtenção de dados na maior extensão possível por parte das *Big Tech*⁶³.

O RGPD representa então a vertente protecionista da União, com o objetivo de gerir os dados com base nos direitos fundamentais ao abrigo da Carta. Assim, para efetiva realização de transferências, depende-se da conformidade um número limitado de mecanismos que asseguram que estas transferências aos países terceiros não enfraqueçam o alto nível de proteção dos dados pessoais garantido em território europeu.

4. Mecanismos de garantia de proteção.

4.1. Decisões de adequação.

De acordo com o art. 45.º, n.º 1 RGPD, as transferências internacionais são admissíveis quando a Comissão tenha decidido que “o país terceiro, um território ou um ou mais setores específicos desse país terceiro em causa, assegura um nível adequado de proteção”, não exigindo aqui uma autorização específica. No Considerando (103), a Comissão pode decidir, com efeitos na União, que tal país oferece um nível adequado de proteção tendo em consideração as circunstâncias associadas à transferência ou a uma categoria de transferências que seja considerado apto a assegurar tal nível, plasmado pelos princípios da segurança jurídica e uniformidade a nível da UE. O que seria então a “adequação do nível de proteção”?

Constituem, elementos de ponderação da Comissão, na avaliação da adequação do nível de proteção, do potencial recetor dos dados pessoais a serem transferidos⁶⁴: (i) o primado do Estado de Direito; (ii) a existência e o efetivo funcionamento de uma ou mais autoridades de controlo independente; e (iii) os compromissos internacionais assumidos pelo sujeito recetor dos dados.

Ao primeiro elemento, a Comissão considera que quem receba os dados transferidos deve dar garantias que assegurem um nível adequado de proteção

⁶¹ Considerando (101).

⁶² CASIMIRO, Sofia de Vasconcelos (2020), p.104-125.

⁶³ Exemplos: *Amazon.com, Apple, Facebook, Inc. e Microsoft Corporation*.

⁶⁴ PINHEIRO, Alexandre Sousa [et. al.]; GONÇALVES, Jorge Carlos (2018), p. 504-511.

fundamentalmente similar ao assegurado na União, sendo os dados tratados num ou mais setores específicos, por exemplo, utilizando critérios claros e objetivos⁶⁵.

No segundo parâmetro, deverá o país terceiro garantir o controlo efetivo e independente da proteção dos dados, estabelecendo regras de cooperação com autoridades de proteção de dados dos Estados-membros, conferindo também aos titulares dos dados direitos efetivos e oponíveis, com vias de recurso administrativo e judicial efetivas⁶⁶.

No terceiro elemento, a Comissão terá em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de Janeiro de 1981 e ao seu Protocolo Adicional.

Adicionalmente, deverá a Comissão consultar o Comité aquando da avaliação do nível de proteção nos países terceiros⁶⁷. Ademais, uma vez avaliada a adequação do nível de proteção, através de um ato de execução, a Comissão pode decidir pela garantia do nível de proteção adequado por parte do recetor dos dados e que este respeita os elementos descritos.

O procedimento de avaliação periódica está relacionado com a necessidade de a UE controlar, de forma continuada, os desenvolvimentos pertinentes no país terceiro no intervalo de tempo em causa na matéria de proteção de dados, importância clara atribuída ao controlo da Comissão da eficácia das decisões de adequação sobre o nível de proteção assegurado num país terceiro⁶⁸. Por conseguinte, a Comissão deverá ter em consideração as conclusões realizadas por parte do Parlamento e Conselho⁶⁹, bem como outros organismos relevantes no tema. E o deverá fazer num prazo razoável⁷⁰.

⁶⁵ Considerando (104).

⁶⁶ Ibidem.

⁶⁷ Considerando (105).

⁶⁸ Decisões adotadas com base no art. 25.º n.º 6 ou no art. 26.º n.º 4 da Diretiva 95/46/CE.

⁶⁹ Considerando (106).

⁷⁰ UNIÃO EUROPEIA, Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011.

É publicitado no Jornal Oficial da União e no site da Comissão uma lista dos países terceiros, territórios e setores específicos de um país terceiro/organização internacional⁷¹, cujos atos de execução tenham assegurado, ou não, um nível de proteção adequado⁷².

Se, num eventual procedimento de avaliação periódica, a informação disponível constatar que um determinado recetor de dados pessoais deixou de assegurar o nível exigido, a Comissão revoga, altera ou suspende a decisão, sem efeitos retroativos. Subsequente, a Comissão inicia consultas com o país terceiro para a correção da situação. Esta decisão de inadequação do nível de proteção não prejudica as transferências de dados, desde que os responsáveis apresentem garantias adequadas (*a seguir*).

4.2. Garantias adequadas.

No caso de a Comissão não ter adotado uma decisão de adequação que reconheça o nível de proteção adequado, mediante ato de execução e nos termos do art. 45.º, n.º 3 RGPD as transferências internacionais de dados para países terceiros ficam sujeitas à apresentação de “garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes”⁷³.

Como dito, se a Comissão reconhecer que um país terceiro deixou de assegurar nível adequado de proteção, proíbe a transferência de dados pessoais, a menos que sejam cumpridos os requisitos relativos às transferências sujeitas as garantias adequadas⁷⁴. Em concordância com o art. 46.º, n.º 2 RGPD estas garantias podem ser previstas, dispensando a autorização específica da autoridade de controlo, por meio de⁷⁵:

- a) Instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
- b) Regras vinculativas aplicáveis às empresas, cfr. art. 47.º;
- c) Cláusula-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame, cfr. art. 93.º n.º 2;

⁷¹ Em 15 de Janeiro de 2024 a Comissão Europeia concluiu com êxito a revisão de 11 decisões de adequação existentes. Estas decisões tinham sido adotadas ao abrigo da legislação da UE em matéria de proteção de dados que precedeu o RGPD. No seu relatório, a Comissão considera que os dados pessoais transferidos da União Europeia para *Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Ilha de Man, Israel, Jersey, Nova Zelândia, Suíça e Uruguai* continuam a beneficiar de garantias adequadas em matéria de proteção de dados. https://commission.europa.eu/document/f62d70a4-39e3-4372-9d49-e59dc0fda3df_en [consult. a 28/Fev/2024].

⁷² PINHEIRO, Alexandre Sousa [et. al.]; GONÇALVES, Jorge Carlos (2018), p. 512.

⁷³ Art. 46.º, n.º 1 RGPD.

⁷⁴ Considerando (107).

⁷⁵ Alíneas a) - f).

- d) Cláusula-tipo de proteção adotada por uma autoridade de controlo e aprovada pela Comissão pelo procedimento de exame, cfr. art. 93.º n.º 2;
- e) Código de conduta, aprovado nos termos do art. 40.º; ou
- f) Procedimento de certificação, aprovado nos termos do art. 42.º.

Preocupa-se aqui em assegurar o cumprimento dos requisitos à proteção de dados e o respeito pelos direitos dos titulares assim como na União, em especial, sublinhando a necessidade à existência do direito fundamental à tutela jurisdicional.

Ainda, a utilização de cláusula-tipo de proteção adotada pela Comissão ou por autoridade de controlo não impede que o responsável pelo tratamento e o subcontratante as incluam num contrato mais abrangente, nem que acrescentem outras cláusulas ou garantias adicionais; desde que não entre em conflito com as designadas pela Comissão ou por uma autoridade de controlo.

O art. 47.º RGPD trata das regras vinculativas aplicáveis às empresas, em que compete às autoridades de controlo aprovar por meio do procedimento de controlo da coerência previsto no art. 63.º⁷⁶, por exemplo (n.º 2): a aplicação dos princípios gerais de proteção de dados (alínea d)) e os direitos dos titulares dos dados quanto ao tratamento e regras do exercício desses direitos (alínea e)).

4.3. Acordos internacionais.

Autores como Pinheiro e Gonçalves (2018)⁷⁷ criticam a nomenclatura escolhida para a epígrafe do art. 48.º do RGPD, acreditando ser incompleta no que toca ao seu conteúdo. O artigo trata do reconhecimento ou da execução de decisões judiciais ou administrativas estrangeiras, isto é, a União pode obstruir o reconhecimento de medidas jurídicas de países terceiros que entrem em conflito com os seus valores próprios. Trata-se de um método para alargar o alcance global do direito comunitário, uma vez que se baseia numa afirmação dos valores da UE em relação a medidas jurídicas adotadas por um país terceiro⁷⁸.

De acordo com Christopher Kuner (2017):

“Esta disposição é semelhante aos chamados "*blocking statutes*" que protegem as partes na UE das consideradas afirmações jurisdicionais exorbitantes por parte de países terceiros (...)"⁷⁹⁸⁰

⁷⁶ PINHEIRO, Alexandre Sousa [et. al]; GONÇALVES, Jorge Carlos (2018), p. 519-522.

⁷⁷ Ibidem, p. 523.

⁷⁸ KUNER, Christopher (2017).

⁷⁹ Ibidem, p.26.

⁸⁰ Tradução nossa.

Dito isto, limita-se decisões de um país terceiro adotadas no exercício das funções jurisdicionais ou administrativas a qual exijam aos responsáveis pelo tratamento ou subcontratante a transferência ou divulgação de dados. Não obstante, na UE, isto só será possível se houver como base um acordo internacional, exemplo, acordos de assistência judiciária mútua entre o país terceiro em questão e a UE ou um dos seus Estados-Membros.

***4.4.Situações específicas*⁸¹.**

Este último mecanismo de garantia de proteção compõe-se por situações taxativamente previstas no RGPD. Isto é, o legislador europeu considerou ainda permissível efetuar transferências ao abrigo do art. 49.º, caso seja possível verificar as condições expressamente previstas.

Como explicado em parecer da CNPD: “estas derrogações têm caráter excecional e só podem ser consideradas quando as transferências sejam pontuais, não podendo convocar-se quando tratar de fluxos transfronteiriços com caráter regular”⁸².

As situações dizem respeito à possibilidade de o titular dos dados pessoais dar o seu consentimento explícito, por exemplo, para o cumprimento de um contrato; no caso de motivos importantes de interesse público previsto no direito da União ou o direito de um Estado-membro, a que o responsável pelo tratamento está sujeito. Nessa última, a CEPD elucida que, para esta derrogação não é suficiente que a transferência de dados seja solicitada por uma autoridade de um país terceiro para a investigação que sirva um interesse público do país em causa e que, em abstrato, também exista legislação da União ou dos Estados-membros⁸³.

Isto é, a mera existência de legislação europeia não é, por si só, um fator suficiente para aplicar o art. 49.º, n.º 1, alínea d). Longe disso, antecessores da CEPD⁸⁴, destacaram

⁸¹ Intitulado de “derrogações para situações específicas” em português. Colocamos aqui uma crítica quanto à tradução do Regulamento em comparação com a versão em inglês. É conhecimento público que a União Europeia possui 24 línguas oficiais, isto é, as línguas dos seus vários países membros. Porém, a maior parte dos documentos oficiais dos vários órgãos da União são normalmente redigidos em inglês e/ou francês e, subsequentemente, nas diversas outras línguas oficiais. Desse modo, sendo o título em inglês “*derogations for specific situations*”, e de acordo com a definição jurídica do Diário da República de “derrogação” ser: “(...) a revogação de uma lei por outra, que lhe é posterior, com a particularidade de ser parcial. Isto é, trata-se de uma cessação parcial da sua vigência. (...)”, ou seja, sua anulação, abolição. Não achamos o termo adequado para intitular o artigo 49.º do Regulamento, sendo preferível ter colocado derivações da palavra “exceção”, na medida em que se trata de oportunidades excecionais de transferências de dados pessoais para países terceiros.

⁸² CNPD, PARECER/2022/13 p. 1v, ponto 11.

⁸³ CEPD, Diretrizes 2/2018, p.10.

⁸⁴ GT29, *Opinion 10/2006* (WP128).

que a derrogação só se aplica quando também se pode deduzir do direito da UE, ou do Estado-membro a que o responsável pelo tratamento está sujeito, que essas transferências de dados são permitidas para fins importantes de interesse público, incluído no espírito de reciprocidade para a cooperação internacional. Por exemplo acordos ou convenções internacionais que prevejam a cooperação internacional para promover o objetivo do combate ao terrorismo em concreto⁸⁵, sendo aí indicador de avaliação da existência de um interesse público nos termos do RGPD.

5. Reflexões intermédias.

Em vista do explicitado, a reforma legislativa da proteção de dados na UE com o RGPD constituiu instrumento essencial à concretização e edificação do Mercado Único Digital Europeu⁸⁶, uma vez que (i) permite a Europa manter sua posição privilegiada na economia digital, e (ii) fortificou a segurança dos titulares de dados nas novas tecnologias de informação dando maiores garantias de proteção.

Nas palavras de Ratcliff, De Bono e Martinello (2024):

“O mercado único digital beneficia a economia, reduz os impactos ambientais e melhora a qualidade de vida graças ao comércio eletrónico e à administração pública em linha.”⁸⁷

A posição de privilégio que a Europa possui deriva dos fortes investimentos financeiros da UE em infraestruturas de tecnologia, exemplo, a nova Plataforma de Tecnologias Estratégicas para a Europa (STEP)⁸⁸ e na implementação de fortes normas em matéria de proteção de dados.

Na sequência, iremos examinar os casos em concreto da relação UE – EUA na matéria e processos que tem surgido no TJUE por violações dos direitos fundamentais dos cidadãos europeus, oriundos dos programas de vigilância em massa de entidades públicas americanas⁸⁹.

⁸⁵ UNIÃO EUROPEIA, Conclusões do Conselho (2020).

⁸⁶ Christina RATCLIFF, Jordan DE BONO, Barbara MARTINELLO (2023), p. 1.

⁸⁷ Ibidem.

⁸⁸ UNIÃO EUROPEIA, COM (2023) 335 final.

⁸⁹ SIMON, Joel (*s.d.*). Descreve que: “Os documentos vazados pelo ex-contratado da Agência de Segurança Nacional (NSA, sigla em inglês) *Edward Snowden* mostram que alguns dos programas de espionagem dos EUA operaram com o apoio técnico de empresas de tecnologia sob a jurisdição norte-americana”, em <https://cpj.org/pt/2014/02/ataque-a-imprensa-em-2013-como-a-espionagem/> [consult. 02/Abr/2024].

Capítulo III

6. Quadro UE – EUA em matéria de proteção de dados.

No contexto do diálogo UE e EUA, a estreita cooperação dos Estados-membros atravessam a história pela partilha de valores democráticos e princípios de natureza económica, política, social e de segurança. Ao qual vêm assegurando a conservação dessa relação bilateral⁹⁰. Um exemplo foi a criação do Plano Marshall, pós II Guerra, em que os norte-americanos concluíram que a reconstrução económica da Europa era essencial para o interesse norte-americano⁹¹.

O Parlamento e a Comissão afirmaram que, “as relações económicas entre os EUA e UE são as mais significativas do mundo”⁹², “o comércio transatlântico atingiu um máximo histórico de 1,2 biliões de euros em 2021(...)”⁹³.

Enquanto persistir as transferências de dados pessoais para um país que não tem normas e garantias de proteção semelhante, como é o caso norte-americano, o estudo será de fulcral relevância para a sociedade de informação⁹⁴. Ainda mais porque a movimentação de dados entre UE-EUA constitui o maior fluxo do mundo. Em termos comparativos, representa mais que o dobro do fluxo entre os EUA e a América Latina⁹⁵, por exemplo. O escoamento de dados que atravessa o oceano não se limita aos acordos comerciais⁹⁶, não obstante, inclui os provenientes do uso de plataformas *online*⁹⁷ e monitores de pesquisa *online* gratuitos⁹⁸, na sua maioria com sede nos Estados Unidos.

Num cenário em que não houvesse o direito da UE para a proteção dos titulares de dados dos cidadãos europeus, e considerando que seriam aplicadas regras iguais aos cidadãos norte-americanos, esses dados seriam tratados e armazenados sem qualquer diferenciação, incorrendo no perigo de violações dos direitos fundamentais dos cidadãos europeus.

⁹⁰STEIL, Benn (2019), capítulo quarto.

⁹¹HOGAN, Michael J. (1987), p.26-27.

⁹²UNIÃO EUROPEIA, Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados.

⁹³COMISSÃO EUROPEIA, “*EU trade relations with the United States. Facts, figures and latest developments. Country or region*”, [consult. 5/Mar/2024].

⁹⁴NEGROPONTE, Nicholas (1995).

⁹⁵WEISS, Martin A., ARCHICK, Kristin (2015), p. 4.

⁹⁶OECD (2022).

⁹⁷Exemplo, *Facebook* e *X* (antigo *Twitter*).

⁹⁸Exemplo, *Google*.

Não podendo permitir isso, a União consagrou mecanismos que tutelassem efetivamente a proteção de dados no que toca às transferências internacionais para países terceiros, tornando-as factíveis. Explicado no capítulo anterior.

Tendo em vista a diferença do sistema jurídico americano e europeu na política de proteção de dados pessoais e na linha de Maximillian Schrems⁹⁹, existe aqui uma qualificação díspar de liberdade-segurança. Enquanto na União se exige privacidade, em contrapartida, nos EUA se exige vigilância, conflito esse fundamental. Compreende-se, portanto, a dificuldade nas negociações de decisões de adequação realizadas ao longo dos anos. A problemática resultou na invalidação já de duas decisões de adequação da Comissão¹⁰⁰, através de jurisprudência do TJUE, em que o órgão concluiu pela violação dos direitos fundamentais dos titulares dos dados pessoais.

Apesar de manifestas preocupações por parte do CEPD¹⁰¹ e do PE¹⁰², em 10 de Julho de 2023 a Comissão adotou nova decisão de adequação sobre nível de proteção dos dados pessoais, Decisão “Quadro de Privacidade UE-EUA”¹⁰³.

Logo, analisaremos de forma concisa as duas primeiras decisões de adequação: estrutura e funcionamento; e as consequentes declarações de invalidade pelo TJUE. Em seguida, exploraremos a mais recente decisão, examinando-a sob a ótica da indagação: os mecanismos de decisão de adequação constituem efetivos instrumentos de tutela dos direitos fundamentais nas transferências de dados para países terceiros?

6.1. Decisão de Adequação “Porto Seguro”.

A abordagem norte-americana na proteção de dados é desempenhada por meio de leis dispersas (para setores específicos), regulamentos, autorregulação e jurisprudência¹⁰⁴. Ou seja, não há uma legislação federal de proteção de dados abrangente.

Posto isto, as transferências de dados pessoais para países terceiros, conduzidas por exportadores, devem ser acompanhadas de garantias adicionais ou, em última instância, de derrogações previstas no art. 26.º da Diretiva 95/46/CE, agora art. 49.º do RGPD. No panorama para acautelar os receios dos exportadores e fornecer um enquadramento mais previsível, que foi desenvolvida a Decisão 2000/520/CE, por meio de negociações entre o Departamento de Comércio americano (DOC) e instituições europeias.

⁹⁹ SCHREMS, Maximillian (2021).

¹⁰⁰ Referência n.º 23 e n.º 24.

¹⁰¹ CEPD, Opinion 5/2023.

¹⁰² UNIÃO EUROPEIA, Resolução do Parlamento Europeu, 11 de maio de 2023.

¹⁰³ Cfr. referência n.º 25.

¹⁰⁴ CHIAPPETTA, Aline Holanda (2018), p. 50.

A Decisão “Porto Seguro” (PS) surgiu após pareceres do Grupo de Trabalho do Artigo 29.^{o105}(GT29)¹⁰⁶, junto com as funções de controlo prévio do Parlamento Europeu. Por esta razão surgiu a perspectiva de se atingir uma convergência normativa nas transferências transatlânticas sem, todavia, perder o nível de proteção atribuído na UE.

Com base no art. 25.^o da Diretiva, estabeleceu-se sete princípios a serem observados na Decisão PS: *princípio do aviso, da escolha, de retransferência, da segurança, da integridade dos dados, do acesso e da aplicação*¹⁰⁷. A aferição de um nível de proteção adequada nas transferências de dados para os EUA dava-se com a aplicação em conformidade com as diretrizes previstas nas questões mais frequentes (FAQ)¹⁰⁸, permitindo assim o livre fluxo de informações para empresas sediadas nos EUA. Assemelhando-se às operadas internamente na UE.

Segundo o art. 1.^o n.^o 3, as empresas deveriam fazer comunicar previamente sua adesão ao DOC, e subsequente à análise da adesão, as entidades encarregadas procederiam a publicação *online* de uma lista das organizações que tivessem sido auto certificadas, conforme os princípios. A presença de uma organização na lista, além de possuir caráter informativo às empresas e cidadãos, gerava expectativas legítimas aos titulares dos dados europeus de que seus dados estariam a ser devidamente protegidos.

Apesar da adesão ao sistema de auto certificação ser voluntária, era ainda necessário que as organizações estivessem abrangidas no âmbito de competência da *Federal Trade Commission* (FTC)¹⁰⁹; porém, eram aqui excluídos diversos setores de serviços, sobretudo das finanças e telecomunicações¹¹⁰.

Além disso, o sistema de auto certificação ficava sujeito a uma revisão anual. Caso as organizações não estivessem em conformidade com os princípios aderidos, a Decisão atribuía à FTC competência para impor sanções e medidas coercitivas no caso de

¹⁰⁵ Criado pela Diretiva 95/46/CE, lidou com as questões relacionadas com a proteção da privacidade e dos dados pessoais até 25 de maio de 2018 (entrada em aplicação do RGPD), sendo posteriormente substituído pelo EDPB.

¹⁰⁶ Exemplos: Parecer 1/99 (WP 15) sobre o nível de proteção de dados nos Estados Unidos e as discussões em curso entre a Comissão Europeia e o Governo dos Estados Unidos, Parecer 2/99 (WP 19) sobre a adequação dos "Princípios Internacionais de Porto Seguro" emitidos pelo Ministério do Comércio dos EUA em 19 de abril de 1999 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [consult. 04/Abr/2024].

¹⁰⁷ UNIÃO EUROPEIA, Decisão 2000/520/CE, Anexo I.

¹⁰⁸ Ibidem, Anexo II.

¹⁰⁹ Ibidem, considerando (5).

¹¹⁰ Ibidem, considerando (6).

violações¹¹¹, segundo o *FTC Act*¹¹². Adicionalmente, a Decisão atribuía às autoridades de proteção de dados dos Estados-membros a competência para suspender as transferências em casos específicos¹¹³, passível de reversão quando o Estado-membro fosse informado da cessação da violação.

Por outro lado, no art. 3.º n.º 4, a Decisão ressaltava o caso de organismos americanos competentes não estarem a desempenhar suas funções de forma desejada. Caberia, então, à Comissão informar ao DOC e, se necessário, revogar, suspender ou limitar o âmbito da referida Decisão. Garantia, ainda, que a Decisão poderia ser adaptada em qualquer altura caso houvesse alterações legislativas internas nos Estados Unidos.

Apesar de todos esforços de proteção dos titulares de dados pessoais, a aplicação da Decisão nunca foi pacífica. Muito pelo contrário, vários autores reiteraram preocupações com a efetiva garantia e proteção dos direitos fundamentais dos cidadãos europeus. O GT29 afirmou que “a proteção dos indivíduos no que toca ao processamento dos seus dados pessoais é parte das “liberdades e direitos fundamentais””¹¹⁴.

No decorrer do tempo, o cidadão austríaco Maximilian Schrems, advogado e ativista em matéria de direito da proteção de dados, desenvolveu investigações quanto às políticas de privacidade do *Facebook* e outras redes sociais. Em seus estudos, Schrems tomou conhecimento de que a sede da empresa *Facebook*, nos EUA, possuía e armazenava os dados pessoais dos seus usuários, incluindo utilizadores europeus que tiveram seus dados transferidos ao abrigo da Decisão PS.

Em cumprimento do princípio do acesso¹¹⁵, a política interna da empresa consentia no envio desses dados aos titulares europeus mediante o exercício dos seus direitos. Com base nisso, e através da ONG “*Europe versus Facebook*”, Schrems fez um pedido à empresa norte-americana para que enviassem cópia dos dados que a mesma dispunha sobre si. Em resposta ao pedido, a *Facebook* enviou inúmeras páginas discriminando suas atividades na rede social, desde sua adesão, incluindo conteúdos que o mesmo já havia removido, por exemplo, todos os amigos que foram “*unfriended*”¹¹⁶.

¹¹¹ Ibidem, Anexo V §3.

¹¹² Federal Trade Commission Act Incorporating U.S. SAFE WEB Act amendments of 2006 (Unofficial version), §§ 41-58.

¹¹³ UNIÃO EUROPEIA, Decisão 2000/520/CE, art. 3.º, n.º 1, alíneas a) e b).

¹¹⁴ GT 29, *Opinion* 4/2000 (WP 32), §4.

¹¹⁵ UNIÃO EUROPEIA, Decisão 2000/520/CE, Anexo I.

¹¹⁶ Website *Europe versus Facebook*, “*Facebook’s Data Pool*”, em http://europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html [consult. 06/Abr/2024].

As preocupações se intensificaram em 2013 quando um ex-agente de tecnologia da informação¹¹⁷ da CIA e da NSA, agências americanas de inteligência e segurança, Edward Snowden, trouxe à tona que estas estavam envolvidas na utilização de programas de vigilância em larga escala¹¹⁸¹¹⁹. Tais programas permitiam o acesso e coleta em massa de dados de comunicação telefônica realizadas pelas *Big Tech*, que poderiam ser obrigadas a fornecer o acesso aos dados quando houvesse ordem judicial emitida pelo Tribunal de Vigilância de Inteligência Estrangeira (FISC).

Ora, a operacionalização de tais programas atentava precisamente à garantia de proteção dos dados pessoais ao abrigo da Decisão e da Diretiva europeia, uma vez que os programas permitiam a colheita dos dados de forma indiscriminada.

Em virtude dos acontecimentos, autoridades europeias competentes emitiram declarações e Comunicações¹²⁰, salientando a inadmissibilidade dos programas de vigilância e a insuficiência do acesso administrativo ou judicial para titulares de dados da UE. Era, portanto, absolutamente inacreditável que os titulares europeus não estivessem cientes de que seus dados estavam a ser acedidos pelo governo norte-americano, desconhecendo inclusive as finalidades do acesso e não tendo meios adequados para proteção.

Desse modo, ainda que o Caso *Katz vs. United States* (389 U.S. 347 (1967))¹²¹ tenha expandido a aplicação da Quarta Emenda da Constituição americana¹²² à proteção da privacidade das comunicações e informações pessoais, a discrepância de proteção dos sistemas jurídicos mantinha-se.

Apesar das revelações, e ao contrário da posição do Parlamento¹²³, tendo em consideração a relação comercial entre as partes, bem como os impactos negativos nas empresas, a Comissão decidiu por manter o sistema da Decisão¹²⁴. Salientou, porém, que a aplicação de exceções baseadas por motivos de segurança nacional, apenas poderiam ser justificadas mediante a verificação de dois critérios cumulativos: *critérios da proporcionalidade e da necessidade*.

¹¹⁷ Para desenvolvimentos, GREENWALD, Glenn (2014).

¹¹⁸ Correio Braziliense: Mundo (2023), [consult. 5/Abr/2024].

¹¹⁹ Exemplos dos programas de vigilância e coleta de dados: “PRISM”, “SIGINT”, “UPSTREAM”; Oliver Stone (2016).

¹²⁰ UNIÃO EUROPEIA, COM (2013) 846 final; COM (2013) 847 final.

¹²¹ U.S. Supreme Court, *Katz v. United States*, 389 U.S. 347 (1967). “PRIMARY HOLDING: *It is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a reasonable expectation of privacy, unless certain exceptions apply.*”

¹²² Constitution of the United States, Fourth Amendment.

¹²³ UNIÃO EUROPEIA, Resolução do Parlamento Europeu, de 12 de março de 2014.

¹²⁴ UNIÃO EUROPEIA, COM (2013) 846 final, p.8, § 3

Em decorrência da gravidade das declarações do ex-agente, Schrems recorreu ao DPC irlandês¹²⁵ alegando que os dados recolhidos e transferidos pela *Facebook Ireland* para a *Facebook Inc.* poderiam ser objeto dos programas de vigilância conduzido pelas autoridades norte-americanas “para além do estritamente necessário e proporcional em relação à proteção de segurança nacional”¹²⁶ e, portanto, não estariam sendo objeto de proteção adequada nos EUA. Em 2013, este denuncia a violação de seus direitos fundamentais e solicita que fossem proibidas futuras transferências de seus dados pessoais.

A DPC irlandesa, por entender que não estava obrigada a investigar os factos denunciados e que não existiam provas suficientes quanto a *NSA*, arquivou a denúncia. Insatisfeito com a decisão, *Schrems* recorreu ao Supremo Tribunal de Justiça irlandês (*High Court*)¹²⁷.

O órgão jurisdicional analisou, inicialmente, com base no direito irlandês, concluindo que recaía sob o *Commissioner* (Comissário) a obrigação de investigar, visto que os cidadãos europeus “não possuíam nenhum direito efetivo a serem ouvidos”¹²⁸ nas jurisdições americanas. Por outro lado, considerou que o caso respeitava à aplicação do direito da União, a Decisão 2000/520/CE, a qual não estava a satisfazer os artigos 7.º e 8.º da Carta¹²⁹, princípios assentados no *Ac. Digital Rights Ireland*¹³⁰.

Assim, sob reenvio prejudicial para o TJUE, o *High Court* questionou sobre os poderes das autoridades nacionais de controlo na acessão da Diretiva 95/46/CE e sobre a validade da Decisão PS.

6.1.1. Acórdão “Schrems I” (C-362/14).

Em resposta, o TJUE decidiu que nada obstava que a DPC irlandesa utilizasse a diligência necessária para investigar e decidir denúncias sobre as transferências de dados para países terceiros¹³¹¹³², quando em causa esteja a proteção dos direitos e liberdades fundamentais dos cidadãos europeus¹³³.

¹²⁵ TJUE, C-362/14, § 27.

¹²⁶ *Ibidem*, § 22.

¹²⁷ *Ibidem*, §§ 29 e 30.

¹²⁸ *Ibidem*, C-362/14, § 31.

¹²⁹ *Ibidem*, C-362/14, § 34.

¹³⁰ Referência n.º 44.

¹³¹ Referência n.º 44; *Ac. TJUE, Schrems*, C-362/14, § 43.

¹³² TJUE, C-518/07; C-288/12, §48.

¹³³ *Ac. TJUE, Schrems*, C-362/14, §§ 56 e 57.

Como indicado, as transferências de dados para países terceiros só poderiam ser feitas se obedecessem a um nível de proteção adequado e, como a Diretiva não definiu tal conceito, apenas elencou critérios, o TJUE entendeu que para alcançar este nível era exigido que estes países utilizassem meios judiciais eficazes para garantir a proteção de forma equivalente ao da UE¹³⁴, não mais que isso. Em seguida, o TJUE passou a examinar o nível de proteção adequado nas transferências para os EUA com base na Decisão PS, nos artigos da Diretiva 95/46/CE em causa e da Carta, juntamente com os atos legislativos americanos e as conclusões do Advogado-Geral (AG)¹³⁵.

Em suma, o Tribunal declarou a invalidade do art. 1.º da Decisão PS, entendendo que a Comissão falhou na avaliação do nível de proteção adequado garantido pelos EUA devido à legislação interna deste; e do art. 3.º considerando que a Comissão limitou os poderes das autoridades nacionais de controlo, ultrapassando assim suas competências atribuídas pelo artigo 25.º, n.º 6, da Diretiva. E, uma vez que os artigos 2.º e 4.º da Decisão estavam indissociáveis, a invalidade afetou a Decisão na sua totalidade¹³⁶.

Em decorrência da decisão, o GT29 emitiu declaração chamando para um diálogo aberto com as autoridades norte-americanas, urgente, com o objetivo de encontrar novas soluções para a continuidade das transferências. Afirmou, ainda, que as autoridades nacionais de controlo consideravam que as Cláusulas Contratuais-Tipo (CCT) e as regras vinculativas às empresas (BCRs)¹³⁷ poderiam continuar a ser utilizadas, a fim de dar seguimento às transferências para os EUA. Para proteger os direitos fundamentais, a Comissão¹³⁸ estabeleceu que as transferências não poderiam ser feitas utilizando a Decisão invalidada. E, em consonância com o GT29, definiu quatro conjuntos de CCT (Decisão 2010/87/CE¹³⁹) e BCRs que poderiam ser utilizadas para as transferências.

O Tribunal fixou, juntamente com as autoridades norte-americanas, “novos critérios que a Comissão deve utilizar ao decidir se um país terceiro oferece um nível de proteção adequado”¹⁴⁰. Critérios estes que veremos que continuam a ser insuficientes.

¹³⁴ CHIAPPETTA, Aline Holanda (2018), p. 63-64.

¹³⁵ TJUE, C-362/14, § 89.

¹³⁶ Ibidem, §§ 100-106.

¹³⁷ GT 29, (2015) §§1-4.

¹³⁸ UNIÃO EUROPEIA, COM (2015) 566 final, §7.

¹³⁹ UNIÃO EUROPEIA, Decisão 2010/87, de 5 Fevereiro 2010.

¹⁴⁰ FARINHO, Domingos Soares (2016), p.123-124

6.2. Decisão de Adequação “Escudo de Proteção da Privacidade”.

Após decisão do TJUE e dada a importância das transferências nas relações comerciais gerou-se urgência de providenciar nova estrutura que garantisse a “livre circulação e o respeito ao tratamento dos dados pessoais, com base nos direitos e liberdades fundamentais dos cidadãos europeus”¹⁴¹.

Em 2016, a Comissão lançou o projeto “Escudo de Proteção da Privacidade”, juntamente, com Comunicação referindo-se ao “plano de ação para restaurar a confiança nas transferências de dados no interesse da economia digital europeia”¹⁴², criado em 2013. Objetivos reafirmados nas Orientações Políticas da Comissão de *Jean-Claude Juncker*¹⁴³.

Obedecendo aos trâmites procedimentais europeus, procedeu-se à consulta por parte do GT29 e da Autoridade Europeia para Proteção de Dados (AEDP) para se pronunciarem sobre aspetos de tratamento dos dados, especialmente, no nível de proteção adequado.

No parecer do GT29¹⁴⁴ esse apontou *upgrade* da nova Decisão, porém alertou para permanência de possíveis condutas abusivas das autoridades americanas no acesso aos dados transferidos; a burocratização do acesso à informação pelos particulares e a complexidade no acesso aos novos mecanismos de recurso. E ao novo mecanismo chamado “*Ombudsman*” (figura mediadora de reparação), expôs preocupações de que este não seria suficientemente independente e não possuía poderes adequados para exercer sua atividade com imparcialidade, visto que o cargo era exercido por um Vice-Presidente do Departamento de Estado americano, nomeado pelo Presidente e confirmado pelo Senado¹⁴⁵.

Por sua vez, em parecer¹⁴⁶, a AEDP foi mais rigorosa. Deixou evidente que era imperativo adotar medidas que garantem a proteção à privacidade e à proteção de dados dos cidadãos europeus em todas as operações. Apontou que “o projeto de decisão atual poderá legitimar”¹⁴⁷ uma rotina ao acesso e utilização por parte das autoridades norte-americanas dos dados transferidos para fins comerciais por parte dos serviços de

¹⁴¹ Referência n.º 24, § 1-2.

¹⁴² UNIÃO EUROPEIA, COM (2016) 117 final, p. 2-3.

¹⁴³ *Ibidem*, p. 3 §1.

¹⁴⁴ GT29, Opinion 01/2016 (WP 238).

¹⁴⁵ *Ibidem*, p. 4 § 4 e 49 § 2 ss.

¹⁴⁶ AEDP, Opinião 4/2016, (2016/C 257/05) de 30/Maio/2016.

¹⁴⁷ *Ibidem*, p. 1 § 8.

segurança¹⁴⁸. Transformando a exceção numa regra. Urgia que fosse implementada melhoras significativas:

“(…) obter garantias suplementares em termos de necessidade e proporcionalidade, em lugar de legitimar o acesso sistemático a dados transferidos por parte das autoridades norte-americanas assente em critérios que têm uma base jurídica no país destinatário, mas não na UE, conforme afirmado pelos Tratados, as decisões da UE e as tradições constitucionais comuns aos Estados-Membros.”¹⁴⁹

Concordamos que isso não poderia acontecer, o acesso deveria ser em *circunstâncias excepcionais* e quando fosse indispensável para fins de interesse público *especificado*¹⁵⁰. E, apesar do Ac. *Schrems*, as condutas das autoridades norte-americanas de inteligência e segurança mantiveram-se e ainda viram seus poderes de vigilância expandidos por instrumentos legais americanos¹⁵¹.

Todavia, a Comissão adotou a Decisão 2016/1250, conhecida como “Escudo de Proteção da Privacidade UE-EUA”. E, para colmatar a complexidade do novo sistema, a mesma publicou um guia com orientações para os cidadãos¹⁵².

Em demonstração do compromisso norte-americano o ITA divulgou o *Federal Register* vol. 81, n.º 148¹⁵³, comunicando que as empresas interessadas em fazer uso da nova Decisão poderiam fazê-lo por meio do processo de auto certificação junto ao DOC, órgão responsável por sua avaliação. A adesão aos princípios continuava a ser feita através do sistema de auto certificação voluntária, porém eram agora vinculativos. Em consonância com exigência da Comissão, o DOC lançou site *online* para verificar se uma empresa ou organização dos EUA seguia a nova Decisão¹⁵⁴.

Quanto à estrutura e funcionamento da Decisão assemelhava-se à anterior, mas com melhorias após decisão do TJUE (C-362/14). Assim, permanecendo os princípios orientadores das transferências estes foram desenvolvidos e pormenorizados. O DOC¹⁵⁵, por sua vez, emitiu *princípios suplementares*, anexo II da Decisão, referentes a categorias específicas.

¹⁴⁸ SILVA, Heraclides Sequeira dos Santos (2017), p. 83-87.

¹⁴⁹ *Ibidem*, p. 1 § 1.

¹⁵⁰ Itálico nosso.

¹⁵¹ Exemplo: a Secção 702 do FISA (*Foreign Intelligence Surveillance Act*), *Executive Order* n.º 12333 e a *Presidential Policy Directive* 28 (PPD-28), retratados na nova Decisão e no Parecer da AEDP.

¹⁵² UNIÃO EUROPEIA, COMISSÃO EUROPEIA (s.d.) - Guia Do Escudo De Proteção Da Privacidade UE-EUA, <https://ec.europa.eu/newsroom/just/redirection/document/47776> [consult. 7/Abr/2024].

¹⁵³ DOC, International Trade Administration (2016).

¹⁵⁴ <https://www.dataprivacyframework.gov/> [consult. 7/Abr/2024].

¹⁵⁵ UNIÃO EUROPEIA, Decisão 2016/1250/CE, Anexo II, visão geral I, ponto 1.

Houve a *ampliação dos poderes e mecanismos* de supervisão e administração do DOC¹⁵⁶, com a responsabilidade pela elaboração e atualização da lista das organizações auto certificadas¹⁵⁷. Nesta mesma linha, ao órgão foi concedido tais poderes a fim de dar prioridade às queixas de incumprimento dos princípios submetidas por organismos independentes de resolução de litígio, pelo DOC e pelas APD¹⁵⁸, para determinar se a secção 5 da *FTC Act*¹⁵⁹ (lei relativa à Comissão reguladora do comércio federal) foi violada¹⁶⁰.

Em resposta aos receios da União, foram feitas declarações e compromissos fornecidos pelo governo americano através do ODNI, Anexo VI, sobre a limitação do acesso e utilização de dados pessoais, transferidos ao abrigo da Decisão, pelas autoridades públicas americanas. Criou-se mecanismo de supervisão da ingerência da segurança nacional, o Mediador para o Escudo de Proteção da Privacidade, Anexo III¹⁶¹. Nesse sentido, a acessibilidade e utilização dos dados seriam restringidas ao critério da necessidade e apenas por meio de decretos executivos ou diretivas presidenciais, na época eram o *Executive Order* 12333 (E.O. 12333)¹⁶², *Presidential Policy Directive 28* (PPD-28)¹⁶³ e *Foreign Intelligence Surveillance Act* (FISA).

Enquanto a PPD-28 preza pela privacidade, liberdades cívicas nas atividades de informação, pela necessidade de garantias adequadas¹⁶⁴; não obstante, no âmbito da FISA, “a vigilância da secção 702 consiste exclusivamente em visar cidadãos [de países terceiros] específicos sobre os quais foi feita uma determinação individualizada”¹⁶⁵, com o intuito de coleta de informações de inteligência¹⁶⁶ e com colaboração obrigatória dos serviços de comunicação eletrónica nos EUA, conforme revelado por Snowden.

¹⁵⁶ CHIAPPETTA, Aline Holanda (2018), p 73-74.

¹⁵⁷ UNIÃO EUROPEIA, Decisão 2016/1250/CE, §§ (20), (30)-(37).

¹⁵⁸ Ibidem, § (54).

¹⁵⁹ Ibidem, § (50).

¹⁶⁰ Ibidem, §§ (37), (51)-(55).

¹⁶¹ Ibidem, § (65).

¹⁶² E.O. 12333: *United States Intelligence Activities*, *Federal Register* Vol. 40, n.º 235 (8 de dezembro de 1981).

¹⁶³ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE WASHINGTON, DC 20511, Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014, <https://irp.fas.org/dni/dni-ppd-28.pdf> [consult. 8/Abr/2024].

¹⁶⁴ UNIÃO EUROPEIA, Decisão 2016/12/50/CE, § (69).

¹⁶⁵ Ibidem, § (81).

¹⁶⁶ Ibidem, “(...) constitui a base de dois programas de informações importante geridos pelos serviços de informações dos EUA (PRISM, UPSTREAM) (...)”.

Por seu turno, a E.O. 12333, é reconhecida como uma das principais fundamentações legais que embasam as atividades de inteligência conduzidas pela NSA e outras agências. Conforme delineado na Decisão:

“(…) define os objetivos, as orientações, os deveres e as responsabilidades da procura de informações dos EUA (incluindo o papel dos vários elementos do setor das informações) e estabelece os parâmetros gerais de conduta das atividades dos serviços de informações (em especial a necessidade de promulgar regras processuais específicas)”¹⁶⁷.

Segundo análise da Decisão, foi estabelecido que deveria ser dada prioridade à *recolha seletiva* de informações, em que a recolha em larga escala só seria autorizada quando a recolha seletiva, através de mecanismos discriminantes, não pudesse ser realizada por motivos técnicos ou operacionais¹⁶⁸. Entretanto, na hipótese de não ser possível evitar a recolha massiva, a utilização e acesso posterior deveriam ser estritamente limitados ao objetivo de segurança nacional específico e legítimo¹⁶⁹, estabelecido no Ac. *Schrems*¹⁷⁰.

A Decisão destacava as novas *vias de recurso* acessíveis aos titulares da UE, conforme legislação americana, constantes no Anexo VI, p. V¹⁷¹. As organizações deveriam informar, de forma clara, um ponto de contacto, interno ou externo à organização, que iriam proceder as questões ou queixas, quer sediado nos EUA quer na UE¹⁷². Este direito de apresentar queixa e obter reparação está bem claro no Guia da Comissão¹⁷³.

Em consonância com o Ac. TJUE C-362/14, a Decisão impõe a necessidade de realizar periodicamente uma *reavaliação da adequação*¹⁷⁴, recaindo sob a Comissão juntamente com o DOC e a FTC, a análise de informações abrangentes sobre todos os aspetos relevantes do funcionamento da Decisão¹⁷⁵. E mais, se a Comissão recebesse informações que levantasse dúvidas sobre o nível de adequação, estaria obrigada a averiguar, cabendo os EUA a responsabilidade de informar a Comissão¹⁷⁶.

¹⁶⁷ Ibidem, § (68), nota (59).

¹⁶⁸ Ibidem, § (72).

¹⁶⁹ Ibidem, §§ (75)-(77).

¹⁷⁰ TJUE, C-362/14, n.º 93.

¹⁷¹ ANEXO VI – Carta do Conselheiro-Geral Robert Litt *Office of the Director of National Intelligence* (Gabinete do Diretor dos Serviços Nacionais de Informações).

¹⁷² UNIÃO EUROPEIA, Decisão 2016/12/50/CE, op. cit. §§ (41)-(51).

¹⁷³ Comissão Europeia (s.d.), p.5, ponto 7.

¹⁷⁴ UNIÃO EUROPEIA, Decisão 2016/12/50/CE, §§ (145)-(149).

¹⁷⁵ Ibidem, § (148).

¹⁷⁶ Ibidem, § (146).

Apesar das tentativas na subsistência de um nível de proteção adequado nas transferências internacionais de dados, dúvidas sobre a Decisão 2016/1250/CE permaneceram. Mormente aquando da entrada em vigor do RGPD, a 25 de maio de 2018.

Schrems tinha sido convidado a reformular sua queixa, uma vez que a *Facebook Inc.* alegou que devido a invalidação da Decisão PS, a forma permitida de continuar as transferências de dados pessoais era ao abrigo da Decisão 2010/87/CE que regulava as cláusulas-tipo (CCT)¹⁷⁷. Por sua vez, Schrems manteve sua posição de que a legislação interna americana era incompatível com os níveis de proteção vigentes e exigidos pela UE, impelindo que a DPC irlandesa suspendesse ou proibisse as transferências de seus dados pessoais.

A DPC irlandesa, por entender que a queixa suscitava a questão da validade da Decisão 2010/87/EU (CCT), pede ao *High Court*, com base no Ac. *Schrems* (C-362/14), que submetesse ao TJUE uma questão prejudicial, surgindo assim o Acórdão *Schrems II* (C-311/18)¹⁷⁸. Apesar de apresentar variadas questões¹⁷⁹ ao TJUE, optamos por abordar apenas três delas, com a análise mais detalhada de uma em particular.

- Se o âmbito de aplicação do RGPD abrangia transferências de dados efetuadas ao abrigo da Decisão 2010/87/UE, baseadas no nível de proteção assegurado pelas CCT.
- No contexto em causa, quais as obrigações das autoridades de controlo.
- O nível de proteção exigido pelo RGPD no que toca às transferências de dados à países terceiros (*a ser analisada*).

Ao nível de proteção exigido no que toca às transferências transatlânticas de dados pessoais, isto é, quanto aos elementos a terem em conta no art. 46.º n.º 1 e n.º 2, alínea c) do RGPD, o Tribunal diz que a leitura conjugada desses com o art. 45.º n.º 3, permitia concluir que, caso a Comissão não tenha redigido decisão de adequação, as aludidas transferências era possíveis no caso de o responsável pelo tratamento/subcontratante “apresentem garantias adequadas, e nas condições de os titulares dos dados gozarem de

¹⁷⁷ UNIÃO EUROPEIA, Decisão 2010/87/CE, art. 2.º.

¹⁷⁸ Acórdão de 16 de julho de 2020 *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximillian Schrems* (C-311/18), ECLI:EU:C:2020:559.

¹⁷⁹ *Ibidem*, § 77 ss.

meios para tornar seus direitos oponíveis, e mais, a existência de medidas jurídicas corretivas eficazes”¹⁸⁰. Inclusive as CCT, no n.º 2, alínea c)¹⁸¹.

O Tribunal urge em afirmar que tais requisitos que assegurem os direitos de proteção de dados dos cidadãos no RGPD, devem ter um nível substancialmente equivalente ao garantido pela União lidos à luz da Carta¹⁸², já aqui reforçado. Por fim, afirmou que na avaliação a ser feita do nível de proteção deve-se ter em consideração as estipulações contratuais acordadas entre responsável pelo tratamento/subcontratante da União e o destinatário da transferência em país terceiro quanto a um eventual acesso aos dados transferidos pelas autoridades do país terceiro, nos termos do art. 45.º n.º 2 RGPD.¹⁸³

O reenvio prejudicial ao Tribunal colocou em causa a validade da Decisão CCT e da Decisão 2016/1250/CE. Quanto à primeira, o TJUE colocou que o art. 1.º dispunha de garantias adequadas de proteção da vida privada, assim como dos direitos e liberdades fundamentais das pessoas; e apesar de sinalizar que não havia vinculação perante as autoridades de países terceiros¹⁸⁴, considerou a Decisão válida. Em sentido oposto, sobre a Decisão *Privacy Shield*, o Tribunal considerou que os requisitos da legislação nacional americana, especificamente quanto as ingerências utilizadas pelas autoridades públicas aos dados pessoais dos cidadãos europeus, mesmo com a justificativa de segurança nacional, não satisfaziam os requisitos essencialmente exigidos por legislação europeia, *ipso facto*, não concedia aos titulares direitos oponíveis às autoridades americanas nos tribunais¹⁸⁵.

Posto isto, em julho de 2020, o TJUE invalidou a Decisão Escudo de Proteção da Privacidade.

6.2.1. Acórdão Schrems II (C-311/18).

Como defendido por alguns autores¹⁸⁶, a opção do Tribunal por concluir pela adequação da Decisão (CCT) foi para não gerar um limbo jurídico. Encontrávamos no cenário em que uma segunda Decisão de adequação da Comissão era declarada inválida e que as leis americanas não possuíam mecanismos suficientes para o nível adequado de

¹⁸⁰ Leitura conjunta com artigo 44.º RGPD.

¹⁸¹ TJUE, C-311/18 §§ (103) e (104).

¹⁸² Ibidem, § (105).

¹⁸³ Ibidem

¹⁸⁴ Ibidem, § (125).

¹⁸⁵ CEPD (2020).

¹⁸⁶ NOGUEIRA, Catarina Conde (2019), p 26.

proteção para prevenir a ingerência de suas agências de inteligência nos dados pessoais dos cidadãos europeus.

Na sequência das conclusões do AG¹⁸⁷, o Tribunal confirmou a validade da Decisão CCT, embora estipulando requisitos mais rigorosos para as transferências baseadas na mesma. As cláusulas contratuais-tipo não apresentam motivos lícitos ou ilícitos para a transferência de dados, mas se as entidades pretenderem transferir dados com base neste mecanismo, têm de assegurar que a pessoa em causa dispõe de um nível de proteção essencialmente equivalente ao garantido pelo RGPD e pelo CDFUE¹⁸⁸.

Isto posto, as empresas e organizações atuantes na área de transferências de dados se sentiriam fragilizadas sem ter um instrumento jurídico como garantia concreta. E, sendo o comércio internacional intimamente ligado à capacidade de transferência de dados, compreendemos a escolha do Tribunal por manter mecanismo ao qual possibilitaria tal feito sem violar normas europeias. Apesar de entendermos ser defeituosa. O Tribunal continuou então a perpetuar jurisprudência protegendo os direitos fundamentais dos cidadãos.

Como resultado do *Acórdão Schrems II* e após Decisão vinculativa do CEPD¹⁸⁹, em Maio de 2023, a DPC irlandesa multou a *Meta Platforms Ireland Limited* (ulterior *Facebook Ireland Ltd*) em €1.2 bilhões por violações do art. 46.º n.º 1 do RGPD, por entender que a mesma não garantia o nível de proteção adequado; que as disposições sobre as CCT não podem compensar a inadequada proteção da legislação americana; e que a mesma não poderia invocar as exceções disponíveis no artigo 49.º do RGPD¹⁹⁰.

6.3. Decisão de Adequação “Quadro de Privacidade de Dados”. Será desta?

A análise da Decisão 2023/1795/CE, também conhecida como “Quadro de Privacidade de Dados” (QPD), estará voltada para a indagação: *“As decisões de adequação conseguem efetivamente proteger os direitos fundamentais dos cidadãos?”*. Avaliaremos se nesta Decisão a Comissão supriu as carências presentes em esforços anteriores e se conferiu maiores salvaguardas à proteção dos direitos dos cidadãos europeus quanto à transferência internacional dos seus dados para território norte-americano.

¹⁸⁷ CONCLUSÕES DO ADVOGADO-GERAL (2019), Processo C-311/18.

¹⁸⁸ FONSECA, Diogo Brito [et al.] (2022), p. 165-166.

¹⁸⁹ CEPD, Decisão vinculativa n.º 1/2023.

¹⁹⁰ DPC Irlanda (2023).

Em observação da evolução do quadro jurídico e tecnológico das transferências de dados para os Estados Unidos, a Comissão reconheceu a imperatividade de conceber nova Decisão para a salvaguarda dos direitos fundamentais dos cidadãos europeus perante o contínuo acesso por parte das autoridades norte-americanas.

Ademais, em fevereiro de 2023, o Parlamento emitiu Resolução¹⁹¹, no qual insta que a Comissão não adotasse o novo projeto de decisão de adequação, uma vez que conclui que a mesma não cria equivalência *efetiva* ao nível de proteção. Impele para que se continuasse as negociações com o governo norte-americano¹⁹². Ainda em processo consultivo, a Comissão solicitou ao CEPD parecer sobre o projeto¹⁹³. O órgão, em sua avaliação, teve como pedra angular as normas do quadro europeu em proteção de dados em vigor, incluindo artigos da Carta que resguardam os direitos à vida privada e familiar, direito à proteção de dados, direito à ação e em tribunal imparcial, assim como art. 8.º da CEDH, que protege o direito à vida privada e família.

No parecer do CEPD, de 28 de fevereiro de 2023, este congratula a Comissão por incluir disposições no domínio das decisões automatizadas (como tecnologias de *Artificial Intelligence*). Também, saúda as atualizações efetuadas aos princípios, que iriam constituir o quadro jurídico vinculativo aos aderentes à Decisão. Mas, em contrapartida, aponta que estes princípios permaneceram essencialmente inalterados em comparação com a Decisão anterior, incluindo a manutenção das preocupações com os direitos dos titulares, exemplo, o direito ao acesso e o direito à oposição¹⁹⁴.

Por outro lado, uma das fundamentais problemáticas tratava-se do acesso e utilização, em massa, de dados pessoais transferidos da UE por autoridades norte-americanas em seus serviços de inteligência e segurança. Também pontuado pelo PE.

Após negociações entre a Comissão e o Governo dos EUA, em 7 de outubro de 2022, o Presidente Joe Biden promulgou a *Executive Order* 14086¹⁹⁵ (EO 14086), a qual:

¹⁹¹ UNIÃO EUROPEIA, European Parliament, Committee on Civil Liberties, Justice and Home Affairs – DRAFT MOTION FOR A RESOLUTION, (2023/2501(RSP)).

¹⁹² Ibidem, p.5-6.

¹⁹³ CEPD, Parecer 5/2023.

¹⁹⁴ Ibidem, p. 3-4.

¹⁹⁵ US DEPARTMENT OF STATE, Executive Order 14086, “Policy and Procedures”, Bureau of Intelligence and Research.

- introduzia os *conceitos de necessidade e proporcionalidade*¹⁹⁶ nas atividades de informação de origem eletromagnética dos EUA¹⁹⁷, fortalecendo as garantias; e
- protegia *de forma efetiva* aos direitos dos cidadãos europeus, através do mecanismo do *Data Protection Review Court* (Tribunal de fiscalização da proteção de dados)¹⁹⁸ (DPRC), reforçando a matéria de independência.

O CEPD enfatizou, porém, que esperava que a Comissão desse seguimento ao dever de suspender, revogar ou alterar a decisão de adequação aquando de motivos emergenciais, especialmente se o Presidente dos EUA decidisse restringir as garantias incluídas no *Executive Order*¹⁹⁹.

Para a adoção da Decisão teve-se ainda em consideração os Ac. *Schrems I*²⁰⁰ e Ac. *Schrems II*²⁰¹. Nos acórdãos o Tribunal esclareceu que: não era exigido nível de proteção idêntico, mas sim “essencialmente equivalente”, e que houvesse normas que limitassem a ingerência nos dados transferidos dos titulares europeus²⁰²; ainda, as normas internas americanas limitam a proteção do cidadão europeu, incluindo a falta de vias de recurso interna para salvaguarda dos direitos fundamentais da Carta²⁰³.

Em contrapartida, a Comissão afirmou que analisou cuidadosamente a legislação e prática dos EUA, concluindo que tal parceiro assegurava o nível de proteção adequado aos dados transferidos ao abrigo da QPD²⁰⁴. E em 10 de julho de 2023, a Comissão adotou a Decisão de Execução (UE) 2023/1795 (QPD).

6.3.1. Exame crítico da nova Decisão.

Esta análise da Decisão irá cingir em três pontos específicos que vem sendo objeto de controvérsia e apresentado desafios substanciais, desde as primeiras duas Decisões. São: (1) a aplicação do nível de proteção adequado, (2) mecanismos de garantia efetiva ao acesso à justiça e (3) a ingerência das autoridades norte-americanas no acesso aos dados pessoais através de agências de ferramentas de inteligência e segurança, no qual estão intimamente associados.

¹⁹⁶ Ibidem, § 2(a)(ii)(A) (B) “*Signals intelligence activities may only be conducted when they are “necessary” and “to the extent and in a manner that is proportionate”.*”

¹⁹⁷ CEPD, Parecer 5/2023, p.4.

¹⁹⁸ Ibidem, p.5.

¹⁹⁹ Ibidem, p. 6.

²⁰⁰ TJUE, C-362/14.

²⁰¹ TJUE, C-311/18.

²⁰² UNIÃO EUROPEIA, Decisão 2023/1795/CE, considerando (4).

²⁰³ Ibidem, considerando (5).

²⁰⁴ Ibidem, considerando (1)-(3) e (7).

Autores como Gerke e Rezaeikhonakdar (2024), abordaram a discussão em saber se a EO 14086 consegue assegurar o equilíbrio entre a segurança nacional e o nível de proteção exigido pelo RGPD e pela jurisprudência europeia em proteção de dados dos indivíduos²⁰⁵. Afirmam que:

“A questão é que as atividades de informações de sinais "apenas" podem ser conduzidas quando são "necessárias para fazer avançar uma prioridade de informações validada" e "na medida e de uma forma que seja proporcional à prioridade de informações validada para a qual foram autorizadas".^{206 207}

Segundo estes autores, a interpretação americana dos princípios da necessidade e da proporcionalidade, contida no EO 14086²⁰⁸, é significativamente discrepante da interpretação do TJUE (no âmbito do significado jurídico). Isso porque, caso os EUA recorressem ao mesmo significado utilizado pela UE, teriam de limitar substancialmente os seus sistemas de vigilância em massa para respeitar o conceito de “*proportionate surveillance*” da UE²⁰⁹, que não abrange o acesso em larga escala por autoridades.

No mesmo sentido dos autores supra e no Parecer 5/2023 do CEPD, as atividades de recolha de informação devem ser conduzidas na prossecução de objetivos legítimos numa lista exaustiva²¹⁰, entretanto, o Presidente dos EUA tem completa discricionariedade para atualizar a lista de objetivos e determinar qual atividade pode ser utilizada para recolha de informação²¹¹.

Uma outra crítica está na criação do mecanismo de revisão e qualificação de queixas com “grande independência”, o DPRC, concretizado pelo EO 14086 juntamente com *Attorney General Regulation (AG Regulation)*²¹². O mecanismo é constituído por duas instâncias: (1ª) a investigação inicial das queixas apresentadas é efetuada pelo CLPO do ODNI (*Civil Liberties Protection Officer do Office of the Director of National Intelligence*); e depois (2ª) dá-se a possibilidade de recorrer ao DPRC, para que este reaprecie as decisões do CLPO²¹³.

²⁰⁵ GERKE, Sara and REZAEIKHONAKDAR, Delaram (2024), p. 394 ss.

²⁰⁶ Ibidem.

²⁰⁷ Tradução nossa.

²⁰⁸ Referência n.º 195.

²⁰⁹ “New US Executive Order unlikely to satisfy EU law”, 07 October 2022, em <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> [consult. 9/Abr/2024].

²¹⁰ E.O. 14086, Sec. 2, (b) (i) (A).

²¹¹ E.O. 14086, Sec. 2, (b) (i) (B).

²¹² Attorney General Order n.º 5517-2022, que altera os regulamentos do Department of Justice dos EUA, conforme mandato e autorização constantes do EO 14086.

²¹³ UNIÃO EUROPEIA, Decisão 2023/1795/CE, considerandos (179)-(183); GERKE, Sara and REZAEIKHONAKDAR, Delaram (2024), p. 397.

Uma vez que qualquer cidadão da UE tem o direito de apresentar queixa relativa a alegada violação por parte da legislação norte-americana que afete negativamente seus interesses em matéria de privacidade e liberdades cívicas²¹⁴, é a este mecanismo que devem recorrer. A Decisão QDP e a EO 14086 explicam minuciosamente o funcionamento deste mecanismo. Porém, podemos apontar falhas, a serem elencadas a seguir.

Apesar de apresentarem salvaguardas quanto à independência dos juízes do DPRC, sendo deixada expressa a proibição da intervenção do *Attorney General*, nada é dito quanto ao Presidente dos EUA²¹⁵. Ainda no que toca a “independência”, o autor Savin (2023) pontua que este mecanismo não é um “tribunal independente e imparcial previamente estabelecido por lei” na aceção do art. 47.º da Carta; mas um órgão do executivo, nomeado pelo *Attorney General*²¹⁶. Não solucionando assim a problemática do Ac. *Schrems II*.

Após a conclusão do pedido de análise da queixa, através de autoridade nacional, o DPRC apenas notifica o queixoso que “a análise não identificou qualquer violação ou que o DPRC emitiu uma determinação que exige a reparação adequada”²¹⁷, não havendo qualquer transparência quanto ao processo decisório.

E em termos deliberativos, o CEPD expressou preocupações com o carácter vinculativo e definitivo da decisão do DPRC, ressaltando a ausência de outro meio para que o cidadão possa interpor recurso²¹⁸. Problemática também abordada pela jurisprudência do TJUE no Ac. *Schrems I*²¹⁹ salientando a conseqüente violação do art. 47.º da Carta.

Concordamos então com os autores quando dizem que mesmo após um longo período de negociações entre UE e o Governo norte-americano, a lamentável realidade é que os EUA irão falhar novamente em assegurar o nível adequado de proteção, nos termos do art. 45.º do RGPD, lidos em consonância com os artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União²²⁰, sendo esta base jurídica sólida da União.

²¹⁴ Ibidem, considerandos (176) e (179).

²¹⁵ E.O. 14086, op. cit., Sec. 3(d)(iv); CEPD, Parecer 5/2023, § (225); Decisão 2023/1795/CE, considerando (185).

²¹⁶ SAVIN, Andrej (2024), p. 398.

²¹⁷ E.O. 14086, Sec. 3(d)(i)(H).

²¹⁸ CEPD, Parecer 5/2023, § 241; Decisão 2023/1795/CE, § (191).

²¹⁹ TJUE, Schrems, § (95)

²²⁰ GERKE, Sara and REZAEIKHONAKDAR, Delaram (2024), p. 399.

Conclusão

As transferências internacionais de dados para países terceiros garantidas pelo Capítulo V do RGPD e outras disposições da União, evidencia a magnitude do impacto económico, político e social do mercado digital. Tudo em razão do valor atribuído aos dados pessoais na atual sociedade de informação. E se, por um lado, é necessário compreender o quão crucial é para as relações comerciais globais o fluxo desses dados, em contrapartida, é preciso ter especial atenção à proteção dos direitos fundamentais dos cidadãos, principalmente em matéria de privacidade. E foi através do presente trabalho que examinamos esta complexa relação entre UE-EUA.

A análise das normas e dos casos nos mostrou a importância do Tribunal de Justiça da União Europeia no âmbito do seu poder de esclarecimentos e proteção dos cidadãos europeus, no qual têm permitido estabelecer expectativas legítimas de elevada proteção jurídica aos cidadãos, como observado.

É claro que, não obstante as evoluções nas últimas décadas, é impossível não reforçar a ideia de que o sistema legislativo americano, principalmente em matéria de proteção de dados, é extremamente falho sobretudo no que diz respeito à utilização dos serviços de inteligência por parte das autoridades norte-americanas²²¹. Há, porém, quem defenda²²² a criação de uma Lei Federal de Privacidade norte-americana (*U.S. Federal Privacy Law*) para harmonizar legislações já existentes de alguns estados que atribuem aos consumidores direitos sob seus dados. A expectativa é que com uma lei federal todos os cidadãos seriam adequadamente protegidos, que talvez poderiam ser tão efetivas quanto as normas europeias. Porém, sendo realista, a probabilidade de as autoridades norte-americanas restringirem a atuação dos serviços de inteligência é ínfima.

Assim, as invalidades das ulteriores decisões de adequação só reforçaram a necessidade de conciliação dos interesses económicos e sociais das duas potências. Porém, como explicitado, as imperfeições não são poucas, e após anos de trabalho a Comissão e o Governo americano não conseguiram garantir um *framework* que ajustasse as transferências de dados de acordo com os parâmetros estabelecidos pelo TJUE²²³.

No site da ONG “*noyb*”, Max Schrems, afirmou que “apesar de ambos agora usarem a palavra “proporcional”, discordavam do significado e que a Comissão estaria

²²¹ CEPIK, Marco Aurélio Chaves (2014), p. 3-18.

²²² GERKE, Sara e REZAEIKHONAKDAR, Delaram (2024), p 400-401.

²²³ Ibidem, p 399.

novamente a “fechar os olhos” às leis norte-americanas, permitindo a continuação da vigilância dos europeus. Mas que, entretanto, a definição do TJUE iria prevalecer”²²⁴²²⁵.

Autores afirmam²²⁶ ainda que há grande probabilidade desta nova Decisão “cair” em um possível caso “*Schrems III*” com o mesmo fundamento: de que os EUA verdadeiramente falham em garantir um nível de proteção adequado assim como exigido pela União e pelo TJUE. Neste mesmo sentido, em julho de 2023, a mesma ONG expôs que apenas estão a espera que o novo sistema de transferências de dados seja implementado pelas empresas nos próximos meses, que muito provavelmente iria trazer à tona novos casos com problemas de proteção dos direitos fundamentais dos cidadãos europeus; e pretendiam, assim, preparar um caso a ser levado ao Tribunal²²⁷.

Por fim, de mencionar o Processo *Latombe/Comissão* (T-553/2)²²⁸, interposto a 6 de setembro de 2023, em que o recorrente já colocou em causa a Decisão 2023/1795/CE (QPD) invocando os mesmos argumentos aqui abordados: a insuficiência de garantias dos direitos fundamentais; a falta do direito à ação e de um tribunal independente; a falta de garantia contra as decisões automatizadas e a falta de segurança dos dados tratados.

Concluimos, portanto, a dizer que nos aparenta que a Comissão tem dado prioridade à sua relação econômica e política com os EUA em detrimento da sua responsabilidade primordial: de agir como guardião dos Tratados e de priorizar os direitos dos cidadãos europeus. Esta tendência sugere uma possível negligência das obrigações institucionais da Comissão em favor de interesses de natureza econômica e geopolítica.

²²⁴SCHREMS, Max (2022), em <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> [consult. 10/Abr/2024].

²²⁵ Tradução nossa.

²²⁶ GERKE, Sara e REZAEIKHONAKDAR, Delaram (2024), p 395.

²²⁷ Website noyb (2023), em <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> [consult. 10/Abr/2024].

²²⁸Tribunal Geral (2023), Processo T-553/23, *Latombe/Comissão*, <http://data.europa.eu/eli/C/2023/348/oj> [consult. 10/Abr/2024].

Bibliografia

AEPD (2016) – *Síntese do parecer da Autoridade Europeia para a Proteção de Dados relativo ao projeto de decisão sobre o nível de proteção adequado do Escudo de Proteção da Privacidade UE-EUA*, Opinião 4/2016, (2016/C 257/05), de 30 de Maio de 2016, disponível em https://www.edps.europa.eu/sites/default/files/publication/16-07-15_privacy_shield_adequacy_decision_pt.pdf [consultado a 7 de Abril de 2024].

_____. disponível em https://www.edps.europa.eu/_en [consultado a 7 de Abril de 2024].

ALVES, Joel A. (2021) – *O Novo Modelo de Proteção de Dados Pessoais Europeu – Da Heterorregulação à Autorregulação Publicamente Regulada*, Coimbra, EDITORA ALMEDINA.

BOEHM, Franziska (2015), EUROPEAN PARLIAMENT'S POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *A comparison between US and EU data protection legislation for law enforcement purposes*, Study for the LIBE Committee, disponível em [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2015\)536459](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2015)536459) [Consultado em 7 de Março de 2024].

BORRELL, Josep (2021), “Relações estreitas entre a UE e os EUA continuam a ser vitais para a segurança mundial”, Blogue do AR/VP, 17.10.2021, disponível em https://www.eeas.europa.eu/eeas/rela%C3%A7%C3%B5es-estreitas-entre-ue-e-os-eua-continuam-ser-vitais-para-seguran%C3%A7a-mundial_pti [Consultado em 5 de Março de 2024].

CALVÃO, Filipa Urbano (*s.d.*) – “A proteção de dados pessoais na Internet: desenvolvimentos recentes”, *s.l.*

CASIMIRO, Sofia de Vasconcelos (2020) – “Novas Guerras em Novos Campos de Batalha: o RGPD EUROPEU e as gigantes tecnológicas norte-americanas”, in *Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado*, Curitiba, GEDAI/Universidade Federal do Paraná.

CEPD (2023), Parecer 5/2023 sobre o projeto de decisão de execução da Comissão Europeia sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Quadro UE-EUA de Privacidade dos Dados, Adotado em 28 de fevereiro de 2023, disponível em https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_pt.pdf [consultado a 9 de Abril de 2024].

_____. (2023) Decisão vinculativa n.º 1/2023 relativa ao litígio apresentado pela autoridade de controlo irlandesa sobre as transferências de dados efetuadas pela *Meta Platforms Ireland Limited* para o seu serviço *Facebook* (artigo 65.º do RGPD), Adotada em 13 de abril de 2023, disponível em https://www.edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_pt.pdf [consultado a 10 de Abril de 2024].

_____. (2028) Diretrizes 2/2018 relativas às derrogações do artigo 49.º do Regulamento (UE) 2016/679, 25 de Maio de 2018, disponível em https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_pt [Consultado em 2 de Abril de 2024].

_____. (2020) *Perguntas frequentes sobre o acórdão do Tribunal de Justiça da União Europeia no Processo C-311/18 – Data Protection Commissioner contra Facebook Ireland Limited e Maximillian Schrems*, Adotado em 23 de julho de 2020, disponível em https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_pt.pdf [consultado a 8 de Abril de 2024].

_____. (2019) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version 2.1, 12 November 2019, disponível em https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [Consultado em 1 de Abril de 2024].

_____. (2023), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0, Adopted on 14 February 2023, disponível em https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf [Consultado em 1 de Abril de 2024].

_____. Legado: Grupo de Trabalho do Artigo 29.º, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_pt [consult. 4/Abr/2024].

CEPIK, Marco Aurélio Chaves (2014) – “*Origens do Sistema de Inteligência dos Estados Unidos: 1775-1946*”, Publicação da Associação Brasileira de Relações Internacionais, *CARTA INTERNACIONAL*, Vol. 9, n. 1, jan. -jun. 2014 [p. 3 a 18], disponível em <https://cartainternacional.abri.org.br/Carta/article/download/133/75/505> [consultado a 10 de Abril de 2024].

CHIAPPETTA, Aline Holanda (2018) - *Transferências Transatlânticas de Dados Pessoais na Era Pós-Snowden à Luz do Regulamento Geral sobre a Proteção De Dados*, Dissertação em Ciências Jurídico-Empresariais Menção em Direito Empresarial. Coimbra, Faculdade de Direito da Universidade de Coimbra.

Christina RATCLIFF, Jordan DE BONO, Barbara MARTINELLO (2023) – *A Ubiquidade Do Mercado Único Digital*, Fichas técnicas sobre a União Europeia – 2024, disponível em https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/pt/FTU_2.1.7.pdf [Consultado em 5 de Março de 2024].

CNPD (2023), Parecer/2022/13, disponível em <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121965> [Consultado em 5 de Março de 2024].

CONCLUSÕES DO ADVOGADO-GERAL (2019), apresentadas em 19 de dezembro de 2019, Processo C-311/18, [pedido de decisão prejudicial apresentado pela High Court (Tribunal Superior, Irlanda)], disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CC0311> [consultado a 8 de Abril de 2024].

CONSTITUTION OF THE UNITED STATES, Fourth Amendment, disponível em <https://constitution.congress.gov/constitution/amendment-4/> [consultado a 5 de Abril de 2024].

Convenção Europeia dos Direitos do Homem (1950), disponível em <https://www.conventions.coe.int>. [Consultado a 5 de Janeiro de 2024].

Correio Braziliense: Mundo (2023), “O que mudou após dez anos após vazamentos de Snowden?”, 05/jul/2023. <https://www.correio braziliense.com.br/mundo/2023/06/5099696-o-que-mudou-apos-dez-anos-apos-vazamentos-de-snowden.html> [consultado a 5 de Abril de 2024].

DE JESUS, Inês Oliveira Andrade (2018) – “O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?” in *Anuário da Proteção de Dados*, PEREIRA COUTINHO, Francisco e Canto Moniz, Graça (coord.), Universidade Nova de Lisboa, Faculdade de Direito; CEDIS, Centro de I & D sobre Direito e Sociedade de Campolide, Lisboa.

Dennis D. Hirsch (2014), *The Glass House Effect: Big Data, The New Oil, and the Power of Analogy*, 66 Me. L. Rev. 373.

DPC Ireland, In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited), Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation, DPC Inquiry Reference: IN-20-8-1, disponível em https://www.edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf [consultado a 10 de Abril de 2024].

ESTADOS UNIDOS (2016), Department of Commerce, International Trade Administration (2016) - *Notice of Availability of Privacy Shield Framework Documents*. Federal Register / Vol. 81, No. 148 / Tuesday, August 2, 2016 / Notices, disponível em <https://www.govinfo.gov/content/pkg/FR-2016-08-02/pdf/2016-17961.pdf> [consultado a 7 de Abril de 2024].

_____. (1981) E.O. 12333: *United States Intelligence Activities*, *Federal Register* Vol. 40, n.º 235 (8 de dezembro de 1981), disponível em <https://dpcl.d.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf> [consultado a 8 de Abril].

_____. (2006) *Federal Trade Commission Act Incorporating U.S. SAFE WEB Act amendments of 2006* (Unofficial version), §§ 41-58, disponível em

https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf [consultado a 6 de Abril de 2024].

_____. (2014) Office Of The Director Of National Intelligence Principal Deputy Director Of National Intelligence Washington, DC 20511, Presidential Policy Directive-28, "Signals Intelligence Activities," January 17, 2014, disponível em <https://irp.fas.org/dni/dni-ppd-28.pdf> [consultado a 8 de Abril de 2024].

_____. US Department of State, Executive Order 14086, "Policy and Procedures", BUREAU OF INTELLIGENCE AND RESEARCH, disponível em <https://www.state.gov/executive-order-14086-policy-and-procedures/> [consultado a 9 de Abril de 2024].

_____. Web do Departamento de Comércio dos EUA – lista das empresas dos EUA que fazem parte do Escudo de Proteção da Privacidade, disponível em <https://www.dataprivacyframework.gov/> [consultado a 7 Abril de 2024].

FARINHO, Domingos Soares (2016) – “(Un)Safe Harbour: Comentário à decisão do TJUE C-362/14 e suas consequências legais”, in Fórum de Proteção de Dados, n.º 2 (janeiro/2016), p.123-124.

FONSECA, Diogo Brito, *et al.* (2022) – “*The International Data Transfer Framework and its Political Consequences: a Practical Approach*”; Pereira Coutinho, Francisco e Canto Moniz, Graça (coord.). In Anuário da Proteção de Dados 2020. Lisboa: CEDIS, 2022.

FUSTER, Gloria González (2014) – *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Brussels, Springer.

GDPR-TEXT.COM, <https://gdpr-text.com/pt/> [última consult. 16 de Abril de 2024].

Geppert, Nadine – “*Could the 'EU-US Privacy Shield' Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries?*”, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928064 [Consultado em 4 de Abril de 2024].

GERKE, Sara and REZAEIKHONAKDAR, Delaram (2024) – “Privacy Shield 2.0 — A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States”, *Cardozo Law Review*, Vol. 45, No. 2, 2023 (Feb. 2024).

GONÇALVES DA VEIGA, Adélcia Solange Pereira (2020) – *Proteção De Dados: O Direito À Privacidade Na Era Digital*, Tese de mestrado em Direito. Lisboa, Departamento de Direito da Universidade Autónoma de Lisboa.

GOUVEIA, Jorge Bacelar (1991), “Os Direitos Fundamentais à Proteção dos Dados Pessoais Informatizados”, in *Revista da Ordem dos Advogados*, ano 51, 1991-III, p.699-732, disponível em <http://hdl.handle.net/10362/15159>, [Consultado a 24 de Janeiro de 2024].

GREENWALD, Glenn (2014) – *No place to hide: Edward Snowden, the NSA and the Surveillance State*, Picador; Reprint edition (April 28, 2015).

HOGAN, Michael J. (1987) – *The Marshall Plan America, Britain, and the reconstruction of Western Europe, 1947-1952*, Cambridge University Press, UK, 1987.

<https://poseur.portugal2020.pt/pt/media/not%C3%ADcias/comiss%C3%A3o-europeia-lan%C3%A7a-brochura-dez-prioridades-para-a-europa/> [consult. 7/Abril/2024].

Kuner, Christopher (2017), “The Internet and the global reach of EU law”, in: *Marise Cremona and Joanne Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* 112-145 (Oxford University Press 2019), p. 25-26, disponível em <https://ssrn.com/abstract=2890930> [Consultado em 29 de Fevereiro de 2024].

MACHLUP, Fritz (1962) – *The Production and Distribution of Knowledge in the United States*, Princeton University Press, Published Jan 21, 1973.

MACIEJEWSKI, Mariusz; Departamento Temático dos Direitos dos Cidadãos e dos Assuntos Constitucionais do Parlamento Europeu (2023) - *Proteção de Dados Pessoais*, in *Fichas técnicas sobre a União Europeia – 2024*, disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf [Consultado a 12 de Janeiro de 2024].

Madsen, W. (1992). “Western European Initiatives”. In: *Handbook of Personal Data Protection*. Palgrave Macmillan, London. https://doi.org/10.1007/978-1-349-12806-8_3.

MARTINHO, Lúscas Pires (2018) – “Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems”, in *Anuário da Proteção de Dados, Lisboa, CEDIS*, 2018.

MCLUHAN, Marshall (1964) – *Understanding Media The extensions of man*, publisher McGraw-Hill, Londres and Nova Iorque.

MENEZES CORDEIRO, A. Barreto (2022) – *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*, Coimbra, EDIÇÕES ALMEDINA, S.A.

NEGROPONTE, Nicholas (1995) - *Being Digital*, Hodder and Stoughton, A division of Hodder Headline PLC, London.

NOGUEIRA, Catarina Conde (2021) – “Privacy Shield vs. Acórdão C-311/18 – “Schrems II””, *CyberLaw by CIJIC*, Edição n.º XI – Março de 2021.

OCDE, (2022), *A Preliminary Mapping of Data Localisation Measures*. OECD Trade Policy Papers, N. 262, OECD publishing.

Oliver Stone (2016), Snowden, franco-teuto-estadunidense, distribuição Open Road Films, suporte Prime Video [assistido a 5 de Abril de 2024].

ONG “Europe versus Facebook”, disponível em http://europe-v-facebook.org/EN/Complaints/Safe_Harbor/safe_harbor.html [consultado a 6 de Abril de 2024].

ONG “noyb” (2023), “European Commission gives EU-US data transfers third round at CJEU”, 10/07/2023, disponível em <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> [consultado a 10 de Abril de 2024].

_____. (2022) “New US Executive Order unlikely to satisfy EU law”, 07 October 2022, disponível em <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> [consultado a 9 de Abril de 2024].

PINHEIRO, Alexandre Sousa (Coord.); autores COELHO, Cristina Pimenta... [et al.] (2018) – *Comentário ao Regulamento Geral de Proteção de Dados*, Lisboa, EDITORA ALMEDINA.

REPÚBLICA PORTUGUESA, Diário da República, lexionário, disponível em <https://diariodarepublica.pt/dr/lexionario/termo/derrogacao-lei> [Consultado em 5 de Março de 2024].

_____. (2016) Programa Operacional Sustentabilidade E Eficiência No Uso De Recursos, Comissão Europeia lança brochura "Dez Prioridades para a Europa", publicado a 08-01-2016, disponível em <https://poseur.portugal2020.pt/pt/media/not%C3%ADcias/comiss%C3%A3o-europeia-lan%C3%A7a-brochura-dez-prioridades-para-a-europa/> [consultado a 7 de Abril de 2024].

RODOTA', Stefano (2009) – “Data Protection as a Fundamental Right”, in Serge Gutwirth, Yves Poullet, Paul Hert, Cécile Terwangne, Sjaak Nouwt (editors), *Reinventing Data Protection?*, Chapter 3, Springer Science+Business Media B.V. 2009.

SAVIN, Andrej (2023) – “The New Framework for Transatlantic Data Transfers” (June 28, 2023). Copenhagen Business School, *CBS LAW Research Paper No. 23-01*, disponível em <https://ssrn.com/abstract=4494289> [consultado a 10 de Abril de 2024].

SCHREMS, Maximillian (2022), “*New US Executive Order unlikely to satisfy EU law*”, noyb website, Data Transfers, 7/10/2022, disponível em <https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law> [consultado a 10 de Abril de 2024].

_____. “Privacy Rights and Data Flows (2021) – A Conversation with Max Schrems”, WoodrowWilsonCenter, de 29 de Junho de 2021, Youtube, disponível em <https://www.wilsoncenter.org/event/privacy-rights-and-data-flows-conversation-max-schrems> [Consultado em 7 de março de 2024].

SILVA, Heraclides Sequeira dos Santos (2017) – *A Protecção De Dados Pessoais Na Era Global: O Caso Schrems*, Dissertação de mestrado em Direito. Lisboa, Faculdade de Direito da Universidade Nova de Lisboa.

SIMON, Joel, “Como a espionagem dos Estados Unidos fortalece o controle da China”, disponível em <https://cpj.org/pt/2014/02/ataque-a-imprensa-em-2013-como-a-espionagem/> [Consultado em 2 de Abril de 2024].

STEIL, Benn (2019) - *The Marshall Plan, Dawn of the Cold War*, Simon & Schuster.

TOFFLER, Alvin (1970) – *The Future Shock*, A Bantam Book / published by arrangement with Random House, Inc.

Tratado de Funcionamento da União Europeia (Tratado de Lisboa) (2007), disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF [Consultado a 5 de Janeiro de 2024].

UNIÃO EUROPEIA (2016) – *Guia Prático Comum do Parlamento Europeu, do Conselho e da Comissão para as pessoas que contribuem para a redação de textos legislativos da União Europeia*, 2ª Edição, disponível em <https://eur-lex.europa.eu/content/techleg/PT-guia-de-redacao-de-textos-legislativos.pdf> [Consultado a 30 de Janeiro de 2024].

_____. Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf [Consultado em 2 de Abril de 2024].

_____. Carta dos Direitos Fundamentais da União Europeia (2000), disponível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf [Consultado a 5 de Janeiro de 2024].

_____. Comissão Europeia (s.d.) - Guia Do Escudo De Proteção Da Privacidade UE-EUA, disponível em <https://ec.europa.eu/newsroom/just/redirection/document/47776> [consultado a 7 de Abril de 2024].

_____. Comissão Europeia, “Relações comerciais da UE com os Estados Unidos. Factos, números e desenvolvimentos mais recentes”, disponível em <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries->

[and-regions/united-states_en?prefLang=pt&etrans=pt](#) [Consultado em 5 de Março de 2024].

_____. Comité Europeu para Proteção e Dados e do Parlamento Europeu, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, Adopted on 28 February 2023, disponível em https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf [Consultado em 7 de Março de 2024].

_____. Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), Brussels, 6.11.2015 COM(2015) 566 final, disponível em [https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0566/COM_COM\(2015\)0566_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0566/COM_COM(2015)0566_EN.pdf) [consultado a 6 Abril de 2024].

_____. Comunicação da Comissão ao Parlamento Europeu e ao Conselho – “*Restabelecer a confiança nos fluxos de dados entre a UE e os EUA*”, COM (2013) 846 final, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013DC0846> [consultado a 5 de Abril de 2024].

_____. Comunicação da Comissão ao Parlamento Europeu e ao Conselho – “*Sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na EU*”, COM (2013) 847 final, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013DC0847> [consultado a 5 de Abril de 2024].

_____. Comunicação da Comissão ao Parlamento Europeu e ao Conselho Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas, Bruxelas, 29.2.2016, COM (2016) 117 final, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0117> [consultado a 7 de Abril de 2024].

_____. Conclusões do Conselho sobre a ação externa da UE no domínio da prevenção e da luta contra o terrorismo e o extremismo violento, 16 de Junho de 2020,

disponível em <https://data.consilium.europa.eu/doc/document/ST-8868-2020-INIT/pt/pdf> [Consultado em 2 de Abril de 2024].

_____. Conselho da Europa, Convenção 108 para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981.

_____. Decisão da Comissão de 5 de Fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho [notificada com o número C(2010) 593], disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0087> [consultada a 8 de Abril de 2024].

_____. Decisão da Comissão, de 26 de Julho de 2000, nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520> [Consultado em 28 de Fevereiro de 2024].

_____. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016D1250&from=DE> [Consultado em 28 de Fevereiro de 2024].

_____. Decisão de Execução (UE) 2023/1795 da Comissão de 10 de julho de 2023 nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:JOL_2023_231_R_0005 [Consultado em 7 de Março de 2024].

_____. European Parliament, Committee on Civil Liberties, Justice and Home Affairs – DRAFT MOTION FOR A RESOLUTION, on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), disponível em https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf [consultado a 9 de Abril de 2024].

_____. Proposal for a regulation of The European Parliament and of The Council establishing the Strategic Technologies for Europe Platform (‘STEP’) and amending Directive 2003/87/EC, Regulations (EU) 2021/1058, (EU) 2021/1056, (EU) 2021/1057, (EU) No 1303/2013, (EU) No 223/2014, (EU) 2021/1060, (EU) 2021/523, (EU) 2021/695, (EU) 2021/697 and (EU) 2021/241, 9 de Fevereiro de 2024, disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0335> [Consultado em 2 de Abril de 2024].

_____. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

_____. Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão.

_____. Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, disponível em https://commission.europa.eu/document/f62d70a4-39e3-4372-9d49-e59dc0fda3df_en [Consultado em 28 de Fevereiro de 2024].

_____. Resolução do Parlamento Europeu, de 11 de maio de 2023, sobre a adequação da proteção conferida pelo quadro UE-EUA em matéria de proteção de dados (2023/2501(RSP)), disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_PT.pdf [Consultado em 7 de Março de 2024].

_____. Resolução do Parlamento Europeu, de 12 de março de 2014, sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos (2013/2188(INI)), disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52014IP0230> [consultado a 5 de Abril de 2024].

_____. Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)), disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016IP0233> [Consultado em 5 de Março de 2024].

_____. Working Party on the Protection of Individuals with regard to the Processing of Personal Data (1999) – WP 15, *OPINION 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf [Consultado em 4 de Abril de 2024].

_____. Working Party on the Protection of Individuals with regard to the Processing of Personal Data (1999) – WP 19, *Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp19_en.pdf [Consultado em 4 de Abril de 2024].

_____. WP 21, *Parecer 4/99 sobre as questões mais frequentes a publicar pelo Departamento de Comércio dos EUA no quadro da proposta de princípios de "porto seguro"*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [consultado em 4 de Abril de 2024].

_____. WP 23 (1999), *Documento de trabalho sobre o avanço das negociações entre a Comissão Europeia e o Governo dos Estados Unidos da América relativas aos "princípios internacionais de porto seguro"*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [consultado em 4 de Abril de 2024].

_____. WP 27, *Parecer 7/99 sobre o nível de proteção de dados fornecido pelos princípios de "porto seguro", publicados em conjunto com as questões mais frequentes (FAQ) e outros documentos conexos, em 15 e 16 de Novembro de 1999, pelo Department of Commerce dos EUA*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [última consulta a 5 de Abril de 2024].

_____. WP 31, *Parecer 3/2000 relativo ao diálogo UE/EUA sobre o Acordo de "porto seguro"*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [consultado a 4 de Abril de 2024].

_____. WP 32, *Parecer 4/2000 relativo ao nível de proteção facultado pelos acordos de "porto seguro"*, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [consultado a 5 de Abril de 2024].

_____. WP Article 29.º - Adequacy Referential Adopted on 28 November 2017, As last Revised and Adopted on 6 February 2018, WP 254 rev. 01, disponível em <https://ec.europa.eu/newsroom/article29/items/614108/en> [consultado a 9 de Abril de 2024].

_____. WP Article 29.º - Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision Adopted on 13 April 2016, 16/EN WP 238, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [consultado a 7 de Abril de 2024].

_____. WP article 29.º - Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015, in the *Maximilian Schrems v Data Protection Commissioner* case (C-362-14), disponível em https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [consultado a 6 de Abril de 2024].

VEIGA, P. (2020): “Digitalização e Estado Constitucional”, in *Boletim da Faculdade de Direito da Universidade de Coimbra*, Vol. 96, Tomo II, Coimbra, pp. 1127-1139,

disponível em <https://apps.uc.pt/mypage/files/pveiga/2283>, [Consultado a 23 de Janeiro de 2024].

_____. (2021), «Tomemos a sério a digitalização: *rule of law* também na rede!», in Ana Cláudia Nascimento Gomes, Bruno Albergaria e Mariana Rodrigues Canotilho (coord.), *Estudos em Homenagem ao Professor Doutor J. J. Gomes Canotilho pelo 80.º Aniversário*, Editora Fórum, Belo Horizonte, Brasil, pp. 915-925.

- **Jurisprudência.**

Acórdão TJUE *Google Spain e Google*, de 13 de Maio de 2014, proc. C-131/12, ECLI:EU:C2014:317, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [último consultado a 2 de Abril de 2024].

Acórdão TJUE *Maximillian Schrems v Data Protection Commissioner.*, de 6 de Outubro de 2015, proc. C-362/14, ECLI:EU:C:2015:650, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [última consulta a 16 de Abril de 2024].

Acórdão TJUE *Tele 2 Sverige*, de 21 de Dezembro de 2016, processos apensos C-203/15 e C-698/15, ECLI:EU:C:2016:970, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [última consulta a 3 de Abril de 2024].

U.S. SUPREME COURT, *Katz v. United States*, 389 U.S. 347 (1967), disponível em <https://supreme.justia.com/cases/federal/us/389/347/> [consultado a 5 de Abril de 2024].

Acórdão TJUE Comissão/Alemanha, de 3 de Dezembro de 2009, C-518/07, EU:C:2010:125.

Acórdão *Data Protection Commissioner vs. Facebook Ireland Ltd & Maximillian Schrems*, de 16 de julho de 2020, (C-311/18) ECLI:EU:C:2020:559, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0311> [última consulta a 8 de Abril de 2024]

TRIBUNAL GERAL, Processo T-553/23: Recurso interposto em 6 de setembro de 2023 — Latombe/Comissão, Documento 62023TN0553, ELI: <http://data.europa.eu/eli/C/2023/348/oj> [consultado a 10 de Abril de 2024].

Acórdão TJUE *Lindqvist*, de 6 de Novembro de 2003, proc. C-101/01, ECLI:EU:C:2003:596, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [último consultado a 3 de Abril de 2024].

Acórdão TJUE Comissão/Hungria, de 8 de abril de 2014, C-288/12, EU:C:2014:237.

Acórdão TJUE *Digital Rights*, de 8 de Abril de 2014, proc. C-293/12 e C-594/12, ECLI:EU:C:2014:238, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [último consultado a 2 de abril de 2024].

Acórdão TJUE *Scarlet*, de 24 de Novembro de 2011, proc. C-70/10, ECLI:EU:C:2011:771, disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/ [último consultado a 3 de Abril de 2024].