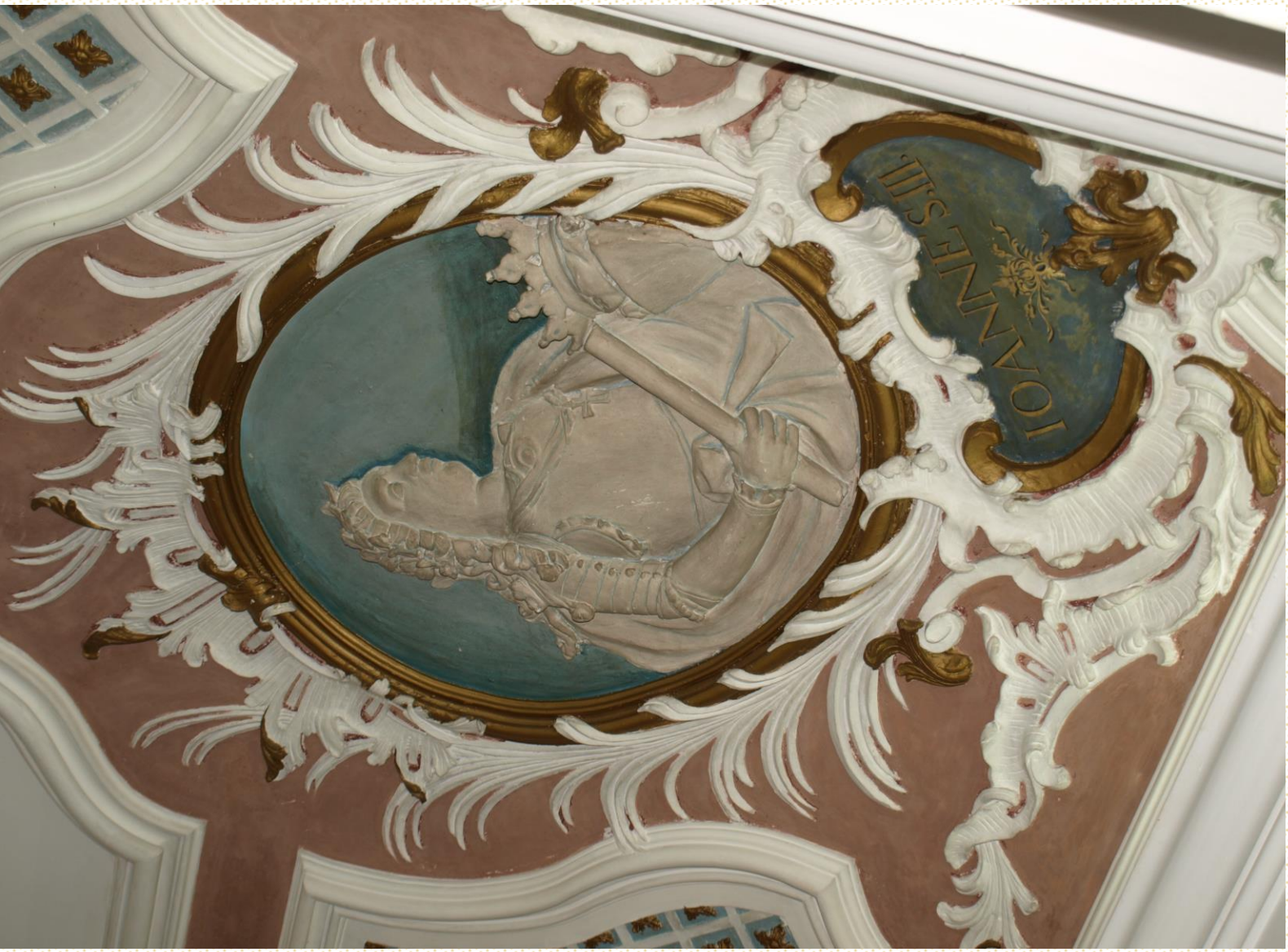

Aline Holanda Chiappetta

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

2018

· U C ·

UNIVERSIDADE DE COIMBRA

Aline Holanda Chiappetta

TRANSFERÊNCIAS TRANSATLÂNTICAS DE DADOS PESSOAIS NA ERA PÓS-SNOWDEN À LUZ DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS

Transatlantic transfers of personal data in the post-Snowden era under the General Data Protection Regulation

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Empresariais, Menção em Direito Empresarial.

Orientador: Alexandre Libório Dias Pereira

Coimbra

2018

RESUMO

Os desenvolvimentos tecnológicos dos últimos 20 anos revolucionaram a forma pela qual os dados são coletados, armazenados e partilhados. As novas tecnologias, em especial os avanços nos ramos da tecnologia da informação e da comunicação, aliadas ao fenómeno da massificação da Internet e da globalização contribuíram para o surgimento da economia da informação e da sociedade da informação.

Neste âmbito, os dados pessoais assumem o papel da principal moeda de um mercado multimilionário, o qual utiliza técnicas como os algoritmos para analisar as informações pessoais e identificar o produto e/ou serviço que melhor se adequa às vontades e necessidades dos consumidores.

Enquanto principal moeda deste novo mercado, os dados pessoais assumem a posição de ativos que podem ser comercializados entre organizações de diferentes partes do globo, tornando a transferência de dados entre países uma atividade de presença constante na atual sociedade da informação.

No entanto, e à diferença das demais moedas, os dados pessoais são um elemento indissociável da vida privada dos seus titulares, direito fundamental garantido pela Carta dos Diretos Fundamentais da União Europeia. Destarte, demandam o respaldo jurídico necessário à garantia da efetividade da sua proteção.

A proteção dos dados pessoais ganhou maior destaque nos últimos cinco anos, em especial no ano de 2013, após as revelações de Edward Snowden sobre as coletas indiscriminadas e em larga escala das informações pessoais realizadas sob o âmbito de programas de vigilância de autoridades públicas dos Estados Unidos. As referidas revelações incitaram o debate sobre a efetividade da proteção dos dados tanto no cenário americano como no cenário europeu.

À época, a União Europeia já havia proposto uma reforma em sua legislação concernente à proteção dos dados pessoais, a qual tinha como objetivo não só adequar o direito da UE às novas tecnologias, mas também harmonizar as legislações vigentes nos Estados-Membros, ao mesmo tempo em que reforçava os direitos e liberdades dos titulares dos dados.

Fruto da referida reforma, o instrumento jurídico que atualmente regula a proteção dos dados a nível da União Europeia é o Regulamento Geral sobre a Proteção de Dados, o qual passou a ser aplicado em 25 de maio de 2018.

A presente dissertação objetiva analisar as transferências transatlânticas dos dados pessoais na era pós-Snowden à luz do novo quadro jurídico da União Europeia. A pertinência e adequação dos principais instrumentos utilizados pelos exportadores de dados para fundamentar as transferências de dados pessoais a dois dos maiores parceiros comerciais da UE, quais sejam, os Estados Unidos e o Canadá, será a questão principal a ser examinada por este estudo. Para tanto, abordar-se-á não só o quadro legal e a jurisprudência da União Europeia referente à proteção e transferência dos dados pessoais, como também os desenvolvimentos dos sistemas jurídicos canadiano e americano neste âmbito.

PALAVRAS-CHAVE: PROTEÇÃO DE DADOS; TRANSFERÊNCIAS DE DADOS; RGPD; PIPEDA, *PRIVACY SHIELD*.

ABSTRACT

The technological developments of the last 20 years have revolutionized the way data is collected, stored and shared. The new technologies, especially the developments in the fields of information and communications technologies, allied to the phenomenon of the Internet and globalization have contributed to the emergence of the information society and the information economy.

In this context, personal data assume the role of the main currency of a multi-million dollar market, which uses techniques such as algorithms to analyze personal information and identify the product and/or service that best fits the desires and needs of consumers.

As the main currency of this new market, personal data became an asset that can be traded between organizations from different parts of the globe, making the transfer of data between countries an activity of constant presence in the current information society.

However, unlike other currencies, personal data is inseparable from the private life of their holders, a fundamental right guaranteed by the Charter of Fundamental Rights of the European Union. Therefore, they demand the legal support necessary to guarantee the effectiveness of their protection.

Personal data protection has gained more prominence in the last five years, especially in 2013, following the revelations of Edward Snowden on the indiscriminate and large-scale collection of personal information held under US government surveillance programs. These revelations stimulated the debate on the effectiveness of data protection both in the American scene and in the European scenario.

At the time, the European Union had already proposed a reform of its legislation concerning the protection of personal data, which was intended not only to bring EU law into line with new technologies, but also to harmonize existing legislation in the Member States, strengthening the rights and freedoms of data subjects.

As a result of this reform, the legal instrument currently governing data protection at the level of the European Union is the General Data Protection Regulation, which was implemented on May 25, 2018.

The present dissertation aims to analyze the transatlantic transfers of personal data in the post-Snowden era, under the European Union new legal framework. The relevance and adequacy of the main instruments used by data exporters to fundament their data transfers to two of the EU's biggest trading partners, namely the United States and Canada, will be the principal question to be examined by this study. To do so, it will be analyzed not only the EU case law and legal framework regarding the protection and transfers of personal data, but also the developments of the Canadian and American legal systems in this regard.

KEYWORDS: DATA PROTECTION, DATA TRANSFERS, GDPR, PIPEDA, PRIVACY SHIELD.

SIGLAS E ABREVIATURAS

Acordo Económico e Comercial Global (CETA)

Autoridades nacionais de controlo (ANC)

Canadian Security Intelligence Service (CSIS)

Carta dos Direitos Fundamentais da União Europeia (CDFUE)

Comité do Escudo de Proteção da Privacidade (CEPP)

Data Protection Comissioner (DPC)

Departamento de Comércio dos EUA (DC)

Escudo de Proteção da Privacidade (EPP)

Estados Unidos da América (EUA)

Estados-Membros (EM)

Fair Information Practices (FIPs)

Personal Information Protection and Electronic Documents Act (PIPEDA)

Porto Seguro (PS)

Regulamento Geral sobre a Proteção de Dados (RGPD)

Resolução alternativa de litígios (RAL)

Tratado de Funcionamento da União Europeia (TFUE)

Tribunal de Justiça da União Europeia (TJUE)

União Europeia (UE)

ÍNDICE

INTRODUÇÃO

Os desenvolvimentos tecnológicos dos últimos vinte anos alteraram significativamente a forma pela qual os dados pessoais são coletados, armazenados e partilhados. As novas tecnologias possibilitaram a realização do tratamento dos dados em uma quantidade e velocidade nunca antes vista.

No âmbito da sociedade da informação, os dados pessoais são coletados às vezes nas sutilezas das atividades quotidianas, seja por meio de *softwares* ou *hardwares*, especialmente aqueles desenvolvidos com base na tecnologia da "*Internet das Coisas*" (IoT – *Internet of things*). [1-2]

Muitas vezes os referidos dados são requisitados para que o seu titular utilize um serviço "gratuitamente" oferecido no âmbito digital, a exemplo das redes sociais, motores de pesquisa e plataformas de mercado digital, como o *Facebook*, *Gmail*, *Twitter*, *Amazon* e *E-bay*.

Apesar da aparente gratuidade dos serviços, as referidas organizações estão a coletar e analisar os dados dos seus utentes, atividade que tem como objetivo entender com maior profundidade os seus perfis e oferecer serviços e bens que melhor se adequem às suas vontades e necessidades. [3] Por meio da oferta personalizada, as empresas tendem a

[1]A Internet das Coisas é um conceito tecnológico utilizado para identificar "todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à Internet, sendo capazes de se identificar na rede e de comunicar entre si." CENTRO NACIONAL DE CIBERSEGURANÇA, *A Internet das Coisas (IOT – Internet of Things)*, Governo de Portugal, Disponível em: < https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/> Acesso em: 23-12-2017

[2] Neste sentido, os dados pessoais podem ser coletados, por exemplo, quando o seu titular faz uso do *smartphone* (GPS, Histórico de pesquisa) e das redes sociais; em uma compra realizada no mercado digital; quando utiliza um *smartwatch* que pode analisar dados da saúde como batimento cardíaco, temperatura corporal, quilómetros percorridos, entre tantos outros exemplos.

[3] Ao utilizar a maioria dos serviços oferecidos no âmbito da Internet, os titulares dos dados criam um "rastro digital" que poderá ser posteriormente analisado por algoritmos capazes de prever as preferências dos referidos utentes. Neste sentido, merece destaque a passagem de Filipa Calvão: "A navegação na Internet implica a exposição, consciente ou inconsciente, de informação pessoal, alguma da qual, *per se*, ou no seu conjunto, é suscetível de revelar muito da nossa saúde, do nosso património ou rendimentos, dos nossos hábitos ou dos nossos gostos, em suma, da nossa vida privada. [...] Tudo serve para alimentar este processo: o URL do ponto de origem da comunicação, o URL do ponto de destino, hora e tempo da ligação, sítios consultados ou acedidos, informação consultada. Se a isto somarmos informação obtida por via de técnicas de geolocalização ou da Internet das coisas [...], temos uma massa alargada de informação associada a um sujeito específico." Para maior desenvolvimento, ver CALVÃO, Filipa Urbano, «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual*, 2015/2, p. 67-84, p. 68

obter um maior número de vendas e clientes, o que gera, consequentemente, maior lucro e uma maior quantidade de dados coletados pelas referidas entidades.

Neste sentido, os referidos dados posam atualmente como a principal matéria-prima da economia da informação, ao ponto de serem referidos como o "petróleo do século XXI". [4] No entanto, e à diferença das demais moedas, os dados pessoais são expressão direta da dignidade humana [5] e elemento indissociável da vida privada dos seus titulares, direito fundamental garantido pela Carta dos Direitos Fundamentais da União Europeia (CDFUE).[6] Por conseguinte, merecem a proteção adequada.

O instrumento jurídico que atualmente regula a proteção dos dados pessoais no âmbito da União Europeia (UE) é o Regulamento Geral sobre a Proteção de Dados (RGPD), [7] o qual passou a ser aplicado no dia 25 de maio deste ano (2018).

Tendo em consideração a importância dos dados pessoais não só enquanto direito fundamental, mas também como uma das mais importantes moedas do globalizado mercado digital, o RGPD estabelece mecanismos que garantem a manutenção do nível de proteção dos dados quando estes são transferidos a um país terceiro, atividade corriqueira na atualidade.

Neste sentido, como regra geral, o RGPD veda a realização das aludidas transferências a países terceiros, apenas permitindo a sua execução em casos específicos nos quais exista uma garantia de que os aludidos dados serão devidamente protegidos. [8] É o caso da transferência com base na decisão de adequação emitida pela Comissão (artigo 45º do RGPD) ou, na inexistência da referida decisão, as transferências com base na utilização de garantias adequadas pelo exportador dos dados (artigo 46º do RGPD).

---

[4] KUNEVA, Meglena, *Roundtable on Online Data Collection, Targeting and Profiling*, Bruxelas, 31 de março de 2009, Disponível em <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> Acesso em 01 de maio de 2018: "*Personal data is the new oil of the internet and the new currency of the digital world*."

[5] CALVÃO, Filipa Urbano, «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual*, 2015/2, p. 67-84, p. 82

[6] Carta dos Direitos Fundamentais da União Europeia, artigo 7º, JO C 83 de 30.3.201, Disponível em:< https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:pt:PDF> Acesso em: 23-01-2018.

[7] 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).

[8] Para maior desenvolvimento, ver MARTINHO, Lucas Pires, «Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems», *Anuário da Proteção de Dados 2018*. Lisboa: CEDIS, 2018, p. 96

Grande parte dos dados pessoais transferidos a dois dos maiores parceiros comerciais da UE – quais sejam os Estados Unidos e o Canadá – são realizadas com base em decisões de adequação, especificamente a Decisão de Execução 2016/1250 (Estados Unidos) [9] e a Decisão 2002/2/CE (Canadá). [10]

O presente trabalho tem como objetivo realizar uma análise sobre os referidos mecanismos utilizados para fundamentar as transferências transatlânticas de dados entre a UE e os Estados Unidos e o Canadá na era pós-Snowden, tendo em consideração o contexto no qual foram desenvolvidos e as implicações do novo Regulamento Geral sobre a Proteção de Dados nas aludidas transferências.

Para tanto, no primeiro capítulo, abordar-se-á o desenvolvimento histórico das legislações de proteção de dados até o advento do RGPD. Já no segundo capítulo, serão analisados os instrumentos oferecidos pelo RGPD para realização das transferências de dados em questão.

Na segunda metade do trabalho, serão analisados os principais instrumentos utilizados pelo Canadá e pelos EUA para recebimento das transferências de dados pessoais provenientes da UE, nomeadamente a Decisão de adequação 2002/2/CE, e a Decisão 2016/1250, respetivamente.

No primeiro capítulo desta segunda parte, serão abordadas as transferências de dados entre a UE-EUA, sendo analisado, neste contexto, o princípios de "Porto Seguro" (*Safe Harbour*), a invalidação deste sistema pelo Tribunal de Justiça da União Europeia (TJUE) no caso *Schrems*, bem como o seu sucessor, o Escudo de Proteção da Privacidade (*Privacy Shield)*. Por outro lado, no segundo e último capítulo deste trabalho, será analisada a decisão de adequação parcial canadiana e a sua pertinência face às modificações introduzidas pelo RGPD.

[9] COMISSÃO EUROPEIA, 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 [notificada com o número C(2016) 4176]

[10] COMISSÃO EUROPEIA, Decisão 2002/2/CE da Comissão de 20 de Dezembro de 2001 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos (Personal Information and Electronic Documents Act) [notificada com o número C(2001) 4539]

CAPÍTULO I – EVOLUÇÃO HISTÓRICA DAS LEIS DE PROTEÇÃO DOS DADOS PESSOAIS

A proteção específica dos dados pessoais por meio de diplomas legais remonta ao início dos anos 70 do século passado, período no qual registou-se um grande avanço tecnológico no âmbito do processamento dos dados. As novas tecnologias da informação possibilitaram a coleta e a posterior criação de uma grande quantidade de bancos de dados, os quais eram, em sua maioria, controlados por órgãos públicos.

É neste sentido que as primeiras leis de proteção dos dados pessoais tinham como foco as concessões de autorização para criação dos referidos bancos, bem como o seu posterior controlo pelos órgãos públicos,[11] sendo o objetivo central destas leis a limitação do poder estatal e a garantia da transparência dos bancos de dados controlados pelas referidas entidades públicas e por algumas organizações privadas de grande porte. [12]

Neste contexto, esta primeira geração de leis estava muito mais focada em regular a nova tecnologia que permitia a criação e armazenamento dos referidos bancos do que propriamente oferecer proteção à privacidade e aos dados pessoais. Como consequência, estas leis são caracterizadas pela tecnicidade da linguagem consagrada em seus textos.

Em resposta ao crescente tratamento automatizado dos dados pessoais, no início dos anos 1970, o Governo dos Estados Unidos formulou princípios de proteção da privacidade e dos dados pessoais (FIPs - *Fair Information Practices*) no relatório intitulado "*Records, Computers and the Rights of Citizens*".[13] O FIPs tinha por base cinco princípios fundamentais, a saber: 1. Não poderá existir um banco de dados cuja existência seja secreta; 2. O titular cujo dado é recolhido deve saber quais são esses dados e de que forma estão sendo utilizados; 3. O titular deve ter o direito de impedir a utilização do seu dado se este for manipulado de uma forma para a qual não foi dado o consentimento; 4. Deve ser oferecido ao titular meios para corrigir ou emendar seus dados; 5. Qualquer organização

[11] DONEDA, Danilo, «A proteção dos dados pessoais como um direito fundamental», *Revista Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 95

[12] KISS, Attila; SZOKE , Gergely László, «Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation», in *Reforming European Data Protection Law*, Law, Governance and Technology Series, [S.L]: Ed. Springer, 2015, p. 313

[13] Comité Consultivo sobre dados pessoais automatizados da Secretaria dos EUA, *Records, Computers and the Rights of Citizens (1973)*, Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> Acesso: 29-05-2018.

que crie, mantenha, utilize ou compartilhe dados pessoais deve tomar precauções para evitar o uso indevido dos dados. [14-15]

Este documento teve uma grande influência na elaboração de legislações no âmbito da privacidade e da proteção de dados pessoais, tendo servido de inspiração para uma série de instrumentos legais, não só no ordenamento jurídico norte-americano, como também no de outros países. [16]

Pouco tempo depois, em 1974, o Congresso dos EUA promulgou o *Privacy Act*, o qual, em conformidade com os princípios constantes do FIPs, regulava a coleção, manutenção, uso e disseminação de dados pessoais por meio das agências executivas federais daquele país. [17] Já no cenário canadiano, em 1983 entrou em vigor o *Privacy Act*,[18] lei federal do Canadá que regula o uso dos dados pessoais tratados por órgãos governamentais federais.

No quadro europeu, a regulação da proteção dos dados pessoais deu seus primeiros passos no início dos anos 1970. [19] A primeira legislação europeia em termos de proteção de dados pessoais foi publicada em 1970 pelo Estado de Hesse, na Alemanha. Já a primeira legislação europeia nacional sobre o referido tema foi publicada pela Suécia, em 1973, sendo acompanhada, nos anos seguintes, por outros países europeus, a exemplo da Alemanha e da França, em 1977 e 1978, respectivamente.

---

[14] FRANCIS, et al. *Privacy: what everyone needs to know*. 1 ed. [S.L.]: Oxford University Press, 2017, p. 56

[15] STRANDBURG Katherine J; RAICU, Daniela Stan, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, [S.L.]:Ed. Springer US, 2006, p. 200: "*FIPs require entities collecting data to notify individuals of the data collection and of its purpose, to limit the use of the data for the stated purpose absent the individual's consent to other uses, to provide access and correction rights to the data, to minimize the collection of data, to ensure that the adequacy of the data matches its intended use, to provide adequate security, and to be accountable for the implementation of these rules*."

[16] Os princípios presentes no FIPs serviram de inspiração para a elaboração das *Guidelines* da OECD, bem como para a Diretiva 95/46/CE, instrumentos que não só adotaram como também desenvolveram alguns dos princípios contidos no referido texto americano. Para maior desenvolvimento, ver TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies», *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Volume 34, fevereiro de 2018, p. 135

[17] DEPARTAMENTO DE JUSTIÇA DOS ESTADOS UNIDOS, *Overview of the Privacy Act of 1974*, Disponível em: <https://www.justice.gov/opcl/introduction>. Acesso em: 12-10-2017

[18] CANADÁ, *Privacy Act*, R.S.C., 1985, Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/p-21/page-1.html> Acesso em 13-11-2017

[19] DONEDA, Danilo, *Um Código para a proteção de dados pessoais na Itália*, Disponível em: < https://www.researchgate.net/profile/Danilo_Doneda> Acesso em: 13-02-2018

Ainda no mesmo período, no âmbito do Conselho da Europa, o Comité dos Ministros adotou duas Resoluções cujo objetivo era regular a proteção dos dados pessoais no que concerne ao processamento automático dos bancos de dados. Neste sentido, foram adotadas as Resoluções (73) 22 [20] e (74) 29 [21] sobre a proteção da privacidade dos indivíduos quando do processamento eletrônico de bancos de dados no setor privado e público, respetivamente em 1973 e 1974.

No entanto, a tecnicidade desta primeira geração de leis não tardou a demonstrar a sua insuficiência para realizar uma eficiente regulação dos direitos à proteção dos dados. As referidas leis francesa (1978) e alemã (1977) foram as primeiras legislações a atribuir destaque à privacidade no manuseio dos referidos dados, enquanto as leis anteriores a esta se centravam no fenômeno da proteção dos dados pessoais sob a óptica computacional, sem privilegiar a privacidade enquanto liberdade negativa dos cidadãos. [22]

É incontestável que os computadores possuem uma capacidade de processamento e de armazenamento infinitamente superior ao das técnicas manuais de processamento de dados. O início dos anos 1980 foi marcado pela utilização cada vez mais frequente daquelas máquinas para o tratamento dos dados pessoais, tanto pelo setor público como pelo setor privado, fator que promoveu um aumento considerável do fluxo destes dados entre as fronteiras europeias. [23]

Em 1981, o Conselho da Europa adotou a Convenção para proteção dos indivíduos em matéria de processamento automático de dados pessoais (Convenção 108), [24] a qual entrou em vigor em 1985.

---

[20] COMITÉ DE MINISTROS DO CONSELHO DA EUROPA, Resolução (73) 22 do Comité de Ministros do Conselho da Europa (1973), relativa à proteção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector privado, de 26 de Setembro de 1973.

[21] COMITÉ DE MINISTROS DO CONSELHO DA EUROPA, Resolução (74) 29 do Comité de Ministros do Conselho da Europa (1974), relativa à protecção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector público, de 20 de Setembro de 1974.

[22] DONEDA, Danilo, «A proteção dos dados pessoais como um direito fundamental», *Revista Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 97

[23] A inclusão da proteção dos dados pessoais no ordenamento jurídico dos países europeus esteve intimamente ligada ao desenvolvimento das tecnologias da informação e sua aplicação tanto nos setores privados quanto na administração pública. Para maior desenvolvimento, ver DONEDA, Danilo, *op cit*, p. 315

[24] Até o ano de 2017, a referida Convenção já havia sido ratificada por 50 países, dentre os quais países da África e do continente americano. CONSELHO DA EUROPA, *Chart of signatures and ratifications of Treaty 108*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal

A supracitada convenção estabeleceu *standards* mínimos [25] de proteção dos dados pessoais que deveriam ser observados pelos Estados signatários, sendo esta convenção o primeiro instrumento jurídico vinculante, a nível internacional, que tratou especificamente sobre a proteção dos referidos dados, estabelecendo garantias, princípios e definindo conceitos sobre a proteção em análise.

Por mais que a aludida convenção estabeleça um patamar mínimo de proteção da privacidade e dos dados pessoais, os países signatários mantiveram a liberdade de estabelecer requerimentos de proteção mais rigorosos no âmbito de seus ordenamentos internos, bem como poderiam estabelecer restrições a algumas das disposições da Convenção 108 quando estivessem em causa interesses superiores, a exemplo da segurança do Estado. [26]

Além dos supracitados fatores, os EM ratificaram a aludida Convenção em ritmos diferentes, e nem sempre consagraram o mesmo nível de proteção aos dados após a referida ratificação. [27] Por conseguinte, havia uma discrepância entre o nível de proteção dos dados pessoais entre os Estados-Membros da União Europeia, fator que dificultava a transferência de dados entre os referidos Estados, e, consequentemente, o desenvolvimento do mercado interno europeu. [28-29]

Data Status as of 13/06/2018, Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=YuekXg7n> Acesso em: 13-06-2018

[25] O capítulo II da Convenção estabelece, entre os requerimentos mínimos de proteção, os seguintes: "*the requirement to have personal data obtained and processed fairly and lawfully, stored for specified and legitimate purposes and not used in a way incompatible with those purposes. A stricter legal regime applies for automated processing of the more sensitive data ("special categories of data"). Personal data must also be adequate, relevant and not excessive in relation to purposes for which they are stored, as well as accurate and kept up to date (where necessary). They also must not be kept in a form permitting identification of data subjects for longer than required for the purpose for which they are stored.*" Cf. GUMZEJ, Nina, *The Council Of Europe And The Right To Personal Data Protection: Embracing Postmodernity,* Conference of the International Journal of Arts & Sciences, Faculdade de Direito da Universidade de Zagreb, Croácia, 2013, p. 15

[26] Cf. Artigo 9º da Convenção 108.

[27] HUSTINX, Peter, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en> Acesso em: 17-11-2017, p. 9

[28] TAKA, Anni-Maria, *Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications*, Dissertação apresentada à Faculdade de Direito da Universidade da Upsália na área de especialização em Direito Internacional, 2017, p. 26

[29] Esta dificuldade é ressaltada no considerando n. 7 da Diretiva 95/46, senão, vejamos: "Considerando que as diferenças entre os Estados-Membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas

Para minimizar este desnível – e afastar os obstáculos à circulação dos dados pessoais - foi adotada, em 1995, a Diretiva do Parlamento Europeu e do Conselho em matéria de proteção dos dados pessoais. [30]

1.1 Diretiva 95/46/CE

A utilização doméstica da internet no começo dos anos 1990 e o fenómeno da globalização alteraram a sociedade em diferentes planos. A livre circulação de mercadorias e serviços no mercado digital tornava imprescindível a livre circulação de dados, a qual não poderia ser realizada se os Estados-Membros compartilhassem diferentes níveis de proteção dos dados pessoais. [31]

A Diretiva 95/46/CE [32] foi adotada em um período no qual a maioria dos países da UE já possuía uma lei nacional que regulava a proteção dos dados pessoais. [33] Por conseguinte, um dos principais objetivos da aludida diretiva era harmonizar estas legislações internas, de forma a estabelecer um padrão mínimo de proteção dos dados pessoais entre os Estados-Membros da União Europeia. [34-35]

Para que tivesse aplicação nos EM, a diretiva precisava ser transposta em lei interna em cada ordenamento jurídico nacional. Os dispositivos da Diretiva 95/46 foram

---

diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de atividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de proteção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;"

[30] Para maior desenvolvimento, ver OXMAN, Stephen A, «Exemptions to the European Union Personal Data Privacy Directive: will they swallow the directive?», *Boston College International Comparative Law Review*, vol. 24, 2000-2001, p. 193: "*At the time the Directive was passed, some individual European countries, such as Germany, already had passed their own legislation regulating the processing of personal data. Disparities among these various regulations, however, created potential obstacles to the free flow of personal data among Member States. The purpose of the Directive, therefore, was to create EU-wide privacy rights that would remove those obstacles and harmonize the transfer of personal data within the ED*"

[31] CONSELHO DA EUROPA, *Handbook on European data protection law*, Luxemburgo: Publications Office of the European Union, 2014, p. 17

[32] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, JO L 281 de 23.11.1995.

[33] CONSELHO DA EUROPA, *op cit*, p. 18

[34] *Ibid.*, p.19

[35] Neste sentido, os objetivos definidos no artigo 1º da Diretiva 95/46 indicam que este instrumento almejava proteger os direitos fundamentais e as liberdades das pessoas naturais, ao mesmo tempo em que buscava assegurar o livre fluxo de dados pessoais entre os Estados-Membros da União. Percebe-se, assim, que os objetivos da Diretiva, não obstante intimamente conectados, possuíam naturezas distintas. Para maior desenvolvimento, ver LYNSKEY, Orla, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, Oxford: Oxford University Press, 2015, p. 47

transpostos à ordem jurídica portuguesa através da Lei 67/98, [36] a qual é aplicada aos prestadores estabelecidos no referido país, independentemente da origem e do destino dos dados, abrangendo tanto empresas como órgãos públicos. [37-38]

Em todo caso, o objetivo de harmonização das legislações internas não logrou êxito, uma vez que o processo de transposição não foi realizado de forma homogênea, fator que gerou, como consequência, uma fragmentação da aplicação do referido instrumento jurídico nos diferentes Estados-Membros da UE.

Desta forma, o nível de proteção dos dados pessoais nos Estados-Membros da UE, ainda que mais consistente, continuava com uma grande margem de discrepância, dificultando, portanto, a circulação dos referidos dados e o desenvolvimento do mercado interno. [39] Conforme bem observa a Comissão Europeia na proposta do regulamento relativo à proteção dos dados pessoais [40]

> *As diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e das liberdades das pessoas, nomeadamente do direito à proteção dos dados pessoais, no que respeita ao tratamento desses dados, podem impedir a livre circulação de dados pessoais no conjunto da União. Estas diferenças*

[36] PORTUGAL, Lei nº 67/98, Lei da Protecção Dados Pessoais (transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados, Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=156&tabela=leis> Acesso em: 30/01/2018.

[37] DIAS PEREIRA, Alexandre Libório, «Big Data, E-Health e «Autodeterminação Informativa»: A Lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR) », *Lex Medicinae – Revista Portuguesa de Direito da Saúde*, n.o 29 (2018), p. 5

[38] Para maior desenvolvimento sobre a Lei 67/98, ver DIAS PEREIRA, Alexandre Libório, «Marco Civil da Internet" e seus Reflexos no Direito da União Europeia», *RJLB*, Ano 2 (2016), nº 4, p. 53-106, p. 72: "A Lei 67/98 delimita o seu âmbito de aplicação, não apenas material (noção de dados pessoais), mas também geográfico (prestador estabelecido em Portugal independentemente da origem e do destino dos dados) e subjetivo (i.e. os destinatários do regime jurídico, abrangendo tanto empresas como organismos públicos, e com exclusão de atividades puramente domésticas ou particulares). O tratamento de dados pessoais está sujeito a obrigação de notificação à Comissão Nacional de Proteção de Dados (art. 27º), mero registo ou autorização prévia (e.g. dados sensíveis, dados de crédito e solvabilidade). A noção de dados pessoais é ampla, abrangendo 'seguramente, o nome de uma pessoa a par do seu contacto telefónico ou de informações relativas às suas condições de trabalho ou aos seus passatempos', incluindo os dados de IP na medida em que tornam identificável a pessoa (Diretiva 67/98, considerando 26). Uma categoria especial de dados, para efeitos de regime, é composta pelos chamados dados sensíveis, incluindo filiação sindical, dados de saúde (físicos ou psíquicos), dados genéticos, vida privada (por ex. orientação sexual, consumo de drogas), raça e etnia, etc."

[39] HUSTINX, Peter, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en> Acesso em: 17-11-2017, p. 23

[40] COMISSÃO EUROPEIA, Proposta de regulamento do parlamento europeu e do conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012, p. 19

> *podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da UE, falsear a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Estas diferenças nos níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.*

A Diretiva 95/46/CE foi elaborada em meados dos anos 1990, época em que apenas 1% da população europeia utilizava a Internet. [41] Destarte, não é difícil concluir que a sociedade na qual nos encontramos destoa consideravelmente daquela na qual - e para a qual – o referido instrumento foi elaborado.

É natural que, com a evolução tecnológica, o fenômeno da Internet e a globalização, o instrumento jurídico ora em estudo tornar-se-ia obsoleto, e, portanto, incapaz de regular eficazmente a sociedade na qual vivemos.

Atualmente, contamos com tecnologias que permitem a recolha, o armazenamento e a transferência de dados de uma forma nunca antes vista. Outrossim, os cidadãos estão a disponibilizar os seus dados com uma frequência muito maior do que aquela registada há 20 anos, quando a Diretiva 95/46 foi elaborada.

Não obstante tenha sido constatado um aumento no compartilhamento dos dados, ainda persiste um considerável nível de desconfiança por parte dos seus titulares quanto ao uso que será atribuído às suas informações. [42]

---

[41] THE WORLD BANK, *Indivíduos que utilizam a internet (% da população)*, Disponível em: < https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EU&name_desc=false> Acesso em: 19-01-2018.

[42] TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies», *Computer Law & Security Review:* The International Journal of Technology Law and Practice, Volume 34, Fevereiro de 2018, p. 2: "*As a result of technological development, along with globalisation, new and increased challenges for personal data protection have emerged. Although new technologies and services benefit both businesses and consumers, they also generate serious privacy risks. This situation may decrease people's trust in companies that collect data for their service production. The lack of trust can slow down the development of the innovative use and adoption of new technologies, and many new business opportunities may be missed if appropriate data protection practices are not implemented.*"; No mesmo sentido, COMISSÃO EUROPEIA, *Acordo sobre reforma da proteção de dados na UE proposta pela Comissão estimula mercado único digital,* Bruxelas, 15 de dezembro de 2015, Disponível em: <http://europa.eu/rapid/press-release_IP-15-6321_pt.htm> Acesso em: 19-04-2018: "A reforma permite que as titulares retomem o controlo sobre os próprios dados. Segundo um inquérito Eurobarómetro recente, dois terços dos europeus (67 %) declararam-se preocupados por não terem controlo total das informações que fornecem em linha. Sete em cada dez europeus estão apreensivos quanto ao potencial de utilização das informações fornecidas por parte das empresas. A reforma da proteção de dados vem reforçar o direito à proteção dos dados pessoais – direito fundamental da UE – e criar a confiança necessária para fornecer dados pessoais."

Por conseguinte, sentiu-se a necessidade da elaboração de normas que não só regulassem os novos cenários gerados pelo avanço tecnológico, mas também fortalecessem os direitos dos titulares dos dados, gerando, assim, uma maior confiança aos titulares de dados pessoais quando estes precisassem compartilhar os referidos dados.

Entre os anos de 2009 a 2011, a Comissão Europeia realizou duas fases de consulta pública sobre a necessidade de uma reforma na Diretiva 95/46/CE. [43] A principal inquietação da Comissão era saber se o referido instrumento continuava atualizado e capaz de oferecer o direito à proteção dos dados pessoais numa sociedade que já não mais correspondia àquela na qual o referido instrumento foi formulado. [44]

Esta questão ganhou ainda mais relevância em 2009, após a entrada em vigor da Carta dos Direitos Fundamentais da União Europeia, [45] a qual consagra em seu artigo 7º o direito fundamental ao respeito pela vida privada e familiar, ao passo em que assegura no artigo 8º o direito fundamental à proteção dos dados.

Como forma de adequar a legislação europeia aos novos desafios impostos pela sociedade da informação, a Comissão anunciou, em 2012, um pacote de reforma do direito europeu em matéria da proteção de dados, o qual era composto pelo Regulamento Geral sobre a Proteção de Dados e pela Diretiva da Proteção de Dados destinados às autoridades policiais e judiciais. [46-47]

---

[43] COMISSÃO EUROPEIA, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012, p. 3

[44] As questões realizadas na referida consulta pública foram as seguintes:
"– 'Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation.'
– 'In your views, the current legal framework meets these challenges?' – 'What future action would be needed to address the identified challenges?'" Cf. COMISSÃO EUROPEIA, Directorate C : Fundamental rights and Union citizenship Unit C.3 : Data protection, Summary Of Replies To The Public Consultation About The Future Legal Framework For Protecting Personal Data, Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf>, Acesso em: 22/10/2017

[45] Carta dos Direitos Fundamentais da União Europeia, JO C 83 de 30.3.201, Disponível em:< https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:pt:PDF> Acesso em: 23-01-2018

[46] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, pp. 89-131)

Além da atualização do direito europeu, a aludida reforma almejava harmonizar a proteção dos dados pessoais nos ordenamentos jurídicos dos diferentes Estados-Membros. Por conseguinte, havia a necessidade não só de fortalecer o direito à proteção dos dados, mas também de torná-lo mais consistente. [48-49]

1.2 Regulamento Geral sobre a Proteção de Dados (RGPD)

Ao possibilitar a transposição de um *standard* mínimo de proteção dos dados pessoais, atribuindo aos Estados-Membros o poder de regulamentar as demais facetas dos seus regimes internos de proteção dos referidos dados, a Diretiva 95/46/CE deu azo a um regime europeu de proteção dos dados desarmônico, gerando as falhas que foram discutidas no tópico precedente.

Aliado a este fator, os dispositivos da Diretiva 95/46/CE já não conseguiam realizar uma regulação eficiente das novas tecnologias surgidas nos últimos 20 anos, as quais revolucionaram os meios pelos quais os dados são tratados.

Como seria inviável que os Estados-Membros solucionassem, de forma autónoma, a questão da discrepância no quadro europeu relativo ao nível de proteção dos dados pessoais, surgiu a necessidade de desenvolver um instrumento jurídico que estabelecesse uma proteção uniforme, de forma a permitir uma *transferência transfronteiriça fácil dos dados pessoais na UE, assegurando simultaneamente a proteção efetiva de toda as*

---

[47] COMISSÃO EUROPEIA, *Acordo sobre reforma da proteção de dados na UE proposta pela Comissão estimula mercado único digital*, Bruxelas, 15 de dezembro de 2015, Disponível em: <http://europa.eu/rapid/press-release_IP-15-6321_pt.htm> Acesso em: 19-04-2018

[48] HUSTINX, Peter, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en> Acesso em: 17-11-2017, p. 27

[49] Segundo a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), estava na "altura de adotar um quadro jurídico de proteção dos dados mais sólido e coerente na UE, apoiado por uma aplicação rigorosa das regras, que permita à economia digital desenvolver-se em todo o mercado interno, às pessoas singulares controlar os seus próprios dados, bem como reforçar a segurança jurídica e prática para os operadores económicos e as entidades públicas" COMISSÃO EUROPEIA, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012, p. 3

pessoas singulares no conjunto da UE. [50] O referido instrumento é o Regulamento Geral sobre a Proteção dos Dados.

O RGPD foi adotado em abril de 2016, entrando em vigor nesta data. Em todo caso, tendo em consideração as alterações impostas pelo instrumento jurídico em apreço, foi atribuído o período de dois anos de adaptação, de forma que o regulamento só passou a ser aplicado em 25 de maio de 2018.

De acordo com o artigo 288º do Tratado de Funcionamento da União Europeia (TFUE), o regulamento possui aplicabilidade direta, [51] isto é, torna-se automaticamente lei em todos os Estados-Membros, sem que estes precisem transpor os dispositivos do RGPD para os ordenamentos jurídicos nacionais.

Na qualidade de Regulamento da União Europeia, o RGPD prevalece sobre as legislações internas dos Estados-Membros, os quais estão proibidos de promulgar leis que diminuam o nível de proteção estabelecido no regulamento em análise.

Dessa forma, almejou-se com a adoção do regulamento não só fortalecer os direitos dos titulares dos dados, como também reduzir a fragmentação jurídica que existia sob a vigência da Diretiva 95/46/CE, estabelecendo, neste sentido, um quadro harmonizado de proteção dos dados pessoais nos Estados-Membros da UE.

Além de facilitar o livre fluxo dos dados entre os EM, a imposição de um quadro de proteção reforçado e coerente fortalece a confiança dos titulares dos dados e, como consequência, estes mostram-se mais propensos a compartilhar suas informações – uma vez que possuem um controlo maior sobre o uso que é atribuído aos seus dados – fator que facilita e impulsiona o desenvolvimento do mercado. [52]

---

[50] COMISSÃO EUROPEIA, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012, p. 6

[51] KUNER, C, «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law», *Bloomberg BNA Privacy and Security Law Report*, 2012, p. 4: "*However, a regulation leads to a greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; has legal effect independent of national law; and overrides contrary national laws*".

[52] COMISSÃO EUROPEIA, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

Para garantir os referidos objetivos, o regulamento fortaleceu tanto os direitos dos titulares dos dados, como também as obrigações dos responsáveis pelo tratamento e dos subcontratantes, além de consagrar princípios essenciais à proteção dos dados [53] em análise, a exemplo do princípio da licitude, lealdade e transparência, [54] do princípio da limitação da conservação [55] e do princípio da minimização dos dados. [56]

Neste sentido, alguns dos direitos atribuídos aos titulares dos dados pessoais na Diretiva 95/46/CE foram reforçados para que pudessem passar a oferecer maior controlo a estes sujeitos - a exemplo do direito de acesso aos próprios dados – como também foram instituídos novos direitos aos titulares, como o direito à portabilidade (artigo 20º), e o direito ao esquecimento (artigo 17º).

O direito à portabilidade permite que o titular dos dados solicite a uma entidade ou empresa que devolva os dados pessoais que a estas foram oferecidos tanto por via do consentimento, como por via contratual, e que os transmita diretamente a outra organização ou empresa, caso seja tecnicamente possível. Ao instituir essa

---

desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012, p. 6

[53] O RGPD consagra em seu artigo 5º sete princípios fundamentais que devem ser observados pelos responsáveis pelo tratamento e subcontratantes quando realizarem o tratamento dos dados, a saber: princípio da licitude, lealdade e transparência, princípio da limitação das finalidades, princípio da minimização dos dados, princípio da exatidão, princípio da limitação da conservação, o princípio da integridade e confidencialidade, e, por fim, o princípio da responsabilidade.

[54] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Artigo 5º, 1, a.

[55] Previsto no artigo 5º, 1, e, do RGPD, o princípio da limitação da conservação determina que os dados só devem ser conservados durante o período necessário à realização do fim que ensejou a sua coleta. Neste sentido, os dados pessoais coletados não podem ser armazenados por tempo indeterminado. Em verdade, devem ser descartados quando já não mais estiverem a ser utilizados. Por conseguinte, deve ser realizada uma avaliação periódica sobre a necessidade de manutenção dos dados armazenados, devendo ser eliminados aqueles que já não mais tiverem utilidade. O princípio em questão deverá ser interpretado tendo em consideração o direito ao esquecimento previsto no artigo 17º do RGPD.

[56] A Diretiva 95/46/CE consagrava o princípio da minimização dos dados na alínea c), 1, do artigo 6 º, onde dispunha que os dados pessoais devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente. O RGPD, por seu turno, fortalece a proteção dos dados ao determinar que estes deverão ser limitados ao que é **necessário** relativamente às finalidades para as quais são tratados. Para garantir a observância deste princípio, o responsável pelo tratamento e o subcontratante poderão aplicar medidas técnicas e organizativas que assegurem a coleta apenas dos dados necessários à finalidade do tratamento, a exemplo da pseudonimização. O RGPD consagra o princípio da minimização dos dados em seu artigo 5º, 1, c.

transmissibilidade entre as entidades que detém os dados, o regulamento não só fomenta a livre circulação dos dados na UE, como também estimula a concorrência. [57]

Já o direito ao esquecimento confere ao titular a faculdade de requerer ao responsável pelo tratamento o apagamento dos seus dados, sem demora injustificada, em seis casos específicos previstos nas alíneas do número 1 do artigo 17º, a exemplo das situações nas quais os dados deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento, ou quando houver a retirada do consentimento em que se baseia o tratamento dos dados, não existindo outro fundamento jurídico sobre o qual aquele tratamento possa se basear. [58] Insta ressaltar que este direito não é absoluto, devendo ser afastado quando estiver em confronto com outros direitos e interesses, como o exercício da liberdade de expressão e de informação, ou por motivos de interesse público no domínio da saúde pública, além de outras situações previstas no n. 3 do artigo 17º do RGPD.

Para alcançar o escopo do fortalecimento da proteção dos dados pessoais, o regulamento altera igualmente o quadro de obrigações estabelecido na antiga Diretiva 95/46/CE, e passa a consagrar novos encargos aos responsáveis pelo tratamento e subcontratantes, como a proteção de dados desde a conceção e por defeito (artigo 25º), o registo das atividades de tratamento (artigo 30º), a avaliação de impacto sobre a proteção de dados (artigo 35º), e, em certos casos, a necessidade de indicação de um Encarregado da Proteção de dados (artigos 37º, 38º, 39º).

As novas tecnologias tornaram muito mais fáceis o compartilhamento, o processamento e o armazenamento dos dados pessoais, criando, por conseguinte, maiores riscos aos direitos e liberdades do titular dos dados em apreço.

---

[57] COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades* – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de dados a partir de 25 de maio de 2018. Bruxelas, 24.1.2018, COM(2018) 43 final, p. 2

[58] Nomeadamente, (1) Quando esses dados deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; (2) Quando houver a retirada do consentimento em que se baseia o tratamento dos dados e se não houver outro fundamento jurídico sobre o qual aquele tratamento possa se basear; (3) Quando o titular se opuser ao tratamento e não existirem interesses legítimos prevalecentes que autorizem o tratamento; (4) Se os dados pessoais forem tratados de forma ilícita; (5) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; (6) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.o, n.1 . Cf. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Artigo 17º.

Ciente dessa nova realidade, e buscando adequar-se à sociedade da informação, de forma a melhor regulá-la, o RGPD estabelece ao responsável pelo tratamento - auxiliado, sendo o caso, pelo encarregado da proteção dos dados - a obrigação de proceder a uma avaliação do impacto do tratamento dos dados pessoais, antes do início deste processo, sempre que o tratamento for suscetível de implicar um elevado risco aos direitos e liberdades dos titulares dos dados.

Neste sentido, a avaliação busca determinar quais são os riscos envolvidos no tratamento, de forma que o responsável por este processo possa adotar as medidas técnicas e organizativas suficientes e necessárias para eliminar ou minimizar o risco em questão, além de assegurar a proteção dos dados e demonstrar a observância ao RGPD.

As referidas medidas técnicas e organizativas devem ser utilizadas pelo responsável pelo tratamento tanto no momento em que este define e desenvolve o sistema que será utilizado para o tratamento dos dados (proteção desde a conceção), como também no momento da realização do próprio tratamento, de forma a assegurar que, por defeito, só serão tratados os dados necessários às finalidades que fundamentaram a sua recolha. [59]

A avaliação de impacto é uma medida de natureza preventiva, devendo ser realizada antes do início do tratamento justamente para antecipar os possíveis riscos e minimizá-los, como dito acima. No entanto, é possível que a referida avaliação seja realizada no decorrer de uma atividade de tratamento, quando o objeto, os meios ou as finalidades deste tratamento são alterados de forma tal que essa atividade passa a implicar um risco elevado aos direitos e liberdades dos titulares dos dados pessoais.

O RGPD ainda estabelece aos responsáveis pelo tratamento e ao subcontratante - no caso deste sujeito estar a realizar o tratamento dos dados em nome do responsável pelo tratamento - a obrigação de manter um registo das atividades de tratamento que foram executadas sob sua responsabilidade.

Apesar de ser uma obrigação, o dever de registar as atividades de tratamento pode ser benéfico àquele que o cumpre, uma vez que será mais fácil atender aos pedidos de informações requeridos tanto pelas autoridades de controlo, como pelos titulares dos dados, os quais possuem o direito de acesso aos seus dados pessoais que estão a ser objeto

[59] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Artigo 25.

de tratamento. Além disso, a conservação do aludido registo aumenta a transparência dos processos de tratamento e facilita a comprovação da observância do RGPD. [60]

O incumprimento das aludidas obrigações legais pode ser penalizado com a aplicação de severas coimas, as quais podem alcançar, a depender do caso, o teto máximo de 20 mil milhões de euros ou até 4% do volume de negócios anual da empresa a nível mundial, consoante o que for mais elevado.

1.2.1 Âmbito de aplicação material

De acordo com o artigo 2º do RGPD, este será aplicado a qualquer tratamento de dados pessoais, realizado por meios parcial ou totalmente automatizados ou não automatizados, entendendo-se por tratamento qualquer operação realizada sobre os dados pessoais, a exemplo do registo, recolha, conservação, utilização, difusão, limitação e apagamento. Esta definição tão abrangente do âmbito de aplicação material reflete o objetivo do aludido regulamento de estabelecer um alto nível de proteção dos dados pessoais.

Caso o tratamento dos dados seja realizado de forma manual, isto é, executado por humanos, sem o auxílio de máquinas, deverão estar presentes dois requisitos para que o RGPD seja aplicado: (1) Os dados pessoais devem estar contidos em ficheiros ou a eles destinados; [61] (2) Os referidos dados devem estar organizados de acordo com um critério específico, podendo este ser ordem alfabética ou cronológica, por exemplo. [62]

Ainda o mesmo artigo esclarece que o RGPD não abrangerá os tratamentos realizados por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.

1.2.2 Âmbito de aplicação territorial

[60] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 44
[61] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 2º, 1.
[62] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (15)

1.2.2.1 Artigo 3º, 1

Conforme exposto no tópico precedente, o RGPD terá aplicação direta em todos os Estados-Membros da União Europeia, prescindindo da transposição do seu texto em lei interna nestes Estados.

Desenvolvendo o seu âmbito de aplicação territorial, o Regulamento 2016/679 explicita que seus dispositivos serão aplicados ao tratamento de dados pessoais realizados no contexto das atividades de um estabelecimento de responsáveis pelo tratamento ou subcontratantes que se encontrem em um dos Estados-Membros da União, independentemente de o tratamento ocorrer dentro ou fora da União.

Destarte, o direito aplicável será determinado com base no local onde o responsável pelo tratamento ou subcontratante possui um estabelecimento no qual sejam realizadas atividades relacionadas com o tratamento dos dados pessoais, sem que seja decisivo para a incidência do RGPD o local onde os dados estão a ser tratados. [63]

1.2.2.2 Artigo 3º, 2

Sob a vigência da antiga Diretiva 95/46/CE, as entidades que não possuíssem um estabelecimento em um dos Estados-Membros da União apenas estariam sujeitas às disposições nacionais de um dos EM, adotadas por força da diretiva, se recorressem para o tratamento dos dados, a meios, automatizados ou não, situados no território desse EM, a não ser que os meios só fossem utilizados para o trânsito no território da UE. [64]

Da adoção da aludida diretiva até os dias atuais, houve uma mudança significativa na economia global e na forma por meio da qual as empresas se comportam no mercado. Os desenvolvimentos das tecnologias de informação, e a evolução e disseminação da internet e do *e-commerce* simplificaram e tornaram muito mais acessíveis não só a oferta de bens e serviços por entidades que não se situam na União, como também o câmbio de dados pessoais entre entidades situadas em diferentes partes do globo.

---

[63] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide,* Switzerland: Springer International Publishing, 2017, p. 22

[64] Diretiva 95/46/CE, artigo 4º, 1, c.

Diante deste cenário, o RGPD amplia significativamente o alcance do seu âmbito de aplicação territorial, de forma a abranger as entidades que, não obstante não situadas fisicamente na União Europeia, tenham como alvo os consumidores que se encontrem no mercado europeu.

Este âmbito de abrangência buscou amenizar as discrepâncias entre os diferentes níveis de proteção dos dados pessoais previsto entre ordenamentos jurídicos distintos, estabelecendo como *standard* mínimo aquele consagrado na União Europeia, qual seja o RGPD.

Isto porque o desenvolvimento das leis de proteção dos dados pessoais realizou-se de uma forma desarmonizada não só entre os países da União Europeia, como também entre estes e demais países não membros desta União, a exemplo dos Estados Unidos. A falta de harmonia entre estes diplomas dificultava a transferência de dados e, consequentemente, o desenvolvimento do mercado.

É neste sentido que o número 2 do artigo 3º do RGPD sujeita à aplicação do regulamento todo aquele que monitorar o comportamento de cidadãos residentes na União Europeia, ou que ofereça bens e serviços aos residentes na UE, [65] ainda que a entidade em questão não esteja sediada na União. Esta previsão ajuda a estabelecer condições de concorrência equitativas para todas as empresas que operam no mercado da UE. [66]

Para auferir se determinada companhia oferece bens ou serviços aos residentes da UE, pode-se observar se há, dentre outros fatores, a possibilidade de envio daquele produto a um dos Estados-Membros da União; se há a possibilidade de realização do pagamento em euros; ou se o domínio do sítio web refere-se a um dos Estados-Membros (a exemplo de "xxx.com.pt" ou "xxx.com/it"). [67]

[65] Ressalta-se que os bens e serviços podem ser oferecidos até mesmo de forma gratuita. Não é necessário o pagamento do bem ou serviço para que esta atividade esteja sujeita ao RGPD.
[66] COMISSÃO EUROPEIA, Comunicação da Comissão do Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades* — Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018, Bruxelas, 24.1.2018 COM(2018) 43 final, p. 2
[67] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 26

Por outro lado, o RGPD também será aplicável àquelas entidades que, ainda que estabelecidas em países terceiros, monitorem o comportamento de consumidores residentes na UE, desde que o comportamento tenha lugar na União. [68]

Caso o RGPD seja aplicável, o responsável pelo tratamento e/ou subcontratante deverá designar, por escrito, um representante em um dos Estados-Membros da UE onde se encontram os titulares cujos dados pessoais são objeto do tratamento no contexto da oferta que lhes é feita de bens ou serviços, ou cujo comportamento é controlado, a não ser que o tratamento *seja ocasional, não inclua o tratamento, em larga escala, de categorias especiais de dados pessoais, nem o tratamento de dados pessoais relativos a condenações penais e infrações, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares*. [69]

Em todo caso, deve-se observar que a designação deste representante não isenta os responsáveis pelo tratamento ou subcontratantes de serem responsabilizados por suas atitudes nos referidos Estados-Membros.

Ora, a União Europeia é o maior bloco económico na atualidade, o que torna muito difícil – se não impossível – às grandes companhias que utilizam a Internet como plataforma para o comércio não estarem sujeitas à observância do RGPD.

Destarte, o âmbito de aplicação do RGPD acaba por ser global, se estiverem reunidas as condições supracitadas. Por conta deste alcance, o RGPD é uma das mais importantes normas que regula a proteção dos dados pessoais na atualidade.

[68] O considerando 24 do RGPD define controlo do comportamento da seguinte forma: "A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes." Cf. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (24).

[69] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (80).

CAPÍTULO II – O RGPD E AS TRANSFERÊNCIAS DE DADOS PESSOAIS PARA PAÍSES TERCEIROS

1. Transferências de dados pessoais para países terceiros ou organizações internacionais.

Como resultado do crescente desenvolvimento das novas tecnologias da informação e da globalização do mercado, as transferências dos dados pessoais tornaram-se um elemento de presença constante na dita sociedade da informação, principalmente no mercado digital.

No âmbito da UE, a proteção dos dados pessoais é um direito fundamental garantido pela Carta dos Direitos Fundamentais da União Europeia.[70] Por conseguinte, o sistema legal da UE estabelece direitos e obrigações voltados à garantia da efetividade da proteção dos dados quando estes são transferidos a países terceiros. Caso contrário, de nada adiantaria consagrar um elevado nível de proteção dos dados se, quando estes fossem transferidos, o referido nível de proteção não os acompanhassem.

O RGPD preocupa-se em manter o nível de proteção dos dados pessoais previsto em seu texto quando do tratamento realizado após a transferência destes dados para um país terceiro [71] ou organização internacional. Por isso, o artigo 44º do referido instrumento dispõe que as transferências em questão só podem ser realizadas se o responsável pelo tratamento ou subcontratante respeitar as disposições do regulamento, de forma a não comprometer o nível de proteção dos dados consagrado no RGPD. A ideia é que as proteções conferidas aos dados na União Europeia os acompanhem quando forem objeto de tratamento após transferência ao país terceiro ou organização internacional.

Sendo assim, as transferências de dados pessoais provenientes da UE para um país terceiro ou organização internacional apenas poderão ser realizadas, regra geral, sob as seguintes condições: (1) A Comissão emitiu uma decisão por meio da qual indica a adequação do nível de proteção dos dados do país terceiro; (2) Diante da ausência da

[70] Cf. Artigo 8º da Carta de Direitos Fundamentais da União Europeia.
[71] Entenda-se por país terceiro aquele que não é um Estado-Membro da União Europeia. Cf. VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 116

decisão de adequação, o exportador dos dados adota garantias adequadas para a realização da transferência; (3) Em último caso, o exportador poderá utilizar uma das derrogações previstas no artigo 49º do RGPD. Os referidos mecanismos estão previstos nos artigos 45º, 46º, 47º, 49º do RGPD, os quais serão a partir de então explorados no presente estudo. [72]

1.1 Artigo 45º – Decisão de adequação

Após realizar uma análise da ordem jurídica e das práticas do país terceiro, a Comissão Europeia poderá emitir uma decisão por meio da qual indica a adequação [73] do nível de proteção dos dados consagrado no país terceiro no qual se encontra o recetor da transferência dos aludidos dados.

Já existente sob a égide da Diretiva 95/46/CE, as decisões de adequação têm o seu âmbito de aplicação alargado pelo RGPD, o qual permite que a Comissão declare a adequação não só de organizações internacionais e de países terceiros, como também de setores específicos ou territórios daquele país.

Não obstante estabeleçam critérios para avaliar a adequação do nível de proteção, nem o RGPD, nem a antiga diretiva desenvolvem detalhadamente o conceito do nível de adequação.

Em todo caso, ao julgar o processo C-362/14 (*Maximillian Schrems v. Data Protection Commissioner*), [74] o Tribunal de Justiça da União Europeia (TJUE) clarificou o aludido conceito de "adequação" ao indicar que este não pode ser entendido como a exigência de um nível de proteção idêntico àquele previsto na União Europeia.

[72] O RGPD mantém as linhas gerais do quadro normativo sobre a transferência de dados consagrado na Diretiva 95/46. No entanto, o aludido regulamento vai além do instrumento jurídico precedente, na medida em que simplifica e clarifica as disposições neste último consagradas, ao mesmo tempo em que introduz novos mecanismos voltados à transferência em apreço. Para maior desenvolvimento, ver COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, 10 de janeiro de 2017, COM(2017) 7 final, p.4

[73] Até o ano de 2018, a Comissão Europeia emitiu 12 decisões de adequação aos seguintes destinatários: Andorra, Argentina, Canadá (organizações comerciais sujeitas ao PIPEDA), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos (limitada às entidades aderentes ao Escudo da Proteção dos dados – *Privacy Shield*).

[74] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

Segundo entendimento do TJUE, o nível de proteção dos dados pessoais do sistema estrangeiro será adequado se for *substancialmente equivalente* ao consagrado na UE. [75] O RGPD acolheu o referido parâmetro utilizado pelo TJUE no seu considerando 104, o qual prevê que o país terceiro deverá *dar garantias para assegurar um nível adequado de proteção essencialmente equivalente àquele assegurado na União*. [76]

Para determinar a adequação, ou seja, a equivalência substancial entre os níveis de proteção dos dados pessoais do país importador e a UE, tanto a Diretiva 95/46/CE como o RGPD preveem uma lista de requisitos que devem ser considerados pela Comissão.

No entanto, como consequência dos desdobramentos do caso *Schrems* - a ser desenvolvido no segundo capítulo deste trabalho - a referida lista prevista no RGPD é mais extensa e elaborada do que aquela consagrada no âmbito da Diretiva de 1995. [77]

O RGPD prevê, nas alíneas "a", "b" e "c" do número 2 do artigo 45º, três dimensões fundamentais a serem consideradas pela Comissão quando da avaliação da adequação do país terceiro.

A alínea "a" diz respeito à avaliação que deve ser realizada tendo como plano de fundo o quadro jurídico do país terceiro. Neste aspeto, o RGPD destaca a necessidade da avaliação da existência do primado do Estado de Direito e o respeito pelos direitos humanos e liberdades fundamentais, tendo em consideração as normas aplicáveis em matéria de segurança pública, defesa, segurança nacional e direito penal, além da legislação referente ao acesso das autoridades públicas aos dados pessoais, das legislações e das regras de proteção de dados, regras profissionais e medidas de segurança, bem como da legislação referente à transferência ulterior de dados pessoais para outro país terceiro ou organização internacional.

Ainda no contexto do quadro legal, a Comissão deverá ter em conta a jurisprudência e as vias de recurso administrativo e judicial que poderão ser utilizadas pelos titulares dos dados.

---

[75] COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, 10 de janeiro de 2017, COM(2017) 7 final, p. 4

[76] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (104).

[77] Para maior desenvolvimento, ver ANDRADE DE JESUS, Inês Oliveira, «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?», *Anuário da Proteção de Dados 2018*. Lisboa: CEDIS, 2018, p.78

A alínea "b", por seu turno, diz respeito à análise sobre a existência de autoridades independentes que deverão garantir a observância e a aplicação das normas referentes à proteção de dados pessoais, devendo, para tanto, ser dotadas de poderes coercitivos para prestar o auxílio necessário e adequado ao titular dos dados quando do exercício dos seus direitos.

Por fim, a alínea "c" discorre sobre a assunção de compromissos internacionais, convenções ou instrumentos jurídicos vinculativos, como também a participação em sistemas multilaterais ou regionais, especialmente aqueles relativos à proteção de dados pessoais. [78]

Por meio destes elementos, o RGPD estabelece a necessidade de uma avaliação global do recetor dos dados, devendo ser analisada não só a existência de um quadro legal que garanta a proteção dos dados pessoais, como também a existência de autoridades que garantam a aplicação e a observância das normas de proteção dos dados, bem como a adoção de sistemas através dos quais os titulares dos dados possam fazer valer os seus direitos.

Caso entenda que o país terceiro ou a organização internacional reúne os elementos suficientes para garantir uma adequada proteção aos dados pessoais, a Comissão poderá emitir a decisão de adequação que permitirá a transferência dos dados em apreço. A partir de então, o exportador ficará isento de apresentar outras garantias ou autorizações para realizar a transferência dos dados. [79-80]

Esta decisão, todavia, não é imutável. A Comissão deverá acompanhar os desenvolvimentos relevantes que possam afetar o nível de proteção dos dados no país terceiro. Neste sentido, deve ser realizada uma avaliação periódica da adequação da decisão, ao menos de quatro em quatro anos, como forma de auferir se os supracitados elementos essenciais ainda se encontram presentes de facto e de direito.

---

[78] Quando da avaliação dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, a Comissão deverá ter em conta, em especial, a adesão à Convenção do Conselho da Europa para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981, e ao seu Protocolo Adicional, de acordo com o Considerando n. 105 do RGPD.

[79] ALSTON & BIRD, *Transferring Data from the EU: Privacy Shield and Data transfers under the GDPR*, Disponível em: <https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf > Acesso em: 10/05/2018, p. 2

[80] COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, 10 de janeiro de 2017, COM(2017) 7 final, p. 4

Caso os aludidos elementos não mais se encontrem presentes, a Comissão deverá consultar o país terceiro ou a organização internacional para que estes corrijam os fatores que afetaram a adequação do nível de proteção dos dados. Se nada for feito, a Comissão deverá, então, revogar, alterar ou suspender a sua decisão de adequação, a depender da situação. [81]

Ainda o mesmo artigo esclarece que as decisões de adequação adotadas pela Comissão com base na Diretiva 95/46/CE continuarão válidas até que sejam alteradas, substituídas ou revogadas por outra decisão adotada pela Comissão com base no RGPD.

1.2 Artigo 46º – Garantias adequadas

Diante da ausência de uma decisão de adequação, o responsável pelo tratamento ou subcontratante só poderá realizar a transferência dos dados pessoais se adotar os instrumentos necessários à colmatação da insuficiência da proteção dos dados no país terceiro, oferecendo, por conseguinte, garantias adequadas à proteção dos dados transferidos, *e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes*. [82]

Essas garantias costumam ser referidas como "mecanismos alternativos de transferência dos dados pessoais", em uma alusão ao facto de que enquanto a decisão de adequação emitida pela Comissão representa o cenário ideal à transferência dos dados em questão, as garantias adequadas restariam como segunda opção, apenas utilizadas no caso da inexistência da aludida decisão. [83]

Neste sentido, o RGPD elenca uma série de comportamentos e instrumentos que podem funcionar como garantias adequadas, sendo estes os instrumentos juridicamente vinculativos e com força executiva entre autoridades ou organismos públicos; as regras

[81]COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, 10 de janeiro de 2017, COM(2017) 7 final, p. 10: "Esta abordagem dinâmica aplica-se também às decisões de adequação já emitidas que foram adotadas ao abrigo da Diretiva de 1995, e que deverão ser revistas se deixarem de satisfazer as normas aplicáveis. Por conseguinte, os países terceiros em causa são convidados a informar a Comissão acerca de qualquer alteração pertinente da legislação ou prática introduzida desde a adoção da decisão de adequação que lhes diga respeito."

[82] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (108) e Artigo 46º.

[83] ALSTON & BIRD, *Transferring Data from the EU: Privacy Shield and Data transfers under the GDPR*, Disponível em: <https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf > Acesso em: 10/05/2018, p. 9

vinculativas aplicáveis às empresas; as cláusulas-tipo de proteção de dados adotadas ou aprovadas pela comissão; e os códigos de conduta e procedimentos de certificação.

Os distintos mecanismos poderão ajustar-se a diferentes cenários, a depender do caso concreto, [84] cabendo às partes que realizam a transferência dos dados identificar aquele que melhor se adequa às suas necessidades.

Nos tópicos seguintes, serão abordadas as garantias consideradas mais relevantes ao estudo da transferência dos dados pessoais a partir da UE com destino a um país terceiro.

1.2.1 Cláusulas contratuais-tipo

Para compensar a falta de um nível mais adequado de proteção, o importador e o exportador dos dados poderão adotar cláusulas contratuais-tipo emitidas pela Comissão, [85] as quais criam obrigações às referidas partes com vista a assegurar que na transferência, e no posterior tratamento, será mantido um adequado nível de proteção dos dados.

Neste sentido, as referidas cláusulas impõem encargos que devem espelhar os direitos e obrigações fundamentais garantidos no direito europeu, assegurando, desta forma, que o nível de proteção de dados consagrado na UE os acompanhará quando estes forem transferidos ao país terceiro. [86]

---

[84] COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, Bruxelas, 10 de janeiro de 2017, COM(2017) 7 final, p. 11

[85] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 119

[86] Neste sentido, os conjuntos de cláusulas tipo adotadas pela Comissão "incluem obrigações relativas, designadamente, às medidas de segurança, à informação do titular dos dados em caso de transferência de dados sensíveis, à notificação ao exportador de dados dos pedidos de acesso pelas autoridades competentes pela aplicação da lei dos países terceiros ou de qualquer acesso acidental ou não autorizado, bem como aos direitos dos titulares dos dados em matéria de acesso, retificação e supressão dos seus dados pessoais, e ainda regras sobre a reparação do titular dos dados em caso de danos decorrentes de uma violação por qualquer uma das partes das cláusulas contratuais-tipo. As cláusulas tipo exigem, igualmente, que o titular de dados da UE tenha a possibilidade de invocar, perante uma autoridade de proteção de dados e/ou um tribunal do Estado-Membro no qual o exportador dos dados está estabelecido, os direitos que decorrem das cláusulas-tipo na qualidade de terceiro beneficiário." Cf. COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre a transferência de dados pessoais da EU para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems), COM(2015) 566 final, Bruxelas, 6.11.2015

A importância das cláusulas em questão é notável, uma vez que são um dos instrumentos mais utilizados pelos responsáveis pelo tratamento e subcontratantes como garantia adequada para fundamentar as transferências para países terceiros. [87]

1.2.1.1 Cláusulas-tipo e a Diretiva 95/46/CE

As cláusulas-tipo já encontravam previsão na Diretiva 95/46/CE, sob o âmbito da qual eram consagradas como uma das derrogações ao disposto no artigo 25º daquele instrumento, artigo que estabelecia que as transferências de dados para um país terceiro só poderiam ser realizadas se este país assegurasse um nível de proteção adequado.

Não obstante a previsão do referido artigo, a diretiva reconhecia a possibilidade de realização das transferências em questão desde que o responsável pelo tratamento apresentasse garantias adequadas e suficientes de proteção da vida privada e dos direitos e liberdades fundamentais, bem como do exercício dos referidos direitos. O artigo 26º da Diretiva 95/46 previa que as garantias em questão poderiam resultar da adoção de cláusulas contratuais adequadas. [88]

À época, algumas das autoridades de proteção de dados dos EM [89] estabeleciam a necessidade da aprovação das transferências realizadas com base nas aludidas cláusulas. Este cenário tornava consideravelmente burocrática a adoção das referidas garantias, especialmente aos responsáveis pelo tratamento que exportassem dados pessoais de titulares que estivessem em diferentes EM da UE.

Ainda sob a vigência da Diretiva 95/46/CE, almejando a facilitação da utilização desta garantia, a Comissão Europeia emitiu quatro decisões referentes às cláusulas-tipo, duas das quais tratam sobre as transferência de dados realizada por responsáveis pelo tratamento estabelecidos na UE, tendo como destinatário os responsáveis pelo tratamento

[87] Aproximadamente 80% das organizações europeias que transferem dados pessoais aos EUA utilizam as cláusulas-tipo para fundamentar as aludidas transferências. Cf. EDWARDS, Elaine, *All You Need to Know in the Max Schrems-Facebook Case*, Irish Times, Fev. 6, 2017, Disponível em: <http://www.irishtimes.com/business/technology/all-you-need-to-know-in-the-max-schrems-facebook-case-1.2965482>, Acesso em: 06/05/2018.

[88] Diretiva 95/46/CE, artigo 26º, 2.

[89] Era o caso das autoridades de proteção de dados da Áustria, Bulgária, Dinamarca, Estónia, França, Luxemburgo, Malta, Espanha, Polónia, Eslovênia, por exemplo. Para maior desenvolvimento, ver GRUPO DE TRABALHO DO ARTIGO 29, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" considered as compliant with the EC Model Clauses*, WP 226, adotado em 26 de novembro de 2014, p. 2

sediados fora da UE e do Espaço Económico Europeu (EEE): a primeira delas adotada em 2001 e a segunda adotada em 2004,[90] a qual modificou a decisão adotada 3 anos antes; ao passo em que as outras duas referem-se às transferências de dados aos responsáveis pelo tratamento sediados na UE aos subcontratantes estabelecidos fora da UE e do Espaço Económico Europeu (EEE). A primeira delas, adotada em 2002 (Decisão 2002/16/CE)[91] foi revogada pela Decisão 2010/87/UE, atualmente em vigor. [92-93]

1.2.1.2 Cláusulas-tipo e o RGPD

Em seu artigo 46º, o RGPD formaliza a utilização das cláusulas-tipo como uma das garantias adequadas que poderão ser utilizadas como fundamento das transferências dos dados para um recetor que se encontre em um país terceiro para o qual não foi emitida uma decisão de adequação. O aludido regulamento ainda prevê a possibilidade da emissão destas cláusulas não só pela Comissão, como também pelas autoridades de controlo, as quais deverão obter a aprovação das suas cláusulas pela Comissão.

Uma vez que as cláusulas adotadas pelas autoridades de controlo tenham recebido a referida aprovação, o responsável pelo tratamento/subcontratante poderá utilizá-las sem que necessite de uma autorização adicional por parte da aludida autoridade, fator que facilita e desburocratiza a utilização das garantias em questão, em comparação ao sistema vigente à época da Diretiva 95/46/CE. [94]

---

[90] COMISSÃO EUROPEIA, Decisão da Comissão de 15 de Junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE [notificada com o número C(2001) 1539] (2001/497/CE); e COMISSÃO EUROPEIA, Decisão da Comissão de 27 de Dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros [notificada com o número C(2004) 5271] (2004/915/CE)

[91] COMISSÃO EUROPEIA, Decisão 2002/16/CE da Comissão, de 27 de dezembro de 2001, relativa a cláusulas contratuais tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, JO L 6, 10.1.2002

[92] COMISSÃO EUROPEIA, Decisão 2010/87/UE 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 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, JO L 39 de 12.2.2010

[93] Em 2016, as decisões 2001/497/CE e 2010/87/EU foram alteradas pela Decisão de Execução 2016/2297 da Comissão, como forma de adequá-las às modificações introduzidas através do acórdão proferido pelo TJUE no caso *Schrems*. Cf. VAN DEN BULCK, Paul, *Transfers of personal data to third countries*, Academia de Direito Europeu, Fórum 2017, ERA 2017, p.242.

[94] A utilização das referidas cláusulas como garantia adequada precisaria da aprovação da autoridade de controlo competente no caso das cláusulas em questão terem sido elaboradas entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados

Para que funcionem como garantias adequadas às transferências em análise, as cláusulas-tipo deverão ser adotadas em sua integralidade, em conformidade com as decisões da Comissão. No entanto, deve ser ressaltado que a adoção das referidas cláusulas não impede que os contratantes estabeleçam garantias adicionais que complementem e atribuam maior segurança à transferência dos dados pessoais, desde que estas previsões complementares não contrariem o disposto no RGPD, nem violem os direitos dos titulares dos dados. [95]

1.2.1.3 Vantagens e desvantagens

Por serem pré-aprovadas pela Comissão, o processo de adoção das referidas cláusulas é mais prático e menos burocrático do que a adoção das regras vinculativas aplicáveis às empresas. Além disso, as cláusulas-tipo não estão limitadas às transferências realizadas entre entidades de um mesmo grupo empresarial, ou entre grupos de empresas envolvidas numa atividade económica conjunta, como é o caso das regras vinculativas aplicáveis às empresas. Ademais, por terem que ser adotadas sem modificações, o padrão de proteção por estas cláusulas acolhido não pode ser prejudicado no curso das negociações entre as partes. [96]

Em todo caso, esta última vantagem pode implicar na desvantagem das partes não poderem usufruir da flexibilidade necessária para adequar com facilidade as cláusulas às especificidades de cada caso.

1.2.2 Regras vinculativas aplicáveis às empresas

As regras vinculativas aplicáveis às empresas são mecanismos legais que podem ser utilizados como garantias adequadas à proteção dos dados pessoais quando estes são transferidos entre entidades de um mesmo grupo empresarial, ou entre grupos de empresas envolvidas numa atividade económica conjunta.

---

pessoais no país terceiro ou organização internacional (Cláusulas *ad hoc*), previstas no artigo 46º, 3 do RGPD.

[95] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (109).

[96] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 122

As aludidas regras devem estabelecer uma política interna que consagre um adequado nível de proteção dos dados, o qual deve ser suficiente para garantir os direitos e liberdades dos titulares cujos dados são transferidos para entidades que, apesar de pertencerem ao mesmo grupo empresarial, não podem receber livremente o fluxo dos referidos dados uma vez que se encontram em um país terceiro para o qual não foi emitida uma decisão de adequação.

Neste sentido, as regras vinculativas devem incluir todos os *princípios essenciais* [97] *e direitos oponíveis que visem assegurar garantias adequadas às transferências ou categorias de transferências de dados pessoais*. [98] Por conseguinte, as empresas que utilizem as referidas regras como base para a transferência dos dados conseguem demonstrar com maior facilidade a conformidade de suas atividades com o RGPD.

O artigo 47º do RGPD especifica que as aludidas regras devem ser juridicamente vinculantes e aplicáveis a todas as empresas de um grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, de forma a garantir que todas as transferências realizadas entre as empresas daquele grupo estarão sujeitas a um adequado nível de proteção de dados. [99]

Dessa forma, as regras vinculativas criam um *standard* de proteção capaz de garantir, no âmbito dos grupos empresariais, um nível adequado de proteção dos dados pessoais, fator que autoriza a transferência destes dados mesmo para entidades daquele grupo que estão localizadas em países para os quais não foi emitida uma decisão de adequação. [100]

---

[97] De acordo com a alínea d, 2 do artigo 47º do RGPD, as regras vinculativas deverão especificar a aplicação dos princípios gerais de proteção de dados, "nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas." Cf. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 46º, 2,d.

[98] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (110).

[99] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 126: "*BCR create an intra-group data protection standard that guarantees an adequate level of data security corresponding to EU legal standards. This instrument should become especially relevant as the GDPR does not provide for an intra-group privilege*."

[100] VOIGT, Paul; VON DEM BUSSCHE, Axel, , *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 125

Desenvolvidas pelo Grupo de Trabalho do Artigo 29 (GTA29) como forma de facilitar a transferência de dados para outras entidades de um mesmo grupo localizadas em um país para o qual não havia sido emitida uma decisão de adequação, as regras vinculativas não eram expressamente reconhecidas como sendo uma das garantias adequadas às transferências dos dados pessoais a países terceiros no texto da Diretiva 95/46/CE. [101] Grande parte da regulamentação das aludidas regras era realizada no âmbito dos textos emitidos pelo GTA29. [102]

Àquela época, a utilização desta garantia não era muito prática, na medida em que os exportadores dos dados tinham que obter a aprovação de algumas das autoridades de proteção de dados dos Estados-Membros de onde desejassem transferir os dados pessoais.

Por conseguinte, antes do início da aplicação do RGPD, o processo de aprovação das regras vinculativas era complexo e burocrático, especialmente no que concerne ao envolvimento de mais de uma autoridade de controlo e à necessidade de posterior aprovação de algumas autoridades de controlo para que a transferência pudesse ser realizada.

Com vista a minimizar os referidos óbices e garantir uma proteção uniforme em todos os EM, o RGPD institui um processo de aprovação que tenciona ser mais simples e célere. [103] Neste sentido, o artigo 47º do RGPD estabelece que o exportador dos dados deverá submeter as regras vinculativas à autoridade de controlo competente para que esta

[101] VOIGT, Paul; VON DEM BUSSCHE, Axel, , *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 125

[102] Em especial, nas recomendações 74, 107, 108, 133, 153, 154, 155, 195, 195a, 204 e 212. Cf. GABEL, Detlev; HICKMAN, Tim; *Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation*, Disponível em: <https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection> Acesso em 27/05/2018.

[103] PATERAKI, Anna, «EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?», *World Data Protection Report*, Vol. 16, número 3, Março 2016, p. 3: "*The most significant procedural change under the GDPR is that the BCRs approval process will trigger the ''consistency mechanism'' (Article 43 (1) and Article 57). The consistency mechanism is a new concept introduced by the GDPR that enhances and formalizes the cooperation of DPAs through their participation in the EDPB. Today, the European DPAs have developed specific mechanisms to cooperate in the context of approving BCRs (i.e., mutual recognition procedure 14), cooperation procedure15). Under the consistency mechanism, DPA cooperation will include more detailed processes, including deadlines, that typically do not apply today*."

analise e decida se irá aprovar ou não as aludidas garantias, aplicando o procedimento de controlo de coerência previsto nos artigos 63º e seguintes. [104]

A aprovação das regras vinculativas sob a vigência do RGPD não seguirá um processo especializado e desenvolvido somente para as referidas regras, já que o aludido procedimento de coerência estabelece um mecanismo geral de cooperação entre as autoridades de controlo que também poderá ser aplicado a uma série de questões, a exemplo das avaliações de impacto e dos critérios de acreditação de um organismo de certificação. [105]

Após a realização do referido procedimento de controlo de coerência, restará à autoridade de controlo competente a aprovação das regras vinculativas, caso estas tenham sido elaboradas de acordo com o RGPD. Uma vez aprovadas, o exportador não precisará de autorizações adicionais para que possa utilizar as aludidas regras como garantias adequadas às transferências de dados.

1.2.2.1 Vantagens e desvantagens

A simplificação do processo de aprovação das regras vinculativas é de grande valia para as entidades que utilizam o referido instrumento, uma vez que estas passarão a economizar os custos que antes eram dispendidos com toda a burocracia que estava associada ao aludido processo.

Ainda como vantagem, pode ser ressaltada a flexibilidade e a capacidade de adaptação das regras vinculativas às necessidades do grupo empresarial, à diferença das cláusulas-tipo.

---

[104] A autoridade de controlo competente irá revisar as regras vinculativas apresentadas e emitir um projeto de decisão que deverá ser comunicado ao Comité Europeu para a Proteção de Dados (CEPD), o qual irá emitir uma opinião sobre a referida decisão. Apesar de não ser vinculante, a autoridade de controlo competente deverá ter em consideração a opinião do CEPD antes de emitir a sua decisão final. Caso a referida autoridade de controlo discorde da opinião do CEPD, será acionado o mecanismo de resolução de litígio previsto no artigo 65º do RGPD. O CEPD será então acionado a adotar uma decisão vinculante adotada por 2/3 dos seus membros. Cf. CONSELHO DA EUROPA, *Handbook on European data protection law*, Luxemburgo: Publications Office of the European Union, 2018, p. 263

[105] PATERAKI, Anna, «EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?», *World Data Protection Report*, Vol. 16, número 3, Março 2016, p. 4

Por outro lado, as entidades que utilizem as regras vinculativas como garantia adequada deverão ter o cuidado de mantê-las atualizadas e coerentes com o desenvolvimento do grupo empresarial. [106]

1.2.3 Códigos de Conduta e Procedimentos de Certificação

Entidades localizadas em países terceiros para os quais não foi emitida uma decisão de adequação podem aderir a um código de conduta que as auxiliem a observar e aplicar as normas e princípios dispostos no RGPD. Ainda que os referidos códigos não versem exclusivamente sobre as transferências dos dados, mas sim sobre a conformidade com o RGPD, no geral, o regulamento considerou-os garantias adequadas à realização das transferências ora em análise. [107]

Além da adesão a um código de conduta, as referidas entidades podem utilizar-se de uma certificação emitida de acordo com as regras estabelecidas no artigo 42º do RGPD como garantia adequada para as transferências em questão. Assim como os códigos de conduta, as certificações indicam a conformidade das operações de tratamento do responsável pelo tratamento/subcontratante com o RGPD. As certificações são emitidas por um período máximo de 3 anos, podendo ser renovadas caso os requerimentos para emissão ainda estejam presentes, além de poderem ser revogadas a qualquer momento, no caso de sua violação. [108]

Por mais que os códigos de conduta e as certificações tenham que seguir um procedimento de aprovação, a transferência com base nestas garantias prescinde da autorização das autoridades nacionais de proteção dos dados. [109]

Insta ressaltar que os códigos de conduta e as certificações apenas servirão como base para as supracitadas transferências internacionais se os responsáveis pelo tratamento

---

[106] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 242

[107] VAN DEN BULCK, Paul, *Transfers of personal data to third countries*, Academia de Direito Europeu, Fórum 2017, ERA 2017, p. 245

[108] *Ibid*., p. 246

[109] GABEL, Detlev; HICKMAN, Tim; *Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation*, Disponível em: < https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection> Acesso em 27/05/2018.

ou subcontratantes no país terceiro assegurarem a aplicação das referidas garantias por meio de um compromisso vinculativo e com força executiva. [110]

1.3 Artigo 49º – Derrogações para situações específicas

O RGPD estabelece uma hierarquia entre os mecanismos de transferência, sendo o mais recomendando a decisão de adequação da Comissão. [111] Em segundo lugar, estão as garantias adequadas previstas no artigo 46º, a exemplo de cláusulas contratuais e das regras vinculativas aplicáveis às empresas.

Em último caso, podem ser aplicadas as derrogações previstas no artigo 49º, [112] a saber: (1) o consentimento informado do titular dos dados; (2) a necessidade da transferência para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados; (3) a necessidade da transferência para celebração ou execução de contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa; (4) importantes razões de interesse público; (5) transferência necessária à declaração, ao exercício ou à defesa de um direito num processo judicial; (6) transferência necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se o titular estiver física ou legalmente incapaz de dar o seu consentimento; (7) e, por fim, a transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto. [113]

Para realizar a aludida transferência, o responsável pelo tratamento dos dados deverá cumprir não só os requisitos do artigo 49º, como também deverá observar os

---

[110] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 130

[111] A referida hierarquia, não obstante não estar expressamente prevista na Diretiva 95/46/CE, já era aplicada sob a sua vigência. VAN DEN BULCK, Paul, *Transfers of personal data to third countries*, Academia de Direito Europeu, Fórum 2017, ERA 2017, p. 232

[112] ALSTON & BIRD, *Transferring Data from the EU: Privacy Shield and Data transfers under the GDPR*, Disponível em: <https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf > Acesso em: 10/05/2018

[113] Cf. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 49º.

princípios da proteção dos dados consagrados no artigo 5º do RGPD, e os requisitos da licitude do tratamento previstos no artigo 6º do aludido regulamento. [114] Como exceção que são, as derrogações apenas poderão ser utilizadas nos casos acima descritos se todas as condições necessárias estiverem presentes, e se da sua aplicação não resultar uma violação aos direitos fundamentais do titular dos dados. [115]

Por fim, deve ser observado que, na falta de uma decisão de adequação, o RGPD prevê a possibilidade do direito da União ou de um Estado-Membro estabelecer limites às transferências de certas categorias de dados, tendo como base razões importantes de interesse público, fator que pode restringir ainda mais a aplicação das derrogações em questão. [116]

1.3.1 Artigo 49º, 1, a - Consentimento

Para que o consentimento seja válido, é preciso que os requisitos previstos no artigo 7º e no número 11 do artigo 4º do RGPD estejam presentes, ou seja, *o consentimento deverá ser uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*. [117]

No entanto, a alínea "a", 1, do artigo 49º impõe requisitos adicionais para que o consentimento possa ser utilizado como base para a transferência de dados para um país terceiro ou organização internacional. Neste sentido, além das condições gerais de emissão de um consentimento válido, o artigo 49º indica que o consentimento deverá ser emitido estando o titular bem informado e consciente dos riscos daquela transferência, considerando que os dados serão enviados a um país terceiro para o qual não foi emitida uma decisão de adequação, e que não foram adotadas as garantias adequadas previstas no artigo 46º do RGPD.

Para que titular esteja, de facto, bem informado, deverá ser comunicado com exatidão os dados que serão transferidos, bem como quem será o recipiente e onde este está

[114] GRUPO DE TRABALHO DO ARTIGO 29, *Diretrizes sobre o artigo 49 do Regulamento 2016/679*, WP 262, adotado em 6 de fevereiro de 2018, p.3
[115] *Ibid*., p.4
[116] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 49º, 5.
[117] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 4º, 11.

localizado, além da indicação dos riscos associados ao tratamento e demais informações relevantes sobre o referido processo. [118]

De igual forma, o titular deverá estar ciente da possibilidade de revogar o seu consentimento a qualquer momento, faculdade que dificulta a utilização prática desta derrogação como base para a transferência dos dados pessoais.

Uma vez que o titular dos dados esteja bem informado sobre as condições do tratamento, estará em condições de emitir o seu consentimento, o qual deverá ser explícito e específico para aquela transferência, tendo em consideração os riscos envolvidos na realização desta. [119]

Por fim, insta salientar que, segundo o número 3 do artigo 49º, a derrogação em questão não pode ser aplicável a atividades realizadas por autoridades públicas no exercício dos seus poderes.

1.3.2 Artigo 49º, 1, b - Transferência for necessária a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou diligências prévias à formação do contrato

Caso a execução de um contrato dependa da transferência dos dados pessoais, o RGPD permite a realização da aludida transferência mesmo diante da ausência de uma decisão de adequação ou da previsão das garantias adequadas dispostas no artigo 46º do referido regulamento.

Neste sentido, deverá ser analisada a necessidade da transferência dos dados para a realização do contrato caso a caso. Se o propósito do contrato for alcançado sem que seja necessária a transferência ao país terceiro ou organização internacional, não poderá ser aplicada a exceção.

Por exemplo, no caso de um contrato com uma companhia de viagens, a transferência dos dados do titular por parte da referida companhia ao hotel no qual o titular

[118] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 118

[119] O RGPD requer o consentimento explícito dos titulares dos dados em situações nas quais há um sensível risco envolvido nas atividades de tratamento. Para maior desenvolvimento, ver GRUPO DE TRABALHO DO ARTIGO 29, *Diretrizes sobre o artigo 49 do Regulamento 2016/679*, WP 262, adotado em 6 de fevereiro de 2018, p. 6.

ficará hospedado é essencial para a execução do contrato, e seu propósito (organização da viagem) não pode ser alcançado sem que a transferência seja realizada. [120] Neste caso, aplica-se a derrogação prevista no artigo 49º, 1, b. Por fim, insta ressaltar que, de acordo com o considerando 111 do RGPD, a transferência deverá ser ocasional.

1.3.3 Artigo 49º, 1, e - Transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial.

O considerando 111 esclarece que deve ser possível realizar a transferência de dados quando esta seja ocasional e necessária em relação a um contrato ou a um contencioso judicial, independentemente da natureza do procedimento, seja judicial, administrativa ou mesmo não judicial. [121]

Em todo caso, essa derrogação não poderá ser utilizada para justificar a transferência de dados com base apenas na possibilidade da instauração de um processo, como dispõe as orientações do Grupo de Artigo 29, devendo ser analisada a real necessidade de cada transferência casuisticamente. [122]

> *As a transfer needs to be made in a procedure, a close link is necessary between a data transfer and a specific procedure regarding the situation in question. The abstract applicability of a certain type of procedure would not be sufficient*.

1.3.4 Artigo 49º, 1, f - Transferências necessárias para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento.

A derrogação prevista no artigo 49º, 1, f tem sua aplicação prevista, em grande parte, aos casos de emergência médica nos quais o paciente não está em condições de emitir o seu consentimento, e a transferência dos dados é necessária para que seja oferecido o tratamento médico adequado. [123]

---

[120] VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017, p. 131
[121] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (111).
[122] GRUPO DE TRABALHO DO ARTIGO 29, *Diretrizes sobre o artigo 49 do Regulamento 2016/679*, WP 262, adotado em 6 de fevereiro de 2018, p. 12
[123] *Ibid.*, p. 13

A derrogação em questão busca proteger não só a integridade física como também a integridade mental do titular dos dados, o qual pode não estar apto a emitir o seu consentimento por razões físicas ou legais. [124] No conflito entre os direitos fundamentais à proteção dos dados e o direito à vida e à integridade física, o RGPD privilegia, com razão, este último.

1.3.5 Transferência necessária para efeitos dos interesses legítimos visados pelo responsável pelo tratamento

Caso nenhuma dos supracitados instrumentos possa ser aplicado, ainda resta a possibilidade, em casos limitados, da transferência dos dados quando esta for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, sob a condição de que estes interesses não se sobreponham aos interesses ou direitos e liberdades do titular dos dados. [125] Em todo caso, o RGPD não estabelece um conceito fechado para os aludidos "interesses legítimos", limitando-se a exemplificar situações nas quais este interesse estaria presente. [126]

O exportador dos dados deverá estar em condições de demonstrar que não havia possibilidade de realizar a aludida transferência com base no artigo 46º ou nas derrogações previstas no número 1 do artigo 49º, restando-lhe como única opção a transferência com base na exceção ora em análise.

Como forma de garantir a excecionalidade desta derrogação, o RGPD impõe uma série de condições que devem ser observadas quando da transferência realizada com base neste fundamento.

---

[124] GRUPO DE TRABALHO DO ARTIGO 29, *Diretrizes sobre o artigo 49 do Regulamento 2016/679*, WP 262, adotado em 6 de fevereiro de 2018, p. 13*:* "*This ability to make a valid decision can depend on physical, mental but also legal incapability. A legal incapability can encompass, without prejudice to national representation mechanisms, for example, the case of a minor. This legal incapability has to be proved, depending on the case, through either a medical certificate showing the mental incapability of the person concerned or through a governmental document confirming the legal situation of the person concerned*."

[125] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 49º, 1, § 2

[126] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (47): "Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade."

Neste sentido, o exportador dos dados apenas poderá valer-se desta exceção quando a transferência afetar um número limitado de titulares de dados, requerimento que deve ser avaliado caso a caso à luz dos critérios da proporcionalidade e necessidade.

Ainda neste âmbito, o exportador deverá balancear os seus interesses legítimos e os direitos e liberdades dos titulares dos dados, devendo prever os riscos associados ao tratamento e as medidas adequadas para minimizar os referidos riscos, de forma a salvaguardar os aludidos direitos e liberdades dos titulares dos dados.

Por conta dos riscos envolvidos, esta derrogação deve ser utilizada apenas como último recurso às transferências em apreço, não sendo adequadas à fundamentação das transferências sistemática e volumosa de dados pessoais. [127]

Por fim, o responsável pelo tratamento ainda deverá informar que está a realizar a transferência dos dados com base nesta exceção tanto à autoridade de controlo relevante, como a todos os titulares cujos dados foram transferidos.

[127] ALSTON & BIRD, *Transferring Data from the EU: Privacy Shield and Data transfers under the GDPR*, Disponível em: <https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf > Acesso em: 10/05/2018, p. 17

PARTE II - TRANSFERÊNCIAS TRANSATLÂNTICAS DE DADOS PESSOAIS

CAPÍTULO III - TRANSFERÊNCIAS DE DADOS ENTRE A UNIÃO EUROPEIA E OS ESTADOS UNIDOS

Os Estados Unidos são o maior parceiro comercial da União Europeia. No cenário atual, as relações económicas entre a UE e os Estados Unidos são as de maior expressão em todo o mundo, com um comércio total no valor de 1,09 biliões de dólares em 2014. [128]

No contexto da atual sociedade da informação, as trocas comerciais envolvem cada vez mais a transferência de dados entre os países que estão a negociar, sendo o fluxo de dados entre os Estados Unidos e a Europa o maior do mundo, representando quase o dobro do fluxo entre aquele país e a América Latina.[129]

O fluxo dos dados pessoais, todavia, não se restringe à área comercial. Em muitos casos, os próprios titulares dos dados os disponibilizam em troca da prestação de serviços gratuitos, a exemplo da utilização de redes sociais como o *Facebook* e o *Twitter*; ou de mecanismos de pesquisa como o *Google*, "gigantes da internet" que estão sediados, em sua maioria, nos Estados Unidos. Destarte, é natural que haja um grande fluxo de dados pessoais proveniente dos países dos utentes dos referidos serviços com destino à sede das aludidas organizações.

No entanto, para que haja a transferência de dados pessoais entre a União Europeia e um país terceiro, é imprescindível que seja garantido neste último um adequado nível de

[128] PARLAMENTO EUROPEU, Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)), Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016 0233+0+DOC+PDF+V0//PT> Acesso em: 16/05/2018

[129] WEISS, Martin A; ARCHIK, Kristin, *The EU-U.S Safe Harbor Agreement on Personal Data Privacy: In Brief*, Congressional Research Service, Relatório do serviço de pesquisa do Congresso, Outubro de 2015, p. 6: "*According to a 2014 study, cross-border data flows between the United States and Europe are the highest in the world—almost double the data flows between the United States and Latin America and 50% higher than data flows between the United States and Asia*.", No mesmo sentido, LINN, Emily, «A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement», *Vanderbilt Journal of Transnational Law*, Vol 50, 2017, p. 1314: "*The European Parliament recognized the importance of the EU-U.S. trade relationship; noting that cross-border data flows between the European Union and the United States are the highest in the world-50 percent higher than any other transfer-and acknowledging personal data as an essential component*"

proteção aos dados pessoais. Caso contrário, os titulares ficariam desprotegidos assim que seus dados fossem transferidos para além das fronteiras da UE, o que tornaria ineficaz o alto nível de proteção dos dados consagrado no direito europeu.

Após análise do quadro jurídico e das práticas adotadas no país terceiro, a Comissão poderá indicar a adequação do nível de proteção dos dados consagrado no referido país por meio da emissão de uma decisão de adequação, a qual equipara o país terceiro a um EM da UE no que concerne às transferências de dados pessoais. Destarte, a decisão de adequação do país terceiro garante o livre fluxo dos dados pessoais entre a UE e o referido país. [130]

Conforme analisado em tópico precedente, para que esta decisão possa ser emitida, o nível de proteção de dados do país terceiro deverá ser substancialmente equivalente àquele consagrado na UE.

As consideráveis diferenças entre o sistema jurídico americano e europeu impossibilitariam a emissão da referida decisão, motivo pelo qual o Departamento de Comércio dos Estados Unidos negociou com a Comissão Europeia a criação de um sistema que permitisse a livre transferência dos dados entre a UE e as entidades americanas que aderissem ao aludido sistema.

Como resultado das referidas negociações, surgiram os Princípios de "Porto Seguro" ("*Safe Harbour Principles of Privacy*"), [131] ao qual foi reconhecido o nível adequado de proteção dos dados pessoais em julho de 2000 pela Comissão Europeia, de acordo com os requisitos dispostos no artigo 25º da Diretiva 95/46/CE, quando este instrumento ainda estava em vigor.

No entanto, após as revelações de Edward Snowden sobre os programas de vigilância em massa das agências de inteligência americanas, a validade do sistema Porto Seguro (PS) foi posta em prova.

[130] É livre a circulação dos dados pessoais entre os EM da União Europeia. Cf. DIAS PEREIRA, Alexandre Libório, «Big Data, E-Health e «Autodeterminação Informativa»: a Lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR) », in *Lex Medicinae – Revista Portuguesa de Direito da Saúde*, n.o 29 2018, p. 10

[131] BENDER, David, «Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International», *Data Privacy Law*, Vol. 6, No. 2, 2016, p. 117

Neste capítulo, será abordado, em um primeiro momento, o sistema Porto Seguro - *Safe Harbour*, suas características principais, bem como o contexto de sua aplicação e posterior invalidação. Neste sentido, abordar-se-á o caso *Schrems* e as consequências que decorreram do acórdão do Tribunal de Justiça da União Europeia (TJUE). Por fim, analisar-se-á o Escudo de Proteção da Privacidade - *Privacy Shield*, suas implicações para as transferências de dados transatlânticas, bem como o cenário futuro das transferências de dados pessoais entre a UE e os EUA, à luz do RGPD.

1. Princípios de "Porto Seguro" - *Safe Harbour Principles of Privacy*

O modelo europeu de proteção dos dados distingue-se de forma significativa do modelo americano. Enquanto o direito europeu preza por uma proteção dos dados realizada em um instrumento jurídico uniforme e harmônico,[132] nos Estados Unidos a proteção destes dados é realizada por meio da regulamentação, autorregulamentação, bem como através de leis esparsas e setoriais, sem que haja uma autoridade de controlo uniforme que garanta a aplicação dos instrumentos legais relativos à proteção dos dados.

As divergências entre os sistemas jurídicos dos EUA e da UE impediriam que a Comissão emitisse uma decisão de adequação àquele país, o que dificultaria, mas não impossibilitaria as transferências de dados para os EUA, uma vez que os exportadores dos dados ainda poderiam utilizar garantias adicionais que assegurassem um nível de proteção adequado para realizar as aludidas transferências, ou, em último caso, as derrogações previstas à época no artigo 26º da Diretiva, e, no contexto atual, no artigo 49º do RGPD.

---

[132] 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> Acesso em: 16/05/2018, p. 5: "*In Europe, the tendency historically has been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress*." Neste sentido, insta destacar a seguinte passagem do Departamento de Comércio dos EUA "*the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these differences, the [1995 Directive] could have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions*." DEPARTAMENTO DE COMÉRCIO DOS ESTADOS UNIDOS, *U.S.-EU Safe Harbor Overview*, Disponível em: <http://build.export.gov/main/ safeharbor/eu/eg_main_018476> Acesso em 17/05/2018.

Certo era que os Estados Unidos não iriam alterar o seu sistema legal, nem mesmo introduzir uma nova lei, apenas para adequar-se aos requerimentos da diretiva europeia. No entanto, as empresas americanas também não desejavam ter suas atividades de transferências de dados com um dos seus maiores parceiros comerciais prejudicadas por conta da não adequação do quadro jurídico do seu país.

Para ultrapassar este impasse, o Departamento de Comércio dos Estados Unidos (DC) negociou juntamente à Comissão Europeia a elaboração dos princípios de "Porto Seguro" (*Safe Harbour Principles of Privacy)*, sistema cujo objetivo era estabelecer o nível adequado de proteção dos dados exigido pela Diretiva 95/46/CE como requisito para realização das transferências de dados para um país terceiro. Os referidos princípios e as questões mais frequentes sobre a sua aplicação (FAQ) foram publicados pelo DC em 21 de julho de 2000.

O "Porto Seguro" (PS) prevê sete princípios principais, [133] os quais transpõem direitos e obrigações consagradas no direito da UE, como forma de garantir um adequado nível de proteção aos titulares cujos dados são transferidos aos EUA por meio do sistema em análise.

Neste sentido, os princípios preveem a obrigação do responsável pelo tratamento informar o titular dos dados sobre a finalidade da coleta e sobre a forma como as suas informações serão utilizadas. O titular ainda tem o direito de escolher se suas informações serão ou não partilhadas com um terceiro e se os seus dados poderão ser tratados para finalidades diferentes daquelas para as quais foram coletados.

As entidades que realizam o tratamento deverão, ainda, adotar medidas de segurança adequadas para proteger os dados contra a perda, o uso indevido, o acesso não autorizado, a alteração ou a destruição destes, além do dever de manter a exatidão dos dados, e, quando necessário, atualizá-los. Caso falhem nesta tarefa, o titular dos dados terá o direito de corrigir ou requerer o apagamento dos dados incorretos.

[133] Nomeadamente, princípio do aviso, escolha, retransferência, segurança, integridade dos dados, acesso e aplicação.

Em julho do ano 2000 - após emissão de um parecer do Grupo de Trabalho do Artigo 29 e de um parecer do Comité do Artigo 31 [134] - a Comissão Europeia adotou a Decisão 2000/520/EC, [135] a qual reconheceu que, quando aplicados em conformidade com as orientações dispostas nas diretrizes das questões mais frequentes (FAQs -*Frequently asked questions*), os princípios do PS garantem um adequado nível de proteção dos dados, o que permite a transferência dos aludidos dados às empresas americanas participantes do sistema em análise.

A partir de então, os exportadores de dados pessoais provenientes da UE que desejassem transferir os referidos dados a uma empresa americana que houvesse autocertificado a aderência aos princípios do PS não mais precisariam apresentar garantias adicionais para a realização das transferências em questão.

1.1 Funcionamento do sistema

A adesão aos princípios era voluntária, mas algumas medidas tinham que ser adotadas pelas entidades americanas para que pudessem usufruir a referida decisão de adequação.

Apenas as organizações que estivessem sujeitas à jurisdição da Comissão Federal de Comércio dos EUA poderiam aderir ao sistema,[136] fator que excluía do âmbito de abrangência do PS as entidade do setor financeiro e das telecomunicações. Nos tópicos seguintes serão analisadas as competências das autoridades americanas responsáveis pela administração e garantia do cumprimento dos princípios do sistema PS, quais sejam o Departamento de Comércio dos EUA (DC) e a referida Comissão Federal de Comércio (*Federal Trade Comission* – FTC).

---

[134] COMISSÃO EUROPEIA, 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, Bruxelas, 27 de Novembro de 2013, p. 2

[135] COMISSÃO EUROPEIA, Decisão 2000/520/EC 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 [notificada com o número C(2000) 2441]

[136] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, Janeiro de 2017, p. 7

1.2 Departamento de Comércio dos EUA

A entidade americana que desejasse aderir ao sistema deveria incluir os princípios de proteção de dados previstos no PS, e o compromisso de que iria atuar em conformidade com os referidos princípios, em sua política de proteção da vida privada, a qual deveria ser pública com vista a garantir a transparência de suas atividades.

Em seguida, as empresas americanas deveriam autocertificar a adesão aos referidos princípios ao Departamento de Comércio dos EUA, estando obrigada a realizar a renovação desta autocertificação anualmente.

Neste âmbito, o Departamento de Comércio dos EUA era a autoridade competente não só para analisar as aludidas certificações, como também era responsável pela avaliação das aludidas renovações.

Para garantir a transparência do sistema, o Departamento de Comércio era igualmente responsável pela publicação em seu sítio *web* de uma lista das empresas que declararam observar os aludidos princípios.

1.3 Comissão Federal de Comércio

A partir do momento em que as entidades indicavam que haviam aderido aos princípios do PS, surgia aos consumidores a expectativa legítima de que os seus dados seriam protegidos quando tratados pela entidade autocertificada.

Destarte, as empresas que não cumprissem com os princípios que indicaram ter subscrito estariam a violar as referidas expetativas, praticando, portanto, atos desleais e enganosos aos olhos dos consumidores.

Enquanto entidade competente a proteger o consumidor americano, a Comissão Federal de Comércio dos Estados Unidos (FTC – *Federal Trade Comission*) poderia impor medidas coercivas contra as empresas que praticassem os aludidos atos desleais e enganosos, em conformidade com a secção 5 do *Free Trade Comission Act*. [137] Em todo

[137] Caso a empresa a aplicar os princípios seja do ramo dos transportes aéreos, a entidade competente será o *Departament of Transporations* dos EUA.

caso, raras foram as sanções aplicadas às entidades que apresentaram o aludido comportamento, ao menos nos primeiros anos de execução do acordo. [138]

2. Programas de vigilância das agências americanas e as revelações de Edward Snowden

Em junho de 2013, as revelações de Edward Snowden sobre a existência e o funcionamento de programas de vigilância das agências de inteligência americanas incitaram as autoridades europeias a repensar a segurança da transferência dos dados entre a UE e as empresas americanas que haviam aderido aos princípios do "Porto Seguro".

Isto porque as revelações do antigo analista da agência de segurança nacional americana (NSA) detalharam a existência de programas de vigilância que acessavam os servidores dos "gigantes da internet" para realizar uma coleta indiscriminada e em larga escala dos dados de seus utentes.

Neste sentido, segundo as revelações de Snowden, por meio de programas de vigilância como o "PRISM", a NSA acessava os servidores de grandes empresas americanas como a *Google*, *Facebook*, *Microsoft* e a *Apple* (todas autocertificaram a aderência aos princípios do PS) para coletar informações dos seus utentes, a exemplo do histórico de pesquisa, do conteúdo de e-mails, e da transferência de arquivos – fotos, vídeos, mensagens de voz.

Ora, é inevitável que parte destas informações dissesse respeito aos dados pessoais dos seus utentes, o que tornava a existência e o funcionamento dos referidos programas uma afronta ao direito à proteção destes dados.

No mês seguinte às revelações, a autoridade alemã responsável pela proteção de dados demonstrou a sua preocupação quanto ao nível de segurança da transferência dos dados que estavam a ser realizadas sob o abrigo do acordo PS, ao indicar que era altamente

[138] JONES, Emily, «The Safety of Safe Harbor», *Journal of Direct, Data and Digital Marketing Practice*, 15, 2013, p. 152

provável que os princípios consubstanciados nas decisões da Comissão não estavam a ser respeitados. [139-140]

2.1 Posição da Comissão Europeia

A Comissão Europeia não se quedou inerte face ao cenário pós-Snowden, emitindo, em novembro de 2013, duas comunicações que analisaram as consequências da divulgação dos programas de vigilância da NSA, bem como as medidas que deveriam ser adotadas, a partir de então, como forma de restabelecer a confiança nos fluxos de dados entre a UE e os EUA.

Neste sentido, em 27 de novembro de 2013, a Comissão emitiu a Comunicação "Restabelecer a confiança nos fluxos de dados entre a UE e os EUA" [COM(2013) 846 final], e a Comunicação "sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na EU" [COM(2013) 847 final].

Na Comunicação 846, a Comissão reconheceu a inadmissibilidade dos programas de vigilância generalizada das comunicações privadas dos cidadãos, das empresas ou dos dirigentes políticos, ao mesmo tempo em que destacou a importância da parceria EUA-UE e o relevante papel das transferências de dados neste contexto. [141]

Ainda na referida comunicação, a Comissão reconheceu um conjunto de falhas que dificultavam o bom funcionamento do sistema PS, em especial a falta de transparência das

[139] COMISSÃO EUROPEIA, 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, Bruxelas, 27 de Novembro de 2013, p. 6

[140] PUPALOVA, Nina, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de Oslo, dezembro de 2017, p. 22: "*After the turmoil following the Snowden revelations, the German DPAs voiced their concerns for the significant likelihood that infringements of the SH-Principles and violations of data subjects' rights were happening again. For example, the DPA in Bremen requested that companies transferring data to the US inform them whether and how the receiving companies in the US prevented access to personal data by the NSA*."

[141] COMISSÃO EUROPEIA, 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, Bruxelas, 27 de Novembro de 2013, p. 2

empresas americanas sobre sua adesão ao sistema, e a falta da supervisão eficaz por parte das autoridades americanas competentes. [142]

Não obstante o reconhecimento das deficiências do PS, a Comissão decidiu por reforçar, e não revogar o referido sistema, sob a justificativa de que a revogação afetaria negativamente os interesses das empresas tanto da UE como dos EUA. [143]

Já na comunicação 847, a Comissão realizou uma extensiva análise sobre o sistema PS desde a sua conceção até as reações esboçadas pelas autoridades europeias de proteção dos dados diante das revelações de Snowden.

Para tanto, baseou-se nas informações coletadas pelo grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados, [144] e nas análises contidas em dois relatórios sobre o funcionamento do sistema PS, os quais foram emitidos pela Comissão em 2002 e em 2004. [145]

Por meio da aludida análise, é possível perceber que, desde os primeiros anos da sua aplicação, a Comissão já havia verificado falhas no sistema PS, a maioria das quais havia surgido em consequência da forma pela qual as entidades aderiam ao sistema, qual seja por meio das autocertificações ao DC.

Especificamente no relatório de 2004, a Comissão identificou que um grande número de empresas americanas que utilizavam o sistema PS para a transferência de dados

---

[142] COMISSÃO EUROPEIA, Comunicação da Comissão ao Parlamento Europeu e ao Conselho - *Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas*, COM(2016) 117 final, Bruxelas, 29.2.2016, p. 8

[143] COMISSÃO EUROPEIA, 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, Bruxelas, 27 de Novembro de 2013, p. 8

[144] O grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados foi "criado no seguimento da reunião do Coreper de 18 de julho de 2013 com vista a apurar os factos sobre programas norte-americanos de recolha de informações em grande escala e o seu impacto nos direitos fundamentais da UE e nos dados pessoais dos cidadãos da UE. Analisa o quadro jurídico norte-americano, o modo de recolha e tratamento posterior dos dados e os atuais mecanismos de fiscalização e reparação". AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS, Síntese do parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA» e sobre a 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, (2014/C 116/04), p.2

[145] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (17)

não respeitavam, ou não respeitavam em sua totalidade, os princípios e as regras do acordo. [146]

Neste sentido, a Comissão ressaltou a necessidade da atuação mais transparente das empresas americanas, em especial aquelas que, não obstante houvessem autocertificado a adesão aos princípios, comprometendo-se a observá-los e comunicando ao Departamento de Comércio a sua política de privacidade, não tornaram públicas as referidas políticas de privacidade.

As falhas do PS, todavia, não se limitavam à falta de publicação das políticas de privacidade. As declarações falsas de empresas que diziam ter subscrito aos princípios, sem nunca tê-lo feito, ou sem ter realizado a sua renovação, também eram um inconveniente considerável. [147]

Não obstante os aludidos óbices, a Comissão decidiu manter o sistema PS, mas ressaltou a importância do Departamento de Comércio exercer com maior empenho as suas competências referentes ao controlo das autocertificações das empresas americanas, bem como a verificação da sua renovação anual.

No que concerne aos dados transferidos no âmbito do sistema PS, e acessados por autoridades americanas por meio de programas de vigilância como o PRISM, a Comissão ressaltou que a exceção prevista no anexo I do acordo PS - a qual autoriza a limitação da adesão aos princípios do referido acordo na extensão necessária à garantia da segurança pública, interesse público e execução da lei - deve ser aplicada apenas se for necessária, e de maneira proporcional aos fins que a fundamentaram. Ademais, só deverá ser utilizada se não implicar um comprometimento do nível de proteção dos princípios do acordo PS.

Ora, não parece que a coleta indiscriminada em larga escala dos dados pessoais realizada no âmbito dos programas de vigilância da NSA fosse proporcional e necessária

[146] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (21)
[147] COMISSÃO EUROPEIA, 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]. Bruxelas, 27 de Novembro de 2013, p.6

aos fins de segurança nacional, como reconhece a Comissão no ponto 7 da Comunicação em estudo [148]

> *Todas as empresas que participam no Programa PRISM [programa de recolha de informações em grande escala], que permite às autoridades americanas ter acesso a dados armazenados e tratados nos EUA, parecem estar certificadas no âmbito do sistema de 'porto seguro'»* e que este sistema *«passou, pois, a ser uma das vias através da qual os serviços de informações americanos têm acesso à recolha de dados pessoais inicialmente tratados na UE. [...] uma série de bases jurídicas previstas pela legislação americana permitem recolher e tratar em grande escala dados pessoais, que são armazenados ou tratados por empresas estabelecidas nos EUA.[...]* e que *[c]omo se trata de programas de grande envergadura, é possível que os dados transferidos no âmbito do sistema de 'porto seguro' sejam acessíveis às autoridades americanas e sejam por estas tratados para além do estritamente necessário e proporcional em relação à proteção da segurança nacional, como previsto na derrogação enunciada na Decisão [2000/520]*

Para tornar o cenário ainda mais caótico, a legislação americana não reconhecia aos titulares cujos dados fossem acessados pelas autoridades americanas, no contexto dos seus programas de vigilância, os direito de acesso, retificação, e supressão, nem mesmo havia uma indicação das empresas, nas suas políticas de privacidade, dos casos em que as exceções aos princípios de proteção dos dados poderiam ser aplicadas. [149]

Por conseguinte, os titulares cujos dados haviam sido transferidos desde a UE para uma empresa americana por meio do sistema PS poderiam nem mesmo ter ciência de que os seus dados estavam a ser acessados pelo governo americano.

Ao concluir a análise sobre as transferências transatlânticas de dados ao abrigo do PS, e a despeito do reconhecimento das falhas na aplicação do aludido acordo, a Comissão decidiu por manter o sistema ora em estudo. Para tanto, a autoridade europeia emitiu recomendações para que este sistema fosse melhor aplicado na conjuntura gerada após as revelações dos programas de vigilância das autoridades públicas americanas, especialmente no que concerne à transparência, aos recursos, à aplicação dos princípios e ao acesso aos dados pelas referidas autoridades dos EUA.

Neste sentido, a Comissão ressaltou a necessidade das empresas autocertificadas divulgarem publicamente as suas políticas de proteção da vida privada, as quais devem ser

[148] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (22).
[149] COMISSÃO EUROPEIA, 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]. Bruxelas, 27 de Novembro de 2013, p. 19

formuladas de forma clara e compreensível ao grande público. Como forma de facilitar a verificação da autenticidade da declaração de adesão aos princípios, as referidas políticas deverão conter uma ligação ao sítio *web* do Departamento de Comércio, onde deverão estar incluídas na lista das entidades participantes do sistema PS.

Por fim, a Comissão recomendou que as políticas de privacidade das empresas autocertificadas indiquem se e quando a legislação dos EUA permite a recolha de dados coletados sob o sistema PS por meio das autoridades públicas americanas, ressaltando que a aplicação das exceções fundamentadas em motivos de segurança nacional apenas devem ser aplicadas de *forma proporcional e na medida em que for estritamente necessária.* [150]

2.2. Posição do Parlamento Europeu

O Parlamento Europeu, todavia, não compartilhava a posição adotada pela Comissão Europeia. Em resposta às revelações de Snowden, o Parlamento emitiu em março de 2014 uma resolução na qual defendia a suspensão do sistema PS e solicitava à Comissão que adotasse medidas imediatas para garantir a proteção dos dados transferidos aos EUA. [151]

3. Caso Maximiliam Schrems v. *Facebook Ireland* (Processo C-362/14)

Enquanto a Comissão Europeia estava a revisar o acordo PS, o ativista austríaco Maximiliam Schrems ingressava junto ao Comissário irlandês para a proteção de dados (*Irish Data Protection Comissioner* - DPC) com uma reclamação na qual arguia que os seus dados pessoais não estavam a receber a proteção adequada nos EUA, após terem sido transferidos a este país por meio do acordo PS.

---

[150] COMISSÃO EUROPEIA, 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, Bruxelas, 27 de Novembro de 2013, p. 22

[151] PARLAMENTO EUROPEU, 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)): "Ação 3: suspender o dispositivo «porto seguro» até que tenha sido realizada uma revisão aprofundada e colmatadas as lacunas, garantindo que as transferências de dados para fins comerciais da União para os EUA apenas possam ser realizadas em conformidade com as mais elevadas normas da UE".

Segundo Schrems, os seus dados coletados pela *Facebook Ireland* [152] poderiam ser acessados através dos programas de vigilância de autoridades públicas americanas, quando transferidos à *Facebook Inc*, sede da empresa nos EUA, por meio do sistema PS.

Por conta desta conjuntura, o austríaco requereu ao DPC que a *Facebook Ireland* fosse proibida de transferir os seus dados à sede da referida empresa nos EUA, sob o argumento de que aquele país não oferecia um adequado nível de proteção aos seus dados.

No entanto, a autoridade de controlo irlandesa arquivou o pedido de Schrems sob o argumento de que não havia provas de que a NSA estava, de facto, a acessar os seus dados; bem como foi afirmado pela DPC que qualquer questão referente à adequação do nível de proteção dos dados oferecido pelos EUA deveria ser resolvida à luz da Decisão 2000/520/CE, e que, nesta decisão, a Comissão havia reconhecido que este último país assegurava um nível de proteção adequado.

Inconformado com a decisão do DPC, Schrems interpôs um recurso ao Supremo Tribunal de Justiça da Irlanda. A referida corte realizou, em um primeiro momento, uma análise dos factos à luz do direito irlandês, ressaltando, neste âmbito, que este direito proíbe a transferência de dados pessoais a um país terceiro que não assegure um nível adequado de proteção da vida privada, à semelhança do direito europeu, e que a Constituição irlandesa garante o direito ao respeito à vida privada, de forma que qualquer ingerência sobre este direito deverá não só respeitar os requisitos legais, como também deverá ser proporcionada. [153]

Por conseguinte, o acesso massivo e indiscriminado que estaria a ser realizado pelas autoridades americanas aos dados pessoais transferidos aos EUA era, claramente, contrário ao direito irlandês.

No entanto, o Supremo Tribunal de Justiça entendeu que as questões postas pelo austríaco também se referiam à aplicação do direito da União Europeia, em especial os artigos 7º, 8º, e 48º da CDFUE, razão pela qual a mencionada corte decidiu suspender a instância e submeter duas questões prejudiciais ao Tribunal de Justiça da União Europeia (TJUE).

---

[152] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (27): "Todas as pessoas que residam no território da União e pretendam utilizar o Facebook são obrigadas, no momento da sua inscrição, a celebrar um contrato com a Facebook Ireland, filial da Facebook Inc., com sede nos Estados Unidos."

[153] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (32)

Neste sentido, o TJUE foi acionado para analisar, à luz dos artigos 7º, 8º, e 48º da Carta de Direitos Fundamentais da UE, se caberia à autoridade de controlo nacional investigar a adequação do regime de proteção de dados oferecido por um país terceiro, no âmbito da análise de uma queixa segundo a qual o país terceiro para o qual são enviados os dados não oferece uma proteção adequada, ainda que tenha sido emita uma decisão de adequação que assegure o contrário; ou se a referida autoridade deveria vincular-se às decisões de adequação emitidas pela Comissão. No caso em questão, trata-se da decisão de adequação 2000/520/CE. [154]

3.1 Acórdão do Tribunal de Justiça da União Europeia (Processo C-362/14)

Em outubro de 2015, o TJUE analisou as questões prejudiciais postas pelo Supremo Tribunal de Justiça da Irlanda e emitiu o acórdão que invalidou o PS como fundamento legal para as transferências de dados pessoais provenientes da UE com destino aos EUA. Analisar-se-á, neste tópico, os pontos fundamentais da aludida decisão do TJUE.

3.1.1 Quanto aos poderes das autoridades nacionais de controlo, na aceção do artigo 28.o da Diretiva 95/46, perante uma decisão da Comissão adotada nos termos do artigo 25.o, n.o 6, desta diretiva

O artigo 8º, n. 3, da CDFUE [155] prevê que o cumprimento das regras da UE relativas à proteção dos dados deverá ser fiscalizado por uma autoridade independente,

[154] O Supremo Tribunal de Justiça irlandês submeteu duas questões prejudiciais ao Tribunal de Justiça da União Europeia, a saber: "1) Tendo em conta os artigos 7.°, 8.° e 47.° da Carta […] e sem prejuízo das disposições do artigo 25.o, n.o 6, da Diretiva 95/46, o [Commissioner] encarregad[o] de aplicar a legislação sobre a proteção de dados pessoais no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os Estados Unidos da América) para o qual são enviados dados pessoais não oferecem proteção adequada, está vinculado em termos absolutos pela constatação em sentido contrário da União, contida na Decisão 2000/520?
2) Em alternativa, pode e/ou deve proceder à sua própria investigação sobre a matéria, à luz dos últimos desenvolvimentos de facto ocorridos desde a primeira publicação da decisão da Comissão?" Cf. TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (36)

[155] O número 2 do artigo 16º do Tratado de Funcionamento da União Europeia apresenta previsão semelhante. "Artigo 16.o (ex-artigo 286.o TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação

sendo esta a autoridade de controlo nacional. Por conseguinte, estas autoridades possuem competência para verificar se as transferências realizadas a um país terceiro estão de acordo com os requisitos dispostos na Diretiva 95/46/CE, a exemplo da necessidade do país recetor consagrar um adequado nível de proteção dos dados. [156]

Como exposto em tópico precedente, a Comissão poderá adotar uma decisão que constate a adequação do nível de proteção de dados do país terceiro. Neste âmbito, o TJUE sublinhou que, de acordo com o artigo 288º do Tratado de Funcionamento da UE, a aludida decisão da Comissão possui caráter obrigatório para todos os Estados-Membros destinatários e impõe-se a todos os seus órgãos.

Sendo assim, o TJUE reconhece que os Estados-Membros e os seus órgãos, nestes incluída a autoridade de controlo nacional, não podem adotar medidas contrárias à decisão da Comissão enquanto esta não for declarada inválida, sendo este Tribunal o único competente para declarar a invalidade de um ato da União. [157]

Destarte, ainda que as autoridades de controlo tenham competência, e devam verificar se as transferências realizadas a um país terceiro estão em conformidade com a diretiva, não poderão adotar um *ato destinado a constatar, com efeitos vinculativos, que o país terceiro visado pela referida decisão não assegura um nível de proteção adequado.* [158] De igual forma, os órgãos jurisdicionais nacionais não têm competência para declarar, por si só, a invalidade dos atos da União.

A existência de uma decisão de adequação, todavia, não diminui os poderes das autoridades de controlo, os quais são garantidos tanto pela Carta e pelo TFUE, como também pelo artigo 28º da Diretiva 95/46.

Por conseguinte, as aludidas autoridades deverão continuar a investigar reclamações que digam respeito à proteção dos direitos e liberdades fundamentais de um indivíduo quando da transferência dos seus dados a um país terceiro, mesmo diante da existência de uma decisão da Comissão que assegure a adequação daquele país. Entender o contrário implicaria na impossibilidade do exercício do direito de apresentação de queixas

---

desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes." Cf. TFUE, artigo 16º, 2, Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497 01aa75ed71a1.0019.01/DOC_3&format=PDF> Acesso em: 13-03-2018

[156] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (47)

[157] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (61)

[158] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (57)

às autoridades de controlo por aqueles titulares que tiveram seus dados transferidos para países terceiros para os quais a Comissão havia emitido uma decisão de adequação.

No entanto, as autoridades de controlo não poderão declarar a invalidade da referida decisão. Caso entendam que a reclamação tem fundamento, deverão acionar os órgãos jurisdicionais nacionais para que estes, caso entendam neste sentido, apresentem a questão ao TJUE, órgão competente para declarar a invalidade dos atos da União. Sendo assim, o TJUE responde a questão prejudicial da seguinte forma [159]

> *O artigo 25.o,n.o 6, da Diretiva 95/46/CE [...] lido à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Department of Commerce dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do artigo 28.o desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.*

3.1.2 Quanto à validade da Decisão 2000/520/CE

Enquanto órgão competente para declarar a validade ou invalidade dos atos da União, o TJUE passou a analisar a adequação da Decisão 2000/520/CE à luz da Diretiva 95/46/CE e da Carta, ainda que esta questão não tivesse sido expressamente posta por Schrems.

Em um primeiro momento de sua fundamentação, o Tribunal realiza uma análise do artigo 25º da aludida diretiva, o qual impõe que as transferências de dados pessoais a um país terceiro só poderão ser realizadas se o referido país assegurar um nível de proteção adequado, destacando que, para alcançar este nível de adequação, a ordem jurídica do país terceiro não precisa ser idêntica, mas sim substancialmente equivalente à consagrada na UE. [160]

---

[159] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (107)

[160] Neste sentido, independentemente da utilização de instrumentos idênticos ou diferentes, a ordem jurídica do país terceiro deverá garantir uma proteção substancialmente equivalente àquela consagrada no direito europeu.

Para avaliar a aludida equivalência substancial, faz-se necessária uma análise não só das regras aplicáveis no país terceiro – tanto a legislação interna, como os compromissos internacionais - como também das práticas adotadas naquele país com vista a assegurar o cumprimento das referidas regras.

Esta análise, todavia, não deve restar-se indiferente aos desenvolvimentos do quadro jurídico do país terceiro. É natural que a ordem jurídica daquele país sofra alterações depois que tenha sido considerada "adequada", razão pela qual o TJUE reconheceu que incumbe à Comissão verificar periodicamente se a adequação do nível de proteção dos dados do país terceiro *se continua a justificar de facto e de direito.* [161] O reexame periódico é especialmente relevante no caso da reavaliação da decisão de adequação 2000/520/CE no cenário pós-revelações de Edward Snowden.

Com base nestas constatações, o TJUE passou a examinar a adequação do nível de proteção dos dados pessoais transferidos aos EUA por meio do PS, tendo em consideração não só as disposições da Decisão 2000/520/CE, lidas à luz dos artigos relevantes tanto da Diretiva 95/46/CE como da Carta de Direitos Fundamentais da UE, como também os desenvolvimentos no quadro de proteção de dados dos EUA. Neste sentido, o TJUE destacou os seguintes pontos:

(1) Uma vez que era um sistema baseado na autocertificação, o bom funcionamento do PS só seria alcançado se este sistema previsse mecanismos de fiscalização e de penalização capazes de detetar e sancionar as suas falhas. De acordo com as comunicações da Comissão ressaltadas no tópico precedente, percebe-se que as autoridades americanas responsáveis pela supervisão da aplicação do PS falharam em exercer as suas competências de forma satisfatória; [162]

(2) Os princípios do sistema PS eram aplicáveis unicamente às empresas autocertificadas, sem que as autoridades públicas americanas ficassem a estes sujeitas;

(3) A Decisão 2000/520/CE dizia respeito tão só ao nível adequado de proteção consagrado nos princípios do PS, sem indicar como os EUA garantiriam o referido nível de

[161] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (74)

[162] A Comissão de Comércio dos EUA apenas começou a adotar medidas proativas no sentido de monitorar a aplicação do PS no ano de 2009. Em todo caso, a adoção de medidas coercivas como resultado do não cumprimento do acordo só passou a ser observada por volta de 2011, com o caso *Google Buzz*. Para maior desenvolvimento, ver VOSS, W. Gregory, «The future of transatlantic data flows: Privacy Shield or Bust*?* », *Journal of Internet Law*, Vol. 19, número 11, maio de 2016, p. 11

proteção por meio de sua legislação interna ou compromissos internacionais, conforme estipulava o artigo 25º da Diretiva 95/46/CE; [163]

(4) O anexo I da Decisão 2000/520/CE permitia que a aplicação dos princípios do acordo PS fosse limitada, por exemplo, por motivos de segurança nacional, interesse público e execução da lei;

(5) Se a legislação americana impusesse uma obrigação contraditória aos princípios do PS, as organizações deveriam afastar os princípios e privilegiar a lei, possibilitando, portanto, ingerências nos direitos fundamentais dos titulares cujos dados fossem transferidos da UE para os EUA;

(6) Não havia a previsão de meios ou recursos que oferecessem uma proteção jurídica eficaz contra as referidas ingerências, ou que as limitassem, o que tornava possível que as autoridades americanas acessassem os dados pessoais dos cidadãos europeus dando-lhes um tratamento distinto daquele que justificou a sua transferência. [164]

(7) Os titulares não eram informados sobre a utilização dos seus dados para fins diferentes daqueles para os quais foram recolhidos.

Ora, um instrumento jurídico que estabeleça exceções que possam dar azo a limitações aos direitos fundamentais deverá indicar, de forma clara e precisa, as finalidades e as condições sob as quais as exceções poderão ser aplicadas; bem como deverá prever garantias aos titulares dos dados contra o risco de abuso de direito. Ainda neste sentido, as exceções ao direito à vida privada e à proteção dos dados só poderiam ser aplicadas se fossem estritamente necessárias. [165]

O Tribunal analisou as referidas constatações tendo em consideração as revelações sobre os programas de vigilância realizados nos EUA, por meio dos quais as autoridades americanas poderiam acessar dados pessoais transferidos desde a UE àquele país, onde poderiam ser tratados de forma incompatível com a finalidade para a qual foram recolhidos, e sem que estivesse previsto *um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos,*

[163] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (83)

[164] SILVA, Heraclides Sequeira dos Santos, *A Proteção de Dados Pessoais na Era Global: O caso Schrems*, Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade Nova de Lisboa em janeiro de 2017, p. 51

[165] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, Janeiro de 2017, p. 3

estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam.[166]

A referida vigilância em massa realizada pelas agências de segurança dos EUA é claramente incompatível com o quadro europeu de proteção de dados, uma vez que viola o direito fundamental ao respeito à vida privada, previsto no artigo 7º da CDFUE, bem como o direito fundamental a uma proteção jurisdicional efetiva, garantido pelo artigo 47º da Carta, já que permitia o acesso ao conteúdo das comunicações eletrônicas, sem, todavia, prever meios através dos quais o titular poderia aceder, retificar ou suprimir os seus dados.

Como resultado desta análise sobre o quadro norte-americano de proteção de dados, o TJUE entendeu que o artigo 1º da Decisão 2000/520/CE não avaliou a adequação do nível de proteção dos dados transferidos aos EUA com base na legislação interna ou nos compromissos internacionais daquele país, conforme estipula o artigo 25º, n.º 6 da Diretiva 95/46/CE, razão pela qual deve ser considerado inválido.

Por fim, o TJUE constatou que a Decisão 2000/520/CE impede que as autoridades nacionais de controlo exerçam todas as suas competências garantidas pelo artigo 28º da Diretiva 95/46/CE, [167] na medida em que o artigo 3º, n.º 1, da referida decisão determina que aquelas autoridades podem aplicar as medidas necessárias para garantir o cumprimento das disposições nacionais adotadas em execução da diretiva em questão, salvo as medidas destinadas a garantir a observância do artigo 25º da diretiva. [168-169]

Ocorre que o artigo 25º, n.º 6 da Diretiva não atribuiu à Comissão competência para limitar os poderes das autoridades nacionais de controlo, entidades que devem ter a independência e os poderes necessários para investigar as reclamações dos titulares dos dados relativas tanto à proteção dos seus direitos como à análise da licitude do tratamento dos seus dados. Por esse motivo, o Tribunal julgou inválido o artigo 3º da decisão em análise.

---

[166] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (93)

[167] O artigo 28º da Diretiva 95/46 dispõe sobre os poderes e as competências das autoridades de controlo.

[168] SILVA, Heraclides Sequeira dos Santos, *A Proteção de Dados Pessoais na Era Global: O caso Schrems*, Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade Nova de Lisboa em janeiro de 2017, p. 52

[169] TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*, parágrafo (101)

Diante das supracitadas considerações, e por ter considerado inválidos os artigos 1º e 3º da Decisão, os quais são indissociáveis do 2º e 4º , em 6 de outubro de 2015, o TJUE, enquanto órgão competente para tanto, declarou a invalidade da Decisão 2000/520/CE.

4. Escudo de Proteção da Privacidade - *Privacy Shield*

A declaração de invalidade da decisão de adequação 2000/520/CE deu azo a um cenário de forte insegurança para as entidades americanas que utilizavam o PS como fundamento para as transferências de dados pessoais provenientes da UE.

Tendo em consideração as estreitas relações comerciais entre o mercado europeu e o americano, tornou-se imprescindível que os EUA e a Comissão Europeia negociassem um novo acordo que pudesse estabelecer um nível mais elevado de proteção dos dados e que efetivamente respeitasse os direitos fundamentais à proteção dos dados e à vida privada.

Enquanto um novo acordo não fosse negociado, as empresas americanas passaram a valer-se de outras garantias – como as cláusulas-tipo e as regras vinculativas - para assegurar a continuidade do fluxo de dados entre os EUA-UE.

Após meses de negociações, em fevereiro de 2016, a Comissão Europeia divulgou o rascunho do Escudo de Proteção da Privacidade – "EPP" (*Privacy Shield*), acordo cujo objetivo principal é restaurar a confiança nas transferências de dados transatlânticas por meio do estabelecimento de garantias que assegurem um adequado nível de proteção dos dados que são transferidos aos EUA.

No entanto, as reações ao rascunho do EPP não foram acolhedoras. As críticas ressaltaram que os compromissos assumidos pelos EUA eram muito vagos, ou não eram fortes o suficiente para garantir o respeito ao direito fundamental à proteção dos dados, especialmente porque o acordo ainda permitia que as agências de inteligência dos EUA coletassem em larga escala os dados pessoais que fossem transferidos àquele país.

Além deste fator, em declaração emitida em abril de 2016, o Grupo de Trabalho do Artigo 29 (GTA29) expressou suas preocupações quanto à falta de claridade do rascunho do EPP quanto à elaboração do princípio da limitação das finalidades, quanto à ausência de

menção ao princípio da retenção dos dados e quanto à falta de indicação das proteções que deveriam ser oferecidas contra as decisões automatizadas. [170]

Apesar de reconhecer os avanços do Escudo de Proteção da Privacidade, o GTA29 recomendou que a Comissão revisasse as preocupações supracitadas, e fornecesse os esclarecimentos necessários para assegurar que a proteção aos dados oferecida pelo EPP era essencialmente equivalente àquela garantida na UE. [171] As aludidas recomendações receberam o apoio do Parlamento Europeu em uma comunicação deste órgão emitida em maio de 2016. [172]

Ainda no que concerne às recomendações de revisão do rascunho do EPP, insta salientar a posição do Supervisor Europeu de Proteção dos Dados, Giovanni Buttarelli, o qual defendeu que o referido sistema fosse desenvolvido tendo em consideração as disposições do RGPD, haja vista a proximidade do prazo de aplicação do regulamento. Dessa forma, evitar-se-ia que as entidades que desejassem subscrever aos princípios de proteção do EPP tivessem que alterar suas políticas de privacidade quando do início da aplicação do regulamento, em adequação a este instrumento jurídico. [173]

No seguimento das recomendações à revisão do EPP, o Comité do artigo 31 votou pela adoção do referido sistema, e, em 12 de julho de 2016, a decisão de adequação foi adotada (Decisão 2016/1250),[174] entrando em vigor na mesma data, após notificação dos Estados-Membros da UE. O Departamento de Comércio dos EUA passou a receber as autocertificações de aderência aos princípios de proteção dos dados em 1º de agosto daquele mesmo ano.

---

[170] GRUPO DE TRABALHO DO ARTIGO 29, *Opinião 01/2016 sobre o rascunho da decisão de adequação do Escudo da Proteção dos Dados – EU – EUA*, adotada em 13 de abril de 2016, WP 238, p. 4

[171] *Ibid*., p.2

[172] PARLAMENTO EUROPEU, Resolução do Parlamento Europeu de 26 de maio de 2016 sobre a transferência transatlântica de dados (2016/2727(RSP)), parágrafo 12: "12. Solicita à Comissão que aplique plenamente as recomendações formuladas pelo Grupo de Trabalho do artigo 29.º no seu parecer 01/2016 sobre o projeto de decisão relativa à adequação do escudo de proteção da privacidade UE-EUA;"

[173] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, Janeiro de 2017, p. 21

[174] COMISSÃO EUROPEIA, 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 [notificada com o número C(2016) 4176]

4.1 Estrutura do Escudo de Proteção da Privacidade

À semelhança do *"*Porto Seguro", o "Escudo de Proteção da Privacidade" é um sistema de autocertificação por meio do qual as entidades declaram anualmente a aderência aos princípios de proteção de dados emitidos pelo Departamento de Comércio dos Estados Unidos, os quais estão previstos no anexo II da decisão de execução 2016/1250 da Comissão. As entidades americanas deverão adotar os referidos princípios em suas políticas de privacidade, as quais deverão ser publicadas, como forma de torná-las acessíveis à população, garantindo a transparência das atividades das organizações autocertificadas.

Através da aludida aderência aos princípios, as entidades americanas garantem oferecer um nível adequado de proteção aos cidadãos europeus cujos dados foram transferidos aos EUA.

Assim como no PS, a adesão aos princípios é voluntária. No entanto, uma vez que a entidade tenha declarado ter subscrito aos princípios, ficará vinculada às regras nestes contidas, estando a partir de então sujeita aos poderes das autoridades americanas responsáveis pela administração e garantia do cumprimento dos princípios, quais sejam o Departamento e a Comissão de Comércio dos EUA, e o Departamento de Transportes.

Como ressaltado no tópico precedente, o objetivo primeiro do EPP é restaurar a confiança nas transferências de dados transatlânticas por meio do estabelecimento de um quadro de direitos e obrigações que assegure um adequado nível de proteção dos dados pessoais que são transferidos aos EUA. Para alcançar o referido escopo, era necessário que o EPP fosse desenvolvido de forma a corrigir as falhas apontadas pelo TJUE ao seu predecessor, adotando as recomendações formuladas por aquele Tribunal no âmbito da decisão *Schrems*.

Neste sentido, o EPP impôs obrigações mais elaboradas tanto às entidades que autocertificaram os seus princípios, como às autoridades americanas responsáveis pelo controlo da observância dos aludidos princípios; ao mesmo tempo em que desenvolveu novos mecanismos e instrumentos de recurso, e incluiu garantias de autoridades americanas de que as agências de inteligência daquele país não mais realizariam a coleta indiscriminada e em larga escala dos dados transferidos aos EUA.

4.2 Princípios de proteção dos dados contidos no Escudo de Proteção da Privacidade

Os princípios de proteção dos dados previstos no EPP muito se assemelham àqueles consagrados no PS, à diferença de que o EPP estabelece obrigações mais elaboradas às entidades autocertificadas, com vista a afastar as falhas do acordo precedente.

Os princípios de proteção de dados estão previstos no Anexo II da decisão de adequação do EPP, sendo 16 princípios complementares e 7 fundamentais, aos quais ficam sujeitos tanto o responsável pelo tratamento como o subcontratante, a saber:

Princípio de aviso

Segundo este princípio, antes de processar os dados, a organização deverá informar o titular sobre elementos fundamentais ao tratamento, a exemplo dos tipos dos dados recolhidos, finalidade do tratamento e da existência do direito de acesso. Com base nessas informações, as quais devem ser prestadas de forma clara e inteligível, o titular dos dados estará melhor informado sobre os seus direitos e poderá, consequentemente, exercê-los com maior facilidade.

Apesar de não ser um princípio inovador, uma vez que já estava previsto no elenco do PS, o princípio de aviso estabelece novas obrigações às entidades autocertificadas como forma de mitigar algumas das falhas do sistema anterior, qual seja a falta de publicação da política de privacidade por parte das referidas entidades e a falta da indicação de um órgão ao qual os titulares poderiam voltar-se caso tivessem seus direitos violados.

Neste sentido, o princípio em questão introduz a obrigação das entidades americanas tornarem públicas as suas políticas de privacidade, nas quais devem indicar a observância aos princípios do EPP, bem como estabelece o dever das aludidas entidades indicarem mecanismos de resolução alternativa de litígios e ligações tanto para o sítio *web* do DC como para a lista do Escudo de Proteção da Privacidade. [175]

Princípio da integridade dos dados e limitação dos fins.

De acordo com o princípio em questão, os dados pessoais deverão ser tratados apenas na medida em que são relevantes à finalidade do tratamento. Neste sentido, a entidade certificada não poderá tratar os referidos dados de acordo com finalidades

[175] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (20).

diferentes daquelas que motivaram a recolha, ou de acordo com fins diferentes daqueles que tenham sido posteriormente autorizados pelo titular dos dados. O mesmo princípio ainda impõe às organizações que estas assegurarem a correção, exatidão e atualização dos referidos dados.

De igual forma, os dados deverão ser conservados apenas enquanto a sua utilização seja conforme à finalidade para as quais foram recolhidos ou posteriormente autorizados. [176]

Princípio da escolha.

Através do princípio da escolha, o EPP introduz ao titular a faculdade de se opor (*opt-out*) à divulgação dos seus dados a terceiros ou ao tratamento destes para uma finalidade diversa daquela que motivou a recolha, ainda que compatível com a finalidade inicial.

No caso da recolha de dados sensíveis, aplica-se a lógica inversa (*opt-in*), estando as organizações obrigadas a obter a autorização afirmativa expressa dos titulares dos dados para que estes possam ser tratados.

O EPP, todavia, é silente quanto à forma por meio da qual este direito poderá ser exercido, bem como quanto ao prazo durante o qual os titulares poderão exercer o supracitado direito de oposição, à exceção dos casos que envolvam *marketing* direito, quando o EPP expressamente prevê que este direito poderá ser exercido a qualquer momento. [177]

Princípio da segurança.

O princípio da segurança impõe que as empresas certificadas apliquem medidas razoáveis e apropriadas para garantir a segurança dos dados quando do tratamento destes. Neste sentido, o responsável pelo tratamento deverá analisar cada caso concreto, tendo em consideração a natureza dos dados que serão tratados e os riscos que podem surgir do referido tratamento, para então estar em condições de escolher as medidas de segurança apropriadas. O EPP, todavia, não oferece detalhes sobre os tipos de instrumentos que poderão ser aplicados.

[176] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (23).
[177] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, Janeiro de 2017, p. 24

Princípio do acesso

O princípio de acesso atribui aos titulares a faculdade de obter das entidades não só a confirmação de que seus dados estão a ser tratados, como também o direito de acessar as referidas informações – o que inclui o acesso à finalidade do tratamento, os tipos de dados que estão a ser tratados, e a quem esses dados estão a ser revelados – além de poder corrigir, emendar e apagar as suas informações, sempre que estas estejam incorretas ou tenham sido tratadas em violação aos princípios. [178]

Princípio da responsabilização pela transferência ulterior

De acordo com o referido princípio, as transferências ulteriores só poderão ser realizadas para fins limitados e específicos, desde que baseadas em um contrato escrito – ou outro instrumento equivalente - no qual esteja previsto que a parte que receberá os dados por meio da aludida transferência adotará instrumentos que assegurem o mesmo nível de proteção garantido pelos princípios do EPP.

Sendo assim, o nível de proteção consagrado no EPP deverá acompanhar os dados pessoais mesmo quando estes forem o objeto de uma transferência ulterior a um terceiro que não faça parte do sistema.

Caso o terceiro reconheça que não mais possui condições de garantir o mesmo nível de proteção, deverá informar a organização aderente ao EPP, a qual deverá pôr termo ao tratamento ou adotar as medidas necessárias ao restabelecimento do referido nível de proteção.

Ainda neste âmbito, a finalidade do tratamento realizado após a referida transferência ulterior não poderá ser incompatível com a finalidade para a qual o titular dos dados emitiu seu consentimento.

Princípio de recurso, aplicação e responsabilidade.

Segundo este princípio, as empresas deverão adotar mecanismos que assegurem que sua atuação esteja em conformidade com as disposições do Escudo de Proteção da Privacidade, incluindo, neste âmbito, vias de recurso aos titulares cujos dados tenham sido tratados de modo contrário aos dispositivos do EPP. Os mecanismos de recurso devem ser independentes e de fácil acesso e utilização pelos titulares que se sentiram lesados pelo tratamento dos seus dados pessoais.

[178] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (25).

O sistema ainda deverá prever sanções rigorosas o suficiente para garantir que a organização que tenha violado os princípios de proteção dos dados atue em conformidade com os aludidos princípios.

4.3 Poderes reforçados das autoridades americanas

Ao avaliar a validade da decisão de adequação 2000/520/CE, o TJUE deixou claro que o recurso a um sistema de autocertificação, como é o caso do PS e do EPP, não é contrário à exigência da Diretiva 95/46/CE segundo a qual os dados pessoais só poderão ser transferidos entre a UE e um país terceiro se este último possuir um nível adequado de proteção dos dados.

No entanto, o mesmo Tribunal reconheceu que a fiabilidade deste sistema depende da existência de mecanismos eficazes de fiscalização que permitam identificar e punir as violações das regras que garantem a proteção dos direitos fundamentais à proteção dos dados e à vida privada.

Por conseguinte, o sistema de autocertificação deve prever poderes e deveres às autoridades competentes não só para detetar a não observância ou violação dos princípios, mas também para aplicar as sanções necessárias às entidades que não cumpram com as obrigações que lhes foram atribuídas pelo sistema EPP.

Elaborado para ser um substituto reforçado do PS, o EPP identificou as falhas apontadas no âmbito do julgamento do caso *Schrems* e buscou reforçar a fiabilidade do sistema ao prever maiores poderes e obrigações às autoridades americanas responsáveis pelo controlo da observância dos princípios de proteção do EPP.

4.3.1 Departamento de Comércio

De acordo com o EPP, o Departamento de Comércio dos EUA passa a ser responsável não só pela elaboração de uma lista das entidades que autocertificaram os princípios de proteção, como também pela atualização da aludida lista, que deverá ser realizada de forma a retirar as entidades que não mais cumpram os princípios, que não

recertifiquem a sua aderência, ou ainda que apresentem um padrão de incumprimento dos referidos princípios. [179]

Além destes deveres, o DC mantém a obrigação de verificar a existência e adequação das autocertificações das entidades que desejam aderir ao EPP, tarefa que sob a égide deste sistema inclui igualmente verificar se as entidades registaram um mecanismo independente de resolução de litígios, e se tornaram pública a sua política de privacidade.

Já no âmbito de suas funções de fiscalização e monitoramento da observância dos princípios, o DC deverá revisar o cumprimento dos princípios por parte das empresas autocertificadas em três casos principais: (1) quando recebe uma reclamação contra a entidade; (2) quando a organização não providenciar respostas satisfatórias aos questionamentos enviados por aquele Departamento; (3) quando houver dúvidas sobre o cumprimento ou não dos princípios pela organização investigada. [180]

Se, após a fiscalização, o DC concluir que a organização participante violou constantemente os princípios do EPP, deverá proceder à eliminação da referida organização da lista que indica as entidades participantes do sistema em questão.

4.4 Recursos

Além dos poderes das autoridades americanas, outro aspeto do EPP que foi criticado pela decisão *Schrems* refere-se à falta de mecanismos de recurso oferecidos aos titulares cujos dados pessoais foram transferidos às entidades americanas através do referido sistema. A falta das vias de recurso era especialmente sensível diante das violações causadas em decorrência da coleta indiscriminada e em larga escala dos dados pessoais pelos programas de vigilância das agências de inteligência americanas.

Para garantir o direito fundamental a uma proteção jurisdicional efetiva, os titulares dos dados deverão ter à sua disposição meios de recurso independentes por meio dos quais sejam capazes de expor suas reclamações e obter uma solução de forma rápida e a baixo

[179] Por conseguinte, o DC mantém duas listas: uma referente às entidades autocertificadas, e outra referente às entidades que foram removidas da primeira lista, a qual é acompanhada pelos razões que motivaram a remoção da aludida entidade. Para maior desenvolvimento, ver LINN, Emily, «A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement», *Vanderbilt Journal of Transnational Law*, Vol 50, 2017, p. 1329

[180] PUPALOVA, Nina, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* Dissertação de Mestrado apresentada à Faculdade de Direito de Oslo, dezembro de 2017, p. 31

custo/custo zero. Como forma de assegurar o referido direito, e, consequentemente, um nível de proteção adequado aos dados transferidos às entidades americanas, o EPP prevê diferentes mecanismos de recurso que devem ser oferecidos aos titulares dos dados.

Nesse sentido, as entidades que desejam aderir aos princípios do EPP deverão disponibilizar aos titulares dos dados mecanismos de recurso *independentes e facilmente acessíveis e eficazes, através dos quais as queixas e os litígios possam ser examinados e resolvidos sem custos para os titulares dos dados.* [181]

Destarte, diante da violação dos seus direitos, os titulares dos dados poderão escolher se querem apresentar uma queixa, optando pela via de recurso que lhes parecer mais adequada entre as várias opções que são oferecidas, a saber [182]

> *1. Junto da própria empresa aderente ao Escudo de Proteção da Privacidade;*
> *2. Perante um mecanismo de recurso independente (RAL ou APD);*
> *3. Junto do Departamento do Comércio dos EUA, unicamente por intermédio de uma APD;*
> *4. Junto da Comissão Federal do Comércio dos Estados Unidos (ou do Departamento dos Transportes dos EUA se a queixa disser respeito a uma companhia aérea ou a uma agência de viagens);*
> *5. Junto do Comité do Escudo de Proteção da Privacidade, se certas opções de recurso tiverem falhado.*

(1) Primeiramente, os titulares são encorajados a apresentar a queixa à entidade que autocertificou a aderência aos princípios do EPP, a qual possui o prazo de 45 dias para responder às reclamações que lhes forem enviadas. Para garantir a efetividade do exercício deste direito, as referidas entidades deverão tornar público [183] e de fácil acesso o contacto da pessoa responsável pela resolução das queixas, a qual poderá ser interna ou externa à organização.

(2) Em segundo lugar, o EPP recomenda a utilização dos organismos independente de resolução de litígios. Neste sentido, a entidade autocertificada poderá indicar com seu organismo independente de resolução de litígios os mecanismos de resolução alternativa de litígios (RAL) ou as autoridades nacionais de proteção dos dados (APD).

Caso opte pela adoção da resolução alternativa de litígios como seu mecanismo de recurso independente, a organização autocertificada deverá indicar em seu sítio *web* um

[181] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (39).
[182] COMISSÃO EUROPEIA, *Guia para o Escudo da Proteção de dados*, Direção-Geral da Justiça e dos Consumidores, 2016, p. 5
[183] A indicação do contacto da pessoa responsável por resolver as queixas indica demonstra a importância da publicação das políticas de privacidade das entidades que subscreveram aos princípios de proteção do EPP. Para maior desenvolvimento, ver PUPALOVA, Nina, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de Oslo, dezembro de 2017, p. 31

ponto de contacto para que o titular possa informar-se sobre como realizar sua queixa, estando isento do pagamento de custos para o exercício do direito em questão. [184]

Como forma de garantir o bom funcionamento do sistema, o Departamento de Comércio dos EUA comprometeu-se a verificar se a entidade está, de facto, registada com o organismo de resolução de litígios que indicou em sua política de privacidade e no seu sítio *web*.

Uma vez apresentada a queixa, o aludido organismo deverá investigar se houve a violação aos princípios, oferecendo na sequência da investigação uma decisão que solucione a reclamação, podendo, neste âmbito aplicar as sanções necessárias para atingir o referido objetivo.

Caso a entidade autocertificada não cumpra a decisão do órgão em questão, este deverá notificar o Departamento de Comércio dos EUA e à FTC ou ao Departamento de Transportes daquele mesmo país, a depender do caso, para que as referidas autoridades investiguem o aludido incumprimento. [185] De igual forma, o organismo de resolução de litígios poderá notificar o tribunal competente.

(3) Regra geral, as autoridades autocertificadas podem escolher as autoridades nacionais de proteção de dados (APD) como seus mecanismos de recurso independente. No entanto, caso a entidade trate dados de recursos humanos, será obrigada a cooperar com as autoridades de controlo nacionais.

As instruções das autoridades de proteção dos dados serão emitidas por um painel informal composto pelas referidas autoridades à nível da União. Caso a entidade obrigada a cooperar com a APD não siga a recomendação emitida pelo painel das autoridades de controlo, e não apresente uma justificação para tanto, o painel comunicará à entidade americana a sua intenção de levar o caso à FTC, a qual poderá impor as medidas coercitivas previstas no *FTC Act*.

Ainda na sequência do incumprimento da recomendação, o painel pode entender que o compromisso de cooperação foi violado, o que o levará a acionar o Departamento de Comércio, que, por seu turno, poderá considerar a retirada da empresa da lista de entidades

[184] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, janeiro de 2017, p. 27

[185] PUPALOVA, Nina, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de Oslo, dezembro de 2017, p. 35

participantes do EPP, caso a organização continue a não cumprir os pareceres que lhe são dirigidos. [186]

Insta ressaltar que, ainda que não tenham sido indicadas pela autoridade autocertificada como seu mecanismo de resolução de litígios, as autoridades nacionais de controlo podem ser acionadas pelos titulares dos dados. Nestes casos, as queixas poderão ser dirigidas ao Departamento de Comércio ou ao FTC. Como forma de facilitar essa cooperação, tanto o DC como o FTC comprometeram-se a designar um ponto de contacto com as autoridades nacionais de controlo (ANC) para recebimento das aludidas queixas. O DC terá 90 dias, a contar do recebimento da reclamação, para analisar o caso e providenciar uma resposta à ANC. [187]

(4) Os titulares dos dados ainda poderão apresentar queixas diretamente à FTC [188] por meio do seu website: "www.ftc.gov/complaint", ou ao Departamento de Transportes (no caso da entidade ser uma companhia aérea ou agência de viagens). Indiretamente, a FTC também devér analisar as queixas que lhe forem enviadas pelo Departamento de Comérico, pelos mecanismos de RAL e pelas autoridades nacionais de controlo.

A FTC deverá garantir de forma eficaz o cumprimento dos princípios de proteção dos dados previstos no EPP. Para tanto, as organizações participantes do referido sistema estarão sujeitas aos poderes de investigação e de execução da referida autoridade americana, a qual poderá aplicar decisões adminsitrativas (injunções) às referidas organizações que tenham atuado em desconformidade com os princípios do EPP. [189]

Caso a entidade participante do EPP falhe em cumprir a decisão, a FTC poderá submeter o caso ao tribunal competente, solicitando, se necessário, as sanções de caráter civil e outras reparações pelos danos que podem ter sido causados como consequência dos atos ilegais praticados pela entidade que descumpriu a sua decisão (FTC). [190]

(5) Os titulares dos dados poderão, por fim, recorrer ao Comité do Escudo de Proteção da Privacidade (CEPP), como *ultima ratio*, no caso de não terem obtido a solução do seu litígio por meio da utilização dos recursos supracitados. Apesar de o CEPP ser

[186] COMISSÃO EUROPEIA, *Guia para o Escudo da Proteção de dados*, Direção-Geral da Justiça e dos Consumidores, 2016, p. 7
[187] *Ibid*., p. 16
[188] Assim como o DC, a FTC "comprometeu-se a criar um processo de transmissão de queixas normalizado, a designar um ponto de contacto no organismo para a receção de queixas das APD e a proceder ao intercâmbio de informações sobre as mesmas." Decisão de Execução (UE) 2016/1250, Considerando (54)
[189] Decisão de Execução (UE) 2016/1250, Considerando (55).
[190] Decisão de Execução (UE) 2016/1250, Considerando (55).

composto por 20 árbitros, todos indicados pelo Departamento de Comércio, as queixas serão analisadas por um conjunto de um até três árbitros imparciais, os quais emitirão decisões vinculativas que poderão ser executadas perante tribunais americanos. [191] Em todo caso, as medidas aplicadas pelo Comité para corrigir o incumprimento dos princípios não poderão ser de caráter monetário.

4.5 Acesso aos dados pessoais pelas autoridades públicas americanas

Não obstante as duras críticas às exceções previstas no texto do PS, o EPP mantém a previsão da limitação da aplicação dos princípios de proteção dos dados para observar os requisitos de segurança nacional, interesse público ou aplicação da lei, disposição que facilitou a coleta indiscriminada e em larga escala de dados pessoais transferidos aos EUA por meio do PS.

Como forma de amenizar as preocupações europeias concernentes às atividades de vigilância dos EUA, o Gabinete do Diretor dos Serviços Nacionais de Informações (*Office of the Director of National Intelligence* - ODNI) apresentou à Comissão, no Anexo VI da decisão 2016/1250,[192] uma carta na qual assegura que se os dados pessoais transferidos aos EUA por meio do EPP forem acessados sob a supracitada exceção, será apenas na medida do necessário, estando este acesso sujeito às limitações e às garantias previstas em lei, em especial, o Decreto Executivo 12333 (EO1233), o *Presidential Policy Directive* 2867 (PPD-28)[193], e o *Foreign Intelligence Surveillance Act* – FISA.

Neste âmbito, deve ser ressaltado que os princípios da proteção dos dados não são absolutos, sendo permitidas derrogações aos referidos princípios desde que as interferências ao direito fundamental à proteção dos dados seja justificável em uma sociedade democrática, e que sejam aplicáveis as garantias essenciais à proteção do direito em análise.

---

[191] COMISSÃO EUROPEIA, *Guia para o Escudo da Proteção de dados*, Direção-Geral da Justiça e dos Consumidores, 2016, p. 9

[192] COMISSÃO EUROPEIA, Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, ANEXO VI Carta do Conselheiro-Geral Robert Litt Office of the Director of National Intelligence (Gabinete do Diretor dos Serviços Nacionais de Informações) 22 de fevereiro de 2016

[193] O PPD-28 "estabelece limitações e garantias relativamente à utilização pelas autoridades nacionais de segurança dos dados pessoais, independentemente da nacionalidade da pessoa." Cf. COMISSÃO EUROPEIA, Relatório da Comissão para o Parlamento Europeu e o Conselho sobre a primeira revisão anual sobre o funcionamento do Escudo da Proteção dos dados EU-US, Bruxelas, 18.10.2017, COM (2017) 611 final, p. 4

De acordo com a decisão de adequação 2016/1250, apesar de permitir que as autoridades públicas dos EUA acessem e utilizem os dados pessoais transferidos através do EPP, a referida legislação americana prevê mecanismos de supervisão e reparação que oferecem *garantias suficientes para a proteção eficaz dos dados contra a ingerência ilegal e o risco de abuso*. [194] Passemos a analisar os pontos centrais da referida legislação.

4.5.1 PPD -28

O PPD-28 consiste em uma diretiva do Presidente dos Estados Unidos cujo objetivo principal é prescrever os limites e as condições para recolha e tratamento dos dados pessoais realizados pelos programas de vigilância daquele país.

Neste sentido, o PPD-28 prevê que as informações de origem eletromagnética podem ser *recolhidas exclusivamente nos caso em que exista um objetivo de espionagem externa ou de contra-espionagem ou para apoiar missões nacionais e departamentais,*[195] e que a recolha dos dados deve ser "tão seletiva quanto possível",[196] devendo ser coletados apenas os dados relevantes aos motivos que fundamentaram o afastamento dos princípios de proteção dos dados.

Por conseguinte, a recolha em larga escala [197] deve ser uma exceção a ser utilizada apenas quando a recolha seletiva não puder ser executada por motivos técnicos ou operacionais, [198] e a referida informação coletada só poderá ser utilizada de acordo com um dos seguintes fins específicos: *deteção e combate a determinadas atividades de potências estrangeiras; luta contra o terrorismo; luta contra a proliferação; cibersegurança; deteção e combate às ameaças para as forças armadas dos EUA ou dos aliados; e combate às ameaças criminosas transnacionais, nomeadamente evasões a sanções*.

---

[194] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (65). No mesmo sentido, considerando 88: "Tendo em conta tudo o que precede, a Comissão conclui que existem normas em vigor nos Estados Unidos destinadas a limitar qualquer ingerência para efeitos de segurança nacional nos direitos fundamentais das pessoas cujos dados pessoais são transferidos da União para os Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA ao estritamente necessário para a consecução do objetivo legítimo em questão."

[195] Decisão de Execução (UE) 2016/1250 da Comissão, Considerando (70)

[196] COMISSÃO EUROPEIA, Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, ANEXO VI Carta do Conselheiro-Geral Robert Litt Office of the Director of National Intelligence (Gabinete do Diretor dos Serviços Nacionais de Informações) 22 de fevereiro de 2016

[197] Recolha em larga escala seria aquela realizada sem a utilização de discriminantes, a exemplo de identificadores específicos e termos de seleção. Cf. Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, ANEXO VI, p. 93

[198] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (72).

Não obstante a imposição das supracitadas limitações, percebe-se que alguns dos conceitos são consideravelmente amplos, a exemplo da "luta contra o terrorismo" e da "cibersegurança", fator que não só contribui para a falta de transparência das atividades de vigilância conduzidas pelos EUA, como também facilita a recolha dos dados em larga escala e de forma indiscriminada.

No seguimento da exposição das garantias e limitações estabelecidas no âmbito do PPD-28, o Diretor do ODNI ressalta que, embora não possam confirmar nem desmentir operações ou métodos de recolha de informação, no evento das autoridades públicas recolherem e acessarem dados transferidos aos EUA por meio do EPP, serão observadas as disposições da referida PPD-28, independentemente do tipo ou fonte dos dados recolhidos. [199] Destarte, as previsões deste instrumento devem ser aplicadas aos dados dos cidadãos europeus transferidos aos EUA por meio do EPP.

4.5.2 Secção 702 do FISA

Por seu turno, a secção 702 do FISA autoriza as autoridades americanas a coletar dados de cidadãos de países terceiros que estejam localizados fora do território dos EUA, com a assistência obrigatória dos fornecedores de serviços de comunicações eletrônicas dos EUA, para fins de coleta de "informações de inteligência no estrangeiro". [200] O FISA é a base legal para programas de vigilância como o PRISM e o UPSTREAM, ambos detalhados pelas revelações de Snowden.

As atividades de recolha e tratamento dos dados realizadas em conformidade com a referida secção devem estar sujeitas às previsões do PPD-28, e, neste sentido, devem incidir em alvos legítimos e individualmente identificados, [201] não devendo ser maciças nem indiscriminadas.

Não obstante as supracitadas garantias, nenhuma evidência material foi apresentada para fundamentar a declaração do ODNI de que as recolhas dos dados realizadas com fundamento na secção 702 não são indiscriminadas e que o acesso aos dados não é realizado de forma generalizada, motivo pelo qual o GTA29 indicou na 1ª revisão anual do

[199] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, anexo VI, p. 95
[200] GOVERNO DOS ESTADOS UNIDOS, Comité permanente sobre a inteligência, *FISA Section 702*, Disponível em: < https://intelligence.house.gov/fisa-702/> Acesso em: 02-03-2018
[201] Para tanto, deverão ser utilizados seletores individuais como número de telefone ou correio eletrónico.

EPP a necessidade da referida autoridade assumir compromissos vinculantes como forma de substancializar as aludidas declarações. [202-203]

O GTA29 também pleiteou a realização de avaliações independentes para averiguar a necessidade e a proporcionalidade das definições dos alvos dos programas de vigilância autorizados no âmbito da aludida secção do FISA, a exemplo do UPSTREAM. [204]

4.6 Mediador para o Escudo de Proteção da Privacidade - Ombudsperson

Com vista a compensar o complexo e incerto sistema dos mecanismos de recurso perante uma corte americana, [205] foi prevista no anexo III da decisão de execução 2016/1250, em carta assinada pelo Secretário de Estado dos EUA, John Kerry, a criação da figura do Mediador para o Escudo de Proteção da Privacidade (MEPP), novo mecanismo de supervisão da ingerência da segurança nacional por meio do qual os governos estrangeiros poderão expressar suas preocupações sobre as atividades de informação de origem eletromagnética dos EUA. [206]

---

[202] GRUPO DE TRABALHO DO ARTIGO 29, *Primeira revisão anual do Escudo da Proteção da Privacidade*, WP 255, adotado em 28 de novembro de 2017, p.3 e p. 15: "*Indeed, the WP29 calls for further evidence or legally binding commitments to substantiate the assertions by the U.S. authorities that the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program*." "*the* ***definition of targets and the tasking of selectors*** *provided for in statute and the corresponding internal procedures and policies mention that U.S. signal intelligence activities under section 702 are "as tailored as feasible", as envisaged in the Presidential Policy Directive 28 (PPD 28)19. However no material evidence to demonstrate this, such as additional examples of categories of selectors, has been provided during the Joint Review*."

[203] Neste sentido, insta destacar a passagem de Lucas Pires Martinho, "Ora estas cartas pretendem vincular as entidades em causa à execução dos princípios de *Privacy Shield*. No entanto, tal declaração não é um instrumento com força de lei. Ou seja, o poder vinculativo destas declarações é reduzido, pois são meras declarações de intenções. Basta que os titulares das direções ou os órgãos políticos superiores da administração norte-americana mudem de posto para que uma nova direção possa dar ordens diferentes da anterior. Visto que o sucesso dos princípios do *Privacy Shield* está dependente da sua efetivação prática por parte dos reguladores, dentro do sistema de auto-certificação, e das autoridades de segurança nacional, coloca-se o problema de saber até que ponto é que estas declarações vão ou não ser cumpridas" Cf. MARTINHO, Lucas Pires, «Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems», *Anuário da Proteção de Dados 2018*. Lisboa: CEDIS, 2018, p. 114

[204]GRUPO DE TRABALHO DO ARTIGO 29, *op cit*, p.3: "*Furthermore, the Privacy and Civil Liberties Oversight Board (PCLOB) should be in a position to prepare and issue an updated report building on the report issued in 2014 further assessing the necessity and proportionality of the definition of "targets" and of the tasking of selectors under section 702 (including in the context of the UPSTREAM program should it be maintained), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this conte*xt."

[205] Para interpor uma ação às cortes americanas, os cidadãos europeus devem demonstrar que sofreram, ou irão sofrer danos diretos ou prejuízos que podem ser remediados. No entanto, nem a secção 702 da FISA nem o EO12333 notificam os titulares dos dados que estes estão a ser objeto de vigilância. Cf. GRUPO DE TRABALHO DO ARTIGO 29, *op cit*, p.4

[206] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (116).

O Mediador detém poderes de supervisão, com competências de investigação, para analisar as queixas individuais que lhe são postas pelos titulares que tenham razões para acreditar que os seus dados foram utilizados de forma indevida pelas agências de segurança nacional americanas.

Ao final de sua análise, o Mediador deverá indicar se a lei americana foi ou não cumprida, e, no caso da não observância à lei, deverá indicar a correção do incumprimento, como forma de garantir uma resposta positiva ao titular dos dados que apresentou a queixa. [207]

Neste sentido, é competência do MEPP avaliar se os dados pessoais transferidos aos EUA foram tratados pelos programas de vigilância daquele país para além das finalidades necessárias e legítimas previstas na lei americana. [208]

Para realização de suas atividades, o Mediador contará com o auxílio de outros órgãos de supervisão dos EUA, [209] fator que facilitará o acesso aos conhecimentos especializados necessários para resolução das queixas. [210]

Os cidadãos europeus poderão apresentar as referidas queixas às autoridades nacionais de proteção de dados, na conveniência de estar em seu próprio país, utilizando sua língua-mãe. As autoridades nacionais, por seu turno, remeterão as aludidas queixas a um organismo centralizado a nível europeu, este então competente a enviar as reclamações ao Mediador. [211]

Por meio da criação desta nova via de recurso, os EUA buscaram afastar uma das críticas ao acordo PS, qual seja a não previsão de mecanismos de recurso que assegurassem a aplicação do direito fundamental a uma proteção jurisdicional efetiva, tal como consagrado no artigo 47º da Carta.

O referido objetivo parece ter surtido efeito, uma vez que, diante de todas as promessas e garantias que envolvem a figura do Mediador, a Comissão concluiu que os EUA passaram a *assegurar uma proteção jurídica eficaz contra as ingerências por parte dos serviços de informações nos direitos fundamentais das pessoas cujos dados são*

[207] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (120).
[208] LINN, Emily, «A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement», *Vanderbilt Journal of Transnational Law*, Vol 50, 2017, p. 1329
[209] A exemplo dos serviços de informações nacionais, dos organismos de supervisão independentes (como os inspetores-gerais).
[210] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (118).
[211] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (119)

transferidos da UE aos EUA. [212] Neste sentido, a Comissão congratulou os avanços do sistema americano no âmbito da proteção dos dados no considerando 112 da Decisão de execução 2016/1250. [213]

> *Globalmente, este mecanismo assegura que as queixas individuais serão investigadas de forma aprofundada e tratadas, e que, pelo menos no domínio da vigilância, se recorra a organismos de supervisão independentes com as competências e os poderes de investigação necessários e um Mediador que possa exercer as suas funções sem quaisquer influências indevidas, especialmente a nível político. Além disso, as pessoas poderão apresentar queixas sem terem de demonstrar, ou mesmo fornecer elementos que indiquem que foram objeto de vigilância. Tendo em conta estes elementos, a Comissão congratula-se por ver que existem garantias adaptadas e eficazes contra os abusos.*

As funções do MEPP serão exercidas por um funcionário do Departamento de Estado dos EUA, o qual deverá atuar de forma independente em relação aos serviços de informação dos EUA, não recebendo, por conseguinte, instruções deste último para o exercício de suas funções. A referida independência, em todo caso, não o impede de atuar em colaboração com outros organismos de supervisão e investigação, conforme explicitado anteriormente neste tópico.

No entanto, o MEPP limitará sua análise à conformidade ou não com a lei americana, de forma que não indicará se o titular dos dados foi alvo dos programas de vigilância dos serviços de inteligência dos EUA.

Até setembro de 2017, quando foi realizada a primeira revisão anual do EPP, [214] ainda não havia sido indicado quem iria assumir permanentemente a posição do Mediador, sendo esta indicação uma das recomendações emitidas pela Comissão para aperfeiçoar a execução do sistema em análise. [215] De acordo com o GTA29, a referida indicação deveria ter sido realizada até o passado dia 25 de maio de 2018. [216]

---

[212] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (123).
[213] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, Considerando (122).
[214] GRUPO DE TRABALHO DO ARTIGO 29, *Primeira revisão anual do Escudo da Proteção da Privacidade*, WP 255, adotado em 28 de novembro de 2017, p.3: "A primeira reapreciação conjunta anual teve lugar em 18 e 19 de setembro de 2017, em Washington, DC. Foi aberta pela Comissária da UE responsável pela Justiça, Consumidores e Igualdade de Género, Věra Jourová, e pelo Secretary of Commerce (equivalente a Ministro do Comércio) dos EUA, Wilbur Ross. Do lado da UE, a reapreciação anual foi conduzida por representantes da Direção-Geral da Justiça e dos Consumidores da Comissão Europeia."
[215] COMISSÃO EUROPEIA, Relatório da Comissão para o Parlamento Europeu e o Conselho sobre a primeira revisão anual sobre o funcionamento do Escudo da Proteção dos dados EU-US, Bruxelas, 18.10.2017, COM (2017) 611 final, p. 6
[216] Até o momento, a Embaixadora Judith G. Garber está a atuar como a Mediadora para o Escudo da Privacidade. No entanto, ainda não foi esclarecido se Garber foi permanentemente apontada para exercer a função em questão.

5. Será o Escudo de Proteção da Privacidade - Privacy Shield suficiente para garantir o nível adequado de proteção dos dados?

Tendo em vista a inegável importância dos fluxos de dados entre os EUA e a UE para o comércio internacional, os representantes dos setores comerciais acolheram o acordo de bom grado, tanto no âmbito americano, como no cenário europeu, especialmente aqueles do ramo da tecnologia da informação e comunicação. [217]

Não obstante o reconhecimento dos melhoramentos introduzidos no âmbito do Escudo de Proteção da Privacidade, este sistema foi recebido de forma bastante cética pelos defensores dos direitos à proteção dos dados e à vida privada, os quais ressaltaram a grande semelhança entre o PS e o EPP, especialmente no que concerne à manutenção das exceções que permitem o afastamento da aplicação dos princípios de proteção dos dados por motivos de segurança nacional, interesse público, e execução da lei.

Como forma de apaziguar as desconfianças e as críticas que poderiam surgir contra as atividades de vigilância dos EUA, o ODNI apresentou garantias de que, se os dados pessoais que foram transferidos àquele país por meio do EPP fossem acessados sob a supracitada exceção, o acesso seria realizado apenas na medida do necessário e estaria sujeito às limitações previstas em lei. A legislação americana pertinente à questão foi explorada pelo ODNI no anexo VI do EPP.

Apesar de congratular as autoridades americanas pela transparência na exposição da legislação aplicável à coleta dos dados pelas agências de segurança dos EUA, o GTA29 notou que a legislação americana não exclui a realização da recolha em larga escala dos dados pessoais provenientes da UE, atividade que não poderia ser considerada necessária e proporcional em uma sociedade democrática. [218 - 219] Diante deste cenário, é difícil concluir

[217] Para maior desenvolvimento, ver SILVA, Heraclides Sequeira dos Santos, *A Proteção de Dados Pessoais na Era Global: O caso Schrems*, Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade Nova de Lisboa em janeiro de 2017, p. 90

[218] GRUPO DE TRABALHO DO ARTIGO 29, *Opinião 01/2016 sobre o rascunho da decisão de adequação do Escudo da Proteção dos Dados – EU – EUA*, adotada em 13 de abril de 2016, WP 238, p.4

[219] Em 11 de janeiro de 108, o Congresso dos EUA reautorizou a secção 702 do FISA por mais seis anos, sem ter em conta as considerações emitidas pela Comissão e pelo GTA 29 na primeira avaliação anual do EPP. PARLAMENTO EUROPEU, Comité de Liberdades Cívicas, Justiça e Assuntos Internos, 2018/2645(RSP), 10 de abril de 2018, p. 5

que a crítica que em grande parte fundamentou a invalidade do PS foi completamente solucionada pelo seu sucessor. [220]

Já no que concerne às vias de recurso, ainda que o EPP tenha desenvolvido novos mecanismos de revisão, o sistema continua complexo, e, em certos casos, de difícil acesso sob a ótica dos cidadãos europeus, fatores que podem tornar as referidas vias ineficazes. [221-222]

Ainda no âmbito dos mecanismos de recurso e supervisão, não obstante os elogios da Comissão, a nova figura do Mediador parece não ser suficientemente independente para exercer suas funções, à luz do artigo 8º da CDFUE, [223] uma vez que este cargo deverá ser exercido por um vice-secretário do Departamento do Estado, além de não serem previstas regras específicas para a destituição deste cargo. [224]

Para além da questão da independência, também é questionado se o Mediador possui os poderes necessários para exercer eficazmente as suas funções, as quais não foram suficientemente detalhadas nem pela carta do Departamento de Estado que prevê a criação desta figura, nem pela decisão de adequação 2016/1250 emitida pela Comissão. Por conseguinte, não se sabe se o MEPP terá acesso direto aos dados coletados, podendo, neste sentido, realizar a sua própria investigação; ou se dependerá dos relatórios produzidos por oficiais do governo americano. [225] Por fim, insta destacar que o EPP não prevê vias de recurso às decisões do mediador.

Já no que concerne aos princípios, por mais que tenha consagrado o princípio da escolha, o EPP reconhece o exercício do direito à oposição apenas em algumas situações específicas. Neste sentido, o GTA29 ressalta que o direito à oposição ao tratamento deve

[220] COMISSÃO EUROPEIA, Relatório da Comissão para o Parlamento Europeu e o Conselho sobre a primeira revisão anual sobre o funcionamento do Escudo da Proteção dos dados EU-US, Bruxelas, 18.10.2017, COM (2017) 611 final, p. 3

[221] MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, Janeiro de 2017, p. 32

[222] GILBERT, Françoise, «WP29: Thumbs Down to Draft EU-US Privacy Shield», *American Law Institute*, Agosto de 2016, p. 46

[223] O artigo 8º, n. 3 da CDFUE, prevê que o cumprimento das regras de proteção de dados pessoais deverá ficar sujeito à fiscalização por parte de uma autoridade independente.

[224] SILVA, Heraclides Sequeira dos Santos, *A Proteção de Dados Pessoais na Era Global: O caso Schrems*, Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade Nova de Lisboa em janeiro de 2017.

[225] GRUPO DE TRABALHO DO ARTIGO 29, *Opinião 01/2016 sobre o rascunho da decisão de adequação do Escudo da Proteção dos Dados – EU – EUA*, WP 238, adotada em 13 de abril de 2016, p. 50

ser oferecido sempre que o titular dos dados tenha motivos legítimos para tanto, não devendo ter o seu exercício restrito a casos específicos.

As referidas críticas levam a crer que, por mais que tenha introduzido um quadro de proteção de dados mais adequado do que seu predecessor, o EPP ainda não consagra um nível de proteção essencialmente equivalente àquele garantido pelo direito da UE. [226]

Nas palavras do Supervisor Europeu de Proteção dos Dados, Giovanni Buttarelli, o EPP é um instrumento provisório que deve ser utilizado até que seja desenvolvido um sistema de proteção mais robusto. [227]

6. Escudo da Proteção da Privacidade- Privacy Shield e RGPD

De acordo com o artigo 45º do RGPD, a decisão que reconheceu a adequação do nível de proteção dos dados do EPP continuará válida até que seja alterada, substituída ou revogada por outra decisão da Comissão, razão pela qual as organizações autocertificadas não deverão preocupar-se com uma mudança no *status* de validade do EPP como consequência direta do início da aplicação do RGPD.

No entanto, em conformidade com as considerações do TJUE no caso *Schrems*, o RGPD estabelece à Comissão a obrigação de acompanhar a eficácia das decisões adotadas com base no artigo 25º, n. 6 da Diretiva,[228] e, assim, revisar periodicamente as decisões de adequação que por esta entidade foram emitidas, ao menos de 4 em 4 anos. Destarte, a decisão que reconheceu a adequação do PS deverá ser revista o mais tardar até o ano de 2022.

Neste sentido, insta ressaltar que, quando da realização da reavaliação, a Comissão deverá ter como base os critérios de avaliação de adequação do nível de proteção dos dados estabelecidos no artigo 45º do RGPD, os quais são mais abrangentes e rigorosos do que aqueles previstos no artigo 25º da antiga diretiva, conforme analisado no capítulo precedente.

---

[226] GRUPO DE TRABALHO DO ARTIGO 29, *Opinião 01/2016 sobre o rascunho da decisão de adequação do Escudo de Proteção da Privacidade – EU – EUA*, WP 238, adotada em 13 de abril de 2016, p. 7: "*24. Is concerned as to whether the current Privacy Shield arrangement provides the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the European Court of Justice*."

[227] STUPP, Catherine, *EU privacy watchdog: Privacy shield should be temporary*, Disponível em: < https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/> Acesso em: 03/06/2018

[228] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (106).

Em todo caso, o próprio EPP estabelece um mecanismo de revisão anual conjunta, [229] de forma que a próxima avaliação deverá ser realizada ainda no ano de 2018, sendo esta a segunda revisão anual do referido sistema. [230]

Não obstante os avanços em matéria de proteção dos dados alcançados pelo EPP, este sistema ainda herda uma série de falhas do acordo precedente, o que fundamenta a alegação de que o EPP não assegura um nível de proteção essencialmente equivalente àquele consagrado na UE, a despeito da decisão da Comissão que assegura o contrário.

Destarte, é possível que ativistas ou até mesmo uma das autoridades nacionais de controlo dos Estados-Membros questionem a validade do EPP [231] antes mesmo que a Comissão realize a reavaliação da decisão que assegurou a adequação do nível de proteção deste sistema. [232]

Esta suposição é corroborada pela emissão de pareceres e opiniões tanto do Parlamento Europeu quanto do Grupo de Trabalho do Artigo 29. Em seu relatório sobre a primeira análise anual do EPP, o referido grupo ressaltou que se as falhas deste acordo persistirem até a segunda avaliação anual, a ser realizada ainda no ano de 2018, o próprio GTA29 iria adotar as medidas necessárias para sanar as referidas falhas, o que pode incluir acionar os tribunais nacionais para que estes questionem a pertinência da adequação da decisão 2016/1250 ao TJUE, tornando o futuro do EPP consideravelmente incerto. [233]

Neste sentido, o Comité de Liberdades Cívicas, Justiça e Assuntos Internos do Parlamento Europeu indicou que a Comissão e as autoridades competentes devem elaborar o quanto antes um plano de ação para solucionar os óbices do EPP, ao mesmo passo em

---

[229] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Considerando (147): "Para realizar a reapreciação conjunta anual a que se referem os anexos I, II e VI, a Comissão reunirá com o *Department of Commerce* e a FTC, acompanhados, se adequado, de outros departamentos e serviços envolvidos na aplicação das disposições do Escudo de Proteção da Privacidade, bem como, no que se refere a questões relativas à segurança nacional, representantes do ODNI, outros elementos do setor das informações e o Mediador. A participação nesta reunião será aberta às APD da UE e aos representantes do grupo de trabalho do artigo 29º."

[230] Primeira revisão anual do *Privacy Shield* ocorreu em setembro de 2017, tendo a Comissão concluído que o referido sistema ainda apresenta um nível adequado de proteção dos dados, não obstante tenha reconhecido alguns pontos falhos no acordo. COMISSÃO EUROPEIA, Relatório da Comissão para o Parlamento Europeu e o Conselho sobre a primeira reapreciação anual do funcionamento do Escudo de Proteção da Privacidade UE-EUA, Bruxelas, 18.10.2017, COM (2017) 611 final

[231] As autoridades de controlo nacional podem acionar as cortes nacionais para que estas questionem a validade do EPP junto ao TJUE.

[232] O TJUE já recebeu duas ações que puseram em questão a validade do EPP, a saber: Digital Rights Ireland v Commission (Processo T-670/16) e La Quadrature du Net e o./Comissão (Processo T-738/16).

[233] GRUPO DE TRABALHO DO ARTIGO 29, *Primeira revisão anual do Escudo da Proteção da Privacidade*, WP 255, adotado em 28 de novembro de 2017

que demonstrou o receio de que o atual enquadramento do sistema pode não oferecer o nível de proteção requerido à luz do direito europeu. [234]

Em todo caso, ainda que o EPP venha a ser declarado inválido, ou que a decisão de adequação seja revogada pela Comissão quando da realização da reavaliação neste ou nos próximos 4 anos, o fluxo de dados pessoais entre a UE e os EUA poderá continuar a ser realizado com base nos demais instrumentos reconhecidos pelo RGPD, a exemplo das garantias adequadas previstas no artigo 46º, como as cláusulas contratuais-tipo e as regras vinculativas para empresas, ou, em último caso, das derrogações previstas no artigo 49º, como é o caso do consentimento explícito do titular dos dados.

7. Transferências de dados entre UE- EUA com base nas cláusulas contratuais-tipo

Ainda que figure no artigo 46º do RGPD como uma das garantias adequadas à realização das transferências de dados para um país terceiro, as cláusulas contratuais-tipo podem não ser o instrumento mais seguro, no momento, para fundamentar as transferências de dados pessoais entre a UE e os EUA.

Isto porque a aludida garantia está a ter a sua validade questionada pela autoridade de proteção dos dados da Irlanda, a qual foi acionada pelo mesmo autor da ação que culminou na invalidação do PS, Maximillian Schrems. Diante da invalidação do PS, Schrems reformulou sua queixa à autoridade de proteção de dados irlandesa para indicar a persistência da inadequação do nível de proteção dos dados oferecida nos EUA aos dados pessoais que eram transferidos da UE àquele país, desta vez com base nas cláusulas-tipo.

Não obstante a invalidação do PS, a transferência dos dados pessoais entre a UE e os EUA continuava a poder ser realizada por meio da utilização das aludidas cláusulas. Destarte, uma vez transferidos aos EUA, os dados pessoais dos cidadãos europeus continuavam a poder ser acessados por meio dos programas de vigilância em massa conduzidos por autoridades americanas, sem que existisse um remédio judicial por meio do qual os titulares pudessem adotar as medidas necessárias para proteção dos seus dados.

Schrems ressaltou que o artigo 4º das decisões da Comissão que adotam as cláusulas-tipo (2001/497/EC, 2010/87/UE) prevê a possibilidade de os EM proibirem ou

[234] PARLAMENTO EUROPEU, Comité de Liberdades Cívicas, Justiça e Assuntos Internos, 2018/2645(RSP), 10 de abril de 2018, p. 8

suspenderem o fluxo de dados para países terceiros, a fim de proteger as pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos em que a lei a que o importador de dados está sujeito lhe imponha o dever de não observar as regras pertinentes de proteção de dados, e tal exigência ultrapasse as restrições necessárias ao funcionamento de uma sociedade democrática. [235]

Ora, no caso em questão, a lei americana obriga o *Facebook Inc* [236] a tornar disponíveis os dados pessoais de seus utentes a algumas autoridades americanas, a exemplo da NSA e do *Federal Bureau of Investigation* (FBI). A vigilância e a coleta em larga escala dos referidos dados pessoais, sem previsão de remédios judiciais aos seus titulares, constituiria, portanto, uma violação aos artigos 7º, 8º e 47º da Carta.

Neste sentido, a autoridade irlandesa acionou o Supremo Tribunal daquele país para que este questionasse o TJUE sobre a validade das decisões da Comissão que adotam as cláusulas-tipo, quais sejam as decisões 2001/497/EC, 2004/915/EC, 2010/87/UE, à luz dos artigos 7º, 8º e 47º da Carta.

Em 12 de abril de 2018, a juíza da Suprema Corte da Irlanda, Caroline Costello, emitiu ao TJUE onze questões prejudiciais sobre a validade das aludidas decisões da Comissão.[237] Aguarda-se o posicionamento do TJUE.

[235] COMISSÃO EUROPEIA, Decisão 2001/497/EC, artigo 4º, 1; e Decisão 2010/87/UE, artigo 4º, 1.
[236] Ainda que a queixa de Maximiliam Schrems diga respeito à utilização dos seus dados pelo *Facebook*, a invalidação das decisões que adotam as cláusulas contratuais-tipo afetaria todas as transferências aos EUA fundamentadas nesta garantia.
[237] SUPREMO TRIBUNAL DE JUSTIÇA DA IRLANDA, *The Data Protection Commisioner e Facebook Ireland e Maximilian Schrems*, Processo n. 2016 4809P, Disponível em: < https://www.alstonprivacy.com/wp-content/uploads/2018/04/ref.pdf> Acesso em: 14/05/20108

CAPÍTULO IV – TRANSFERÊNCIAS DE DADOS ENTRE A UNIÃO EUROPEIA E O CANADÁ

A União Europeia é o segundo maior parceiro comercial do Canadá, estando atrás apenas dos Estados Unidos. [238] Tão somente no ano de 2016, as trocas comerciais em bens entre a UE e o Canadá ultrapassaram os 64 mil milhões de euros, ao passo em que no ano de 2015, as trocas comerciais em serviços rondavam a casa dos 30 mil milhões de euros. [239]

Como resultado dessa próspera relação comercial, foi assinado o Acordo Económico e Comercial Global (CETA - *Comprehensive Economic and Trade Agreement*), acordo de livre comércio entre a União Europeia e o Canadá que prevê a quase eliminação de direitos aduaneiros de uma série de produtos comercializados entre as partes do CETA, fator que representará uma economia estimada em 590 milhões de euros às empresas europeias. [240]

Após a ratificação do aludido acordo pelos Estados-Membros da UE, espera-se que ocorra uma intensificação das trocas comerciais entre o Canadá e a referida União como consequência natural dos benefícios introduzidos pelo CETA.

É sabido que, na atual sociedade da informação, os dados pessoais constituem uma das mais importantes moedas do mercado digital, e a sua importância não seria diferente no âmbito das trocas comerciais entre a União Europeia e o Canadá.

Por conseguinte, espera-se que a intensificação das trocas comerciais entre o Canadá e a UE reflita, de igual modo, na intensificação do fluxo de dados entre as partes contratantes do CETA.

No entanto, para que as aludidas transferências sejam realizadas, é preciso que as entidades europeias e canadianas atuem em conformidade com as regras concernentes à

[238] STATISTICS CANADA, *Imports, exports and trade balance of goods on a balance-of-payments basis, by country or country grouping*, Disponível em: <http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/gblec02a-eng.htm>. Acesso em: 01/04/2018
[239] COMISSÃO EUROPEIA, *Guide to the Comprehensive Economic and Trade Agreement (CETA)*, Luxemburgo: Escritório de Publicações da União Europeia, 2017, p. 5
[240] *Ibid*., p. 6

transferência de dados entre a UE e países terceiros, as quais foram analisadas na primeira parte deste trabalho.

Neste capítulo, analisar-se-á como as referidas regras serão aplicadas para regular as transferências de dados pessoais entre a União Europeia e o Canadá. No primeiro tópico, serão abordadas as leis canadianas em matéria de proteção de dados, de forma a contextualizar a análise que se seguirá sobre as transferências dos dados pessoais àquele país. Em seguida, discorrer-se-á sobre a decisão de adequação parcial emitida pela Comissão Europeia ao Canadá em 2001 (2002/2/CE), [241] sendo realizada uma análise sobre a pertinência ou não de sua adequação à luz do RGPD.

1. Quadro legal canadiano referente à proteção dos dados

A legislação canadiana em matéria de proteção de dados está divida em 4 principais instrumentos, sendo o de maior relevância O *Personal Information Protection and Electronic Documents Act* (PIPEDA), o qual consiste em uma lei federal aplicável *às organizações do setor privado que recolhem, utilizam ou divulgam dados pessoais no exercício das suas atividades comerciais.* [242-243]

Em todo caso, para garantir a autonomia das províncias canadianas legislarem sobre as matérias de sua competência, o PIPEDA prevê na secção 26(2) a possibilidade da não aplicação do seu texto nas províncias que possuem legislação em matéria de proteção dos dados substancialmente semelhante à referida lei federal. Assim ocorre nas províncias da Colúmbia Britânica, Alberta, e do Québec, nas quais a aplicação do PIPEDA restringe-se aos setores cuja regulação é de competência federal exclusiva, a exemplo do bancário, transportes e telecomunicações. [244-245]

---

[241] COMISSÃO EUROPEIA, Decisão da Comissão de 20 de Dezembro de 2001 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos (Personal Information and Electronic Documents Act) [notificada com o número C(2001) 4539] (2002/2/CE)]

[242] Decisão 2002/2/CE, Considerando (5).

[243] Por atividades comerciais, entende-se "*any transaction or any regular course of conduct that is of a commercial character including the selling, battering or leasing of donor, membership of other fund-raising lists.*" Cf. GRUPO DE TRABALHO DO ARTIGO 29, *Opinião 2/2001 sobre a adequação do canadiano PIPEDA*, adotada em 26 de janeiro de 2001, WP39, p. 3

[244] Alberta - *Personal Information Protection Act* (PIPA Alberta); Colúmbia Britânica - *Personal Information Protection Act* (PIPA British Columbia); e *Privacy Act* do Québec.

Essa exoneração, todavia, não é absoluta. As organizações e entidades que se encontrem nas referidas províncias apenas estarão isentas da aplicação do PIPEDA nas transações que ocorram no interior da província na qual se encontram.

Destarte, a aplicação do PIPEDA subsiste nas províncias acima referidas quando da realização das atividades de tratamento ou transferências de dados internacionais e interprovinciais realizadas pelas organizações que estão sujeitas à lei em questão.

Já no âmbito do setor público, o *Privacy Act* de 1983 é a lei federal canadiana que regula o tratamento dos dados pessoais por órgãos governamentais federais. De acordo com a referida lei, os dados pessoais apenas devem ser tratados pelas entidades governamentais na medida em que exista uma relação direta com a política ou atividade da entidade em questão. [246]

O Escritório do Comissário para a Proteção da Vida Privada *(Office of the Privacy Comissioner of Canada)* é a entidade canadiana responsável pela supervisão da conformidade da aplicação tanto do *Privacy Act* como do PIPEDA.

2. Decisão de adequação 2002/2/CE

Em dezembro de 2001, a Comissão Europeia emitiu a decisão de adequação 2002/2/CE, a qual reconheceu que o PIPEDA oferece um nível adequado de proteção aos dados pessoais. A partir de então, as transferências destes dados entre a União Europeia e o Canadá passaram a poder ser realizadas sem que os exportadores de dados tivessem que utilizar garantias adicionais.

No entanto, a aludida decisão de adequação é apenas parcial, uma vez que o PIPEDA aplica-se apenas às entidades do setor privado que desenvolvam atividades comerciais. Os exportadores que desejarem transferir dados pessoais desde a UE às demais

---

[245] DIVISÃO DA SOCIEDADE DA INFORMAÇÃO, *Anexo à resposta ao Ofício nº 259/2015/GAB-SAL-MJ (Processo nº 08027.000032/2015-11)*, Informações recebidas de Embaixadas do Brasil no exterior, Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/18-Canad%C3%A1.pdf>. Acesso em: 03/05/2018

[246] DIVISÃO DA SOCIEDADE DA INFORMAÇÃO, *Anexo à resposta ao Ofício nº 259/2015/GAB-SAL-MJ (Processo nº 08027.000032/2015-11)*, Informações recebidas de Embaixadas do Brasil no exterior, Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/18-Canad%C3%A1.pdf>. Acesso em: 03/05/2018

entidades e organizações canadianas que não estão sujeitas ao PIPEDA deverão, portanto, adotar as medidas pertinentes para garantir um nível de proteção adequado dos dados em questão. Como exemplo, podem valer-se das cláusulas contratuais-tipo e das regras vinculativas aplicáveis às empresas.

2.1 Pertinência da adequação

A decisão de adequação 2002/2/CE foi emitida pela Comissão Europeia em dezembro de 2001, em uma sociedade que muito destoa da atual. Nesta última década, assistiu-se a um desenvolvimento tecnológico sem precedentes, que alterou significativamente a forma pela qual os dados pessoais são coletados e tratados.

A internet, as inovações tecnológicas e a globalização tornaram possível a coleta, o compartilhamento, e o armazenamento de dados em um nível significativamente superior àquele permitido pela tecnologia existente no começo dos anos 2000.

Além do desenvolvimento tecnológico, a própria sociedade tornou-se mais propensa à divulgação dos seus dados pessoais, seja enquanto usuários de redes sociais ou como consumidores do mercado digital.

Ora, o Direito existe para regular a sociedade, e, se esta se altera de forma significativa, as leis devem acompanhar e regular esta mudança. Caso contrário, tornar-se-ão obsoletas.

O quadro jurídico da União Europeia referente à proteção dos dados pessoais, especificamente a Diretiva 95/46/CE, já não condizia com a realidade da atual sociedade da informação, um dos motivos pelo qual foi proposta a reforma em matéria de proteção dos dados, a qual é composta pelo Regulamento Geral sobre a Proteção de Dados (RGPD) e pela Diretiva de Cooperação Policial. [247]

No que concerne ao cenário canadiano, sancionado em 2000, o PIPEDA parece não estar a acompanhar o aludido desenvolvimento tecnológico de forma satisfatória, existindo

[247] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, JO L 119 de 4.5.2016.

um considerável descompasso entre a lei canadiana e o direito europeu, a despeito das emendas realizadas à lei federal em análise.

Não obstante a aparente desatualização do PIPEDA, as decisões de adequação emitidas sob a vigência da Diretiva 95/46/CE continuarão em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com os requisitos previstos no RGPD. [248]

Conforme discutido em tópico anterior, o aludido regulamento estabelece a necessidade da realização de uma avaliação periódica das decisões de adequação como forma de averiguar a manutenção da aludida adequação diante dos desenvolvimentos pertinentes no país terceiro, pelo menos de quatro em quatro anos.

Por conseguinte, a decisão de adequação do Canadá deverá ser reavaliada nos próximos quatro anos, e só continuará em vigor se assim entender a Comissão Europeia, por meio da emissão de uma decisão adotada em conformidade com os requisitos previstos no RGPD.

Diante deste cenário, questiona-se se a adequação que o PIPEDA ostentava há mais de uma década ainda estará presente nos dias atuais, face aos novos requerimentos previstos no RGPD e aos desenvolvimentos que ocorreram no quadro legal e político canadiano.

2.1.1 Requisitos mais rigorosos

Antes da emissão de uma decisão de adequação, a Comissão deve realizar uma análise global do quadro jurídico do país terceiro que almeja gozar a aludida decisão, de forma a identificar se os direitos dos titulares dos dados e as obrigações daqueles que estão envolvidos no tratamento são suficientes para garantir um adequado nível de proteção aos dados em questão.

Tanto a Diretiva 95/46/CE como o RGPD preveem listas não exaustivas que indicam os elementos que deverão ser analisados pela Comissão quando da avaliação da adequação do nível de proteção do país terceiro.

[248] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 45º, 9.

A decisão de adequação parcial do Canadá foi emitida em 2001, período no qual ainda estava em vigor a Diretiva 95/46/CE. Por conseguinte, os requisitos utilizados para avaliar a adequação da legislação canadiana foram aqueles previstos na referida diretiva, mais especificamente em seu artigo 25º, números 2 e 6.

Segundo a aludida diretiva, a adequação do nível de proteção dos dados poderia ser constatada após a análise de todas as circunstâncias que influenciassem a transferência dos dados, a exemplo da natureza destes, da finalidade e da duração do tratamento, dos países de origem e de destino final, das regras de direito em vigor no país terceiro, e regras profissionais e medidas de segurança que são respeitadas no país. A Comissão ainda deveria ter em conta a legislação interna do país terceiro, nesta incluída a inserção ou não dos princípios da proteção dos dados, devendo ser igualmente analisados os compromissos internacionais do país terceiro. [249]

No entanto, após as revelações de Edward Snowden e a invalidação do "Porto Seguro" pelo TJUE no caso *Schrems*, constatou-se a necessidade não só da realização de avaliações periódicas, como também da adoção de requisitos mais rigorosos e abrangentes quando da análise da aludida decisão de adequação.

Neste sentido, para determinar a adequação do nível de proteção de dados do país terceiro, o RGPD estabelece que a Comissão deve realizar uma análise global das práticas e do ordenamento jurídico vigente no país terceiro, incluindo, neste âmbito, o exame da existência e efetividade do primado do Estado de direito, do respeito pelos direitos humanos e liberdades fundamentais; bem como dos compromissos internacionais e da participação em sistemas multilaterais ou regionais.

Ainda neste sentido, o artigo 45º do RGPD estabelece que a Comissão deverá avaliar as legislações pertinentes e vigentes no país terceiro, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, além do quadro legal respeitante ao acesso das autoridades públicas a dados pessoais – concretizando, de certa forma, a previsão genérica da Diretiva 95/46/CE referente à necessidade de avaliar a legislação interna, geral ou setorial, em vigor no país terceiro.

[249] Por exemplo, a ratificação da Convenção 108.

Para garantir a efetividade dos direitos e liberdades dos titulares dos dados, deve ainda ser aferido se a legislação do país terceiro prevê a existência de autoridades que supervisionem a aplicação dos instrumentos que garantem os direitos dos titulares dos dados, e que ofereçam suporte a estes quando seus direitos tenham sido violados. [250]

Percebe-se, portanto, que a avaliação da adequação a ser conduzida pela Comissão com base no artigo 45º do RGPD é bem mais rigorosa e abrangente do que aquela prevista na antiga diretiva, e será com base nestes requisitos que a Comissão irá reavaliar a adequação das decisões que foram emitidas durante a vigência da Diretiva de 1995, como é o caso do PIPEDA. Como observa Daniel Therrien, o Comissário de Privacidade do Canadá [251]

> *Canada's adequacy status is 'partial', in that it covers only PIPEDA, and that all future adequacy decisions will involve a comprehensive assessment of a country's privacy regime, including access to personal data by public authorities for law enforcement, national security, and other public interest purposes*.

Por conseguinte, na reavaliação da decisão de adequação de 2001, que abrange apenas o PIPEDA, deverá ser realizada uma análise extensiva do ordenamento jurídico canadiano relativo à proteção dos dados e à privacidade, incluindo, como dito acima, as leis canadianas concernentes à defesa, à segurança nacional, e ao acesso das autoridades públicas a dados pessoais.

3. Lei de segurança nacional canadiana

Conforme exposto em tópico precedente, as revelações de Edward Snowden e as implicações do caso *Schrems* determinaram a aplicação de requisitos mais rigorosos e abrangentes não só à avaliação da adequação do nível de proteção daqueles que desejam receber dados provenientes da União Europeia, como também à reavaliação das decisões de adequação já emitidas.

---

[250] GRUPO DE TRABALHO DO ARTIGO 29, *Transferências de dados pessoais para países terceiros: Aplicação do artigo 25 e 26 da Diretiva de proteção de dados da UE*, WP12, adotado em 24 de julho de 1998.

[251] CÂMARA DOS COMUNS DO CANADÁ, Comitê sobre o Acesso à Informação, Privacidade e Ética, 1ª Seção, 42nd Parliament, 16 Feveireiro de 2017, 1540 (Daniel Therrien)

De acordo com o Comissário de Privacidade do Canadá, Daniel Therrien, diante deste cenário, a avaliação da adequação do nível de proteção dos dados deve ser realizada tendo em consideração não só as regras de proteção dos dados pessoais na esfera comercial, como também a forma pela qual os mencionados dados são protegidos pela legislação e pelas práticas do país terceiro no que concerne à segurança nacional e à execução da lei.

> *The Schrems decision, of course, demands a more holistic approach to adequacy than what was in force when Canada's PIPEDA was determined "adequate". Now, adequacy is not limited to a consideration of rules that protect personal data in the commercial sphere—one must also carefully consider how rights are protected by laws and practices related to national security and law enforcement.* [252]

De acordo com os requisitos supracitados, entende-se que o Canadá não encontraria dificuldades em comprovar a adequação do nível de proteção dos dados pessoais tendo como base o elemento do primado do Estado de direito e do respeito aos direitos humanos.

No entanto, a sua legislação referente à segurança pública e ao acesso das autoridades públicas aos dados pessoais poderá ser um óbice à renovação da decisão de adequação, caso nada seja feito para afastar os dispositivos que ameaçam a proteção dos dados pessoais no país em questão.

Em 2015, enfrentando forte oposição de ativistas e de organizações não governamentais defensoras dos direitos à privacidade e à proteção dos dados, o Canadá aprovou a Lei Antiterrorismo de 2015 (antigo projeto de lei C-51/ *Bill* C-51), [253] instrumento que alargou consideravelmente os poderes da agência de espionagem do Canadá (CSIS- *Canadian Security Intelligence Service*), bem como de instituições e departamentos do governo daquele país, sob o pretexto da luta contra o terrorismo.

A secção 3 da parte 1 da referida lei prevê que seu objetivo é encorajar e facilitar o compartilhamento de informações entre instituições do Governo do Canadá, atividade

[252] THERRIEN, Daniel, *Remarks at the Privacy Laws and Business International Conference*, 5 de julho, 2016, Cambridge, Reino Unido. Disponível em:< https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160705/> Acesso em: 03/04/2018

[253] Apresentada durante o Governo do conservador Stephen Harper, a Lei Antiterrorismo de 2015 tanto inclui novas legislações, como emenda instrumentos jurídicos já existentes, a exemplo do Código Penal canadiano. A primeira parte da referida lei introduz o *Security of Canada Information Sharing Act* (SCISA), sendo esta uma das secções mais criticadas da legislação em análise.

realizada no intuito de proteger este país contra qualquer prática que ponha em risco a sua segurança. [254]

Neste cenário, 17 agências e departamentos do governo do Canadá responsáveis pelo exercício de funções relativas à segurança pública passaram a poder receber fluxos de informações sobre cidadãos canadianos, desde que estas fossem consideradas relevantes à segurança nacional.

No entanto, a lei em questão desenvolveu uma definição tão ampla [255] do conceito de "segurança nacional" que tornou possível a coleta, análise e compartilhamento dos dados de qualquer canadiano, não estando esta atividade restrita apenas aos dados dos suspeitos de envolvimento em atividades terroristas. Nas palavras do Comissário de Privacidade do Canadá, Daniel Therrien, [256]

> *The scale of information-sharing between government departments and agencies proposed in this bill is unprecedented. The new powers that would be created are excessive and the privacy safeguards proposed are seriously deficient. All Canadians – not just terrorism suspects – will be caught in this web. Bill C-51 opens the door to collecting, analyzing and potentially keeping forever the personal information of all Canadians in order to find the virtual needle in the haystack.*

Para agravar este cenário, a lei em questão não prevê instrumentos que assegurem a proteção dos cidadãos canadianos cujos dados estão a ser compartilhados, nem mesmo institui mecanismos efetivos para supervisionar as referidas atividades de compartilhamento.

---

[254] CANADÁ, LEI ANTITERRORISMO, 2015, Disponível em: <http://lawslois.justice.gc.ca/eng/AnnualStatutes/2015_20/page-1.html#h-2>. Acesso em: 07/05/2018: "*PURPOSE AND PRINCIPLES*
3. The purpose of this Act is to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."

[255] O conceito de "informação relevante à segurança nacional" é a definição mais ampla de segurança já codificada na lei canadiana. Cf. ROACH, Kent; FORCESE, Craig, «Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience», *DesLibris*, v. II, Fevereiro de 2015, p. 7

[256] THERRIEN, Daniel, *Without big changes, Bill C-51 means big data*, The Globe and Mail, Disponível em: < https://www.theglobeandmail.com/globe-debate/without-big-changes-bill-c-51-means-big-data/article23320329/>. Acesso em: 03/05/2018. No mesmo sentido, AUSTIN, Lisa M; GOOLD, Benjamin J, *How C-51 undermines privacy*, National Post, 30 de março de 2015, Disponível em: <http://nationalpost.com/opinion/how-c-51-undermines-privacy>. Acesso em 01/06/2018: "*low test of relevance to the recipient's responsibilities, coupled with unrestricted disclosure and a broad definition of national security that goes far beyond terrorism, potentially sweeps up a vast amount of information about people who are not suspected of anything*".

A Lei Antiterrorismo foi alvo de fortes críticas não só no cenário canadiano, como também no cenário internacional. Neste sentido, o Comité de Direitos Humanos da Organização das Nações Unidas ressaltou a ameaça que a lei em questão apresenta à proteção dos dados ao permitir a vigilância em massa e o aludido compartilhamento dos dados pessoais, sem prever garantias suficientes que assegurem os direitos dos seus titulares. [257]

> *10. The Committee takes note of the State party's need to adopt measures to combat acts of terrorism, including the formulation of appropriate legislation to prevent such acts. However, the Committee is concerned about information according to which: a) Bill C-51 amendments to the Canadian Security Intelligence Act confers a broad mandate and powers on the Canadian Security Intelligence Service (CSIS)* ***to act domestically and abroad,*** *thus potentially resulting in* ***mass surveillance*** *and* ***targeting activities*** *that are protected under the Covenant* ***without sufficient and clear legal safeguards****; b) Bill C-51 creates under the Security of Canada Information Sharing Act, an increased sharing of information among federal government agencies on the basis of a* ***very broad definition of activities*** *that undermine the security of Canada which does not fully ensure that inaccurate or irrelevant information is shared ; […]. The Committee is also concerned about* ***the lack of adequate and effective oversight mechanisms*** *to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities (arts. 2, 14, 17, 19, 20, 21, 22).*(Grifos meus)

Como forma de apaziguar as aludidas críticas à Lei Antiterrorismo, foi proposto o *National Security Act 2017* (projeto de lei C-59/*Bill* C-59),[258]cujo objetivo é mitigar as falhas da referida lei federal, introduzindo no ordenamento do aludido país medidas que fortaleçam a segurança nacional sem comprometer os direitos e liberdades dos canadianos. [259]

Ainda que seja considerado um avanço face ao seu predecessor, o *Bill* C-59 não só mantém algumas das referidas previsões que podem pôr em risco o direito à proteção dos dados dos canadianos, nomeadamente o compartilhamento de dados pessoais entre agências governamentais, ainda que estes dados não sejam relevantes à segurança nacional;

---

[257] COMITÉ DE DIREITOS HUMANOS DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS, *Human Rights Committee discusses the report of Canada*, Disponível em: <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16215&LangID=E>. Acesso em: 04/05/2018.

[258] Durante as eleições canadianas de 2015, a introdução de uma nova legislação que afastasse os pontos problemáticos da Lei Antiterrorismo era uma das promessas do então candidato do Partido Liberal, Justin Trudeau, atual Primeiro-ministro do Canadá.

[259] O projeto de lei em questão ainda tenta desenvolver um conceito mais conciso de "segurança nacional", como forma de diminuir o âmbito de compartilhamento das informações sobre os cidadãos canadianos entre as entidades governamentais.

como também atribui novas competências à *Communications Security Establishment* (CSE), agência de criptografia canadiana.

Neste sentido, o *Bill* C-59 permite que o CSE colete e analise dados pessoais acessíveis ao público, ou que tenham sido tornados públicos, podendo ser o titular dos aludidos dados tanto canadianos como qualquer outro indivíduo que se encontre no Canadá.

De acordo com a primeira leitura do *Bill* C-59, [260] o *Communications Security Establishment Act* define "informação disponível ao público" como informações que foram divulgadas ou partilhadas para consumo público, informações acessíveis ao público em uma estrutura de informação global (como a Internet) ou ainda as informações disponíveis ao público através de uma requisição, subscrição ou aquisição.

Com base nesta previsão genérica, o CSE teria poderes não só para analisar dados que houvessem sido ilegalmente publicados, como também para comprar bases de dados obtidos de forma ilegal, fator que poderia incentivar a criação de um mercado de coleta e posterior venda de dados pessoais ao Governo do Canadá. [261]

Diante das críticas direcionadas a esta previsão, na segunda leitura do *Bill* C-59, realizada em maio deste ano (2018), foi introduzida uma emenda à referida definição de "informação disponível ao público", a qual passou a prever que não serão abrangidas pelo aludido conceito de informação pública as informações a respeito das quais os canadianos ou as pessoas que se encontrem no Canadá tenham uma expectativa razoável de privacidade. A definição de "informação disponível ao público" foi mantida pela terceira leitura do projeto de lei na Câmara dos Comuns do Canadá, a qual foi realizada em 19 de junho de 2018. Ainda não se sabe se como esta previsão será interpretada, nem mesmo se será mantida nas próximas leituras do projeto de lei em estudo.

[260] Realizada em 20 de junho de 2017.
[261] KENYON, Miles, *Joint Letter Concerning Bill C-59, National Security, and Human Rights,* 19 de setembro de 2017, Disponível em: <https://citizenlab.ca/2017/09/joint-letter-concerning-bill-c-59/> Acesso em: 22-05-2018.

O *Bill*-C59 ainda está nas primeiras fases do processo legislativo. [262]As disposições que mantém as ameaças aos direitos da proteção de dados estão a ser novamente criticadas, e a pressão para que estas sejam alteradas de forma a oferecer um maior nível de proteção aos dados pessoais continua intensa.

Em março do presente ano (2018), o Comissário de Privacidade do Canadá, Daniel Therrien, emitiu duas cartas ao Comité da Segurança Pública e da Segurança Nacional da Câmara dos Comuns daquele país a recomendar alterações no texto do projeto de lei com vista a afastar os dispositivos que apresentam riscos à proteção dos dados pessoais dos canadianos. [263]

4. Divergências entre o PIPEDA e o RGPD

Para que um país terceiro esteja em condições de receber uma decisão de adequação, não é necessário que a sua legislação seja uma cópia fiel da legislação da UE em matéria de proteção dos dados. De acordo com as conclusões do TJUE no caso *Schrems*, o nível de proteção dos dados será adequado se for essencialmente equivalente àquele consagrado na UE.

Ao analisar o quadro jurídico canadiano, todavia, percebe-se que as leis de proteção de dados daquele país, nestas incluído o PIPEDA, não consagram alguns dos direitos dos titulares dos dados previstos no RGPD, a exemplo do direito ao esquecimento e do direito à portabilidade, bem como não preveem certas obrigações do responsável pelo tratamento, a exemplo da proteção desde a conceção e por defeito. [264]

---

[262] O projeto de lei C-59 passou por três leituras na Câmara dos Comuns, sendo a primeira delas realizada em 20 de junho de 2017, a segunda em 11 de junho de 2018, e a terceira em 19 de junho de 2018. No momento da escrita desta dissertação, o projeto de lei encontrava-se no Senado do Canadá.

[263] THERRIEN, Daniel, *Submission to the Standing Committee on Public Safety and National Security regarding the review of Bill C-59, An Act Respecting National Security Matters*, Disponível em: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_sub_180305/> Acesso em: 23-05-2018

[264] ZIMMER, Bob, *Towards Privacy by Design: Review of The Personal Information Protection and Eletronic Documents Act*, Report Of The Standing Committee On Access To Information, Privacy And Ethics, Fevereiro de 2018, p. 62: "*The GDPR contains some provisions that did not appear in the current Directive and also do not appear in PIPEDA, such as data portability, data erasure, and privacy by design and default*."

A maior discrepância entre os textos, todavia, refere-se à falta de poderes de execução do Comissário da Privacidade canadiano em comparação às prerrogativas das autoridades de controlo consagradas no RGPD. Isto porque a aludida autoridade canadiana não possui a capacidade de emitir, diretamente, ordens vinculantes, nem mesmo possui o poder de aplicar coimas pecuniárias para penalizar as entidades que violem o texto do PIPEDA, fator que pode contribuir para a diminuição da eficácia de suas instruções.

O RGPD, por seu turno, atribui às autoridades de controlo a possibilidade de aplicação de coimas pecuniárias em montantes que podem alcançar até 20 mil milhões de euros, ou 4% do volume dos negócios anuais a nível mundial de uma empresa, consoante o que for mais elevado. [265]

Diante destas discrepâncias, ao considerar a adequação do PIPEDA ao RGPD, o Supervisor Europeu de Proteção dos Dados, Giovanni Buttarelli, recomendou que, quando da reforma do PIPEDA, as autoridades canadianas não se preocupassem tanto em replicar ponto a ponto todas as inovações consagradas no RGPD - tais como o direito ao esquecimento e a proteção desde a conceção e por defeito - mas sim em reforçar os poderes de suas autoridades de controlo. [266] Segundo Buttarelli, *We would encourage that there be a global approach and that you not have a sort of point-to-point replication of every single rule.… [T]he restrictions, exceptions, and derogations for law enforcement are more important than design and default.* [267]

4.2 Atualização do PIPEDA

Parte da discrepância entre o RGPD e o PIPEDA deve-se ao facto de que este último não foi suficientemente atualizado às mudanças tecnológicas dos últimos anos, fator que pôs em risco a sua capacidade de regular todas as nuances da atual sociedade da informação.

---

[265] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, artigo 83º, 6.

[266] Posição acompanhada por outras importantes vozes académicas canadianas, a exemplo de Teresa Scassa, professora da Faculdade de Direito da Universidade de Ottawa "*I certainly think the biggest weakness in PIPEDA in terms of conformity with European norms is on the enforcement side. There are simply not enough powers for the commissioner.*" Cf. CÂMARA DOS COMUNS DO CANADÁ, Comitê sobre o Acesso à Informação, Privacidade e Ética, Evidência, 1ª Seção, 42nd Parliament, 13 junho 2017, 1210 (Giovanni Buttarelli)

[267] *Ibid.*

É pacífica a necessidade de atualização do PIPEDA. Em todo caso, a doutrina canadiana divide-se em relação aos fundamentos que baseiam a necessidade da realização da aludida atualização.

Neste sentido, ciente da proximidade da reavaliação da decisão de adequação parcial do Canadá, parte da doutrina canadiana defende a atualização deste ato para melhor adequação ao regulamento europeu, como forma de manter a adequação que foi atribuída à lei federal em questão no ano de 2001. [268]

Por outro lado, a corrente contrária à supracitada defende a necessidade de atualização do PIPEDA independentemente da reavaliação da decisão de adequação da Comissão, tendo em vista a necessidade de adaptação deste ato aos desenvolvimentos tecnológicos. Neste sentido, insta ressaltar a passagem de Krista Campbell, Diretora Geral do Departamento de Inovação, Ciência e Desenvolvimento económico do Governo do Canadá [269]

> *Our privacy regime needs to continue to evolve regardless of what the European Commission does, simply because the Internet of things is coming[…]. We need to make sure our regime is evolving because of changes in technology and the challenges we face—not just because the Europeans are doing it.*

Não obstante as aludidas divergências, ambas as correntes concordam que a reforma para atualização do PIPEDA deve ser realizada em um futuro próximo.

[268] Posicionamento de Chantal Bernier, Comissária interina de Privacidade do Canadá durante os anos de 2013-2014.

[269] CÂMARA DOS COMUNS DO CANADÁ, Comitê sobre o Acesso à Informação, Privacidade e Ética, 1ª Seção, 42nd Parliament, 9 Maio 2017, 1645 (Krista Campbell). No mesmo sentido, Colin Bennett, professor de Ciência Política na Universidade de Victoria, Canadá. "*We should modernize PIPEDA because it needs modernization, not because it will satisfy a vague and shifting set of standards imposed from Brussels. We should take note of what the Europeans have done and draw lessons. I suspect that serious efforts to update and amend PIPEDA will not go unnoticed on the other side of the Atlantic. On the other hand, I would suspect that leaving the law as it stands will send the wrong message*". Cf. CÂMARA DOS COMUNS DO CANADÁ, Comitê sobre o Acesso à Informação, Privacidade e Ética, 1ª Seção, 42nd Parliament, 9 Maio 2017, 1640 (Colin Bennett).

CONCLUSÃO

Nas últimas décadas, o desenvolvimento tecnológico revolucionou a forma pela qual os dados pessoais são coletados, armazenados e partilhados. O fenômeno da globalização e da massificação da internet impôs dilemas para os quais as legislações que regulavam a proteção dos dados não tinham respostas, e nem poderiam ter, uma vez que foram desenvolvidas em uma sociedade que muito destoa da atual.

Diante deste cenário, e da falta de harmonização das legislações que estavam em vigor nos Estados-Membros da UE, surgiu a necessidade de atualização da Diretiva 95/46/CE.

O Regulamento Geral sobre a Proteção de Dados é um dos instrumentos do pacote da reforma da proteção dos dados realizada pela União Europeia como forma de garantir que o direito fundamental à proteção dos dados seria efetivamente garantido na sociedade da informação.

Para assegurar este objetivo, o RGPD estabelece novos direitos aos titulares dos dados, ao mesmo tempo em que clarifica deveres já previstos na Diretiva 95/46/CE e cria novas obrigações aos responsáveis pelo tratamento e subcontratantes.

No entanto, de nada adiantaria garantir um nível elevado de proteção na UE se quando estes dados fossem transferidos a países terceiros, estes últimos não consagrassem um nível de proteção substancialmente equivalente àquele garantido na União.

É neste sentido que o RGPD proíbe, em regra, as transferências de dados pessoais provenientes da UE para países terceiros ou organizações internacionais, sendo a referida transferência permitida apenas se houver sido realizada de acordo com as disposições do capítulo V do regulamento, a exemplo das transferências com base em uma decisão de adequação ou sujeitas a garantias adequadas.

O presente trabalho analisou o desenvolvimento das transferências transatlânticas dos dados pessoais – entre a UE e os EUA e o Canadá - na era pós-Snowden, à luz da antiga Diretiva 95/46/CE e do novo Regulamento Geral sobre a Proteção de Dados.

Entidades de ambos os países objeto do estudo podem receber as referidas transferências com base em uma decisão de adequação: a Comissão emitiu uma declaração de adequação parcial ao Canadá (Decisão 2002/2/CE), a qual abrange as entidades que estão sujeitas ao PIPEDA; ao passo em que as organizações americanas podem receber os dados provenientes da UE se subscreverem aos princípios do Escudo de Proteção da

Privacidade, ao qual foi reconhecida a adequação por meio da decisão de execução (UE) 2016/1250, emitida pela Comissão em 12 de julho de 2016.

Ainda que a aplicação do RGPD não afete imediatamente as decisões de adequação da Comissão, as quais continuarão válidas até que sejam alteradas, substituídas ou revogadas pela mesma entidade, os destinatários das referidas decisões deverão atentar-se aos novos requisitos de forma a se adequarem ao RGPD e não terem as suas decisões revogadas.

No caso canadiano, os maiores riscos à revogação da decisão de adequação dizem respeito à desatualização do PIPEDA face às novas tecnologias e a falta de previsão neste instrumento de obrigações e direitos fundamentais que são previstos e assegurados no texto do RGPD; bem como à ausência de poderes das autoridades responsáveis pela supervisão da aplicação da referida lei federal.

Ao mesmo tempo, o quadro jurídico canadiano referente à segurança nacional e ao acesso das autoridades públicas a dados pessoais constitui um óbice à renovação da decisão em questão, uma vez que alguns dos seus dispositivos põem em risco o direito à proteção dos dados tanto de cidadãos canadianos como de cidadãos estrangeiros.

Em todo caso, o Canadá demonstra estar ciente de que o seu ordenamento possui as supracitadas falhas, avançando, em ambos as situações, projetos para minimizar as imperfeições e tornar mais adequado o seu quadro jurídico referente à proteção dos dados.

A atualização do PIPEDA para melhor adequação deste instrumento à sociedade da informação é uma necessidade pacífica entre a doutrina canadiana, ainda que esta se divida quanto ao fundamento para tanto: enquanto parte dos académicos e políticos entende que a atualização da referida lei federal deverá ser realizada tendo em consideração as modificações introduzidas no direito da UE, como forma de acompanhar o nível mais elevado de proteção dos dados estabelecido naquele direito, garantindo, assim, a manutenção da decisão de adequação em análise; [270] a outra corrente entende que o PIPEDA deve ser atualizado porque este processo é necessário à garantia da efetividade do direito à proteção dos dados face aos novos desenvolvimentos tecnológicos, não devendo esta atualização ser motivada pelas recentes alterações do direito europeu. [271]

[270] Posicionamento de Chantal Bernier, Comissária interina de Privacidade do Canadá durante os anos de 2013-2014

[271] Posicionamento de Colin Bennett, professor de Ciência Política na Universidade de Victoria, Canadá.

No que concerne ao quadro jurídico canadiano referente à segurança pública, já se encontra no Senado daquele país um projeto de lei cujo objetivo é afastar da Lei Antiterrorismo do Canadá (2015) os dispositivos que colocam em risco a proteção dos dados pessoais dos cidadãos canadianos.

Ainda que o referido projeto de lei não elimine as ameaças ao direito em questão por completo, a sua simples existência demonstra o compromisso do Canadá em tentar corrigir as falhas de sua legislação como forma de oferecer àqueles que estão sujeitos ao seu ordenamento jurídico um adequado nível de proteção dos dados.

Como a reavaliação da decisão do PIPEDA deverá ocorrer nos próximos quatro anos, e o Canadá não só demonstra ter ciência das falhas do seu sistema jurídico no que concerne à proteção dos dados, bem como aparenta estar disposto a corrigi-las, não deverá haver grandes óbices à renovação da decisão de adequação do PIPEDA, desde que as referidas imperfeições sejam retificadas a tempo.

Quanto aos Estados Unidos, todavia, o cenário é diverso. Muito embora a Comissão tenha reconhecido a adequação do sistema do Escudo de Proteção da Privacidade, permitindo que os exportadores de dados da UE realizem as transferências às organizações participantes do EPP sem ter que apresentar garantias adicionais, as críticas direcionadas às falhas do aludido sistema tornam o seu futuro incerto.

O clima de incerteza jurídica ainda ronda as empresas americanas, apesar de a Comissão ter mantido a validade do EPP na primeira revisão anual realizada em setembro de 2017. Em seu relatório sobre a referida revisão, o GTA29 indicou que, se as aludidas falhas do EPP não forem sanadas até a segunda revisão anual, a decorrer ainda neste ano (2018), o próprio GT2A9 irá adotar as medidas adequadas, o que inclui acionar os tribunais nacionais para que estes questionem o TJUE sobre a validade do EPP. [272]

Ainda que seja o mecanismo mais prático e menos burocrático, as decisões de adequação são apenas um dos instrumentos oferecidos pelo RGPD para fundamentar a transferência de dados pessoais a um país terceiro.

Mesmo diante da ausência de uma decisão de adequação, os dados pessoais provenientes da UE poderão ser transferidos a uma entidade que se encontre em um país terceiro se o exportador dos dados utilizar as garantias adequadas previstas no artigo 46º do RGPD, a exemplo das cláusulas contratuais-tipo e das regras vinculativas, ou, em último

[272] GRUPO DE TRABALHO DO ARTIGO 29, *Primeira revisão anual do Escudo da Proteção da Privacidade*, WP 255, adotado em 28 de novembro de 2017, p.4

caso, se utilizar uma das exceções previstas no artigo 49º, a exemplo do consentimento expresso prestado pelo titular dos dados.

Por mais que assegurem a continuidade do fluxo de dados, o processo de adesão às supracitadas garantias adequadas e derrogações é muito mais burocrático, e, em alguns casos, muito mais custoso do que a adesão a um sistema como o EPP. No caso das transferências realizadas com base no consentimento previsto no artigo 49º, a própria natureza das exceções, e a possibilidade do titular dos dados revogar a qualquer momento o seu consentimento impossibilitam a utilização desta derrogação para fundamentar a transferência sistemática e em larga escala dos dados pessoais.

E, ainda neste caso, as empresas americanas enfrentam um cenário de insegurança jurídica, já que a validade das cláusulas contratuais-tipo também está a ser questionada, tornando o seu futuro igualmente incerto. [273]

Tendo em conta a importância do fluxo de dados entre a UE e os EUA, é imprescindível que um mecanismo eficiente de transferência dos dados subsista. Neste sentido, e tendo em consideração os benefícios da utilização do EPP, a opção mais viável seria acatar as recomendações que foram emitidas na primeira revisão anual, bem como adequar o referido sistema ao nível de proteção dos dados consagrado no RGPD, visando não só a solução das críticas que mais põem em risco a proteção dos dados pessoais, mas também, e, principalmente, a manutenção da validade do sistema em questão.

[273] SUPREMO TRIBUNAL DE JUSTIÇA DA IRLANDA, *The Data Protection Commisioner e Facebook Ireland e Maximilian Schrems*, Processo n. 2016 4809P, Disponível em: < https://www.alstonprivacy.com/wp-content/uploads/2018/04/ref.pdf> Acesso em: 14/05/20108

BIBLIOGRAFIA

ALSTON & BIRD, *Transferring Data from the EU: Privacy Shield and Data transfers under the GDPR*, Disponível em: <https://files.alston.com/files/docs/Roadmap-to-the-GDPR-International-Data-Transfers.pdf > Acesso em: 10/05/2018

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS, Síntese do parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Restabelecer a confiança nos fluxos de dados entre a UE e os EUA» e sobre a 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, (2014/C 116/04)

AUSTIN, Lisa M; GOOLD, Benjamin J, *How C-51 undermines privacy*, National Post, 30 de março de 2015, Disponível em: <http://nationalpost.com/opinion/how-c-51-undermines-privacy>. Acesso em 01/06/2018

BENDER, David, «Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International», *Data Privacy Law*, Vol. 6, No. 2, 2016

CALVÃO, Filipa Urbano, «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual*, p. 67-84, 2015/2

CÂMARA DOS COMUNS DO CANADÁ, Comitê sobre o Acesso à Informação, Privacidade e Ética, 1ª Seção, 42nd Parliament, 16 Feveireiro de 2017, 1540 (Daniel Therrien)

_____, Comitê sobre o Acesso à Informação, Privacidade e Ética, Evidência, 1ª Seção, 42nd Parliament, 13 junho 2017, 1210 (Giovanni Buttarelli)

_____, Comitê sobre o Acesso à Informação, Privacidade e Ética, Evidência, 1ª Seção, 42nd Parliament, 9 Maio 2017, 1640 (Colin Bennett).

CENTRO NACIONAL DE CIBERSEGURANÇA, *A Internet das Coisas (IOT – Internet of Things)*, Governo de Portugal, Disponível em: < https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/> Acesso em : 23-12-2017

Comité Consultivo sobre dados pessoais automatizados da Secretaria dos EUA, *Records, Computers and the Rights of Citizens (1973)*, Disponível em: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> Acesso: 29-05-2018.

COMITÉ DE MINISTROS DO CONSELHO DA EUROPA, Resolução (73) 22 do Comité de Ministros do Conselho da Europa (1973), relativa à proteção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector privado, de 26 de Setembro de 1973.

_____, Resolução (74) 29 do Comité de Ministros do Conselho da Europa (1974), relativa à protecção da privacidade das pessoas singulares perante os bancos electrónicos de dados no sector público, de 20 de Setembro de 1974.

COMISSÃO EUROPEIA, *Acordo sobre reforma da proteção de dados na UE proposta pela Comissão estimula mercado único digital*, Bruxelas, 15 de dezembro de 2015, Disponível em: <http://europa.eu/rapid/press-release_IP-15-6321_pt.htm> Acesso em: 19-04-2018

_____, 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, Bruxelas, 27 de Novembro de 2013

_____, 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]. Bruxelas, 27 de Novembro de 2013

_____, Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre a transferência de dados pessoais da EU para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems), COM(2015) 566 final, Bruxelas, 6.11.2015

_____, Comunicação da Comissão ao Parlamento Europeu e ao Conselho - *Transferência transatlântica de dados: restaurar a confiança através de garantias sólidas*, COM(2016) 117 final, Bruxelas, 29.2.2016

_____, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Intercâmbio e proteção de dados num mundo globalizado*, COM(2017) 7 final, Bruxelas, 10 de janeiro de 2017

_____, Comunicação da Comissão ao Parlamento Europeu e ao Conselho, *Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de dados a partir de 25 de maio de 2018*, Bruxelas, COM(2018) 43 final, 24.1.2018

_____, 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 [notificada com o número C(2000) 2441]

_____, Decisão 2001/497/CE da Comissão de 15 de Junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE [notificada com o número C(2001) 1539]

_____, Decisão 2002/2/CE da Comissão de 20 de Dezembro de 2001 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção proporcionado pela lei canadiana sobre dados pessoais e documentos electrónicos (Personal Information and Electronic Documents Act) [notificada com o número C(2001) 4539]

_____, Decisão 2004/915/CE da Comissão de 27 de Dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros [notificada com o número C(2004) 5271]

_____, Decisão 2010/87/UE 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 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, JO L 39 de 12.2.2010

_____, 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 [notificada com o número C(2016) 4176]

_____, *Directorate C : Fundamental rights and Union citizenship Unit C.3 : Data protection, Summary Of Replies To The Public Consultation About The Future Legal Framework For Protecting Personal Data*, Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf>, Acesso em: 22/10/2017

_____, *Guia do Escudo de Proteção da Privacidade*, Direção-Geral da Justiça e dos Consumidores, 2016

_____, *Guide to the Comprehensive Economic and Trade Agreement (CETA)*, Luxemburgo: Escritório de Publicações da União Europeia, 2017

_____, Recomendação da Comissão de 29 de Julho de 1981 relativa a uma convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal (81/679/CEE)

_____, Relatório da Comissão para o Parlamento Europeu e o Conselho sobre a primeira reapreciação anual do funcionamento do Escudo de Proteção da Privacidade UE-EUA, Bruxelas, 18.10.2017, COM (2017) 611 final

_____, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012) 11 final, 2012/11 (COD), Bruxelas, 25 de janeiro de 2012

COMITÉ DE DIREITOS HUMANOS DA ORGANIZAÇÃO DAS NAÇÕES UNIDAS, *Human Rights Committee discusses the report of Canada*, Disponível em:

<http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16215&LangID=E>. Acesso em: 04/05/2018.

CONSELHO DA EUROPA, *Chart of signatures and ratifications of Treaty 108*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Status as of 13/06/2018, Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=YuekXg7n> Acesso em: 13-06-2018

_____, *Handbook on European data protection law*, Luxemburgo: Publications Office of the European Union, 2014

DIAS PEREIRA, Alexandre Libório, «Big Data, E-Health e «Autodeterminação Informativa»: a Lei 67/98, a jurisprudência e o Regulamento 2016/679 (GDPR) », in *Lex Medicinae – Revista Portuguesa de Direito da Saúde*, n.o 29, 2018

DIAS PEREIRA, Alexandre Libório, «Marco Civil da Internet" e seus Reflexos no Direito da União Europeia», *Revista Jurídica Luso-Brasileira, RJLB*, Ano 2 (2016), nº 4, p. 53-106, 2016

DIVISÃO DA SOCIEDADE DA INFORMAÇÃO, *Anexo à resposta ao Ofício nº 259/2015/GAB-SAL-MJ (Processo nº 08027.000032/2015-11)*, Informações recebidas de Embaixadas do Brasil no exterior, Disponível em: <http://pensando.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/18-Canad%C3%A1.pdf>. Acesso em: 03/05/2018

ANDRADE DE JESUS, Inês Oliveira, «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?», *Anuário da Proteção de Dados 2018*. Lisboa: CEDIS, 2018

DEPARTAMENTO DE COMÉRCIO DOS ESTADOS UNIDOS, *U.S.-EU Safe Harbor Overview*, Disponível em: <http://build.export.gov/main/ safeharbor/eu/eg_main_018476> Acesso em 17/05/2018.

DEPARTAMENTO DE JUSTIÇA DOS ESTADOS UNIDOS, *Overview of the Privacy Act of 1974*, Disponível em: <https://www.justice.gov/opcl/introduction>. Acesso em: 12 de Outubro de 2017

DONEDA, Danilo, «A proteção dos dados pessoais como um direito fundamental», *Revista Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011

DONEDA, Danilo, *Um Código para a proteção de dados pessoais na Itália*, Disponível em: < https://www.researchgate.net/profile/Danilo_Doneda> Acesso em: 13-02-2018

EDWARDS, Elaine, *All You Need to Know in the Max Schrems-Facebook Case*, Irish Times, Fev. 6, 2017, Disponível em: <http://www.irishtimes.com/business/technology/all-you-need-to-know-in-the-max-schrems-facebook-case-1.2965482>, Acesso em: 06/05/2018

EUROPE VERSUS FACEBOOK, *Privacy Shield – Press Breakfast by MEP Jan Albrecht*, Bruxelas, 12 de Julho de 2016. Disponível em <http://www.europe-v-facebook.org/PA_PS.pdf>. Acesso em 01/05/2018

FRANCIS, et al. *Privacy: what everyone needs to know*. 1 ed. [S.L.]: Oxford University Press, 2017

GABEL, Detlev; HICKMAN, Tim; *Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation*, Disponível em: < https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection> Acesso em 27/05/2018.

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> Acesso em: 16/05/2018

GILBERT, Françoise, «WP29: Thumbs Down to Draft EU-US Privacy Shield», *American Law Institute*, Agosto de 2016

GOVERNO DOS ESTADOS UNIDOS, Comité permanente sobre a inteligência, *FISA Section 702*, Disponível em: < https://intelligence.house.gov/fisa-702/> Acesso em: 02-03-2018

GRUPO DE TRABALHO DO ARTIGO 29, *Transferências de dados pessoais para países terceiros: Aplicação do artigo 25 e 26 da Diretiva de proteção de dados da UE*, WP12, adotado em 24 de julho de 1998

_____, *Opinião 2/2001 sobre a adequação do canadiano PIPEDA*,WP39, adotada em 26 de janeiro de 2001

_____, *Opinião 01/2016 sobre o rascunho da decisão de adequação do Escudo de Proteção da Privacidade – UE– EUA*, WP 238, adotada em 13 de abril de 2016

_____, *Primeira revisão anual do Escudo de Proteção da Privacidade*, WP 255, adotado em 28 de novembro de 2017

_____, *Diretrizes sobre o artigo 49 do Regulamento 2016/679*, WP 262, adotado em 6 de fevereiro de 2018

_____, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" considered as compliant with the EC Model Clauses*, WP 226, adotado em 26 de novembro de 2014

GUMZEJ, Nina, *The Council Of Europe And The Right To Personal Data Protection: Embracing Postmodernity*, Conference of the International Journal of Arts & Sciences, Faculdade de Direito da Universidade de Zagreb, Croácia, 2013

HUSTINX, Peter, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en> Acesso em: 17-11-2017

JONES, Emily, «The Safety of Safe Harbor», *Journal of Direct, Data and Digital Marketing Practice*, n. 15, 2013

KENYON, Miles, *Joint Letter Concerning Bill C-59, National Security, and Human Rights*, 19 de setembro de 2017, Disponível em: < https://citizenlab.ca/2017/09/joint-letter-concerning-bill-c-59/> Acesso em: 22-05-2018.

KISS, Attila; SZOKE , Gergely László, «Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation», in *Reforming European Data Protection Law*, Law, Governance and Technology Series, [S.L]: Ed. Springer, 2015

KUNER, C, «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law», *Bloomberg BNA Privacy and Security Law Report*, 2012

KUNEVA, Meglena, *Roundtable on Online Data Collection, Targeting and Profiling*, Bruxelas, 31 de março de 2009, Disponível em <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm> Acesso em 01 de maio de 2018.

MARTINHO, Lucas Pires, «Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems», *Anuário da Proteção de Dados 2018*. Lisboa: CEDIS, 2018

MCKINSEY GLOBAL INSTITUTE, *Digital globalization: The new era of global flows* (2016), Disponível em: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-eraof-global-flows> Acesso em: 08/04/2018

LINN, Emily, «A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-U.S. Privacy Shield Agreement», *Vanderbilt Journal of Transnational Law*, Vol 50, 2017

LYNSKEY, Orla, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law, Oxford : Oxford University Press, 2015

MONTELEONE, Shara; PUCCIO, Laura; *From Safe Harbour to Privacy Shield - Advances and shortcomings of the new EU-US data transfer rules*, European Parliamentary Research Service, Members' Research Service, janeiro de 2017

OXMAN, Stephen A. «Exemptions to the European Union Personal Data Privacy Directive: will they swallow the directive?», *Boston College International Comparative Law Review*, vol. 24, 2000-2001

PATERAKI, Anna, «EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?», *World Data Protection Report*, Vol. 16, número 3, Março 2016

PARLAMENTO EUROPEU, Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)), Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//PT> Acesso em: 16/05/2018

_____, 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)).

_____, Comité de Liberdades Cívicas, Justiça e Assuntos Internos, 2018/2645(RSP), 10 de abril de 2018

_____, Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre a transferência transatlântica de dados (2016/2727(RSP)), Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//PT> Acesso em: 16/05/2018

_____, 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)).

PUPALOVA, Nina, *Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?* Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de Oslo, dezembro de 2017

ROACH, Kent; FORCESE, Craig, «Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience», *DesLibris*, v. II, fevereiro de 2015

SILVA, Heraclides Sequeira dos Santos, *A Proteção de Dados Pessoais na Era Global: O caso Schrems*, Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade Nova de Lisboa, janeiro de 2017.

STATISTICS CANADA, *Imports, exports and trade balance of goods on a balance-of-payments basis, by country or country grouping*, Disponível em: <http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/gblec02a-eng.htm>. Acesso em: 01/04/2018

STUPP, Catherine, *EU privacy watchdog: Privacy shield should be temporary*, Disponível em: <https://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/> Acesso em: 03/06/2018

STRANDBURG Katherine J; RAICU, Daniela Stan, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, [S.L.]:Ed. Springer US, 2006

TAKA, Anni-Maria, *Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications*, Dissertação apresentada à Faculdade de Direito da Universidade da Upsália na área de especialização em Direito Internacional, 2017

THERRIEN, Daniel, *Without big changes, Bill C-51 means big data*, The Globe and Mail, Disponível em: < https://www.theglobeandmail.com/globe-debate/without-big-changes-bill-c-51-means-big-data/article23320329/>. Acesso em: 03/05/2018.

_____, *Remarks at the Privacy Laws and Business International Conference*, 5 de julho, 2016, Cambridge, Reino Unido. Disponível em:< https://www.priv.gc.ca/en/opc-news/speeches/2016/sp-d_20160705/> Acesso em: 03/04/2018

_____, *Submission to the Standing Committee on Public Safety and National Security regarding the review of Bill C-59, An Act Respecting National Security Matters*, Disponível em: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_sub_180305/> Acesso em: 23-05-2018

THE WORLD BANK, *Indivíduos que utilizam a internet (% da população)*, Disponível em: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EU&name_desc=false > Acesso em: 19-05-2018.

TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies», *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Volume 34, fevereiro de 2018

VAN DEN BULCK, Paul, *Transfers of personal data to third countries*, Academia de Direito Europeu, Fórum 2017, 2017

VOIGT, Paul; VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR), a practical guide*, Switzerland: Springer International Publishing, 2017

VOSS, W. Gregory, «The future of transatlantic data flows: Privacy Shield or Bust*?* », *Journal of Internet Law*, Vol. 19, número 11, Maio de 2016

WEISS, Martin A; ARCHIK, Kristin, *The EU-U.S Safe Harbor Agreement on Personal Data Privacy: In Brief*, Congressional Research Service, Relatório do serviço de pesquisa do Congresso, Outubro de 2015

ZIMMER, Bob, *Towards Privacy by Design: Review of The Personal Information Protection and Eletronic Documents Act*, Report Of The Standing Committee On Access To Information, Privacy And Ethics, fevereiro de 2018

Legislação

CANADÁ, LEI ANTITERRORISMO, 2015, Disponível em: <http://lawslois.justice.gc.ca/eng/AnnualStatutes/2015_20/page-1.html#h-2>. Acesso em: 07/05/2018.

CANADÁ, *Privacy Act*, R.S.C., 1985, Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/p-21/page-1.html> Acesso em 13-11-2017

PORTUGAL, Lei nº 67/98, Lei da Protecção Dados Pessoais (transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados, Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=156&tabela=leis> Acesso em: 30/01/2018.

Jurisprudência

SUPREMO TRIBUNAL DE JUSTIÇA DA IRLANDA, *The Data Protection Commisioner e Facebook Ireland e Maximilian Schrems*, Processo n. 2016 4809P, Disponível em: < https://www.alstonprivacy.com/wp-content/uploads/2018/04/ref.pdf> Acesso em: 14/05/20108

TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*