A TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS ACOMPANHADA DE UMA DECISÃO DE ADEQUAÇÃO NO DIREITO DA UNIÃO EUROPEIA

THE TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ACCOMPANIED BY AN ADEQUACY DECISION IN THE EUROPEAN UNION LAW

Alexandra Maria Rodrigues Araújo[*]

José Sebastião De Oliveira[**]

RESUMO

Este artigo tem como objeto de análise o direito da UE sobre as transferências de dados pessoais para países terceiros acompanhadas de uma decisão de adequação. O conteúdo do artigo analisa o conceito de nível de proteção considerado adequado assim como o processo pelo qual esse nível é avaliado. Na primeira parte deste estudo é feita uma abordagem aos instrumentos europeus que protegem os dados de caráter pessoal. A segunda parte do artigo é dedicada ao tema das transferências internacionais de dados pessoais para países terceiros com uma decisão de adequação. O artigo finaliza com umas breves reflexões sobre o tema tratado.

PALAVRAS-CHAVE: direitos fundamentais; dados pessoais; direito europeu.

ABSTRACT

This article analyses the European Union law on transfers of personal data to third countries accompanied by an adequacy decision. The article considers the concept of level of protection deemed appropriate for data protection and the process by which this level is evaluated by the European Commission. In the first part of this study it is taken an approach of the European instruments on personal data protection. The second part of the article is devoted to the topic of the international transfers of personal data to third countries with an adequacy decision. The article concludes with some brief reflections on the subject covered.

KEYWORDS: fundamental rights; personal data; European law.

Introdução

A cada minuto 1 700 bilhões de dados são gerados no mundo. Isto equivale a 360 000 DVD por minuto e seis megabytes de dados diários por pessoa. O setor dos dados está a crescer 40% ao ano -sete vezes mais rapidamente do que o mercado global- e estima-se que os serviços e as tecnologias dos grandes volumes de dados alcancem a cifra de 16,9 mil milhões de dólares americanos em 2015.[1] É nesta nova realidade da economia digital que as pessoas singulares têm o direito fundamental à proteção dos seus dados de caráter pessoal, o que inclui um controlo efetivo sobre os mesmos.[2] Dados pessoais que compreendem quaisquer informações respeitantes a um individuo independentemente de estarem relacionadas com a sua vida privada, profissional ou pública.[3]

Para proteger eficazmente os dados pessoais muitos países desenvolveram legislação específica sobre a matéria. Contudo, a rapidez dos avanços tecnológicos -pense-se na computação em nuvem ou nas ferramentas de recolhimento de dados cada vez mais sofisticadas- suscitam contínuos desafios para o Direito. Tal como a tecnologia, a forma como os nossos dados de caráter pessoal são usados está em permanente evolução. Para o legislador nacional é um desafio estabelecer um quadro jurídico eficaz no tempo diante da complexidade da evolução e a dinâmica da informatização. Do mesmo modo, o caráter globalizado e crescente dos fluxos de dados exige um reforço, a nível internacional, da proteção dos direitos

* Doutora Europeia em Direito pela Universidade de Navarra (Pamplona, Espanha); Licenciada em Direito pela Universidade Católica Portuguesa (Porto, Portugal); Investigadora Integrada do Centro de Estudos em Direito da União Europeia da Faculdade de Direito da Universidade do Minho (Braga, Portugal); desde maio de 2014 é pesquisadora pós-doutoral no Programa de Pós-Graduação em Ciências Jurídicas do Centro Universitário de Maringá (UNICESUMAR) no âmbito do Programa Nacional de Pós-Doutorado/CAPES (PNPD/CAPES). Endereço postal: Avenida Guedner 1610, Jardim Aclimação, Maringá-PR. E-mail: aaraujo.cedu@direito.uminho.pt.

** Pós-doutor em Direito pela Faculdade de Direito da Universidade de Lisboa; Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP); Mestre em Direito Negocial pela Universidade Estadual de Londrina (UEL); Bacharel em Direito pela Universidade Estadual de Maringá (UEM); professor e Coordenador do Curso de Mestrado em Ciências Jurídicas do Centro Universitário de Maringá (UNICESUMAR); advogado. Endereço postal: Avenida Guedner 1610, Jardim Aclimação, Maringá-PR. E-mail: drjso@brturbo.com.br.

[1] Cf. COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu e ao Comité das Regiões: Para uma economia de dados próspera. COM (2014) 442 final, Bruxelas, 2.7.2014, p. 2.

[2] Entende-se por dados pessoais qualquer informação tal como um nome, uma fotografia, um número de telefone, um endereço postal ou de correio eletrónico, dados bancários, participações em sítios de redes sociais, informações médicas, dados sobre convicções religiosas ou o endereço IP de um computador. No direito da UE é utilizada uma noção ampla de dados pessoais de forma a incluir qualquer informação relativa a uma pessoa singular identificada ou identificável. Tal como define o art. 2.º al. a) da Diretiva 95/46/CE "é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

[3] As pessoas têm direito à proteção de dados pessoais em todos os aspetos da sua vida: em casa, no trabalho, durante as suas compras, num centro de saúde, numa esquadra de polícia ou na Internet.

das pessoas. As leis domésticas que visam a proteção de dados pessoais perdem grande parte da sua eficácia com uma simples transferência desses dados para um país terceiro que não proteja adequadamente os mesmos. Possibilitando, com isso, que dados pessoais sejam utilizados para fins obscuros e em benefício de redes criminosas, para fins de espionagem económica e industrial ou para a definição de perfis por razões políticas entre outras. Por isso são tão necessários mecanismos eficazes que permitam garantir os direitos das pessoas singulares nos fluxos transfronteiriços de dados pessoais. Regras que assegurem um elevado nível de proteção de dados sem contudo imporem restrições inecessárias ao comércio e cooperação internacionais.

No direito da União Europeia, o direito à proteção de dados está desenvolvido na Directiva 95/46/EC do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Diretiva ou Diretiva 95/46/CE).[4] As regras para a transferência de dados pessoais para fora do Espaço Económico Europeu (EEE) estão estabelecidas nos arts. 25.º e 26.º da Diretiva.

Contudo, convém desde já esclarecer que quando se fala em transferência transfronteiriça de dados pessoais no direito da UE se diferenciam várias situações. A distinção mais importante é aquela que se estabelece entre a livre transferência de dados da transferência de dados restritos. Há livre transferência de dados entre Estados-Membros da UE/EEE; entre Estados Parte da Convenção 108 e do Protocolo Adicional do Conselho da Europa; para países terceiros que tenham um adequado nível de proteção; e, por último, para países terceiros nos casos específicos do art. 26.º da Diretiva (derrogações ao disposto no art. 25.º). Há uma transferência de dados restrita quando essa transferência para um país terceiro é feita mediante garantias adequadas. Quer dizer, através de regras vinculativas para empresas (códigos de boas práticas), cláusulas-tipo de proteção de dados ou cláusulas contratuais.

Este artigo versa sobre o caso da livre transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação do nível de proteção. Mais em concreto, versa sobre as transferências acompanhadas por uma decisão da Comissão Europeia que certifica a existência nesse país de um nível adequado de proteção dos dados pessoais transferidos. Esta é a situação considerada ideal para uma transferência de dados para países terceiros ainda que seja a mais complexa de apurar. O artigo procura analisar o conteúdo do

[4] JO L 281 de 23.11.1995, p. 31.

conceito de nível de proteção adequado utilizado na avaliação e o processo pelo qual esse nível é avaliado. Para isso, o artigo está dividido em duas partes. Na primeira, é feita uma abordagem panorâmica dos instrumentos regionais europeus que protegem o direito à proteção de dados. A segunda parte do artigo é dedicada ao tema das transferências internacionais de dados pessoais para países terceiros com uma decisão de adequação. Nesta segunda parte, recebem especial atenção as alterações sobre a matéria que a reforma proposta pela Comissão Europeia ao quadro jurídico da proteção de dados pretende introduzir. O artigo finaliza com umas breves reflexões.

1. Panorama europeu do direito à proteção de dados pessoais

Existe um certo consenso quanto ao conteúdo das regras sobre a proteção de dados nos instrumentos internacionais de proteção dos direitos humanos.[5] Na verdade, as obrigações e direitos previstos na Diretiva 95/46/CE baseiam-se na Convenção 108 adotada em 1981 pelo Conselho da Europa que, por sua vez, se inspiram quer nas linhas diretrizes da Organização para a Cooperação e Desenvolvimento Económico desenvolvidas nas "Guidelines governing the protection of privacy and transborder flows of personal data" (1980, revisão de 2013) e nas linhas diretrizes das Nações Unidas de 1990. A nível europeu destaca-se as regras sobre a proteção de dados do Conselho da Europa e da União Europeia.[6]

1.1. *A proteção de dados no Conselho da Europa*

Tal como o Tribunal Europeu dos Direitos do Homem (TEDH) teve oportunidade de reconhecer expressamente na sua jurisprudência, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH) reconhece o direito à proteção

[5] O direito à proteção de dados pessoais é reconhecido ao nível universal em vários instrumentos adotados sobre o *aegis* das Nações Unidas. Na maioria dos casos como uma extensão do direito à privacidade. Neste sentido, ver o art. 12.º da Declaração Universal dos Direitos Humanos; o art. 17.º do Convénio Internacional dos Direitos Civis e Políticos; o Comentário Geral n.º 16 sobre o respeito da privacidade, família, domicílio e correspondência, e protecção da honra e reputação – art. 17.º; e também, as Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal adotadas pela resolução 45/95 da Assembleia Geral das Nações Unidas em 14 de dezembro de 1990.

[6] A UE e o Conselho da Europa são duas organizações internacionais distintas. O Conselho da Europa é uma organização internacional existente desde 1949 que tem como objetivos proteger os direitos humanos, a democracia e o Estado de Direito. Uma das suas primeiras realizações foi a CEDH. O respeito pelo conteúdo deste instrumento de proteção dos direitos humanos fica assegurado pelo TEDH. O Conselho da Europa conta atualmente com 47 países membros, incluindo todos os Estados-Membros da UE, e a sua sede situa-se em Estrasburgo, na França.

de dados pessoais no seu art. 8.º.[7] Este direito é reconhecido como uma extensão do direito à privacidade.[8]

Também no âmbito do Conselho da Europa foram adotados desde os anos 60/70 do século passado várias resoluções sobre a proteção de dados. Contudo, sobre a matéria, o instrumento mais importante adotado pelo Conselho da Europa foi a Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108) que entrou em vigor na ordem jurídica internacional a 1 de outubro de 1985.

A Convenção 108 aplica-se a todos os ficheiros e tratamentos automatizados de dados de caráter pessoal levados a cabo quer pelo setor público quer pelo setor privado (art. 3.º); e tem como objetivo proteger os indivíduos contra abusos que podem ser cometidos na recolha desses dados (art. 1.º). Os principais princípios estabelecidos para a proteção de dados são: o princípio da obtenção e tratamento dos dados de forma leal e lícita; o princípio da finalidade determinada e legítima dos dados; o princípio da adequação dos dados, pertinência e não excessividade em relação às finalidades para as quais os dados foram registados; exatitude, atualização e conservação dos dados de forma a permitir a identificação das pessoas em causa por um período que não exceda o tempo necessário às finalidades determinantes do seu registo (art. 5.º).

---

[7] Art. 8.º da CEDH:
1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

Para uma exposição detalhada da jurisprudência do TEDH sobre proteção de dados ver, por exemplo, AGÊNCIA EUROPEIA PARA A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS; CONSELHO DA EUROPA. **Handbook on European data protection law**. 2.ª edição. Luxembourg: Publications Office of the European Union, 2014. Um elenco atualizado da jurisprudência do TEDH e do TJUE sobre a matéria encontra-se nas p. 191-199.

[8] Desde o início da jurisprudência da UE protetora dos direitos fundamentais como princípios gerais do direito comunitário, o TJUE/TJCE destacou a importância da CEDH como fonte de inspiração para a proteção destes direitos. O TJ entendeu que ainda que não haja um vínculo formal entre o direito da UE e a CEDH, a UE deve, em todos os casos, respeitar o mínimo denominador comum de um direito tal como consagrado na CEDH (e tal como interpretado pelo TEDH). Para um desenvolvimento mais detalhado dos princípios em que se apoia a relação entre a CEDH e a UE ver, por exemplo, WEILER, Joseph H.H. Fundamental Rights and Fundamental Boundaries: on Standards and Values in the Protection of Human Rights. In: NEUWAHL, N.; ROSAS, A. (Eds.). **The European Union and Human Rights.** The Hague: Martinus Nijhoff Publishers, 1995. principalmente p. 53-54.

Além disso, este instrumento estabelece que os dados sensíveis só poderão ser objeto de tratamento automatizado desde que o direito interno preveja garantias adequadas (art. 6.º). A Convenção 108 também assegura o direito das pessoas a saber que informações sobre elas estão armazenadas e, se necessário, ter o direito de corrigi-las (art. 8.º). O art. 11.º estabelece que as Partes têm a faculdade de conceder aos titulares de dados uma proteção mais ampla deste direito.

Sobre aos fluxos transfronteiriços, a Convenção 108 prevê no art. 12.º que as Partes possam introduzir restrições ao fluxo transfronteiriço de dados quando não haja no outro país uma proteção equivalente dos dados de caráter pessoal. Contudo, sobre esta matéria, e devido à complexidade jurídica que estas transferências de dados foram adquirindo, o Conselho da Europa adotou em 2001 um protocolo adicional à Convenção 108: o Protocolo Adicional à Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Protocolo Adicional). Este instrumento estabelece provisões sobre a transferência de dados para países que não são parte contratantes e para o estabelecimento obrigatório de autoridades nacionais que supervisionem a proteção de dados. Entrou em vigor na ordem internacional a 1 de julho de 2004.

Nos termos do art. 2.º do Protocolo Adicional os fluxos transfronteiriços de dados de caráter pessoal para um destinatário que não está sujeito à jurisdição de uma Parte na Convenção só devem poder ser efetuados se esse Estado ou organização assegura um nível de proteção adequado para a transferência pretendida. Fora destas circunstâncias, uma Parte só pode autorizar a transferência de dados pessoais: a) Se o direito interno o previr em virtude de interesses específicos da pessoa em causa ou interesses legítimos prevalecentes, em especial interesses públicos importantes; ou, b) Se a pessoa responsável pela transferência apresentar garantias consideradas suficientes pelas autoridades competentes, em conformidade com o direito interno (por exemplo, através de cláusulas contratuais). Atualmente, está em curso uma reforma da Convenção 108 com o objetivo de reforçar a proteção da privacidade na era digital.

Todos os Estados Membros da UE ratificaram a Convenção 108 e, em 1999, este instrumento jurídico foi emendada para poder ter como Parte a União Europeia. A Convenção 108 tem um caráter aberto à adesão de Estados que não pertençam ao Conselho da Europa, incluindo Estados não europeus. Atualmente 45 das 46 Partes Contratantes da Convenção 108

são Estados que pertencem ao Conselho da Europa. O primeiro Estado não europeu a aceder à Convenção foi o Uruguai em agosto de 2013.

1.2. ***A proteção de dados no direito da União Europeia***

Na União Europeia o instrumento de direito derivado que estabelece o regime geral sobre a proteção de dados é a Diretiva 95/46/CE. Com a entrada em vigor do Tratado de Lisboa (2009) houve um reforço do direito à proteção de dados na UE. Este direito assume no art. 8.º da Carta dos Direitos Fundamentais da União Europeia a categoria de fundamental e o art. 16.º do Tratado sobre o Funcionamento da União Europeia atribui uma competência específica à UE para legislar em matéria de proteção de dados.

1.2.1. *A Diretiva 95/46/CE*

Com já foi referido, todos os Estados-Membros da UE são Partes Contratantes da Convenção 108. Contudo, a Diretiva 95/46/CE foi adotada com o objetivo de reforçar e expandir os princípios da proteção de dados contidos na Convenção 108. A Diretiva 95/46/CE apoia-se na possibilidade permitida pelo art. 11.º da Convenção 108 de as Partes Contratantes poderem adicionar instrumentos de proteção. A aplicação territorial da Diretiva vai além dos 28 Estados-Membros e inclui também os Estados que não são membros da UE e que formam parte do Espaço Económico Europeu (EEE) e que são a Islândia, o Liechtenstein e a Noruega.

Os objetivos principais da Diretiva são dois: assegurar a livre circulação de dados pessoais entre os Estados-Membros e proteger o direito fundamental à proteção de dados. Neste último sentido, o objetivo das regras contidas na Diretiva é a proteção de seres humanos, quer dizer, de pessoas singulares. Por isso, o direito à proteção dos dados pessoais é universal. Os dados pessoais são assim, em princípio, dados relativos a toda a pessoa viva identificada ou identificável.[9]

A diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como aos tratamentos por meios não automatizados contidos num ficheiro ou a ele destinados. Uma importante isenção na aplicação da Diretiva é a chamada isenção doméstica, quer dizer, o tratamento de dados pessoais por pessoas singulares para uso exclusivamente pessoal ou doméstico (art. 3.º n.º 2).

[9] Os dados que contenham informações relativas a pessoas coletivas em princípio não são abrangidos pela Diretiva. Não obstante, algumas regras de proteção de dados poderão, em circunstâncias específicas, aplicar-se indiretamente à informação relativa a empresas ou a pessoas colectivas. Por exemplo, algumas disposições da Directiva 2002/58/CE sobre a privacidade das comunicações eletrónicas estendem-se às pessoas coletivas.

O âmbito material da Diretiva é limitado às questões do mercado único. Ficam assim de fora do seu âmbito de aplicação as questões do âmbito da cooperação policial e judiciária em matéria penal. Por isso mesmo, esta Diretiva foi completada pela Decisão-Quadro 2008/977/JAI para a proteção de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal.[10] Além disso, como a Diretiva tem como destinatários os Estados-Membros, foi adotado o Regulamento n.º 45/2001 para proteger os dados de caráter pessoal do uso que as Instituições, órgãos e organismos da União Europeia façam deles.[11] Também foi necessário detalhar algumas das disposições cobertas pela diretiva tais como as relativas ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas.[12]

1.2.2. *A Carta dos Direitos Fundamentais da União Europeia*

Com a entrada em vigor do Tratado de Lisboa (1 de dezembro 2009) houve um reforço do direito à proteção de dados na UE ao equiparar-se, no art. 6.º n.º 1 do Tratado da União Europeia (TUE), o valor jurídico da Carta dos Direitos Fundamentais da União Europeia (Carta) ao dos Tratados[13]. A Carta, além de garantir no seu art. 7.º o respeito pela vida privada e familiar, reconhece no art. 8.º o direito fundamental autônomo à proteção de dados pessoais.

---

[10] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60.)

[11] Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1.)

[12] Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), (JO L 201 de 31.7.2002, p. 37).

[13] Em 1999 o Conselho Europeu de Colonia decidiu a redação de uma Carta com o objetivo de dar visibilidade à proteção dos direitos fundamentais na UE. A Carta foi redigida através de um método negociador que se denominou de "Convenção" e que se prolongou desde 17 de Dezembro de 1999 até 2 de Outubro de 2000. Na época, não foi possível obter o consenso necessário no sentido de incluir a Carta no Tratado de Nice e, por isso, a Carta foi aprovada no Conselho Europeu de Biarritz e proclamada solenemente à margem da reunião do Conselho Europeu de Nice em Dezembro de 2000. Consequentemente, o enquadramento jurídico deste documento originou contínuas polémicas ao longo de quase 10 anos. Considerou-se um texto de inquestionável valor político mas carente de caráter juridicamente vinculante. A Carta foi considerada um texto declarativo útil ao dar visibilidade àqueles direitos que já obrigavam os Estados-Membros e que formam parte do Direito da União como princípios gerais do direito. No entanto, o Tratado de Lisboa trouxe importantes inovações em relação à Carta ao equiparar o seu valor jurídico com o do direito originário da UE (cujos expoentes mais importantes são o TUE, o TFUE e o Tratado que institui a Comunidade Europeia da Energia Atómica). Para uma análise mais detalhada da Carta ver, por exemplo, SILVEIRA, A.; Canotilho, M. (Coord.). **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra: Almedina, 2013; MANGAS, A. (Dir.). **La Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo**. Bilbao: Fundación BBVA, 2009; BIFULCO, M.; CARTABIA, M.; CELOTTO, A. (Coords.), **L' Europa dei diritti. Commento alla Carta dei diritti fondamentali dell' Unione Europea**, Bologna: il Mulino, 2001; PICHAREL, C.; COUTRON, L. **Charte des droits fondamentaux de l'Union Européenne et Convention Européenne des Droits de l'Homme**. Brussels: Emile Bruylant, 2010.

O art. 8.º especifica que estes dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Além disso, o art. 8.º n.º 2 consagra o direito de todas as pessoas a aceder aos dados coligidos que lhes digam respeito e, se necessário, de obter a sua respetiva retificação. O número 3 do artigo estabelece que o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. O direito à proteção de dados não é um direito absoluto e por isso as restrições estabelecidas no art. 52.º n.º 1 da Carta aplicam-se-lhe.[14]

1.2.3. *O artigo 16.º do TFUE*

O art. 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) contém uma nova base jurídica para as regras de proteção de dados aplicáveis a todas as atividades abrangidas pelo direito da UE. Reconhece-se no n.º 1 o direito à proteção de dados de caráter pessoal e no n.º 2 uma competência específica da UE para legislar sobre a matéria. Este artigo, tal como configurado pelo Tratado de Lisboa, permite que a UE disponha de um único instrumento para regular a protecção de dados incluindo no domínio da cooperação policial e judiciária em matéria penal.[15]

A reforma do quadro jurídico da proteção de dados da UE, proporcionada pela nova redação do art. 16.º do TFUE, prevê uma mudança substancial das regras da UE sobre a matéria.[16] A reforma apoia-se em duas propostas legislativas: um regulamento que estabelece o quadro geral da UE em matéria de proteção de dados (e que substitui a Diretiva 95/46/CE);[17] e uma diretiva que enuncia as regras relativas à proteção de dados pessoais

[14] Cf. Acórdão do Tribunal de Justiça da União Europeia de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert* c. *Land Hessen* (ECR 2010 I-11063).

O art. 6.º n.º 1 do TUE estabelece que na interpretação e aplicação da Carta é necessário ter em conta as disposições gerais de caráter transversal constantes do Título VII da Carta (arts. 51.º a 54.º). O art. 52.º n.º 1 da Carta tem o seguinte teor: "Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efectivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de protecção dos direitos e liberdades de terceiros."

[15] A política externa e de segurança comum da UE é apenas parcialmente abrangida pelo art. 16.º do TFUE (Cf. Art. 16.º, n.º 2, último parágrafo do TFUE e art. 39.º do TUE).

[16] Neste artigo as referências à Proposta de Regulamento serão quase exclusivamente sobre o capítulo dedicado às transferências internacionais. Para uma visão mais global das reformas ver, por exemplo, VICTOR. J. M. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. **The Yale Law Journal**, New Haven, v. 123, n. 2, p. 513-528, nov. 2013.

[17] 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, Bruxelas, 25.1.2012.

tratados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e atividades judiciárias conexas (e que substitui a Decisão-Quadro 2008/977/JAI16).[18]

2. A transferência de dados pessoais para países terceiros acompanhada de uma decisão de adequação

Com já foi referido na parte introdutória deste artigo, no direito da UE os fluxos transfronteiriços de dados pessoais podem desenrolar-se com diferentes bases legais. Desde logo, deve distinguir-se entre a livre transferência de dados das transferências restritas. Os dados transferem-se livremente entre Estados-Membros da UE/EEE; entre Estados Parte Contratantes da Convenção 108; para países terceiros que tenham um adequado nível de proteção; e para países terceiros nos casos específicos previstos no art. 26 n.º 1 da Diretiva (derrogações ao art. 25.º).

Há uma transferência de dados restrita para países terceiros quando nesses países não há uma constatação da adequação do nível de proteção e, por isso, essa transferência é feita mediante a apresentação de garantias que assegurem que os dados pessoais transferidos terão uma proteção adequada. Em concreto, estas garantias são dadas através da criação de regras vinculativas para empresas (códigos de boas práticas), cláusulas-tipo de proteção de dados ou cláusulas contratuais (ver art. 26 n.º 2 a n.º 4 e art. 27.º da Diretiva).

No que diz respeito ao art. 2.º do Protocolo Adicional há um fluxo transfronteiriço de dados de caráter pessoal quando há um ato de envio ou transmissão de dados pessoais de um país Parte da Convenção para um destinatário que não esteja sujeito à jurisdição de uma Parte na Convenção. Essa transmissão de dados pode ser em papel, por e-mail ou quando o responsável pelo tratamento disponibiliza esses dado para terceiros localizados em países que não sejam Parte na Convenção.

A nível europeu estas transferências de dados apenas são permitidas quando são aplicadas as regras estabelecidas no art. 2.º do Protocolo Adicional e, adicionalmente para os Estados-Membros da EU/EEE, nos arts. 25.º e 26.º da Diretiva 95/46/CE. Na aceção do art. 25.º n.º 1, estes artigos da Diretiva aplicam-se quando há uma "transferência para um país terceiro de dados pessoais objecto de tratamento ou que se destinem a ser objecto de

[18] COMISSÃO EUROPEIA. Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados. COM (2012) 10 final, Bruxelas, 25.1.2012.

tratamento após a sua transferência".[19] Contudo, à que ter em conta o estabelecido pelo Tribunal de Justiça da União Europeia (TJUE) no caso *Bodil Lindqvist* onde aclara que o art. 25.º da Directiva 95/46/CE não se aplica quando uma pessoa que se encontra num Estado-Membro insere numa página Internet dados de caráter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros.[20]

A principal preocupação da UE ao regular os fluxos transfronteiriços de dados pessoais é salvaguardar os dados legalmente recolhidos na UE/EEE quando enviados para países terceiros. O art. 2.º n.º 1 do Protocolo Adicional assim como o n.º 1 do art. 25.º da Diretiva 95/46/CE compartem a mesma regra geral ao estabelecerem que os Estados-Membros da UE/Partes Contratantes da Convenção 108 apenas podem autorizar uma transferência de dados para um país terceiro no caso de esse país assegurar um nível de proteção adequado. O n.º 2 do art. 25.º da Diretiva esclarece que esta adequação deve ser avaliada caso a caso "em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados".

2.1. *A decisão de adequação adotada pela Comissão Europeia*

Atualmente a constatação do nível de proteção adequado pode ser realizada quer pelos Estados-Membros quer, como esclarece o n.º 6 do art. 25.º, pela Comissão Europeia. Os Estados-Membros utilizaram diferentes procedimentos administrativos para dar cumprimento às suas obrigações. Nomeadamente, através da imposição de uma obrigação direta aos responsáveis pelo tratamento dos dados e/ou através do desenvolvimento de um sistema de autorização prévia ou de controlo posterior por parte de uma autoridade nacional.

De acordo com o art. 25.º n.º 6 da Diretiva, a Comissão também é competente para avaliar o nível de adequação da proteção de dados em países terceiros consultando para esse

[19] O art. 4.º n.º 3 da Proposta de Regulamento define "Tratamento de dados pessoais" como "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, o apagamento ou a destruição". Ver, também, art. 2.º al. b) da Diretiva.

[20] Acordão do Tribunal de Justiça da União Europeia de 6 de novembro de 2003 no processo C-101/01, *Göta hovrat* c. *Lindqvist* (ECR 2003 page I-13020), para. 71. Este caso surgiu no contexto de um reenvio prejudicial colocado no âmbito de um processo penal pendente no *Göta hovrat* contra B. Lindqvist, acusada de ter violado a legislação sueca relativa à proteção dos dados de caráter pessoal ao publicar no seu sítio de Internet dados pessoais relativos a várias pessoas que trabalhavam com ela na paróquia de uma Igreja.

efeito o Grupo de Trabalho do art. 29.º (GT 29.º).[21] A Comissão pode fazer uma avaliação de todo o sistema jurídico de um país, de parte desse sistema jurídico ou delimitar a sua avaliação a um só setor. Um adequado nível de proteção significa que os principais princípios sobre a proteção de dados foram efetivamente implementados no direito nacional do país em questão. É necessário, por conseguinte, considerar na avaliação de adequação o conteúdo das regras aplicáveis aos dados pessoais transferidos para um país terceiro assim como o sistema instituído para conferir eficácia a essas regras. Uma vez que nos países terceiros vigoram níveis de proteção diferentes esta análise de adequação deve ser sempre apreciada de maneira a evitar qualquer discriminação arbitrária ou injustificada entre países terceiros em que prevaleçam condições semelhantes.

O processo de análise de adequação tem-se desenvolvido da seguinte maneira. Começa com o envio de uma carta oficial do país terceiro à Comissão em que se transmite o pedido de que se declare que assegura um nível de proteção adequado relativamente às transferências de dados pessoais da UE/EEE. A Comissão, a fim de avaliar se esse país assegura um nível de proteção adequado, solicita um relatório a um grupo de expertos/experto. As autoridades do país terceiro têm oportunidade de apresentar as suas observações em relação ao relatório. Subsequentemente, a Comissão solicita um parecer ao GT 29.º. Os dois documentos gerados no processo prévio (relatório e observações) são analisados por um subgrupo criado pelo GT 29.º e, depois de algum diálogo e troca de informações entre este grupo e as autoridades do país terceiro, este grupo adota o seu parecer sobre o nível e proteção do país em causa.

A Comissão atendendo a todas as circunstâncias que rodeiam a transferência de dados tais como a sua natureza, a finalidade e a duração do(s) tratamento(s) projetados, os países de origem e destino final, as regras de direito gerais ou setoriais que vigoram no país (bem com as as regras profissionais e as medidas de segurança que são respeitadas nesse país) e os compromissos internacionais desse país (art. 25.º n.º 2 e n.º 6 da Diretiva), tendo em conta o parecer do GT 29.º e após consultar a Autoridade Europeia para a Proteção de Dados,[22] adota

[21] Estre grupo conhecido pelo número do artigo que lhe serve de base jurídica é um "grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais" (art. 29.º da Diretiva). Uma das atribuições do Grupo é dar pareceres à Comissão sobre o nível de proteção dos dados pessoais nos países terceiros (art. 30.º n.º 1 al. a)).

[22] A Autoridade Europeia para a Proteção de Dados é uma autoridade independente, criada ao abrigo do artigo 46.º al. k) do Regulamento n.º 45/2001, que tem como função assegurar o respeito dos direitos fundamentais das pessoas singulares, especialmente o direito à vida privada, pelas instituições, órgãos e organismos da UE (o seu regulamento interno encontra-se no JO L 273 de 15.10.2013, p. 41).

a decisão relativa à adequação do nível de proteção dos dados pessoais do país em causa fundamentando a sua decisão nos considerandos do documento.

Todas as decisões de adequação da Comissão são publicadas no *Jornal Oficial da União Europeia* (JOUE). A constatação feita pela Comissão tem efeito vinculativo. Quer isto dizer que todos os Estados-Membros do EEE estão comprometidos com a decisão e os dados podem ser transferidos para esse país terceiro sem posteriores procedimentos de verificação ou licença por parte das autoridades nacionais.

2.1.1. *O parecer do Grupo de Trabalho do artigo 29.º*

O parecer deste grupo adquiriu um papel de destaque no processo de avaliação da adequação e contribuiu significativamente para a interpretação dos arts. 25.º e 26.º da Diretiva. Nas suas avaliações, o grupo teve como referência o documento adotado pelo mesmo a 24 de julho de 1998 intitulado "Transferência de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Directiva Comunitária relativa à proteção de dados". Este documento baseia-se no trabalho de interpretação realizado pelo GT 29.º até então e estipula que uma análise do adequado nível de proteção deve compreender dois elementos: a) uma análise da legislação em vigor; e b) os meios destinados a assegurar a sua efetiva aplicação. Baseando-se na Diretiva e, também, noutros instrumentos internacionais para a proteção de dados, o Grupo chegou a um conjunto de princípios substantivos nucleares da proteção de dados e de requisitos processuais de aplicação cuja observância considera como o mínimo indispensável para a existência de uma proteção adequada. Ainda assim, o Grupo entende que esta lista não pode ser interpretada de forma rígida.[23] Nas próximas páginas apresentam-se estes princípios tal como entendidos pelo GT 29.º. [24]

2.1.1.1. Identificação e análise da legislação em matéria de proteção de dados no país terceiro

Qualquer parecer de adequação começa por uma análise da legislação em matéria de proteção de dados do país terceiro. Em primeiro lugar analisa-se aquelas leis consideradas como "direito hierarquicamente superior": a Constituição escrita desse país ou, na falta desta,

[23] WP 12, p. 5. Ver, também, o WP 4 "Primeiras orientações sobre as transferência de dados pessoais para países terceiros – eventual metodologia a adoptar para avaliar a adequação do grau de proteção" adotado pelo Grupo em 26 de junho de 1997.

[24] A exposição que se vai fazer, tanto dos princípios relativos ao conteúdo assim como dos mecanismos processuais/de aplicação efetiva do direito à proteção de dados pessoais utilizados pelo GT 29.º, segue muito de perto o exposto no WP 12 nas p. 6-8.

aquelas leis que têm relevância constitucional. A primeira averiguação é saber se a proteção de dados é reconhecida como direito fundamental. Importa sublinhar que não é necessário que o direito ao respeito pela vida privada e à proteção de dados pessoais esteja expressamente reconhecido na Constituição de um país. Nestes casos, o GT 29.º procura disposições genéricas da lei fundamental que lidas em conjunto com a legislação desse país sobre a proteção de dados permitam concluir pela existência deste direito fundamental ainda que não esteja expressamente reconhecido.[25]

Após esta primeira observação, identifica-se a legislação nacional que detalha a proteção de dados pessoais e procede-se a uma cuidadosa análise do seu grau de adequação. Analisa-se o âmbito material e territorial de aplicação da legislação e, de seguida, os princípios relativos ao conteúdo e os mecanismos processuais /de aplicação efetiva do direito à proteção de dados pessoais.

2.1.1.1.1. Princípios relativos ao conteúdo

Os princípios observados pelo Grupo como básicos e que devem ser incluídos em qualquer conteúdo da legislação nacional sobre a proteção de dados são os seguintes:

- *Princípio da limitação da finalidade do tratamento*: os dados devem ser tratados para um fim específico e subsequentemente usados ou comunicados apenas na medida em que tal não seja incompatível com o fim da transferência.[26]

- *Princípio da proporcionalidade e da qualidade dos dados*: os dados devem ser exatos, e, se necessário, objecto de atualização. Devem igualmente ser adequados, relevantes e não excessivos em relação aos fins para os quais são transferidos ou posteriormente tratados.

- *Princípio da transparência*: as pessoas em causa devem ser informadas das finalidades do tratamento dos dados e da identidade do responsável pelo seu tratamento no país terceiro, devendo-lhes também ser fornecida qualquer informação necessária para garantir um tratamento imparcial.[27]

[25] Por exemplo, ver Parecer 6/2010 sobre o nível de proteção dos dados pessoais na República Oriental do Uruguai adotado em 12 de outubro de 2010, p. 3.
[26] As únicas exceções admissíveis a esta regra estão estabelecidas no art. 13.º da Diretiva e são as necessárias ao funcionamento de uma sociedade democrática.
[27] As únicas exceções admissíveis devem estar em conformidade com o n.º 2 do art.11.º e com o art. 13.º da Diretiva.

- *Princípio da segurança*: o responsável pelo tratamento dos dados deve tomar as medidas de segurança de caráter técnico e organizativo adequadas ao risco que o tratamento dos dados apresenta. Qualquer pessoa agindo sob a autoridade da pessoa responsável pelo tratamento dos dados, incluindo o subcontratante, não deverá proceder ao tratamento de dados a não ser com base em instruções da pessoa responsável.

- *Direitos de acesso, de retificação e de oposição*: a pessoa cujos dados foram objeto de tratamento tem o direito de obter uma cópia de todos os dados tratados a ela relativos, bem como o direito de retificação desses dados caso se revelem inexactos. Em determinadas circunstâncias, a pessoa deverá também ter o direito de se opor ao tratamento dos dados a ela relativos.[28]

- *Restrições relativas a transferências subsequentes*: as transferências subsequentes de dados pessoais por parte do destinatário da transferência inicial só devem ser permitidas no caso de o segundo destinatário se encontrar igualmente submetido a regras que garantem um nível de protecção adequado.[29]

O Grupo também estabeleceu *princípios adicionais* que devem ser aplicados quando estão em causa determinados tipos de tratamento de dados: *Dados sensíveis*- nestes casos, normalmente são exigidas garantias adicionais previstas na lei; *Marketing direto*- nestes casos a pessoa em causa deverá ter a qualquer momento o direito de se opor à utilização dos seus dados para tais efeitos; *Decisão individual automatizada*- quando a transferência tiver por finalidade uma decisão automatizada a pessoa em causa deverá ter direito a conhecer a lógica subjacente a uma tal decisão, devendo igualmente ser tomadas outras medidas destinadas a garantir a defesa dos interesses legítimos dessa pessoa.

2.1.1.1.2. Mecanismos processuais/de aplicação efetiva

No sentido de providenciar uma base para a avaliação do nível de adequação da proteção garantida, é necessário identificar os objetivos principais de um sistema processual relativo à proteção dos dados, e, partindo dessa base, avaliar os mecanismos processuais judiciais e extrajudiciais existentes no país terceiro. O GT 29.º estabelece os três objetivos principais de um sistema jurídico de proteção de dados:

[28] As únicas exceções a esses direitos deverão estar em conformidade com o art. 13.º da Diretiva.
[29] As únicas exceções possíveis deverão estar em conformidade com o n.º 1 do art. 26.º da Diretiva.

- *Garantir um elevado nível de cumprimento das suas regras* por parte dos responsáveis pelo tratamento de dados. As pessoas titulares dos dados devem ter conhecimento dos seus direitos e meios de os exercer. A existência de sanções efetivas e dissuasivas é considerado um elemento importante que assegura a observância das regras, tal como o são os sistemas de verificação direta por autoridades independentes encarregadas da proteção dos dados.

- *Prestar apoio e assistência às pessoas cujos dados foram objeto de tratamento quando queiram exercer os seus direitos*. As pessoas devem poder exercer os seus direitos de forma rápida e efetiva, sem custos proibitivos. Para tal, deve existir um mecanismo institucional que permita a investigação independente de queixas.

- *Fornecer meios de reparação adequados à pessoa que sofreu danos devido ao não cumprimento das regras relativas à proteção de dados*. Este elemento pressupõe um sistema que assegure a possibilidade de obter uma decisão judicial ou arbitral bem como, quando aplicável, uma compensação e sanções.

2.2. ***As transferências de dados pessoais com uma decisão de adequação na Proposta de Regulamento da Comissão Europeia***

Na Proposta de Regulamento sobre a proteção de dados os artigos referidos à transferência de dados pessoais para países terceiros situam-se no Capítulo V que engloba os arts. 40.º a 45.º. O art. 40.º da proposta de Regulamento -lido em conjunto com o art. 3.º- estabelece como princípio geral que sempre que bens e serviços sejam propostos a pessoas singulares na UE, ou sempre que o seu comportamento seja controlado, as regras sobre a proteção de dados a aplicar são as da UE. Este princípio deve ser aplicado quer à transferência original quer às transferências ulteriores de dados pessoais do país terceiro/organização internacional para outro país terceiro/organização internacional.[30]

Em relação à decisão sobre o nível adequado adotada pela Comissão Europeia a proposta determina, com maior detalhe do que a Diretiva, os critérios, condições e procedimentos para a adoção de uma decisão que certifique a existência de normas adequadas de proteção. O art. 41.º da Proposta de Regulamento estabelece que os critérios pertinentes

[30] Este princípio adquire grande transcendência jurídica ao impor aos provedores mundiais de serviços de informação as normas da UE de proteção de dados. Uma das áreas em que se prevê um impacto significativo é nas atividades relacionadas com a computação em nuvem.

para essa avaliação são: o primado do Estado de direito; a legislação relevante em vigor;[31] a possibilidade de recorrer aos tribunais; um controle independente; os compromissos internacionais assumidos. Deixam assim de fazer parte dos critérios de avaliação o conjunto de circunstâncias que rodeiam a(s) transferência(s) de dados tal como estipula o art. 25.º n.º 2 da Diretiva.

O artigo confirma explicitamente a possibilidade da Comissão avaliar o nível de proteção assegurado por um país terceiro, um território de um país terceiro, um setor de tratamento de dados num país terceiro ou uma organização internacional. Além disso, da leitura do Capítulo V da Proposta de Regulamento depreende-se que, com a nova reforma, a decisão de adequação é centralizada para a Comissão Europeia. Quer dizer, os Estados-Membros deixam de poder fazer esta avaliação de adequação.

O art. 41.º determina que a Comissão pode decidir que um país terceiro, um território ou um setor de tratamento nesse país terceiro, ou uma organização internacional, não assegura um nível de proteção adequado em especial nos casos em que a legislação relevante em vigor no país terceiro/organização internacional, não assegure direitos efetivos e oponíveis, incluindo vias de recurso administrativo e judicial para os titulares de dados, nomeadamente para as pessoas residentes no território da União cujos dados pessoais sejam objeto de transferência. Nestes casos, qualquer transferência de dados pessoais é proibida. Em momento oportuno, a Comissão deverá encetar negociações com o país terceiro/organização internacional, com vista a remediar a situação resultante da decisão de inadequação adotada. O artigo também compromete a Comissão com a publicação no JOUE de uma lista dos países terceiros, territórios e setores de tratamento num país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, que asseguram ou não um nível de proteção adequado.

Por último, a proposta de regulamento incentiva no art. 45.º ao diálogo e às negociações com países terceiros bem como com organizações internacionais relevantes para promover, a nível mundial, a adoção de normas de elevado nível e interoperáveis em matéria de proteção de dados.[32]

---

[31] Inclui tanto a legislação geral como a setorial (regras sobre segurança pública, defesa, segurança nacional, direito penal, regras profissionais ou medidas de segurança).

[32] Por exemplo, com Conselho da Europa, a Organização de Cooperação e Desenvolvimento Económico, a Organização das Nações Unidas, o Comité Europeu de Normalização, a Organização Internacional de Normalização, o Consórcio World Wide Web ou a Task Force de Engenharia da Internet.

2.3. *Comentário sobre o quadro jurídico das transferências de dados para países terceiros com uma decisão de adequação*

Não são muitos os países que a Comissão reconheceu como detentores de um nível de proteção adequado dos dados pessoais ao abrigo do art. 25.º n.º 6 da Diretiva. Até à atualidade a Comissão Europeia reconheceu um adequado nível de proteção à legislação de Andorra[33], Argentina[34], Canadá[35], Suíça[36], Ilhas Faroé[37], Guernesey[38], Israel[39], Ilha de Man[40], Jersey[41], Nova Zelândia[42], Uruguai[43] e aos *International Safe Harbor Principles* (princípios internacionais de porto seguro) do Departamento de Comércio dos EUA.[44] Além disso, com o escândalo da vigilância electrônica em larga escala dos cidadãos da UE efetuada pela Agência Nacional de Segurança dos EUA (NSA), a Comissão Europeia está a ser pressionada para

---

Os outros artigos do Capitulo V da Proposta de Regulamento tratam das condições aplicáveis às transferências através de regras vinculativas de empresas (art. 43.º) e das derrogações para as transferências de dados (art. 44.º).

[33] COMISSÃO EUROPEIA. Decisão da Comissão de 19 de Outubro de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção dos dados pessoais em Andorra (JO L 277 de 21.10.2010, p. 27).

[34] COMISSÃO EUROPEIA. Decisão da Comissão de 30 de Junho de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção dos dados pessoais na Argentina (C(2003)1731 final de 30.6.2003).

[35] 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) (JO L 2 de 4.1.2002, p. 13);

[36] COMISSÃO EUROPEIA. Decisão da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça (JO L 215 de 25.8.2000, p. 1).

[37] COMISSÃO EUROPEIA. Decisão da Comissão de 5 de Março de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativamente à adequação do nível de protecção assegurado pela Lei sobre o tratamento de dados pessoais das Ilhas Faroé (JO L 58 de 9.3.2010, p. 17).

[38] COMISSÃO EUROPEIA. Decisão da Comissão de 21 de Novembro de 2003 relativa à adequação do nível de protecção de dados pessoais em Guernsey (JO L 308 de 25.11.2003, p. 27).

[39] COMISSÃO EUROPEIA. Decisão da Comissão de 31 de Janeiro de 2011 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pelo Estado de Israel no que se refere ao tratamento automatizado de dados (JO L 27 de 1.2.2011, p. 39).

[40] COMISSÃO EUROPEIA. Decisão da Comissão de 28 de Abril de 2004 relativa à adequação do nível de protecção de dados pessoais na Ilha de Man (JO L 151/51 de 30.4.2004, p. 51).

[41] COMISSÃO EUROPEIA. Decisão da Comissão de 8 de Maio de 2008 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Jersey (JO L 138 de 28.5.2008, p. 21).

[42] COMISSÃO EUROPEIA. Decisão de execução da Comissão de 19 de dezembro de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela Nova Zelândia (JO L 28 de 30.1.2013, p. 12).

[43] COMISSÃO EUROPEIA. Decisão de execução da Comissão de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 215 de 25.8.2000, p. 1).

[44] COMISSÃO EUROPEIA. Decisão da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO L 215 de 25.8.2000, p. 7).

rever algumas destas decisões de adequação. Em especial, para rever a decisão de adequação dos princípios de porto seguro uma vez que que as empresas identificadas nas revelações dos meios de comunicação como estando envolvidas nesta vigilância massiva a cidadãos europeus são empresas que declararam a sua adesão a estes princípios.[45]

Quanto à decisão de adequação por parte dos Estados-Membros pôde constatar-se, ao longo destes anos, uma excessiva falta de harmonização sobre a matéria nas legislações nacionais.[46] A Diretiva ao ser transposta para o direito interno de cada país deu lugar a diferentes práticas de avaliação do nível de adequação entre os Estados-Membros. Em alguns Estados-Membros a adequação é avaliada, em primeiro lugar, pelo próprio responsável pelo tratamento que transfere para um país terceiro, algumas vezes sob a supervisão subsequente dos Estados ou da autoridade de proteção de dados. Esta abordagem deu origem a que o nível de proteção das pessoas a que os dados dizem respeito num determinado país terceiro seja apreciado de forma diferente consoante os Estados-Membros. Com o consequente enfraquecimento do direito fundamental à proteção de dados em toda a UE uma vez que, havendo libre circulação de dados no espaço europeu, os fluxos de dados dirigir-se-ão para aquele ponto exportador mais laxo. Outros Estados-Membros decidiram submeter todas as transferências para países terceiros a uma autorização administrativa. Esta abordagem potenciou uma serie de entraves desnecessários ao comércio internacional e, por demasiado rigorosa, um desrespeito na aplicação prática da Diretiva.

Outra crítica apresentada com regularidade ao longo dos anos e, diretamente relacionada com o aspeto referido anteriormente, é a que aponta a que os requisitos para a avaliação da adequação expostos na Diretiva são demasiado vagos. Aponta-se falta de clareza e detalhe no conceito do nível de proteção adequado com os consequentes riscos de fragmentação jurídica que isto acarreta.[47] Desde logo, a falta de uniformidade na avaliação feita pelos Estados-Membros levou a que essa crítica fosse reconhecida por várias instituições

[45] Cf. PARLAMENTO EUROPEU. Resolução do Parlamento Europeu de 12 de março de 2014, sobre a 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 EU e, na cooperação transatlântica no domínio da justiça e dos assuntos internos. 2013/2188(INI), Bruxelas, 12.03.2014.

[46] Cf. COMISSÃO EUROPEIA. Relatório da Comissão: Primeiro Relatório sobre a implementação da directiva relativa à protecção de dados (95/46/CE). COM (2003) 265 final, Bruxelas, 15.5.2003, pp. 18-20.

[47] Ver, por exemplo, ZINSER, A. European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers. **Tulane Journal of Technology and Intellectual Property**, New Orleans, v. 6, p. 172, Spring 2004; 176; SCHWARTZ, P. M. European Data Protection Law and Restrictions on International Data Flows. **Iowa Law Review**, Iowa, v. 80, p. 473, 94-1995.

e organismos da União.[48] Por outro lado, o número reduzido de decisões de adequação da Comissão deixa perceber que este mecanismo está longe de atingir todo o seu potencial.

Por conseguinte, o conteúdo dos arts. 25.º e 26.º da diretiva não conseguiram evitar uma fragmentação na execução destas transferências nem um nível alto de insegurança sobre os seus dados pessoais na generalidade dos cidadãos europeus.[49] Por isso, que a reforma atual do quadro jurídico da UE sobre proteção de dados tenha como um dos objetivos reforçar os procedimentos em vigor para as transferências internacionais de dados de modo a definir com mais rigor e claridade a avaliação do nível de proteção de dados em países terceiros é valorado como positivo. Sobre essa reforma do quadro jurídico para as transferências internacionais de dados há alguns aspetos que nos parecem mais meritórios e que são referidos a continuação.

O primeiro aspeto a referir é de caráter geral. Mudar a base jurídica da proteção de dados de uma diretiva para um regulamento é uma solução acertada. A aplicabilidade direta do regulamento -tal como prevista no art. 288.º do TFUE- permitirá que um único instrumento jurídico vigore em toda a UE. Desta maneira, muita da complexidade e incoerências originadas pelas diversas leis nacionais que transpuseram a Diretiva 95/46/CE vão desaparecer. Um único instrumento em vez de 28 leis nacionais irá reduzir a fragmentação jurídica com os benefícios que isso proporciona.[50]

Outra das mudanças mais significativas apresentadas na Proposta de Regulamento é a de centralizar o processo da decisão de adequação na Comissão Europeia. A proposta parece eliminar a possibilidade dos Estados-Membros realizarem esta decisão. Centralizar o processo de adequação contribui para o estabelecimento de uma abordagem mais coerente na matéria e impede o desenvolvimento pelos governos/autoridades responsáveis pela proteção dos dados nacionais de uma multiplicidade de listas diferentes e eventualmente em conflito umas com as outras. Esta solução é preferível também por razões práticas. Muitas autoridades nacionais não têm o pessoal nem os recursos financeiros adequados para tomarem estas decisões de

[48] Cf. AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union. Brussels, 14.01.2011, p. 14; PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da protecção de dados pessoais na União Europeia. 2011/2025(INI), Bruxelas, 06.07.2011, p. 4.

[49] Cf. COMISSÃO EUROPEIA. **Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union**. Brussels: Opinion & Social, 2011. especialmente p. 137-172.

[50] A mesma opinião tem GUMZEJ, N. Data protection for the digital age: comprehensive effects of the evolving law of accountability. **Juridical Tribune**, v. 2, n. 2, p. 92, dez. 2012.

adequação. A solução proposta pelo regulamento parece ainda justificar-se mais naqueles Estados-Membros que deixam aos responsáveis de tratamento a decisão de adequação. Talvez pela complexidade da decisão ou pelo compromisso que assumem, estes responsáveis têm sido parcos na utilização desta opção.[51]

Contudo, alguns aspetos da proposta podem ainda ser melhorados. Por exemplo, apesar de haver uma maior concreção quanto aos critérios pertinentes para a avaliação de adequação é desejável regras mais precisas sobre o processo de decisão sobre a (in)adequação assim como regras para uma supervisão posterior da Comissão sobre aqueles países que têm uma decisão de adequação. Esperamos que, durante o processo de adoção do ato, estas e outras insuficiências sejam supridas com êxito.[52]

Por último, sublinhar que as normas referentes à transferência de dados só funcionam se há uma aplicação rigorosa dos seus preceitos de modo a que assegurem um sistema que garanta um nível de proteção dos dados transferidos para fora da UE equivalente ao que existe no território da UE.

Conclusão

A nova revolução industrial que estamos a viver só pode ser plenamente realizada se da parte dos particulares houver uma confiança na economia globalizada das tecnologias da informação. Um quadro jurídico moderno, coerente e global em matéria de proteção de dados reforçará a confiança dos cidadãos no ambiente em linha, e aumentará a segurança jurídica. Este ambiente regulamentar é essencial quer para a proteção do direito fundamental dos indivíduos quer para o desenvolvimento de bens e serviços de dados.

Na União Europeia o direito à proteção de dados pessoais é um direito fundamental protegido no art. 8.º da Carta. Por isso, a UE e os Estados-Membros têm o dever de garantir esse direito para todos as pessoas físicas dentro dos limites das suas competências. Num mundo globalizado isto significa que as pessoas podem exigir proteção mesmo que os seus dados sejam tratados fora do espaço da UE/EEE.

---

[51] Cf. Analysis and impact study on the implementation of Directive 95/46 in Member States: Annex to the First Commission's report on the implementation of the Data Protection Directive (95/46/EC). COM (2003) 265 final, Brussels, 15.05.2003, p. 32.

[52] Segundo o estipulado no n.º 2 do art. 16.º do TFUE, as normas sobre a proteção de dados são adotadas de acordo com o processo legislativo ordinário que consiste na adoção de um regulamento, de uma diretiva ou de uma decisão conjuntamente pelo Parlamento Europeu e pelo Conselho, sob proposta da Comissão (art. 289.º n.º 1 do TFUE). As várias fases deste processo vêm detalhadas no art. 294.º do TFUE.

Apesar dos atuais princípios da proteção de dados se manterem válidos, devido aos importantes avanços tecnológicos dos últimos anos, para garantir este direito fundamental é necessário aperfeiçoar os mecanismos previstos nos arts. 25.º e 26.º da Diretiva 95/46/CE de modo a garantir a proteção adequada dos dados pessoais durante a sua transferência e tratamento fora da UE/EEE. E, desta maneira, defender-se o princípio da reciprocidade na proteção dos dados pessoais nas atividades internacionais da União.

Nas transferências internacionais a decisão de adequação a nível europeu, sempre que estejam preenchidos os seus requisitos, é a solução preferida porque vai racionalizar o processo de forma a oferecer aos operadores económicos e aos indivíduos um maior nível de segurança relativamente aos países que se considera com uma proteção adequada. É, também, considerado um fator de incentivo para os países terceiros que se encontram a elaborar ou reformar os seus sistemas de proteção de dados.

Contudo, apesar de todos os esforços no espaço europeu em elevar o nível de proteção dos dados pessoais, num mundo interligado, essa objetivo só se conseguirá alcançar com princípios universais firmes no domínio da proteção de dados. Só através de normas jurídicas globais na matéria é que desaparecem os graves desequilíbrios atualmente existentes a nível internacional na proteção des dados. Por isso, o compromisso estabelecido no art. 45.º da Proposta de Regulamento no sentido de reforçar a dimensão global da proteção de dados através da cooperação da UE com países terceiros e organizações internacionais para a elaboração de normas internacionais sobre a matéria é, na realidade, a chave essencial para se lograr um quadro jurídico internacional em harmonia com o direito fundamental à proteção de dados.

REFERÊNCIAS

AGÊNCIA EUROPEIA PARA A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS; CONSELHO DA EUROPA. **Handbook on European data protection law**. 2.ª edição. Luxembourg: Publications Office of the European Union, 2014.

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union. Brussels, 14.01.2011.

BIFULCO, M.; CARTABIA, M.; CELOTTO, A. (Coords.), **L' Europa dei diritti. Commento alla Carta dei diritti fondamentali dell' Unione Europea**, Bologna: il Mulino, 2001.

COMISSÃO EUROPEIA. Analysis and impact study on the implementation of Directive 95/46 in Member States: Annex to the First Commission's report on the implementation of the Data Protection Directive (95/46/EC). COM (2003) 265 final, Brussels 15.5.2003.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu e ao Comité das Regiões: Para uma economia de dados próspera. COM (2014) 442 final, Bruxelas, 2.7.2014.

COMISSÃO EUROPEIA. Decisão da Comissão de 19 de Outubro de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção dos dados pessoais em Andorra (JO L 277 de 21.10.2010, p. 27).

COMISSÃO EUROPEIA. Decisão da Comissão de 30 de Junho de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção dos dados pessoais na Argentina. C (2003) 1731 final, Bruxelas, 30.6.2003.

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) (JO L 2 de 4.1.2002, p. 13).

COMISSÃO EUROPEIA. Decisão da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção adequado dos dados pessoais na Suíça (JO L 215 de 25.8.2000, p. 1).

COMISSÃO EUROPEIA. Decisão da Comissão de 5 de Março de 2010 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativamente à adequação do nível de protecção assegurado pela Lei sobre o tratamento de dados pessoais das Ilhas Faroé (JO L 58 de 9.3.2010, p. 17).

COMISSÃO EUROPEIA. Decisão da Comissão de 21 de Novembro de 2003 relativa à adequação do nível de protecção de dados pessoais em Guernsey (JO L 308 de 25.11.2003, p. 27).

COMISSÃO EUROPEIA. Decisão da Comissão de 31 de Janeiro de 2011 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pelo Estado de Israel no que se refere ao tratamento automatizado de dados (JO L 27 de 1.2.2011, p. 39).

COMISSÃO EUROPEIA. Decisão da Comissão de 28 de Abril de 2004 relativa à adequação do nível de protecção de dados pessoais na Ilha de Man (JO L 151/51 de 30.4.2004, p. 51).

COMISSÃO EUROPEIA. Decisão da Comissão de 8 de Maio de 2008 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Jersey (JO L 138 de 28.5.2008, p. 21).

COMISSÃO EUROPEIA. Decisão de execução da Comissão de 19 de dezembro de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela Nova Zelândia (JO L 28 de 30.1.2013, p. 12).

COMISSÃO EUROPEIA. Decisão de execução da Comissão de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 215 de 25.8.2000, p. 1).

COMISSÃO EUROPEIA. Decisão da Comissão de 26 de Julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América (JO L 215 de 25.8.2000, p. 7).

COMISSÃO EUROPEIA. Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados. COM (2012) 10 final, Bruxelas, 25.1.2012.

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, Bruxelas, 25.1.2012.

COMISSÃO EUROPEIA. Relatório da Comissão: Primeiro Relatório sobre a implementação da directiva relativa à protecção de dados (95/46/CE). COM (2003) 265 final, Bruxelas, 15.5.2003.

COMISSÃO EUROPEIA. **Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union**. Brussels: Opinion & Social, 2011.

CONSELHO DA EUROPA. Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Estrasburgo. Disponível em <http.www.echr.coe.int>. Acesso em: 20 de agosto de 2014.

CONSELHO DA EUROPA. Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. European Treaty Series - No. 108, Estrasburgo, 28.1.1981.

CONSELHO DA EUROPA. Protocolo Adicional à Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. European Treaty Series – No. 181, Estrasburgo, 8.11.2001.

GRUPO DE TRABALHO DO ART. 29.º. Primeiras orientações sobre as transferência de dados pessoais para países terceiros – eventual metodologia a adoptar para avaliar a adequação do grau de proteção. Working Paper 4, Bruxelas, 26.06.1997.

GRUPO DE TRABALHO DO ART. 29.º. Transferências de dados pessoais para países terceiros: aplicação dos artigos 25.º e 26.º da Directiva Comunitária relativa à proteção de dados. Working Paper 12, Bruxelas, 24.07.1998

GRUPO DE TRABALHO DO ART. 29.º. Parecer 6/2010 sobre o nível de proteção dos dados pessoais na República Oriental do Uruguai. Bruxelas, 12.10.2010.

GUMZEJ, N. Data protection for the digital age: comprehensive effects of the evolving law of accountability. **Juridical Tribune**, v. 2, n. 2, p. 92, dez. 2012.

MANGAS, A. (Dir.). **La Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo**. Bilbao: Fundación BBVA, 2009.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO. Guidelines governing the protection of privacy and transborder flows of personal data**.** C (80) 58/FINAL, as amended on 11 July 2013 by C (2013) 79.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. Directiva 95/46/EC do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção 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).

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu de 12 de março de 2014, sobre a 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 EU e, na cooperação transatlântica no domínio da justiça e dos assuntos internos. 2013/2188(INI), Bruxelas, 12.03.2014.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da protecção de dados pessoais na União Europeia. 2011/2025(INI), Bruxelas, 6.07.2011.

PICHAREL, C.; COUTRON, L. **Charte des droits fondamentaux de l'Union Européenne et Convention Européenne des Droits de l'Homme**. Brussels: Emile Bruylant, 2010.

SCHWARTZ, P. M. European Data Protection Law and Restrictions on International Data Flows. **Iowa Law Review**, Iowa, v. 80, p. 473, 94-1995.

SILVEIRA, A.; Canotilho, M. (Coord.). **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra: Almedina, 2013.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia (JO C de 26.20.2012, p. 391.

UNIÃO EUROPEIA. Tratado da União Europeia (JO C 326 de 26.10.2012, p. 13).

UNIÃO EUROPEIA. Tratada sobre o Funcionamento da União Europeia (JO C 326 de 26.10.2012, p. 47).

VICTOR. J. M. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. **The Yale Law Journal**, New Haven, v. 123, n. 2, p. 513-528, nov. 2013.

WEILER, Joseph H.H. Fundamental Rights and Fundamental Boundaries: on Standards and Values in the Protection of Human Rights. In: NEUWAHL, N.; ROSAS, A. (Eds.). **The European Union and Human Rights.** The Hague: Martinus Nijhoff Publishers, 1995.

ZINSER, A. European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers. **Tulane Journal of Technology and Intellectual Property**, New Orleans, v. 6, p. 172, Spring 2004.