ANUÁRIO DA PROTEÇÃO DE DADOS

2018

COORDENAÇÃO

FRANCISCO PEREIRA COUTINHO

GRAÇA CANTO MONIZ

CEDIS

CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2018

ANUÁRIO DA PROTEÇÃO DE DADOS

2018

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2018

COORDENAÇÃO
Francisco Pereira Coutinho
Graça Canto Moniz

SECRETÁRIA EXECUTIVA
Caroline Costa Bernardo

EDIÇÃO
Universidade Nova de Lisboa. Faculdade de Direito.
CEDIS, Centro de I & D sobre Direito e Sociedade
Campus de Campolide, 1099-032 Lisboa, Portugal

SUPORTE: ELETRÓNICO

Março, 2018

ISBN
ISBN: 978-972-99399-5-2

CATALOGAÇÃO NA PUBLICAÇÃO
PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.).
Anuário da Proteção de Dados 2018. Lisboa: CEDIS, 2018

Nota de Apresentação

O Anuário do Direito da Proteção de Dados Pessoais é uma revista jurídica de livre acesso, disponível em linha no sítio http://protecaodedadosue.cedis.fd.unl.pt/, que pretende divulgar estudos doutrinários sobre o direito à proteção de dados pessoais. O Anuário é editado pelo Observatório para a Proteção de Dados Pessoais, grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa. Aberto a qualquer interessado, o Observatório integra atualmente oito investigadores (dois doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

A edição de 2018 do Anuário do Direito da Proteção de Dados Pessoais reúne, no essencial, textos apresentados no Workshop "O novo regulamento de proteção de dados pessoais", realizado na Faculdade de Direito da Universidade Nova de Lisboa a 15 de dezembro de 2016[1]. O Anuário abre com dois textos que se debruçam sobre o âmbito dos direitos dos titulares de dados pessoais consagrados no regulamento geral relativo à proteção de dados pessoais[2]: o primeiro, de Graça Canto Moniz, foca em particular o direito à portabilidade; o segundo, de Afonso José Ferreira, incide sobre o tema do *profiling* e dos algoritmos autónomos. Segue-se um artigo, de Teresa Vale Lopes, que analisa as principais obrigações e responsabilidades que o

---

[1] O programa do Workshop pode ser consultado aqui: <http://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2016/12/Portfólio-Workshop-15.12.2016-.pdf> (acedido a 31/01/2018).

[2] 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.

regulamento estabelece para as empresas e o respetivo impacto no plano organizacional das mesmas, e três textos, da autoria de Inês Oliveira Andrade de Jesus, Martinho Lucas Pires e Ricardo Rodrigues de Oliveira, que se debruçam sobre transferências internacionais de dados pessoais. O Anuário termina com um artigo de Emellin de Oliveira sobre o *Passanger Name Record* (PNR), aprovado pela Diretiva (UE) 2016/681, relativa à utilização dos dados dos registos de identificação dos passageiros como instrumento de combate ao terrorismo e à criminalidade grave.

A publicação desta obra não teria sido possível sem o patrocínio da SRS Advogados e da Vision Ware, a quem agradeço, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (Vision Ware), o apoio que têm prestado desde a primeira hora a este projeto.

São ainda devidos agradecimentos à Caroline Bernardo, bolseira do CEDIS, pelo auxílio prestado na revisão do Anuário, e à Graça Canto Moniz, coeditora do Anuário e cocoordenadora do Observatório para a Proteção dos Dados Pessoais, cujo entusiasmo e dedicação incansáveis têm alimentado o contínuo desenvolvimento destes projetos.

Por último, deixo uma última palavra de reconhecimento a todos os autores que participam no Anuário, não só por terem aceitado o desafio que lhes foi lançado, mas especialmente pela forma empenhada com que o fizeram, que se reflete no alto nível científico dos textos agora publicados.

Lisboa, 2 de janeiro de 2018

Francisco Pereira Coutinho
Coordenador do Observatório para a Proteção de Dados Pessoais
Professor da Faculdade de Direito da Universidade Nova de Lisboa

Lista de Abreviaturas

API	–	Advance Passanger Information
AEPD	–	Autoridade Europeia para a Proteção de Dados
APDs	–	Autoridades de Protecção de Dados
art.	–	Artigo
CDFUE	–	Carta dos Direitos Fundamentais da União Europeia
CE	–	Comissão Europeia
CIA	–	Central Intelligence Agency
CSS	–	Central Security Service
DOC	–	Department of Commerce
DOJ	–	Department of Justice
DOT	–	Department of Transportation
EIF	–	European Interoperability Framework
ELSJ	–	Espaço de Liberdade, Segurança e Justiça
EU	–	União Europeia
EUA	–	Estados Unidos da América
FISA	–	Foreign Intelligence Surveillance Act
FTC	–	Federal Trade Commission
G29	–	Grupo de Proteção de Dados do Artigo 29.º
GDS	–	Global Distribution System
i.e.	–	isto é
ICAO	–	International Civil Aviation Organization
IPA	–	Interface de Programação de Aplicações
ITA	–	International Trade Administration
n.º	–	Número
NSA	–	National Security Agency
OCDE	–	Organização para a Cooperação e Desenvolvimento Económico

para.	–	Parágrafo
paras.	–	Parágrafos
PNR	–	Passenger Name Record
PPD-28	–	Presidential Policy Directive 28
RGPD ou Regulamento	–	Regulamento Geral sobre a Proteção de Dados
ss.	–	Seguintes
TFUE	–	Tratado sobre o Funcionamento da União Europeia
TJ	–	Tribunal de Justiça da União Europeia
TUE	–	Tratado da União Europeia
UE	–	União Europeia
UIP	–	Unidade de Informações de Passageiros
v.	–	ver

Índice Sumário

Direitos do titular dos dados pessoais: o direito à portabilidade

Graça Canto Moniz*

Resumo: Este texto analisa os direitos do titular de dados pessoais, destacando um novo direito consagrado no Regulamento (UE) 2016/679: o direito à portabilidade. Num primeiro momento debruçamo-nos, de forma sintética, sobre os direitos específicos do titular dos dados pessoais, conforme estão previstos no regulamento para depois apreciarmos os traços essenciais do direito à portabilidade. Veremos as suas dimensões fundamentais, uma individual e outra económica, as faculdades que confere, o âmbito material de aplicação e, por fim, afloramos algumas dificuldades da sua aplicação prática.

Palavras-chave: *Regulamento Geral sobre a Proteção de dados pessoais; titular dos dados; direitos específicos; portabilidade.*

Abstract: This article aims to analyze data subject's rights, focusing the new right to data portability. First it briefly looks at the data subject specific rights present at the Regulation (EU) 2016/679 and, secondly, it describes with detail the right to data portability, highlighting its key dimensions, one individual and the other economic, the claims it recognizes to the data subject, its material scope, and, lastly, some of the practical problems regarding portability's implementation.

Keywords: *General Data Protection Regulation; Data Subject; special rights; portability.*

* Doutoranda na NOVA Direito onde investiga o tema "A extraterritorialidade do Regime Geral de Proteção de dados pessoais", membro do CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa e cocoordenadora do Observatório de Proteção de Dados Pessoais. Este artigo teve o apoio uma bolsa da Fundação para a Ciência e Tecnologia.

Introdução: a *jusfundamentalização* da proteção de dados pessoais na União Europeia

Em larga medida, a legislação sobre proteção de dados pessoais parte de um pressuposto geral: a posição de vulnerabilidade e de desvantagem estrutural das pessoas singulares numa sociedade marcada pela circulação de fluxos informacionais, de várias origens, com vários destinos e finalidades. A necessidade de institucionalizar meios de controlo do uso da informação pessoal, tendo em vista a tutela dos direitos e liberdades fundamentais, é anterior a fenómenos dos nossos tempos como o *Big Data*, a computação em nuvem ou a internet das coisas. Porém, o convulsivo contexto de digitalização da vida social a que vimos assistindo nas últimas décadas, incrementou a dispersão da informação pessoal dificultando, na prática, as possibilidades de conhecimento e controlo do seu titular. O imperativo da proteção de dados pessoais tem sido, justamente, assegurar esse conhecimento e controlo[1].

O compromisso da UE com este imperativo, renovado em 2010[2], tornou-se inequívoco desde a *jusfundamentalização* da proteção de dados pessoais. Não devemos ignorar que o ordenamento jurídico da UE, paredes meias com o direito ao respeito pela vida privada e familiar (art. 7.º da CDFUE) autonomizou o direito fundamental à proteção de dados pessoais, consagrado no art. 8.º daquele diploma e no art. 16.º do TFUE[3]. Sendo legítimas as dúvidas suscitadas sobre a autonomia destes dois direitos[4], certo é que o direito à proteção de dados é concretizado, em legislação secundária, por uma cartilha de direitos específicos, previstos no RGPD , que outorgam ao

---

[1] Sobre a ideia do "controlo individual sobre os dados pessoais", v., *inter alia,* Lynskey, Orla. *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015, pp. 177 e ss.

[2] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, "Uma abordagem global da proteção de dados pessoais na União Europeia", de 4 de novembro de 2010, p. 5 e Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, "Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI", de 25 de janeiro de 2012, p. 2.

[3] Noutras latitudes a proteção de dados pessoais não goza deste estatuto, v. Kuner, Christopher. *Transborder Data Flows and Data Privacy Law.* Oxford: Oxford University Press, 2013, p. 63.

[4] Lynskey, Orla. *The Foundations of EU Data Protection Law,* cit., pp. 89 e ss.

titular dos dados[5] as faculdades necessárias para participar e decidir sobre o destino dos seus dados pessoais.

Contudo, como tem sublinhado o TJ[6], o direito à proteção de dados pessoais não é absoluto, devendo ser perspetivado em relação à função desempenhada na sociedade, exigindo-se uma ponderação com outros direitos fundamentais, em sintonia com o princípio da proporcionalidade[7].

1. Os direitos específicos do titular dos dados pessoais

Assente num princípio liberal de autonomia deliberativa, a legislação de proteção de dados pessoais reconhece um lugar de relevo à vontade individual. De facto, um princípio nodal daquela é a *participação* do titular dos dados, o que, por um lado, lhe garante uma medida de *influência* nas operações de tratamento[8] e, por outro, se reflete numa cartilha de direitos assegurados mesmo nos casos em que a licitude do tratamento não decorre do consentimento do titular dos dados. Este acompanhamento das operações de tratamento consubstancia um controlo individual sobre os dados pessoais, independentemente do fundamento jurídico do tratamento[9].

---

[5] A definição de "titular dos dados" e de "dados pessoais" encontram-se densificadas no próprio regulamento, no art. 4.º, n.º 1, onde se lê: "informação relativa a uma pessoa singular identificada ou identificácel ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

[6] Acordão do TJ, C-275/06, ECLI:EU:C:2008:54, *Promusicae*, de 29 de janeiro de 2008, a propósito do direito à proteção efetiva da propriedade intelectual.

[7] Considerando 4 do RGPD.

[8] Bygrave, Lee. *Data Protection Law. Approaching Its Rationale, Logic and Limits*. The Hague: Wolters Kluwer, 2003, pp. 63 e ss.

[9] Commission Staff Working Paper, "Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", de 25 de janeiro de 2012, p. 53.

O RGPD herda da Diretiva 95/46[10] este conjunto de direitos. Além de algumas novidades, a haver diferenças em relação à diretiva, residem não tanto no seu enunciado quanto nas particularidades e modalidades do seu exercício, detalhadamente expressas no art. 12.º, onde se prescreve o princípio da transparência das informações e das comunicações e as regras para o exercício destes direitos específicos, nomeadamente os prazos que vinculam o responsável pelo tratamento. Tal como na diretiva, estes encontram-se obrigados a adotar medidas adequadas para facilitar o exercício dos direitos do titular dos dados[11]. Por outro lado, nota-se uma particular preocupação do legislador em relação a crianças[12]. Em sintonia com o que dissemos sobre a natureza relativa do direito à proteção de dados pessoais, o direito da União ou dos Estados-Membros pode impor restrições a princípios específicos e a direitos individuais do titular, em face do imperativo da salvaguarda de interesses gerais, como a segurança do Estado entre outros. Naturalmente, estas restrições devem observar a CDFUE e a Convenção Europeia para a Proteção dos Direitos Humanos[13]. É também de salientar que a Autoridade Europeia para a Proteção de Dados criticou o art. 23.º do RGPD por consubstanciar uma ampliação do âmbito destas restrições[14].

O objetivo da reforma de 2012, em matéria de direitos do titular dos dados foi duplo[15]: por um lado, o RGPD corrige as divergências nacionais de implementação da diretiva[16], com ganhos significativos ao nível da segurança

---

[10] Directiva 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, doravante "diretiva".

[11] Nos termos do n.º 8 do art. 12.º a Comissão Europeia é competente para adotar atos delegados para determinar procedimentos-tipo para o exercício dos direitos individuais, deste modo eliminando divergências entre os Estados-Membros.

[12] Considerando 38 do RGPD.

[13] Art. 23.º e considerando 73 do RGPD.

[14] Autoridade para a Proteção de Dados, "Parecer sobre o pacote de reforma legislativa sobre a proteção de dados", de 7 de março de 2012, p. 160.

[15] Uma notável crítica aos objetivos da reforma encontra-se em Koops, B. "The Trouble with European Data Protection Law", *International Data Privacy Law,* n.º 4, 2014, pp. 250 e ss.

[16] Comissão Europeia, "Relatório da Comissão. Primeiro relatório sobre a implementação da diretiva relativa à proteção de dados 95/46/CE", adotado a 15 de maio de 2003, p. 18. Disponível em: <https://www.cnpd.pt/bin/actividade/Pri_rel_implementaDIR.pdf> (acedido a 8/12/2017).

jurídica e da uniformização das garantias do titular dos dados na União[17]; por outro lado, reforçou a transparência das operações de tratamento, com reflexo nas obrigações que recaem sobre o responsável pelo tratamento[18], proporcionando às pessoas singulares meios eficazes para assegurar que estão plenamente informadas quanto ao que sucede aos seus dados pessoais e facilitando o exercício dos seus direitos[19].

1.1. O direito à informação

As informações sobre o tratamento devem ser fornecidas ao titular dos dados no momento da sua recolha (art. 13.º) ou, não sendo esta efetuada junto do titular, dentro de um prazo, dependendo das circunstâncias do caso (art. 14.º). Seja como for, o legislador prevê o conteúdo mínimo da informação a prestar, designadamente a identidade e contacto do responsável pelo tratamento, as finalidades do tratamento, o fundamento jurídico, os destinatários dos dados, a existência de um direito de acesso, retificação, de portabilidade e a (não) obrigatoriedade de responder às questões. O RGPD expande as categorias de informação a prestar com o fim de garantir um "tratamento equitativo e transparente", assumindo particular importância a informação prestada sobre a "existência de decisões automatizadas, incluindo a definição de perfis" e "informações úteis relativas à lógica subjacente" dos perfis. Trata-se de um *direito à explicação* de decisões adotadas com base em algoritmos ou em sistemas automatizados e de inteligência artificial[20]. De resto, do n.º 5.º do art. 14.º decorrem as exceções que dispensam o responsável pelo tratamento desta obrigação de informar.

---

[17] N.º 2 do art. 288.º do TFUE sobre os efeitos do RGPD.

[18] Em sintonia, aliás, com a tendência desta reforma de incutir maior responsabilidade (a ideia de *accountability*) no responsável pelo tratamento de dados pessoais. v. Comunicação da Comissão, "Proteção da privacidade num mundo", cit., p. 7.

[19] Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA Privacy and Security Law Report*, de 6 de fevereiro de 2012, p. 10.

[20] Hildebrandt, Mireille. "The New Imbroglio – Living with Machine Algorithms", *The Art of Ethics in the Information Society*. Amesterdam: Amesterdam University Press, 2016, pp. 55 e ss.

A prestação de informação e o acesso aos dados pessoais – que veremos de seguida – são condições indispensáveis para o titular dos dados exercer os demais direitos e efetuar as verificações necessárias no sentido de escrutinar e apreciar a licitude do tratamento, sujeita aos critérios do art. 6.º. Por isso, estes direitos foram descritos como o núcleo da proteção de dados pessoais, permitindo que os titulares identifiquem os dados sobre si, conhecidos por terceiros, os usos a que estão acometidos, a veracidade e qualidade dos mesmos e a licitude do tratamento[21].

1.2. O direito de acesso

O âmbito deste direito, previsto no art. 15.º, não se restringe ao mero acesso aos dados. O titular pode obter, do responsável pelo tratamento, a confirmação da (in) existência do tratamento e um conjunto de informação suplementar que coincide, em larga medida, com aquela que deve constar da notificação ao abrigo do direito à informação: finalidades do tratamento, categorias de dados, destinatários, prazo de conservação, etc. Devemos salientar aqui a importância que assume, o direito à informação previsto no n.º 2 do art. 15.º, no caso de transferências para um país terceiro ou organização internacional. Sempre que os dados pessoais atravessam fronteiras do território da UE, há um risco acrescido de o titular não conseguir exercer os direitos que lhe assistem[22].

Do ponto de vista prático, o titular dos dados deverá, em primeiro lugar, identificar a quem submeter o pedido de acesso (*i. e*, o responsável pelo tratamento) e, em segundo lugar, determinar o procedimento a seguir para esse efeito (online, por correio normal ou formulário específico fornecido pelo responsável pelo tratamento, etc.)[23]. Para facilitar este procedimento,

---

[21] Lorber, Steven. "Data Protection and Subject Access Requests", *Industrial Law Journal*, vol. 33, 2004, pp. 179 e ss. e L'Hoiry, Xavier e Norris, Clive. "The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European Study", *International Data Privacy Law*, vol. 5, issue 3, 2015, pp. 190 e ss.

[22] Considerando 116 do RGPD.

[23] Sobre esta componente prática v. L'Hoiry, X. e Norris, C. "The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European Study", cit., p. 192.

sempre que for possível, o responsável pelo tratamento deverá facultar um sistema seguro, por via eletrónica, que possibilite o acesso direto aos dados[24].

O acesso abre caminho a uma revisão do tratamento de dados pessoais, realizada diretamente pelo seu titular, para que conheça quais os dados tratados, verifique a qualidade e veracidade dos mesmos bem como a licitude do tratamento.

1.3. O direito de retificação e de apagamento

Verificando a qualidade dos dados e constatando a sua inexatidão ou incompletude, o titular tem o direito de os retificar, nos termos do art. 16.º. Diga-se também que, constatando a inexistência de um fundamento jurídico para o tratamento, sem prejuízo das outras situações dispostas no n.º 1 do art. 17.º, pode requerer o apagamento dos dados. Em bom rigor e verdade, este direito a ser esquecido é uma extensão do direito ao apagamento previsto na alínea b) do art. 12.º da diretiva[25]. Porém, anotam-se três diferenças: (i) em face da "desarmonização" tolerada pela diretiva, o exercício do direito ao apagamento era mais fácil em alguns Estados-Membros[26]; (ii) depois, é manifesta a preocupação com crianças que, quando consentem, não estarão totalmente cientes dos riscos inerentes ao tratamento[27]; (iii) por fim, uma garantia adicional para o titular dos dados pessoais encontra-se plasmada no n.º 2 do art. 17.º, para dados *públicos*, sob a forma de uma obrigação de informação aos "responsáveis pelo tratamento efetivo dos dados" do pedido de apagamento. Antecipando as dificuldades técnicas do controlo da informação no ambiente online, o legislador introduziu critérios de razoabilidade, disponibilidade tecnológica e de custos, flexibilizando esta obrigação e aproximando-a de uma *obrigação de meios* e não de resultado. Esta moderada consagração do apagamento de dados explica-se à luz dos desafios colocados pela internet: multiplicação instantânea e ubiquidade

---

[24] Considerando 63 do RGPD.

[25] Acórdão do TJ, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, de 13 de maio de 2014.

[26] A Comissão recebeu muitas queixas de indivíduos que não conseguiram retirar os seus dados pessoais dos fornecedores de serviços online, designadamente fotografias. v. Comunicação da Comissão, "Uma abordagem global", cit., p. 7.

[27] Considerando 65 do RGPD.

de informação, de difícil controlo em termos técnicos e em relação ao conteúdo[28]. Por outro lado, é uma resposta do legislador à tendência de travar, em sintonia com o TJ[29], a retenção de dados pessoais[30].

1.4. O direito à limitação do tratamento

Ao abrigo da diretiva, o titular dos dados dispunha do direito de bloquear os dados pessoais[31]. Uma faculdade semelhante encontra-se no art. 18.º através de uma restrição[32] das operações de tratamento, nos casos enumerados no n.º 1. Em certa medida, poderá assumir uma natureza *cautelar* bastante útil enquanto o titular dos dados pondera uma estratégia de defesa judicial[33].

O responsável pelo tratamento deverá indicar de forma bem clara, no sistema informático, que o tratamento daqueles dados se encontra restringido, através da "inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro[34]" podendo, nos termos do considerando 67, socorrer-se de "métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados". O efeito desta limitação não tem implicações na conservação dos dados,

---

[28] Zanfir, Gabriela. "The right to data portability in the context of the EU data protection reform", *International Data Privacy Law,* vol. 2, issue 3, 2012, p. 8.

[29] Acórdão do TJ, C-293/12 e C-594/12, ECLI:EU:C:2014:238, *Digital Rights*, de 8 de abril de 2014.

[30] Warner, Jeremy. "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps", *University Ottawa Law and Technology Journal*, vol. 2, 2005, p. 75.

[31] Alínea b), do art. 12.º da diretiva.

[32] De Hert, Paul e Papakonstantinou, Vangelis. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review,* vol. 32, 2016, Southampton, pp. 189 e ss.

[33] *Idem*, p. 189.

[34] N.º 3, do art. 4.º do RGPD.

mas afeta todas as demais operações de tratamento que só podem ser realizadas, excecionalmente, nas situações previstas no n.º 2 do art. 18.º.

1.5. O direito de oposição

O titular dos dados pessoais goza, nos termos do art. 21.º, do poder de se opor ao tratamento de dados, em qualquer momento, por razões preponderantes e legítimas relacionadas com a sua situação particular. Sendo um reconhecimento do direito à autodeterminação, por um lado, o seu exercício não é absoluto – com a exceção dos tratamentos para efeitos de comercialização direta[35] – e, por outro, a sua aplicação não é geral. Desde logo, depende do *juízo de ponderação* entre as "razões imperiosas e legítimas" para o tratamento, invocadas pelo responsável, e os "interesses, direitos e liberdades do titular dos dados". Depois, a previsão legal inclui apenas quatros situações determinadas pelos fundamentos jurídicos do tratamento conforme as alíneas e), f) e o n.º 4 do art. 6.º.

O tratamento de dados para efeitos de comercialização direta é autonomizado nos n.º 2 e 3 do art. 21.º, tal como o tratamento para fins de investigação científica ou história ou para fins estatísticos, no n.º 6 do art. 21.º. Compreende-se esta diferenciação e flexibilização de regimes, já que a comercialização direta se enquadra no ambiente de ubiquidade informacional contemporâneo e os tratamentos de investigação científica e fins semelhantes gozam de um regime legal específico, como se depreende do considerando 156[36].

1.6. Decisões individuais e automatizadas

A criação de perfis, incluída na categoria das decisões automatizadas, constitui um tipo de tratamento de dados pessoais destinado a avaliar determinados aspetos da personalidade do titular dos dados ou a analisar e/ou prever a sua capacidade profissional, situação financeira, localização,

---

[35] N.º 2 e 3 do art. 21.º do RGPD.

[36] Hert, Paul e Papakonstantinou, Vagelis. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", cit., p. 189.

saúde, preferências pessoais, fiabilidade ou comportamento[37]. O art. 22.º baseia-se no anterior art. 15.º, da diretiva, e na recomendação do Conselho da Europa sobre a criação de perfis[38], ensaiando uma inversão numa tendência, registada em processos decisórios das organizações, para a tomada de decisões exclusivamente com base em perfis e sem o conhecimento do titular dos dados. A criação de perfis é um tema que tem suscitado acesos debates: os apologistas da proteção de dados destacam os riscos decorrentes de processos decisórios automatizados; já os seus defensores apontam-lhe os méritos que se sobrepõem àqueles riscos e que, em todo o caso, podem ser mitigados e controlados[39]. Também se tem dito que o problema central não é a definição de perfis *per se* mas a falta de informação acerca da lógica algorítmica que desenvolve esses perfis e afeta o titular dos dados[40]. Nessa medida, o RGPD não proíbe esta prática, mas propõe-se prevenir riscos decorrentes de uma decisão alcançada *sem qualquer intervenção humana*. Daí que se reconheça ao titular dos dados o direito a não ficar sujeito a uma decisão (i) tomada exclusivamente com base num tratamento automatizado, incluindo a definição de perfis e que (ii) produza efeitos na sua esfera jurídica ou que o afete significativamente. Assim, o titular dos dados tem direito a obter a intervenção humana, a expressar o seu ponto de vista e a obter uma explicação sobre a lógica da decisão, podendo sindicá-la.

Como noutros casos, este não é um direito geral e absoluto, sendo o seu campo de aplicação determinado em função do fundamento jurídico invocado para o tratamento dos dados, com se depreende do n.º 2, do art. 22.º do RGPD. Porém, o responsável pelo tratamento deverá sempre,

---

[37] A definição encontra-se no n.º 4 do art. 4.º do RGPD. Sobre os problemas que coloca, v. *inter alia,* Hildebrandt, Mireille e Gutwirth, Serge (eds.). *Profiling the European Citizen. Cross-Disciplinary Perspective*. London: Springer, 2008, pp. 17 e ss.

[38] Conselho da Europa, "Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling", de 23 de novembro de 2010. Disponível em: <https://wcd.coe.int/ViewDoc.jsp?p=&id=1929429&Site=CM&direct=true> (acedido a 8/12/2017).

[39] De Hert, Paul e Papakonstantinou, Vagelis. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", p. 189.

[40] No mesmo sentido, v. Autoridade Europeia para a Proteção de Dados, "Parecer 3/2015, A grande oportunidade da Europa. Recomendações da AEPD sobre as opções da UE para a reforma da proteção de dados", de 28 de julho de 2015. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_pt.pdf> (acedido a 8/12/2017).

pelo menos, adotar "medidas adequadas" para salvaguardar os direitos e liberdades fundamentais, designadamente a intervenção humana e a participação do visado no processo decisório e na sua contestação (art. 22.º, n.º 2).

1.7. Reclamações e recursos judiciais

Para terminar esta explicação perfunctória sobre os direitos do titular dos dados, há que dizer que o titular dos dados pode apresentar uma *reclamação* a uma autoridade de controlo, designadamente no Estado-Membro da sua residência habitual[41]. Tem também o direito a intentar uma *ação judicial*, nos termos do art. 47.º da CDFUE, peticionando a violação dos direitos que lhe são conferidos pelo RGPD pelo responsável pelo tratamento ou subcontratante ou, ainda, se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos[42].

O art. 82.º prevê também o direito de indemnização. O responsável pelo tratamento ou o subcontratante devem reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o RGPD.

2. O direito à portabilidade dos dados pessoais

Inicialmente, "portabilidade" era um termo exclusivamente usado nas discussões entre os entusiastas da tecnologia[43]. Nos dias de hoje, representa uma nova geração de conceitos acolhidos na gramática jurídica da proteção de dados pessoais. O debate sobre a portabilidade gira à volta dos mecanismos de mobilização de categorias de informação transmitida para o ambiente online, entre diferentes sítios da internet, como listas de

---

[41] Art. 77.º do RGPD.

[42] Considerandos 141 e ss. e arts. 78.º e 79.º.

[43] Existem vários tipos de portabilidade noutras áreas, v. G29, "Guidelines on the right to data portability", adotadas a 13 de dezembro de 2016 e revisto no dia 5 de abril de 2017. Desenvolvendo as origens da portabilidade, v. Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer Law & Security Review,* vol. 33, 2017, pp. 57 e ss.

contactos ou endereços de email[44]. Acontece também que, há medida que se banalizou a utilização da computação em nuvem, o interesse neste instituto foi crescendo[45] até a um recente apelo à intervenção dos Estados na criação de políticas públicas uniformes para estimular a interoperabilidade e portabilidade dos serviços de computação em nuvem[46].

Mas a portabilidade é também – e sobretudo – uma "porta de entrada" no ambiente digital para o controlo do utilizador e titular de dados[47]. Com a tendência para a digitalização das atividades humanas e interações sociais, há quem proponha que os dados pessoais, sobretudo quando combinados através de técnicas de *data mining*, constituem uma continuação da personalidade individual no mundo digital, suscitando problemas complexo ao direito[48]. Outros, mais céticos, invocam a incapacidade do utilizador para, num ambiente já bastante complexo, acompanhar e controlar as transmissões dos seus dados entre serviços e a falta de transparência destas operações, além de preocupações com a segurança e, cada vez mais, com o roubo de identidade[49]. Em qualquer caso, consagrada no art. 20.º, a portabilidade é uma das novidades do RGPD.

---

[44] De Hert, Paul e Papakonstantinou, Vagelis. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", cit., p. 189.

[45] O G29 define a "computação em nuvem" como o "conjunto de tecnologias e modelos de serviços centrados na utilização e fornecimento via Internet de aplicações informáticas, de capacidade de tratamento e armazenamento e de espaço de memória". Existe, nos dias de hoje, um consenso alargado sobre as implicações da computação em nuvem para a proteção de dados pessoais. Se, por um lado, as normas de proteção de dados poderão, até certo ponto, dificultar a utilização e o desenvolvimento deste tipo de serviços, por outro lado, a computação em nuvem evidencia limitações nos esquemas lógicos da proteção de dados. Esta dificuldade foi reconhecida pelo G29 e por algumas autoridades de supervisão de proteção de dados pessoais, v. "Parecer 5/2012 sobre Computação na Nuvem", de 1 de julho de 2012.

[46] Zanfir, Gabriela. "The right to data portability in the context of the EU data protection reform", cit., p. 3.

[47] Autoridade Europeia para a Proteção de Dados, Parecer 3/2015, cit., pp. 3 e ss.

[48] Gabriela Zanfir apela, por exemplo, à incorporação do conceito jurídico de personalidade digital, *The right to Data*, cit., pp. 3 e 13, tal como Roosendaal, Arnold. *Digital Personae and Profiles, in Law: Protecting Individuals Rights*. Online Contexts, Wolf Legal Publishers, 2013.

[49] Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", cit., p. 60.

2.1. Ratio: *dimensão individual e económica*

Percebe-se que a dimensão preponderante da portabilidade seja de natureza *individual*, situando-se o seu objetivo imediato na perspetiva do titular dos dados, na sua capacitação, no reforço do controlo sobre os seus dados no ambiente digital ou no "ecossistema de dados[50]". Este direito vem criar uma ferramenta de *autogestão* para o titular determinar os destinos da informação sobre si, de acordo com a sua vontade e os seus interesses, assemelhando-se por isso a uma *extensão do exercício efetivo da manifestação e revogação do consentimento*[51]. A portabilidade permite-lhe reajustar o equilíbrio da relação, estruturalmente desigual, entre o responsável pelo tratamento/prestador do serviço e o titular dos dados, posicionando o segundo no lugar de mediador dos fluxos de dados que lhe digam respeito. Em cenários complexos, como a computação em nuvem, o titular dos dados permanecerá minimamente no controlo da informação sobre si, o que, seguramente, tem impacto na confiança depositada nestes serviços, elemento essencial de uma economia digital[52].

Acresce, também, a importante *dimensão económica* da portabilidade. A intenção de eliminar obstáculos à circulação de dados pessoais na UE continua a ser um dos objetivos do RGPD[53], pelo que a simplificação da transmissão direta de dados pessoais entre responsáveis pelo tratamento cria condições para facilitar os fluxos de dados e para assegurar e estimular a concorrência entre responsáveis pelo tratamento, prestadores de serviços online, de computação em nuvem e para promover a confiança na economia digital[54]. Note-se que a Comissão Europeia fundamentou a introdução deste direito com a necessidade de contornar as dificuldades de transmitir dados pessoais entre aplicações ou serviços, dando nota da

---

[50] G29, *Guidelines on the right*, cit., pp. 3 e ss.

[51] De Hert, Paul e Papakonstantinou, Vagelis. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", cit., p. 189.

[52] De acordo com a Comissão europeia, só 12% dos Europeus que utilizam serviços online se sentem completamente seguros a fazer transações online. v. COMISSÃO EUROPEIA, "Digital Agenda for Europe". Disponível em: <http://eige.europa.eu/resources/digital_agenda_en.pdf> (acedido a 8/12/2017).

[53] Considerando 10 do RGPD.

[54] Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", cit., pp. 59 e 60.

sua importância enquanto fator de competitividade, como foi evidente noutros segmentos de mercado, como a portabilidade do número no setor das telecomunicações[55]. Aliás, é neste contexto que situamos a discussão em torno da possibilidade de a Comissão reagir a uma situação de abuso de posição dominante por empresas que limitem os seus clientes a transferir os dados para outros prestadores[56].

Por outro lado, é hoje inegável que os dados pessoais assumem um valor económico enriquecendo o serviço prestado e permitindo adequar a oferta às necessidades do cliente e a oferta de serviços de melhor qualidade[57]. Desta situação nasce um risco de *lock-in* a um certo fornecedor ou serviço que se recusa a fornecer os dados pessoais para reutilização[58], justificada em limitações técnicas e nos custos à mobilidade e transmissão dos dados. O controlo da reputação dos utilizadores de leilões online, i. é, da acumulação dos resultados das suas transações, evidenciado num caso que envolveu o eBay, é um exemplo do bloqueio à concorrência neste tipo de serviços[59]. É que qualquer limitação à portabilidade dos dados e à

---

[55] Commission Staff Working Paper, Impact Assessment, cit., p. 28. Uma ideia reforçada pelo Comissário para a Concorrência, em 2012, v. "Competition and Personal Data Protection". Disponível em: <http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> (acedido a 8/12/2017).

[56] Graef, Inge; Verschakelen, Jeroen e Valcke, Peggy. "Putting the right to data portability into a competition law perspective", *Annual review. The journal of the Higher School of Economics,* 2013, pp. 53 e ss. Afastando esta hipótese, Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", cit., pp. 61 e ss.

[57] O que se nota, com particular acuidade, nas indústrias do *Quantified Self* e da *Internet of things*, exemplos que espelham os benefícios (e os riscos...) do cruzamento de dados pessoais sobre os diferentes aspetos das nossas vidas, como a atividade física, o consumo calórico, permitindo uma radiografia complete e precisa sobre a vida do visado, resumida num único ficheiro, v. G29, *Guidelines*, cit., p. 5.

[58] "Internet social networks operate for the time-being as closed gardens for their users: once in they enjoy all (free) functionalities, but they may never leave", v. De Hert, Paul e Papakonstantinou, Vagelis. "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", p. 190 e Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", cit., pp. 57 e ss.

[59] Piker, Randal. "Competition and Privacy in the Web 2.0 and the Cloud C", *Coase-Sandor Working Paper Series in Law and Economics,* 2008, p. 9.

interoperabilidade dos sistemas dificulta a migração dos dados entre serviços e, por conseguinte, restringe a faculdade de escolha do consumidor. Por fim, com base em algumas experiências europeias, acredita-se que o controlo e a partilha de dados pelo seu titular dará origem a novos modelos de negócio, estimulando a inovação[60].

2.2. Faculdades: receber e transmitir

O direito à portabilidade reconhece ao titular duas faculdades: a de receber um conjunto de dados pessoais e a de transmitir esses dados entre responsáveis pelo tratamento. Trata-se, antes de mais, do direito a receber um subconjunto de dados pessoais[61], armazenar esses dados num dispositivo privado, sem necessariamente se seguir uma transmissão imediata para outro responsável pelo tratamento. Assim se abrangem não só as situações em que o titular pretende transferir todos os seus dados para outro fornecedor como, também, os casos em que pretende assegurar a interoperabilidade, por exemplo, entre várias "nuvens" que utiliza. Aproximando-se do direito de acesso é, na verdade, mais do que isso: é o seu complemento[62].

A especificidade da portabilidade é a de oferecer uma ferramenta prática para o titular gerir e reutilizar os dados que lhe digam respeito, de acordo com a sua vontade e interesses[63]. Daí a importância de cumprir as caraterísticas técnicas enunciadas no n.º 1: "formato estruturado", "uso corrente" e "leitura automática". É que não se pretende apenas facultar o

---

[60] G29, *Guidelines*, cit., p. 5. Apontam-se as experiências como o MiData no Reino Unido e a MesInfos/SelfData, pela FING, em França.

[61] Veremos que a portabilidade não abrange todos os dados pessoais do titular dos dados mas apenas um certo tipo de dados, v. G29, *Guidelines*, cit., p. 4.

[62] Na proposta do Parlamento, encontravam-se fundidos num só artigo, o art. 15.º v. Parlamento Europeu, "Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)", 2012. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212> (acedido a 8/12/2017).

[63] G29, *Guidelines*, cit., pp. 4 e 5.

acesso aos dados como, ainda (e sobretudo), possibilitar a sua utilização subsequente e agilizar um controlo efetivo[64].

A segunda faculdade, "o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir", foi amplamente disputada nas negociações entre Comissão, Parlamento e Conselho. Inicialmente, a proposta da Comissão reconhecia o direito à transferência *direta* entre os responsáveis pelo tratamento, sem sujeição a nenhuma condição, algo que foi rejeitado pelo Parlamento, que restringiu a transferência *direta* apenas aos casos em que tal seja "tecnicamente possível[65]". Assim, os dados podem ser transmitidos ao titular ou a outro responsável pelo tratamento, sendo que o G29 propôs para esse efeito algumas soluções, como um servidor SFTP, uma WebAPI ou um WebPortal[66].

2.3. Âmbito material de aplicação

O RGPD não consagra um direito *geral* à portabilidade[67]. Em rigor, de acordo com o art. 20.º, o seu âmbito material de aplicação depende de um conjunto de condições cumulativas relacionadas com o *tipo* de dados, com o *fundamento jurídico* que enquadra o tratamento e com o *tipo* de tratamento. Uma primeira limitação, particularmente exigente, quanto ao *tipo* de dados abrangidos pela portabilidade: apenas aqueles que "digam respeito" ao titular e que este "tenha fornecido", com conhecimento e de forma ativa, como a informação pessoal descarregada numa rede social ou preenchida num formulário online. Há, pois, que ter presente que, por exemplo, não são de excluir os dados pseudonimizados já que podem ser relacionados

---

[64] O G29 dá vários exemplos: o titular dos dados pretende recuperar a sua playlist de um serviço de *streaming* de música; a sua lista de contactos da aplicação do *webmail* para criar e preparar uma lista de casamento; pretende aceder ao seu historial de compras de um cartão de fidelização ou avaliar a sua pegada de ecológica, v. *Ibidem*.

[65] Exemplificando, a proposta inicial, que também era especificamente vocacionada para as redes sociais, reconhecia a um utilizador do Facebook o direito de pedir que o Facebook transferisse diretamente para o Google + os seus dados, sem que o titular tivesse de os descarregar para posteriormente os carregar no Google +.

[66] G29, *Guidelines*, cit., p. 16.

[67] Considerando 68 e art. 20.º, n.º 3, do RGPD.

com o seu titular[68]. Por outro lado, o G29 recomenda uma interpretação ampla em torno da expressão "dados pessoais que digam respeito ao titular" de modo a abranger, nos dados "portáveis", informação sobre terceiros, mas neste caso apenas quando o pedido de portabilidade seja para fins pessoais[69].

Sabendo que os responsáveis pelo tratamento, sobretudo os prestadores de serviços online, não tratam apenas informação que é "fornecida" pelo utilizador, analisando-a também para gerar novo *conhecimento* sobre o titular, colocam-se dúvidas quanto à interpretação a dar à expressão "dados que o titular tenha fornecido". A este propósito, o G29 identifica duas categorias de dados "fornecidos pelo titular": (1) os dados ativa e conscientemente transmitidos por si e (2) os dados "observados", i. é, "fornecidos" pelo titular por via da sua utilização do serviço, plataforma ou aparelho[70]. Na primeira categoria, inserem-se os endereços de email, os nomes de utilizador, a idade, ficheiros descarregados, atualizações de estados, fotografias, etc. Na segunda categoria, o histórico de pesquisas, os dados de tráfego, os dados de localização e dados em bruto, como o batimento cardíaco registado num aparelho de fitness.

Entende também aquela entidade, com base num critério de *origem*, que os dados gerados pelo responsável pelo tratamento com base nos dados fornecidos pelo titular, tais como a criação de um perfil de saúde ou de crédito, um processo de recomendação, a categorização do utilizador, resultados algorítmicos, um perfil de crédito e outro tipo de perfis[71] ou o resultado de uma avaliação sobre a saúde do utilizador[72], são excluídos da portabilidade. São dados *inferidos* e dados *derivados*, gerados pelo responsável pelo tratamento, a partir dos dados "fornecidos pelo titular". Ou seja, para efeitos do direito à portabilidade, os dados resultantes da mera *observação* do comportamento e atividade do titular distinguem-se dos dados pessoais

---

[68] N.º 2, do art. 11.º do RGPD e G29, *Guidelines*, cit., p. 7.

[69] Como acontece nos registos de transações bancárias ou nos registos telefónicos, que incluem transações e chamadas recebidas por terceiros. Adiante voltaremos a aflorar este aspeto.

[70] G29, *Guidelines*, cit., p. 8.

[71] G29, *Guidelines*, cit., p. 10.

[72] Note-se, porém, que a exclusão do âmbito da portabilidade não exclui a aplicação de outros direitos, como o direito previsto no art. 22.º do RGPD.

criados pela *análise* desse comportamento. Se, por um lado, esta distinção é melindrosa em relação a modelos de negócio dependentes dos dados pessoais "fornecidos" pelo titular, como sucede no *Online Fashion Advisor*[73] ou com os avatares criados em jogos online como o *World of Warcraft* e o perfil de vendedor em sites de leilões online[74]; por outro lado, restingue os dados que o utilizador por exigir do prestador de serviços, evidente num exemplo da *internet of things* relativo ao aquecimento de um casa: o titular dos dados pode requerer o rastreamento dos movimentos de ocupação da casa, detetados por um termostato inteligente, mas não o horário algoritmicamente determinado para aquecer a casa[75].

No que diz respeito ao *fundamento jurídico,* a portabilidade, associada como se viu à vontade individual e à autodeterminação, é aplicável somente quando o fundamento é o *consentimento* ou o *cumprimento* de um contrato[76]. Exemplificando, os títulos dos livros comprados numa livraria online ou a lista de músicas num serviço de *streaming* são exemplos de dados pessoais tratados com base no cumprimento de um contrato[77]. Tal não exclui que, em termos de boas práticas, a portabilidade seja implementada quando o fundamento jurídico seja outro[78]. Exclui-se, isso é certo, a portabilidade nos casos em que uma instituição financeira trate dados pessoais no âmbito de uma obrigação jurídica, por exemplo para o efeito de prevenção e deteção de lavagem de dinheiro e outros crimes financeiros[79]. Já nos casos de

---

[73] Van Der Auwermeulen, Barbara. "How to attribute the right to data portability in Europe: A comparative analysis of legislations", cit., p. 61.

[74] *Idem*, p. 70.

[75] Urquhart, Lachlan; Sailaja, Neelima e Mcauley, Derek. "Realising the right to data portability for the domestic Internet of things". *Personal and Ubiquitous Computing Economics*. London: Springer 2017, pp. 53 e ss.

[76] Alínea a) do n.º 1, do art. 20.º, do RGPD. Este foi um aspeto criticado pela Autoridade Europeia para a Proteção de Dados no primeiro parecer sobre a proposta de regulamento da Comissão, "Opinion of the European Dat Protection Supervisor on the data protection reform package", de 12 de março de 2012, p. 25. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> (acedido a 8/12/2017).

[77] G29, *Guidelines*, cit., p. 7.

[78] Sendo o interesse legítimo do titular dos dados, v. G29, "Parecer 6/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE", adotado em 9 de abril de 2014, pp. 47 e 48. Disponível em: <http://www.gpdp.gov.mo/uploadfile/2015/0803/20150803050042662.pdf> (acedido a 8/12/2017).

[79] G29, *Guidelines*, cit., p. 8.

tratamentos de dados pessoais relativos a colaboradores e funcionários impõe-se uma análise casuística, porquanto em muitos casos o tratamento fundamenta-se no interesse legitimo do responsável[80].

Por último, o exercício do direito à portabilidade é aplicável apenas a tratamentos automatizados, excluindo ficheiros em papel ou o tratamento de dados necessários ao exercício de funções de interesse público ou de autoridade pública[81].

2.4. Problemas específicos da aplicação prática da portabilidade

A este direito são aplicáveis as regras gerais para o exercício dos direitos dos titulares dos dados, previstas no art. 12.º, designadamente a obrigação de responder "sem demora injustificada e no prazo de um mês a contar da data da receção do pedido, bem como o dever de informar a disponibilidade da portabilidade", nos termos da alínea b), do n.º 2, do art. 13.º e da alínea c), do n.º 2, do art. 14.º, do RGPD[82]. Além disto, deparamo-nos com algumas particularidades em relação à aplicação prática deste direito.

Desde logo, a *portabilidade de dados anónimos*. Ou, melhor dizendo, a relação entre a viabilidade e a eficácia da portabilidade e a anonimização de dados. Aludimos *supra* à exclusão dos dados anónimos do âmbito de aplicação do RGPD pelo que, *prima facie*, tudo indica que a portabilidade não abrange estes dados[83]. O processo de anonimização constitui um "tratamento ulterior", exigindo por isso um fundamento jurídico nos termos do art. 6.º do RGPD[84]. Ora, nenhum problema se coloca nos casos em que o titular dos dados exerça o direito à portabilidade *antes* da operação de anonimização. O mesmo não se pode dizer se *consentir* nesta operação de anonimização, pretendendo, posteriormente, exercer o direito à portabilidade. Se, por um lado, o RGPD exclui do seu âmbito de aplicação os dados anónimos, por

---

[80] *Idem*, p. 9.

[81] Alínea b), do n.º 1, e n.º 3 do art. 20.º do RGPD.

[82] O G29 recomenda que, na informação a prestar seja feita uma explicação sobre a distinção entre a portabilidade e o acesso aos dados pessoais. v. G29, *Guidelines*, cit., p. 11.

[83] Zanfir, Gabriela. "The right to Data portability in the context of the EU data protection reform", cit., pp. 10, 13 e 14.

[84] G29, Parecer 5/2014, cit., p. 7.

outro lado, um dos objetivos da portabilidade – prevenir uma situação de *lock-in* – será difícil de garantir neste segundo caso[85].

Ademais, à data em que escrevemos, são ainda evidentes os problemas técnicos em torno da execução ou implementação deste novo direito que dificultam o respetivo cumprimento por parte dos responsáveis pelo tratamento[86]: (i) quais as ferramentas da portabilidade, i. é, as medidas técnicas a adotar pelos responsáveis pelo tratamento de modo a permitir o exercício deste direito e (ii) qual o formato dos "dados portáveis[87]"? Quanto às ferramentas da portabilidade, os responsáveis pelo tratamento deverão implementar um mecanismo de download direto e, sempre que tecnicamente possível, de transmissão direta dos dados para outro responsável. O G29 recomenda a disponibilização de uma IPA ou *Interface de Programação de Aplicações*[88].

O *formato* dos "dados portáveis" é também um aspeto crucial para a eficácia e viabilidade da portabilidade: o responsável que os "recebe" deve ser capaz de os tratar sem prejuízos para a sua qualidade e rigor. Daí que, segundo o art. 20.º, n.º 1, o formato tem de permitir a sua reutilização, pelo que deverá ser "estruturado, de uso corrente e de leitura automática[89]". O considerando 68 acrescenta, ainda, uma caraterística, a

---

[85] Zanfir, Gabriela. "The right to Data portability in the context of the EU data protection reform", cit., p. 11.

[86] *Idem*, pp. 3 e ss.

[87] G29, *Guidelines*, cit., p. 5.

[88] Definido como "(...) a set of subroutine definitions, protocols, and tool for building software and applications. It refers to the interfaces of applications or web services made available by data controllers, so that other systems or applications can link and work with their systems". G29, *Guidelines*, cit., p. 5, nota de rodapé 5.

[89] Por "leitura automática" deve-se entender "um formato de ficheiro estruturado de modo a ser facilmente possível, por meio de aplicações de *software*, identificar, reconhecer e extrair dele dados específicos. Os dados codificados em ficheiros estruturados num formato legível por máquina são dados legíveis por máquina. Os formatos legíveis por máquina podem ser abertos ou exclusivos; podem ser normas formais ou não. Os documentos codificados num formato de ficheiro que limita o tratamento automático, devido ao facto de ou não ser possível extrair os dados desses documentos ou isso não ser facilmente possível, não deverão ser considerados documentos em formato legível por máquina. Os Estados-Membros deverão, se adequado, encorajar a utilização de formatos abertos legíveis por máquina". v. Diretiva 2013/37/UE do parlamento europeu e do conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público, considerando 21.

"interoperabilidade[90]". Para o G29, as exigências prescritas no n.º 1, daquele artigo, constituem os elementos mínimos para facilitar a interoperabilidade do formato dos dados, i. é, são especificações dos meios para atingir o objetivo da interoperabilidade[91]. Diga-se ainda que o n.º 1 recusa a criação de "impedimentos", como a cobrança de uma taxa[92].

Na proposta original, a Comissão propunha-se especificar este formato. Contudo, constatando a diversidade de tratamentos, as diferenças do *design* e as caraterísticas dos vários responsáveis, a imposição de um formato comportava um processo de adaptação excessivo e caro, criando obstáculos à inovação e ao desenvolvimento de novas aplicações. A adequação do formato dos dados portáveis dependerá de setor para setor, devendo, pelo menos, preencher uma exigência: a *interpretabilidade*. Tratando-se de uma estrutura de dados complexa, o responsável pelo tratamento deve garantir que o titular é capaz de compreender a definição, o esquema e a estrutura dos seus dados. Sugere-se que os dados sejam fornecidos de forma sumária, por subconjuntos, e não em bloco, ou seja: "de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples[93]".

O fim visado pela portabilidade não é incentivar sistemas compatíveis mas garantir sistemas interoperáveis[94]. Por isso, o RGPD não obriga o responsável pelo tratamento a adotar ou manter um sistema de tratamento de dados tecnicamente compatível com os sistemas dos demais[95]. O legislador entendeu que qualquer solução de standardização da portabilidade

---

[90] Recorremos a legislação da UE em vigor para compreender este termo: "a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo e implicando a partilha de informações e conhecimento entre as organizações, no âmbito de processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC". v. Alínea a), do art. 2.º da Decisão n.º 922/2009/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, sobre soluções de interoperabilidade para as administrações públicas europeias (ISA). A norma ISSO/IEC 2382-01 define também este conceito do seguinte modo: "(...) a capacidade de comunicar, executar ou transferir dados entre várias unidades funcionais de tal modo que o utilizador não necessita de ter conhecimentos sobre as caraterísticas únicas dessas unidades".

[91] G29, *Guidelines*, cit., p. 13.

[92] *Idem*, p. 15.

[93] N.º 1 do art. 12.º do RGPD e G29, *Guidelines*, cit., p. 14.

[94] G29, *Guidelines*, cit., p. 14.

[95] Considerando 68 do RGPD.

deverá nascer da cooperação e do consenso alcançado pelos membros das indústrias e associações comerciais interessadas, que deverão estabelecer um conjunto comum e consensual de formatos e standards interoperáveis adequados às exigências da portabilidade. É justamente essa a finalidade do *European Interoperability Framework* (EIF), a entidade encarregue de definir uma estratégia concertada sobre a interoperabilidade para as organizações que pretendam prestar certo tipo de serviços. As instituições europeias, nomeadamente a Comissão, atuarão como dinamizadoras, criando pontes entre os vários interessados, o que já tem vindo a suceder através da criação de programas como o "ISA²"[96]. Na falta de consenso num determinado setor industrial, o G20 propôs a utilização de formatos abertos (XML, JSON, CSV, entre outros), juntamento com os metadados possíveis[97].

Como se depreende do art. 20.º, do n.º 4, o exercício deste direito não prejudica o exercício dos direitos e liberdades de terceiros[98]. Contudo, é possível que a transmissão dos dados entre responsáveis pelo tratamento dificulte o exercício dos direitos de terceiros, como o direito à informação ou ao acesso[99]. Seguindo boas práticas, os responsáveis pelo tratamento, tanto o emissor como o recetor, devem implementar mecanismos que permitam "separar o trigo do joio", selecionar os dados relevantes e excluir os dados de terceiros. Tenha-se ainda presente que a inclusão de dados de terceiros nos dados portáveis pressupõe, por força do art. 6.º, a identificação de um fundamento jurídico autónomo, como o "interesse legítimo" prosseguido pelo responsável pelo tratamento[100].

Os "direitos e liberdades de terceiros", aludidos no n.º 4 do art. 20, incluem o segredo comercial, a propriedade intelectual ou o direito de autor, que protegem o software, e/ou o modelo de negócio do responsável pelo tratamento. Exige-se um exercício de ponderação sobre as implicações

---

[96] Decisão (EU) 2015/2240 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA²) como um meio para modernizar o setor público.

[97] G29, *Guidelines*, cit., p. 18.

[98] Considerando 63 do RGPD.

[99] Um exemplo em concreto acontece com a portabilidade de dados bancários que inclui informação sobre as transações, incluindo sobre terceiros que transferiram dinheiro para a titular daquela conta. G29, *Guidelines*, cit., p. 9.

[100] Alínea f) do n.º 1, do art. 6.º do RGPD.

para estes direitos, prévio à resposta ao pedido de portabilidade, sendo certo, porém, que "essas considerações não deverão resultar na recusa de prestação de *todas* as informações ao titular dos dados[101]". Esta prioridade da portabilidade justifica-se com base na sua *natureza*: não visa permitir a utilização com má fé dos dados portáteis ou constituir uma violação dos direitos de terceiro. Portanto, o potencial (e reduzido) risco económico não escusa o responsável pelo tratamento de responder a um pedido de portabilidade, devendo utilizar mecanismos para excluir dos dados portáteis informação coberta pelo segredo comercial ou pela propriedade intelectual, mas somente dados pessoais que "digam respeito" ao titular[102]. Note-se ainda que reserva-se a possibilidade, ao responsável pelo tratamento, de solicitar ao titular dos dados a especificação das informações e atividades de tratamento a que se refere o seu pedido – mas apenas nos casos de grandes quantidades de informação do determinado titular dos dados[103].

Conclusão

Verificamos a existência de algumas semelhanças no que diz respeito aos direitos específicos do titular dos dados em relação ao regime previsto na diretiva. Todavia, nesta matéria, é inegável que a grande novidade deste novo diploma de proteção de dados pessoais é o direito à portabilidade. Utilizámos, como objeto da nossa análise sobre este novo instituto jurídico, a sua razão de ser, constatando a existência de uma natural dimensão individual sem, contudo, esquecer a sua inserção e o seu impacto na construção de um mercado único digital e, por conseguinte, na pretensão de digitalização da economia europeia. Mas, para apurar o conteúdo deste direito sempre seria essencial determinar quais as faculdades que reconhece ao titular dos dados: receber e transmitir os seus dados. Delineámos ainda o seu âmbito de aplicação material, dependente do próprio conceito de dados pessoais, e verificámos a existência de algumas dúvidas sobretudo em relação aos interesses legítimos dos responsáveis pelo tratamento. Por fim, debruçámo-nos sobre os problemas específicos, técnicos e jurídicos,

---

[101] Considerando 63 do RGPD.

[102] G29, *Guidelines*, cit., p. 10.

[103] Considerando 63 do RGPD.

suscitados pela aplicação prática da portabilidade. Como se depreende, são ainda muitas as dúvidas que restam, designadamente quanto à sua implementação técnica. O seu esclarecimento virá, por certo com o tempo, mas igualmente com o papel dinamizador que a Comissão Europeia tem vindo a assumir criando e estimulando o diálogo entre as industrias e os interlocutores interessados nessa clarificação.

Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição?

Afonso José Ferreira*

Resumo: O novo Regulamento Geral sobre a Proteção de Dados prevê um direito de não sujeição, por parte do titular de dados, às decisões que sejam baseadas no tratamento automatizado de dados ou na definição de perfis (*profiling*). A opinião do legislador europeu parece ser a de que esta forma de tratamento de dados é de alguma forma anormal, e deverá assim ser "proibida", deste modo escudando-se o particular. No presente texto, esta opinião é refutada. Em primeiro lugar, o tratamento automatizado de dados e o *profiling* são hoje considerados como formas legítimas de processamento de dados em setores como o *e-banking* ou o sistema judiciário. Em segundo lugar, seria irrazoável a exigência de que o processador de dados utilizasse apenas métodos manuais para o processamento de uma grande quantidade de dados. Em terceiro lugar, o próprio direito de não sujeição não poderá ser utilizado em situações em que o tratamento de dados pertence à base de uma relação contratual entre o titular e o processador, o que, na prática, retirará utilidade a este direito. Assim, o texto termina por propor outras soluções para os problemas que advêm do uso de algoritmos autónomos, como a responsabilidade fiduciária dos processadores.

Palavras-chave: *Algoritmos autónomos; definição de perfis; direito de não sujeição; responsabilidade algorítmica.*

Abstract: The new General Data Protection Regulation creates a right of non-subjection, granted to the data holder, to decisions which are based on automated processing of data or on profiling. The EU legislator's opinion seems to be that this is an abnormal form of

---

* Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa. Frequenta o Mestrado em Direito Europeu no Colégio da Europa. Bolseiro de Iniciação Científica no CEDIS/FDUNL. Este *paper* foi originalmente apresentado como uma comunicação no *workshop* "O novo regulamento de proteção de dados pessoais", organizado pelo Observatório de Proteção de Dados, integrado no CEDIS/FDUNL, a cujos participantes se agradece desde já pelos preciosos contributos prestados. Este trabalho é financiado por uma Bolsa da Fundação para a Ciência e Tecnologia.

data processing and that it should be thus "forbidden", thus shielding the individual. This text tries to refute this opinion. Firstly, automated processing of data and profiling are nowadays considered as legitimate ways to process data in sectors such as e-banking or the judicial system. Secondly, it would not be reasonable to demand that the responsible for data processing used solely manual methods when processing a large amount of data. Thirdly, the right of non-subjection itself may not be used in situations in which data treatment is in the basis of a contractual relationship between holder and processor, which, in practice, would deprive this right of its utility. Thus, the text will end by proposing other solutions for the problems deriving from the use of autonomous algorithms, such as fiduciary responsibility for processors.

Keywords: *Autonomous algorithms; profiling; right of non-subjection; algorithmic accountability.*

I. A tecnologia tem vindo a evoluir a ritmos incríveis, tornando verdadeira a chamada Lei de Moore, segundo a qual o poder de processamento dos computadores pessoais duplica a cada ano. Assim, os avanços tecnológicos fazem agora parte do quotidiano das nossas vidas. Esta evolução, ligada a uma progressiva normalização da compra, e descida dos preços, dos computadores pessoais e outros mecanismos, como *smartphones* ou *tablets*, têm vindo desde os anos sessenta e setenta a tornar óbvia a necessidade da criação de métodos jurídicos de proteção de dados pessoais[1].

Estes mecanismos, que se revestem tradicionalmente, na Europa, de um caráter geral e amplo, que visa, contrariamente ao que ocorre nos EUA, regular todos os domínios em que é possível prever uma cedência de dados pessoais, têm vindo a evoluir com uma curiosa lentidão face à rapidez evolutiva dos processos tecnológicos. Tomando como exemplo a regulação na União Europeia, sobre a qual, por motivos óbvios, me debruçarei, a última versão da Diretiva de Proteção de Dados – a Diretiva 95/46/CE – data de outubro de 1995, momento em que ainda não existia sequer a Internet como a conhecemos hoje. Ora, tendo em conta este paradoxo, que opõe de forma clara uma tecnologia que evolui com velocidade extrema, e normas jurídicas

[1] Esta história pode ser apreciada, de um método geral, e circunscrevendo-se à Europa – foco principal da minha exposição – em Mayer-Schönberber, Viktor. "Generational development of data protection in Europe", *in*: Agre, Philip E. e Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge: MIT Press, 1998.

que visam regular essa mesma tecnologia e que evoluem com uma lentidão igualmente extremada, é fácil perceber as críticas que a sociedade civil tem vindo a apontar ao legislador europeu quanto à inadaptação daquela Diretiva à regulação dos novos fenómenos tecnológicos.

Assumo-me, imediatamente, como um desses mesmos críticos. De facto, num campo que tem vindo a evoluir de forma tamanha, e com a quantidade de fenómenos da vida social que são diariamente eclipsados pela dimensão digital (como a saúde, o *e-banking* ou a educação, apenas para apontar os casos mais flagrantes), torna-se altamente preocupante assistir à progressiva descredibilização da Diretiva e à interpretação que o Tribunal de Justiça da União Europeia e os tribunais nacionais têm vindo a fazer da mesma, sendo um exemplo o caso *Google Spain*[2], que revela um profundo desconhecimento técnico sobre as tecnologias em causa[3]. Considerando a quantidade e profundidade dos dados pessoais em causa nas indústrias que exemplifiquei anteriormente, não se torna difícil percebermos o porquê da necessidade de um novo quadro jurídico nestas áreas.

O legislador europeu pareceu dar uma resposta aos seus críticos com a adoção do RGPD, cuja aplicação se iniciará em maio de 2018. No entanto, este Regulamento não colmata todas as falhas da teoria regulatória da União Europeia em matéria de novas tecnologias.

Uma destas falhas, que abordarei durante este *paper*, relaciona-se com o processamento de dados por algoritmos autónomos. Por algoritmos autónomos, refiro-me a métodos automáticos de processamento de dados, em que determinados dados são inseridos, direta ou indiretamente, pelo utilizador, num algoritmo que os processa para providenciar ao utilizador um resultado. O processamento de dados através de algoritmos autónomos funciona como uma *black box* – isto é, não é possível perceber o seu funcionamento interior, sendo apenas possível conhecer os *inputs* e os *outputs* da operação de processamento.

Por motivos de concorrência e inovação, estes algoritmos, e a forma como eles funcionam, são tradicionalmente secretos. Ou seja, o utilizador – e, na maior parte dos casos, as pessoas que supervisionam o funcionamento dos algoritmos – não têm acesso ao método de funcionamento do algoritmo.

---

[2] Acórdão do TJ, C-131/12, ECLI:EU:C:2014:317, *Google Spain*, de 13 de maio de 2014.

[3] Para um resumo destas críticas, v. "Google Spain SL *vs* Agencia Española de Protección de Datos", *Harvard Law Review*, vol. 128, 2014, pp. 735-742.

No entanto, a utilização de algoritmos autónomos para o processamento de dados tem-se vindo a tornar extraordinariamente comum. Desde logo, quando utilizamos um motor de busca como o Google, estamos a proceder a uma operação de processamento de dados através de um algoritmo autónomo. No entanto, são também operações de processamento de dados por algoritmos autónomos a procura, pelo Google, de publicidade especificada e personalizada em relação aos nossos históricos de pesquisa, ou de preços e promoções dos produtos que pesquisamos.

Mas estas operações são igualmente comuns em outros domínios. Por exemplo, nos Estados Unidos da América, tem-se vindo a tornar comum o uso de algoritmos para o cálculo da reincidência de criminalidade leve em tribunais de primeira instância. Por outro lado, é já perfeitamente comum a utilização por bancos e seguradoras de algoritmos que calculam as possibilidades de pagamento de empréstimos, ou a probabilidade da morte de um beneficiário no caso de um seguro de vida. Em suma, o uso de algoritmos autónomos tem vindo a tornar-se comum no quotidiano de todos, independentemente do seu contacto direto com as tecnologias. Isto leva a que, regra geral, os utilizadores finais – quer as pessoas que intervêm junto dos algoritmos, alimentando-os com dados, quer aqueles a quem o tratamento de dados ultimamente se destina – não tenham conhecimentos técnicos suficientes para perceber quais são, exatamente, as operações e "raciocínios" feitos pelos algoritmos.

II. Os algoritmos autónomos funcionam, de certo modo, como uma forma de *profiling* ou de definição de perfis. Por *profiling*, refiro-me ao tratamento automatizado de dados por uma entidade processadora, para perceber ou identificar determinados aspetos sobre uma pessoa. Em dadas situações – por exemplo, quando a Google identifica publicidade personalizada para alguém com base no seu histórico de pesquisa –, nem sequer é claro para o utilizador final que está a alimentar um algoritmo com dados pessoais.

Não é, assim, minimamente difícil perceber quais os problemas éticos e, potencialmente, jurídicos, que podem advir do uso de algoritmos autónomos. Identificarei brevemente um dos principais problemas que tem vindo a ser discutido pela doutrina nas ciências sociais e na engenharia informática. Este prende-se com aquilo a que Shirky chama de "autoridade algorítmica", ou, no original, *algorithmic authority*. Brevemente, este conceito refere-se à confiança implícita que a maior parte das pessoas deposita no resultado

dos algoritmos. Ou seja, tendo em conta que o algoritmo é uma máquina © e como tal, é supostamente desprovido de preconceitos ou parcialidades inerentes ao processo de decisão humano –, ser-nos-á mais fácil confiar em decisões feitas por aquele[4]. Esta confiança só tem vindo a ser aumentada através do uso de tecnologias de *machine learning* e do desenvolvimento das experiências e interfaces de utilizador, que tornam o contacto com o algoritmo normalizado e quase "humano".

Este progressivo depósito de confiança nos resultados dos algoritmos é problemático ao considerarmos que, muitas vezes, é impossível assegurar a imparcialidade dos mesmos. Devido a questões de programação e de design de interface do utilizador, os algoritmos funcionam, como referi anteriormente, como uma *black box*. Ou seja, nem o próprio programador, enquanto "monitorizador" do algoritmo, conseguirá perceber o porquê de aquele ter chegado a um determinado resultado.

Consideremos, por exemplo, uma investigação jornalística feita pelo website norte-americano ProPublica[5], que, ao analisar estatisticamente os resultados dos mecanismos algorítmicos de reincidência criminal em vários estados dos Estados Unidos da América, concluiu ser possível perceber a existência de tendências raciais desfavoráveis a pessoas de raça negra, quando comparadas com pessoas de raça branca que tenham o mesmo, ou pior, historial criminal. Colocando de lado o debate sobre o porquê destes resultados – que, embora essencial, é irrelevante na questão da autoridade algorítmica –, é inegável que é necessário garantir o correto funcionamento destes algoritmos.

Além disso, e por força da facilidade da sua utilização e resultados, é igualmente verdade que eles continuarão a ser utilizados e desenvolvidos. Assim, torna-se necessário garantir a independência e a imparcialidade dos algoritmos cujos resultados possam produzir efeitos nas esferas jurídicas dos particulares.

---

[4] Para uma discussão sobre este conceito, v. "A Speculative Post on the Idea of Algorithmic Authority", *Clay Shirky*, de 15 de novembro de 2009. Disponível em: <http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/> (acedido a 15/12/2017).

[5] Angwin, Julia *et al.* "Machine Bias", *ProPublica*, de 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (acedido a 13/12/2017).

III. As áreas da regulação e do *cyberlaw* têm vindo a defender duas soluções primárias para o problema do excesso de autoridade algorítmica. Zittrain, baseando-se no direito norte-americano, propõe o conceito de *information fiduciary*, ou "fidúcia de informação[6]". Este conceito foi originalmente proposto por Balkin, constitucionalista norte-americano, especificamente para as questões de privacidade online[7]. Outra preocupação dos autores é a possibilidade de influência política dos algoritmos, como os do Facebook, que selecionam quais as notícias a que os utilizadores são expostos[8].

Para estes autores, tendo em conta que certas classes profissionais reguladas, como os médicos ou os advogados, têm, nos Estados Unidos, uma responsabilidade fiduciária para com os seus clientes no que diz respeito ao uso da sua informação, também as entidades que utilizam algoritmos autónomos para a produção de resultados deverão ser responsáveis para com os titulares dos dados quanto ao seu correto tratamento. Parece-me que esta solução poderia, em princípio, ser acolhida na tradição romano-germânica sobre as égides da responsabilidade civil e dos direitos de personalidade.

Outra solução, proposta por Pasquale[9], e mais próxima das soluções que têm vindo a ser desenvolvidas na Europa continental, refere-se a uma regulação e limitação dos dados que podem ser assimilados através do uso de algoritmos. Como notei anteriormente, algoritmos como o Google recolhem os inputs que lhes são alimentados pelos utilizadores para criar perfis sobre os mesmos. Pasquale, que chama a esta criação de perfis *runaway data* (algo como "dados em fuga") defende que é necessária regulação prévia que permita delinear com sucesso quais os dados que podem ou não ser recolhidos pelos algoritmos para a construção de perfis. Assim, e tendo em conta o caráter eminentemente privado e secreto dos algoritmos que são usados por empresas (quase como um *trade secret*), Pasquale sugere regulação administrativa nestas áreas, com fiscalização regular.

---

[6] Zittrain, Jonathan. "Facebook Could Decide an Election Without Anyone Ever Finding Out", *New Republic*, 2014. Disponível em: <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> (acedido a 16/11/2017).

[7] Balkin, Jack. "Information Fiduciaries and the First Amendment", *UC Davis Law Review*, vol. 49, n.º 4, 2016, pp. 1183-1234.

[8] Balkin, Jack e Zittrain, Jonathan. "A Grand Bargain to Make Tech Companies Trustworthy", *The Atlantic*, 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/> (acedido a 25/11/2017).

[9] Pasquale, Frank. *The Black Box Society*. Cambridge: Harvard University Press, 2015.

Estas duas soluções partem do pressuposto, a meu ver correto, de que o processamento automático de dados e a construção de perfis vão passar a ser o método comum de processamento de dados, e que, na nossa sociedade, adotarão um papel fulcral. No entanto, os instrumentos legislativos da União Europeia em matéria de proteção de dados não adotam esta perspetiva. Quer na Diretiva, quer no novo Regulamento, o *profiling* é visto como uma forma anormal de processamento de dados, e como uma exceção a ser evitada.

De facto, a única regulação específica que o Regulamento nos oferece no que diz respeito aos algoritmos autónomos e ao *profiling* é a previsão de um direito de não sujeição às decisões que produzam efeitos na esfera jurídica do titular dos dados e que sejam tomadas com base no resultado do tratamento automatizado de dados. Este direito é previsto pelo art. 22.º, n.º 1 do Regulamento.

IV. A previsão deste direito parece-me, no entanto, ser contraproducente. Em primeiro lugar, e observando-o de uma perspetiva regulatória, a previsão de um direito que permita ao particular recusar a adoção de decisões baseadas num algoritmo autónomo é irrisória. De facto, num mundo globalizado em que os algoritmos autónomos são comumente utilizados, e tendo em conta a inserção do RGPD na estratégia da Comissão Europeia de digitalização da economia europeia, a existência deste direito corresponde a um completo afastamento do progresso do comércio jurídico. A meu ver, é uma perspetiva ineficaz e ignorante da parte do legislador europeu.

Em segundo lugar, considero que esse direito não terá qualquer utilidade prática. O art. 22.º, n.º 2, alínea a) do Regulamento prevê que o titular dos dados não poderá exercer o direito de não sujeição quando o *profiling*, ou a decisão dele decorrente, sejam necessários para a celebração ou execução de um contrato entre o titular de dados e a entidade processadora dos mesmos. Ora, na criação desta exceção, o legislador europeu parece esquecer-se de que, em várias situações, o *profiling* e o processamento automatizado de dados fazem parte do objeto e da base de contratos de adesão celebrados entre o titular de dados e a entidade processadora no mero uso do algoritmo.

Na utilização de um motor de busca como o Google, por exemplo, o utilizador está a prestar tacitamente o seu consentimento para com a Política

de Privacidade e os Termos e Condições do serviço. Estes esclarecem que o titular consentirá no agrupamento dos seus dados para a definição de perfis que levem a usos publicitários ou de personalização dos resultados de pesquisa. Eles são, assim, contratos de adesão, cuja justiciabilidade tem vindo a ser afirmada várias vezes por tribunais nacionais, e que tem estado bem clara na jurisprudência norte-americana.

Na situação anteriormente referida, o processamento de dados é, assim, o objeto do contrato de adesão celebrado entre o titular dos dados e a entidade processadora. De outras vezes, no entanto, o uso do algoritmo faz apenas parte do contexto e da base do contrato. Imaginemos, por exemplo, a situação do uso de um algoritmo por um banco para o cálculo das possibilidades de pagamento de um requerente de empréstimo. Nesta situação, o contrato celebrado entre o requerente e o banco envolve o consentimento do tratamento dos dados do requerente, para que o banco possa decidir corretamente. Ora, nesta situação, permitir ao titular dos dados que se opusesse à forma como o banco processa esses dados, impedindo que eles sejam analisados automaticamente e obrigando o banco a utilizar métodos antiquados e incertos, seria fortemente irrazoável.

O titular dos dados teria o seu bolo e comê-lo-ia – embora consentisse no processamento dos dados, recusar-se-ia a que eles fossem processados de uma forma eficaz. Considerando a relevância crescente do processamento automatizado de dados no comércio jurídico, seria, em bom rigor, presumível ao titular de dados que o uso de métodos automatizados seja a forma pré-definida de agir. Assim, parece-me que seria irrazoável, e contra as bases do contrato, que o particular se pudesse opor a este processamento.

Assim, na maior parte das situações, este malogrado direito de não sujeição não terá sequer aplicação prática. De facto, a Comissão Europeia tenta proteger o particular escudando-o do progresso tecnológico – e, no caminho, falha nessa mesma proteção.

V. Ora, tendo em conta as questões, previamente analisadas, que são inerentes ao uso de algoritmos autónomos e que estão na base das preocupações do legislador europeu, que soluções poderiam ser propostas que não fossem anti paradigmáticas e que não perpetuassem o paradoxo da regulação tecnológica?

A primeira solução deriva da teoria da regulação, e, nomeadamente, da corrente do paternalismo justificado defendida por Sunstein[10]. Este autor defende que compete ao Estado orientar os seus cidadãos para que aqueles façam as melhores escolhas possíveis, através de mecanismos como a simplificação visual ou o aumento de informações disponíveis antes da escolha. Assim, a ideia – que é óbvia – baseia-se em tornar mais claro ao titular dos dados que tipo de processamento de dados irá ocorrer; através, por exemplo, do uso de ícones. Deste modo, não ocorreriam situações nas quais um utilizador alimenta indevidamente um algoritmo autónomo.

A segunda solução, e que se baseia nas ideias da fidúcia de informação propostas por Balkin e Zittrain, tem como base a exigência de uma "responsabilidade algorítmica" às entidades responsáveis pelo processamento dos dados. Esta responsabilidade dividir-se-ia em duas fases. Em primeiro lugar, durante a execução dos algoritmos, a sua supervisão seria garantida por entidades independentes, que avaliariam a sua imparcialidade e eficácia, utilizando os métodos técnicos disponíveis. Esta supervisão seria acompanhada de uma transparência para com esta entidade reguladora, que garantiria uma continuação da concorrência face aos rivais do criador do algoritmo. Numa segunda fase, seria permitida a responsabilidade extracontratual nas situações em que o processamento dos dados seja parcial ou incorreto, garantindo-se assim a existência de incentivos à manutenção da imparcialidade e eficácia dos algoritmos.

O uso destas soluções permitiria respeitar aquilo que o legislador europeu vê como essencial na regulação dos algoritmos autónomos – que estes sejam imparciais e eficazes, e que o seu uso não prejudique os titulares dos dados. Por outro lado, no entanto, permitiria que a regulação nesta área se aproximasse do nível de progresso tecnológico que já existe no comércio jurídico, e permitiria igualmente o contínuo desenvolvimento de uma forte economia digital na União Europeia.

---

[10] Sunstein, Cass. *Why Nudge? The Politics of Libertarian Paternalism*. New Haven: Yale University Press, 2014.

Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados

Teresa Vale Lopes*

Resumo: O novo Regulamento Geral sobre a Proteção de Dados apresenta como uma das suas caraterísticas essenciais a consagração dos princípios da responsabilidade e de *data protection by design* e *by default*, bem como o estabelecimento de novas medidas organizativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes. Por outro lado, é prevista a aplicação, por parte das autoridades de controlo, de sanções mais exigentes em caso de incumprimento. O presente texto pretende analisar as principais obrigações e responsabilidades que este Regulamento vem estabelecer para as empresas e o respetivo impacto a nível organizacional.

Palavras-chave: *Regulamento; Proteção de Dados; Responsabilidade; Obrigações.*

Abstract: The new General Data Protection Regulation presents as one of its essential features the acknowledgement of the principles of responsibility and data protection by design e by default, as well as the establishment of organizational and technical measures required to controllers and processors. Additionally, the enforcement of more stringent penalties by supervisory authorities is foreseen in case of non-compliance. This paper intends to analyze the main obligations and responsibilities that this Regulation sets for the companies and the corresponding impact at organizational level.

Keywords: *Regulation; Data Protection; Accountability; Obligations.*

---

* Licenciada em Direito pela Universidade de Coimbra e *LL.M. International Business Law* pela Faculdade de Direito da Universidade Católica Portuguesa. Integra a equipa *Health Care Compliance Iberia* na Johnson & Johnson Medical, com responsabilidade pelo sector em Portugal, e coordena a área de *Data Privacy*, *cross sector*, no Grupo Johnson & Johnson Portugal.

Introdução

Em 27 de abril de 2016, foi adotado pela União Europeia (UE) o RGPD[1], mais de quatro anos após ter sido apresentada pela Comissão Europeia[2] a proposta para a sua implementação. Este regulamento entrou em vigor em maio de 2016 e será diretamente aplicável a todos os Estados-Membros a partir de 25 de maio de 2018 (art. 99.º do RGPD).

O RGPD, que substituirá a atual 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, visa modernizar e harmonizar as regras de proteção de dados entre os Estados-Membros, representando assim um marco fundamental na reforma europeia do regime jurídico de proteção de dados.

Esta reforma constitui um elemento essencial da "Estratégia para o Mercado Único Digital na Europa", lançada em 2015 pela União Europeia, que visa o estabelecimento de um mercado que assegure a livre circulação de pessoas, serviços e capitais e em "que os cidadãos e as empresas podem beneficiar livremente de atividades "on-line" e desenvolver essas atividades em condições de concorrência leal e com um elevado nível de proteção dos consumidores e dos seus dados pessoais, independentemente da nacionalidade ou local de residência", assim como manter a posição da Europa como líder mundial na economia digital[3].

Entre as várias novidades, este novo Regulamento carateriza-se pelo especial enfoque no respetivo cumprimento (*compliance*), sendo consagradas medidas mais rigorosas a nível de governação, responsabilidade e documentação para os responsáveis pelo tratamento ou subcontratantes.

---

[1] Aprovado pelo 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 (RGPD).

[2] 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 (RGPD), de 25 de janeiro de 2012. Disponível em: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf> (acedido a 10/12/2017).

[3] Neste sentido, v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia para o Mercado Único Digital na Europa*, Bruxelas, 6.5.2015, COM (2015) 192 final, p. 3.

Com efeito, enquanto alguns requisitos de natureza burocrática previstos na Diretiva 95/46/CE são suprimidos, tais como a obrigação de notificação prévia às autoridades de controlo das operações de tratamento de dados pessoais[4], são também introduzidas novas "regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades[5]".

Em apreço encontram-se medidas relativas à realização de uma avaliação de impacto sobre a proteção de dados e subsequente consulta prévia às autoridades de controlo, ao registo das atividades de tratamento, à notificação de violação de dados pessoais, bem como a obrigação de nomear um encarregado da proteção de dados, responsável por zelar, de forma independente, pela observância das obrigações legais por parte de cada organização e por ser o ponto de contacto com as autoridades de controlo em matéria de proteção de dados pessoais.

O RGPD incentiva ainda a criação de códigos de conduta pelas associações ou outras entidades representativas de categorias de responsáveis pelo tratamento ou de subcontratantes, de forma a tornar mais efetivo o cumprimento das disposições por parte dos diferentes setores, tendo em consideração as suas especificidades, bem como a certificação na área da proteção de dados e de selos e marcas de proteção.

Por outro lado, é prevista a aplicação pelas autoridades de controlo de sanções administrativas, em caso de incumprimento, que poderão atingir 20.000.000 EUR ou, tratando-se de uma empresa, até 4% do respetivo volume de negócios anual a nível mundial (art. 83.º do RGPD).

---

[4] A este propósito, veja-se a posição da Comissão Europeia, que considera que "outro elemento concreto para a redução da sobrecarga administrativa e dos custos dos responsáveis pelo tratamento seria *a revisão e simplificação do sistema de notificação actual*. É consensual entre os responsáveis pelo tratamento que a actual obrigação geral de notificar todas as operações de tratamento de dados às autoridades de protecção de dados é uma obrigação bastante pesada que não traz, por si só, qualquer valor acrescentado à protecção dos dados pessoais". v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, 4.11.2010, COM (2010) 609 final, p. 11.

[5] Neste sentido, v. o considerando 89 do RGPD.

Com o presente texto, pretende-se analisar algumas das principais obrigações e responsabilidades que o novo Regulamento vem estabelecer para as empresas e o respetivo impacto a nível organizacional.

1. Principais elementos impulsionadores da reforma

A rápida evolução tecnológica, a globalização e o fenómeno do *big data* vieram estabelecer novos desafios em matéria de proteção de dados, levando assim à necessidade de rever o quadro normativo vigente.

Com efeito, em 4 de novembro de 2010, a Comissão Europeia concluiu que, apesar dos princípios nucleares da atual Diretiva 95/46/CE se manterem válidos, este diploma já não respondia aos desafios das novas tecnologias, sendo exigível a reforma e modernização do regime jurídico de proteção de dados, de molde a "desenvolver uma abordagem global e coerente que garanta que o direito fundamental das pessoas singulares à proteção dos dados é plenamente respeitado na UE e fora dela[6]".

As mudanças decorrentes do Tratado de Lisboa, que entrou em vigor em 1 de dezembro de 2009, vieram também impulsionar a necessidade de um envolvimento mais ativo da UE, como entidade supranacional, na regulação destas matérias[7]. Em especial, destaca-se a consagração, no art. 16.º do TFUE, de que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", cabendo ao Parlamento Europeu e ao Conselho estabelecer as normas relativas ao tratamento de dados pessoais e à livre circulação desses dados[8]. Este artigo vem introduzir uma "base jurídica abrangente para a proteção de dados pessoais nas

---

[6] V. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, p. 4. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf> (acedido a 10/12/2017).

[7] Neste sentido, v. também Burri, Mira e Schär, Rahel. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", *Journal of Information Policy*, vol. 6, 2016, p. 481.

[8] Saliente-se que a política externa e de segurança comum não é abrangida pelo art. 16.º do TFUE, visto que, de acordo com o art. 39.º do Tratado da União Europeia, as normas específicas nesta área que regulam o tratamento de dados pelos Estados-Membros devem ser estabelecidas por uma decisão do Conselho.

políticas da União", eliminando a anterior "estrutura em pilares" da UE[9] e permitindo assim que a mesma proteção legal seja aplicada a todo o tipo de tratamento de dados. Adicionalmente, o art. 6.º do TUE veio estabelecer que a Carta dos Direitos Fundamentais da União Europeia – cujo art. 8.º reconhece um direito autónomo à proteção de dados[10] – tem o mesmo valor jurídico que os Tratados (art. 6.º do TUE).

Por outro lado, algumas decisões do TJ vieram estabelecer importantes alterações na prática jurídica existente, bem como no entendimento geral sobre os direitos dos indivíduos à proteção de dados na era digital.

Em apreço destaca-se o acórdão "Google Spain[11]", que introduziu na linguagem jurídica europeia o conceito de "direito a ser esquecido", representando agora um novo direito do titular dos dados, previsto no RGPD.

Outro acórdão merecedor de referência é o *Digital Rights Ireland*[12], que veio declarar inválida a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Tal Diretiva pretendera harmonizar a legislação dos Estados-Membros no sentido de assegurar a conservação de categorias de dados de comunicações telefónicas através de redes fixas, móveis ou de internet, bem como comunicações por e-mail, "por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação" (arts. 5.º e 6.º da Diretiva 2006/24/CE), e foi considerada inválida pelo referido acórdão por implicar restrições aos princípios fundamentais de "respeito pela vida privada" (art. 7.º da CDFUE) e da "proteção de dados pessoais" (art. 8.º CDFUE).

---

[9] Neste sentido, v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, cit., p. 14.

[10] O direito à proteção dos dados constitui um direito fundamental previsto no art. 8.º da Carta de Direitos Fundamentais da União Europeia, autónomo em relação ao direito ao "respeito pela vida privada e familiar" previsto no art. 7.º.

[11] Acórdão do TJ, C-131/12, ECLI:EU:C:2014:317, *Google Spain*, de 13 de maio de 2014.

[12] Acórdão do TJ, C-293/12 e C-594/12, ECLI:EU:C:2014:238, *Digital Rights*, de 8 de abril de 2014.

Por outro lado, o acórdão *Schrems*[13] concluiu pela invalidade do mecanismo de *Safe Harbor*. Este mecanismo consistiu num acordo entre o Departamento de Comércio dos EUA e a Comissão Europeia que permitia às empresas sediadas nos EUA certificarem-se relativamente ao cumprimento de princípios sobre proteção de dados constantes da atual Diretiva 95/46/CE e, por conseguinte, proceder ao tratamento de dados pessoais provenientes de empresas europeias. Atendendo a que o *Safe Harbor* não vinculava as autoridades norte-americanas, prevalecendo sempre o direito interno dos EUA em caso de conflito com os princípios previstos na referida Diretiva, o TJ veio concluir que este mecanismo não conferia um nível de proteção adequado à luz daquela Diretiva.

Por conseguinte, estas decisões não apenas expuseram as deficiências do atual regime jurídico europeu de proteção de dados, como são também o reflexo dos desafios a enfrentar na área de proteção de dados na era digital e das grandes dificuldades em conciliar uma eficaz e efetiva proteção de dados com outros interesses essenciais, tais como a livre circulação da informação, enquanto base da nova economia digital e condição essencial para a liberdade de expressão na internet[14].

2. A "abordagem baseada no risco"

No que respeita às obrigações que recaem sobre o responsável pelo tratamento e subcontratante, é importante desde já salientar que o RGPD adotou a chamada "abordagem baseada no risco[15-16]". Este entendimento vai para além de uma estrita "abordagem centrada nos danos", tendo em consideração todo o potencial ou real efeito adverso avaliado numa escala

---

[13] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, de 6 de outubro de 2015.

[14] Neste sentido, v. Burri, Mira e Schär, Rahel. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", cit., p. 488.

[15] Sobre esta abordagem, v. G29, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN WP 218, de 30 de maio de 2014.

[16] A chamada abordagem baseada no risco não é um conceito novo, tendo já sido adotada em algumas disposições da atual Diretiva: art. 8.º, relativo ao "tratamento de certas categorias específicas de dados", cujo tratamento é considerado de maior risco para os titulares dos dados, art. 17.º, relativo à "segurança do tratamento" e art. 20.º, relativo ao "controlo prévio".

abrangente, desde o impacto no titular dos dados em causa ao impacto geral na sociedade (por exemplo, a perda de confiança social).

Neste sentido, poderão existir diferentes níveis de obrigações e responsabilidades dos responsáveis pelo tratamento e subcontratantes, dependendo do grau de risco colocado pelo tratamento em questão para os titulares dos dados e para a sociedade.

Assim, a necessidade de implementação pelos responsáveis pelo tratamento de medidas técnicas e organizativas que assegurem o cumprimento das regras de proteção de dados (por exemplo, a avaliação de impacto sobre a proteção de dados e consulta prévia, o registo das atividades de tratamento, a implementação de medidas de segurança, a notificação de violação dos dados pessoais, ou a designação do encarregado da proteção de dados) poderá variar consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. Isto significa que um responsável pelo tratamento que realiza um tratamento de dados com um nível de risco relativamente baixo pode não estar vinculado às mesmas obrigações legais que são aplicáveis a um responsável cujo tratamento representa um elevado risco.

Apesar do exposto, os princípios fundamentais aplicáveis aos responsáveis pelo tratamento (*i.e.* licitude, responsabilidade, minimização dos dados, limitação da finalidade, transparência, integridade, exatidão) deverão ser sempre assegurados, independentemente da natureza, âmbito, contexto, finalidades do tratamento e riscos para os titulares dos dados. Ainda assim, uma vez que a natureza e o âmbito do tratamento são sempre parte integrante da aplicação desses princípios, estes são inerentemente escaláveis, consoante os riscos em presença.

Por outro lado, é importante notar que, mesmo com a adoção de uma abordagem baseada no risco, os direitos dos titulares dos dados não deverão sofrer qualquer tipo de enfraquecimento [*i.e.* direitos de acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição (arts. 13.º a 22.º do RGPD)], devendo por isso manter a mesma robustez, ainda que o tratamento em causa envolva riscos reduzidos para os titulares dos dados.

3. O princípio da responsabilidade

O RGPD apresenta como uma das suas principais características a consagração do princípio da responsabilidade, estabelecendo expressamente

que, "tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis", cabe ao responsável pelo tratamento aplicar "as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento" (art. 24.º do RGPD).

Este princípio foi pela primeira vez introduzido no contexto da proteção de dados, a nível internacional, nas *Guidelines* da OCDE, adotadas em 23 de setembro de 1980[17]. A partir dessa data, a sua importância tem vindo a ser discutida em inúmeros fóruns internacionais dedicados à matéria de proteção de dados[18]. Em especial, destaca-se a *Opinion 3/2010 on the principle of accountability*[19], emitida pelo "Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais" contemplado no artigo 29.º da Diretiva 95/46/CE (G29)[20], na qual foi defendida a introdução deste

---

[17] V. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top> (acedido a 10/12/2017). Estas *guidelines*, entretanto atualizadas em 2013, foram aprovadas com o objetivo de consolidar os princípios básicos de proteção de dados entre os Estados-Membros da OCDE e, complementarmente, promover a transferência de dados entre países, procurando resolver os potenciais obstáculos ao desenvolvimento económico provocados por divergências entre as diferentes legislações nacionais.

[18] Tais como, *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) (*S.C.* 2000, c. 5*), Schedule 1,* Cláusula 4.1. Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html> (acedido a 10/12/2017); *"APEC Privacy Framework", 2005* , para. 26 (disponível em: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework); *Accountability Projects*, lançados a partir de 2009 pelo Center for Information Policy Leadership (CIPL) e várias autoridades de proteção de dados; European Data Protection Supervisory, *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*, janeiro 2011. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf> (acedido a 10/12/2017).

[19] V. G29, *Opinion 3/2010 on the principle of accountability*, 00062/10/EN WP 173. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf> (acedido a 10/12/2017).

[20] O Grupo de Trabalho foi instituído pelo art. 29.º da Diretiva 95/46/CE e consiste num órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas atribuições se encontram previstas no art. 30.º da Diretiva 95/46/CE e no art. 15.º da Diretiva 2002/58/CE.

princípio na revisão do regime geral de proteção de dados, com o objetivo de reafirmar e reforçar a responsabilidade do responsável pelo tratamento[21].

Parte do racional desta Opinião é fundado na premissa de que os princípios de proteção de dados e obrigações do responsável pelo tratamento são, no regime de proteção de dados atualmente aplicável, insuficientemente refletidos em medidas e práticas concretas. Desta forma, o princípio da responsabilidade apresenta-se como um mecanismo suscetível de promover a adoção, pelos responsáveis pelo tratamento, de medidas práticas internas que assegurem a eficácia da proteção de dados e, por outro lado, assistam as autoridades de controlo nas tarefas de supervisão e execução.

De acordo com o G29, a maioria dos requisitos inerentes a este princípio não são, em si, uma novidade, uma vez que já decorrem (embora de forma menos explícita) das leis atualmente aplicáveis. Na verdade, na atual Diretiva 95/46/CE, os responsáveis pelo tratamento são já obrigados ao cumprimento dos princípios e obrigações em matéria de proteção de dados pessoais, sendo para tal intrinsecamente necessário estabelecer e aplicar procedimentos para a proteção de dados. Por conseguinte, à luz desta perspetiva, a introdução de um princípio da responsabilidade não visa vincular os responsáveis pelo tratamento de dados a um novo princípio, mas sim promover a adoção de medidas práticas e concretas que assegurem o efetivo cumprimento dos princípios já existentes[22].

Conforme anteriormente referido, a abordagem baseada no risco constitui um dos elementos essenciais do princípio da responsabilidade. Com efeito, de acordo com este princípio, as medidas técnicas e organizativas a adotar pelos responsáveis pelo tratamento deverão ser determinadas em função dos factos e circunstâncias de cada caso em particular, incluindo o tipo de operações de tratamento de dados e os riscos para os direitos e liberdades das pessoas singulares. Mais concretamente, deverão ser tidos em conta aspetos como a dimensão da operação de tratamento de

---

[21] A sugestão de redação do artigo por parte do G29 era a seguinte:

"*Article X – Implementation of data protection principles.*

1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request".

[22] Neste sentido, v. para. 36 da *Opinion 3/2010*.

dados, a sua finalidade, a necessidade de transferência de dados, o tipo de dados que vão ser tratados, incluindo o tratamento de dados pessoais sensíveis[23].

Adicionalmente, o RGPD vem incentivar a adoção, por parte do responsável pelo tratamento, de políticas internas adequadas em matéria de proteção de dados, assim como o cumprimento de códigos de conduta e procedimentos de certificação, que poderão ser utilizados "como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento" (art. 24.º, n.º 2 e 3 do RGPD).

Em complemento ao princípio da responsabilidade, o RGPD estabeleceu um conjunto, não exaustivo, de medidas técnicas e organizativas destinadas a assegurar e demonstrar, por parte do responsável pelo tratamento, o cumprimento das regras de proteção de dados. Algumas destas medidas consistem na avaliação de impacto sobre a proteção de dados e consulta prévia, registo das atividades de tratamento, notificação de violação de dados pessoais, nomeação de um encarregado da proteção de dados, cuja implementação poderá variar, tal como anteriormente referido, consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. O não cumprimento de qualquer uma destas obrigações, poderá implicar, para cada um dos atos, a aplicação de uma coima até 10.000.000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual (art. 83.º, n.º 4 do RGPD).

Nesta sede, cumpre salientar que a obrigação de demonstrar o cumprimento das regras de proteção de dados é suscetível de influenciar um comportamento mais pró-ativo por parte dos responsáveis pelo tratamento, não só no que respeita à implementação de medidas eficazes de proteção de dados nos seus processos de negócio, como também no que concerne à adotação de mecanismos que permitem a avaliação das referidas medidas antes da necessidade de ocorrência de incidentes[24].

De tal forma, enquanto demonstração pró-ativa da capacidade de uma organização em cumprir, a responsabilidade assume-se como um mecanismo

---

[23] A este propósito, v. também para. 45 e 46 da *Opinion 3/2010*.

[24] V. European Data Protection Supervisory, *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"*, paras. 99 e 100.

que poderá conferir maior confiança aos titulares dos dados pessoais e reguladores de que as garantias adequadas à proteção dos dados são implementadas.

Por outro lado, uma vez que as empresas, ao abrigo do princípio da responsabilidade, se encontram obrigadas a demonstrar o cumprimento das regras de proteção de dados, fomentando, por isso, uma maior transparência sobre as suas boas práticas corporativas e programas de *compliance*, os reguladores poderão focar a sua atenção nos atores que não demonstrem capacidade para o cumprimento das obrigações em apreço.

Este princípio assume, portanto, um papel fundamental como instrumento de compliance, ao promover a implementação, por parte do responsável pelo tratamento, das garantias necessárias ao cumprimento das regras de proteção de dados e respetiva demonstração, tanto a nível interno como externo[25-26].

4. Os princípios *data protection by design* e *by default*

Associados ao princípio da responsabilidade resultam também do RGPD outros dois novos princípios fundamentais que devem nortear os processos de tratamento de dados pessoais: a proteção de dados desde a conceção (*data protection by design*) e a proteção de dados por defeito (*data protection by default*) (art. 25.º do RGPD).

Estes princípios visam promover o cumprimento por parte do responsável pelo tratamento das regras de proteção de dados durante todo o ciclo de vida dos projetos que envolvem o tratamento de dados pessoais, *i.e.* desde a fase da sua conceptualização, até ao momento do próprio tratamento dos dados.

---

[25] Neste sentido, v. Alhadeff, Joseph, Alsenoy, Brendan Van, e Dumortier, J. "The accountability principle in data protection regulation: origin, development and future directions", *in*: Guagnin, D; Hempel, L. e Ilten, C. *et al.* (eds.). *Managing Privacy through Accountability*. Palgrave Macmillan, 2012, pp. 49-82.

[26] V. ainda European Data Protection Supervisory, *Opinion 7/2015 – Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*, de 19 de novembro de 2015, pp. 15 e 16. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> (acedido a 10/12/2017).

Com efeito, ao abrigo do princípio *data protection by design*, o responsável pelo tratamento deverá implementar, tanto no momento da determinação dos meios de tratamento, como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, destinadas a aplicar com eficácia os princípios da proteção de dados (tal como o da minimização) e a incluir as garantias necessárias no tratamento, de forma a cumprir com o RGPD e proteger os direitos dos titulares dos dados.

Tais medidas poderão incluir, entre outras, a minimização do tratamento de dados pessoais, a total ou parcial anonimização dos dados pessoais ou a sua pseudonimização o mais cedo possível, a separação funcional[27], a transparência no que respeita às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento, assim como a criação de medidas de segurança por parte do responsável pelo tratamento[28]. Este princípio assume, igualmente, particular importância no âmbito dos processos de avaliação de impacto sobre a proteção de dados, na medida em os resultados desta avaliação deverão ser tidos em conta na determinação das referidas medidas.

Por outro lado, à semelhança do princípio da responsabilidade, o RGPD adota uma abordagem flexível e baseada no risco relativa ao princípio de *data protection by design*[29], prevendo expressamente que para a sua aplicação o responsável pelo tratamento deverá ter em conta as técnicas mais avançadas e custos da sua aplicação, a natureza, âmbito, contexto e finalidades do tratamento dos dados, assim como os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento em causa.

Adicionalmente, de acordo com o princípio *data protection by default*, o responsável pelo tratamento deverá assegurar que, por defeito, só sejam tratados os dados pessoais que forem estritamente necessários para cada finalidade específica de tratamento (minimização do tratamento de dados pessoais). Esta obrigação aplica-se à quantidade de dados pessoais recolhidos,

---

[27] Sobre o conceito de separação funcional, v. G29, *Opinion 3/2013 on purpose limitation*, 00569/13/EN WP 203. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (acedido a 10/12/2017).

[28] Neste sentido, v. o considerando 78 do RGPD.

[29] V., a este título, entendimento da *TaylorWessing – Global Data Hub*. Disponível em: <https://www.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html> (acedido a 10/12/2017).

à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em particular, o responsável pelo tratamento deverá aplicar medidas técnicas e organizativas que garantam que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25.º, n.º 2 do RGPD).

Assim sendo, ao optar por incluir os conceitos de *data protection by design* e *by default* como princípios-chave do RGPD, o legislador europeu visou assegurar que a proteção de dados representa uma componente fundamental na conceção e manutenção dos sistemas de informação e no *modus operandi* de cada organização. Tal pode levar a que potenciais questões de privacidade sejam identificadas numa fase inicial e menos dispendiosa dos projetos e a uma crescente conscientização de temas de privacidade e proteção de dados nas próprias organizações[30].

A violação deste princípio é suscetível de levar à aplicação de coimas até 10.000.000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial (art. 83.º, n.º 4, alínea a) do RGPD).

5. Novas obrigações para os responsáveis pelo tratamento de dados e subcontratantes

Antes de nos debruçarmos sobre as principais obrigações previstas no RGPD, importa desde logo salientar que, embora os princípios da responsabilidade e *data protection by design* e *by default* acima mencionados sejam diretamente aplicáveis aos responsáveis pelo tratamento, o RGPD vem também introduzir alterações ao âmbito de responsabilidade dos subcontratantes.

De acordo com a Diretiva 95/46/CE, o responsável pelo tratamento é identificado como a pessoa ou entidade que "determina as finalidades e os meios de tratamento dos dados pessoais" (art. 2.º, alínea d) da Diretiva 95/46/CE), enquanto o subcontratante é definido como a pessoa ou entidade que "trata os dados pessoais por conta do responsável pelo tratamento" (art. 2.º, alínea e) da Diretiva 95/46/CE).

---

[30] V., também a este propósito, *TaylorWessing – Global Data Hub*, cit.

Esta distinção é essencial, na medida em que, no âmbito da referida Diretiva, é ao responsável pelo tratamento que incumbe assegurar a observância das obrigações legais em matéria de proteção de dados[31], assim como a responsabilidade em caso de incumprimento, nomeadamente perante os titulares dos dados (art. 23.º da Diretiva 95/46/CE).

Por outro lado, a relação entre o responsável pelo tratamento e o subcontratante deverá ser regida por um contrato escrito que estipule que o subcontratante apenas atua mediante instruções do responsável pelo tratamento e fixe as obrigações a que o subcontratante se encontra vinculado, designadamente no que respeita a medidas de segurança de tratamento (art. 17.º da Diretiva 95/46/CE). A relação entre o responsável pelo tratamento e o subcontratante tem assim, no âmbito da Diretiva 95/46/CE, apenas efeito entre as partes, não concedendo por esta via direito aos titulares dos dados para agirem contra o subcontratante.

A divisão entre responsável pelo tratamento e subcontratante, no âmbito da Diretiva 95/46/CE, tem vindo a ser criticada, especialmente devido à crescente complexidade das operações de tratamento de dados, tais como os dados tratados em *cloud*, redes sociais, motores de busca, em que nem sempre é claro para o titular dos dados quem determina se e como os dados são tratados[32] e, portanto, a quem deve ser alocada a responsabilidade. Tal incerteza é suscetível de provocar efeitos negativos no cumprimento das regras de proteção de dados e na eficácia da legislação de proteção de dados como um todo[33].

---

[31] Em especial, obrigação de observância dos princípios relativos à qualidade dos dados (arts. 6.º, n.º 2), obrigações perante os titulares dos dados (arts. 10.º a 12.º e art. 14.º), obrigação de segurança dos dados (art. 17.º), obrigação de notificação à autoridade de controlo (art. 18.º e ss.).

[32] Alguma doutrina argumenta que a Diretiva possibilita, efetivamente, a um conjunto de atores na área de proteção de dados evitar a responsabilidade pelas suas ações. Neste sentido, v. Cuijpers, Colette; Purtova, Nadezhda e Kosta, Eleni. "Data Protection Reform and the Internet: The Draft Data Protection Regulation". *Tilburg Law School Research Paper No. 03/2014*, p. 6. Disponível em: <https://ssrn.com/abstract=2373683> (acedido a 10/12/2017).

[33] A este título, v. G29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, p. 2. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> (acedido a 10/12/2017). Ainda de acordo com esta Opinião, se não estiver suficientemente claro o que deve ser exigido de cada ator, existe um risco claro que pouco, ou nada, aconteça em caso de incumprimento e que as disposições legais permaneçam inefetivas.

Por sua vez, o G29, reconhecendo as dificuldades em aplicar na prática as definições da Diretiva 95/46/CE, veio clarificar, na *Opinion 1/2010 on the concepts of "controller" and "processor"*, os conceitos de responsável pelo tratamento e de subcontratante, nomeadamente conferindo orientações para aplicar a sua distinção pragmaticamente e para avaliar, na determinação da origem do controlo efetivo sobre a decisão de tratar os dados, não só as cláusulas legais e contratuais aplicáveis, como também, as circunstâncias de facto[34]. O G29 articulou igualmente a possibilidade de múltiplos corresponsáveis pelo tratamento, com iguais ou diferentes graus de controlo e de responsabilidade.

O RGPD mantém a distinção da Diretiva 95/46/CE entre responsável pelo tratamento e subcontratante, sendo tais conceitos definidos no mesmo sentido. Contudo, vem introduzir novas obrigações e responsabilidades na esfera do subcontratante.

Com efeito, as obrigações do subcontratante que devem constar do contrato escrito a celebrar com o responsável pelo tratamento são especificadas de uma forma muito mais detalhada em relação àquelas que estão previstas na Diretiva 95/46/CE (art. 28.º, n.º 3 do RGPD).

Adicionalmente, o RGPD estabelece obrigações e responsabilidades que são aplicáveis, tanto ao responsável pelo tratamento como ao subcontratante, tais como a obrigação de manter registos das atividades de tratamento (art. 30.º, n.º 2 do RGPD), a obrigação de cooperar com as autoridades de controlo (art. 31.º do RGPD), a obrigação de implementar as medidas de segurança apropriadas, tais como, pseudonimização, cifragem, teste (art. 32.º do RGPD), a obrigação de, em certos casos, designar um encarregado da proteção de dados (art. 37.º do RGPD), o direito dos titulares dos dados proporem uma ação judicial contra o responsável pelo tratamento ou o subcontratante em caso de violação dos seus direitos nos termos do RGPD (art. 79.º, n.º 2 do RGPD) e receberem uma indemnização dos mesmos (art. 82.º, n.º 1 do RGPD).

Por outro lado, no RGPD a distinção entre o responsável pelo tratamento e subcontratante é aplicada pragmaticamente e é expressamente reconhecida a possibilidade de responsáveis múltiplos ou conjuntos. Neste sentido, o diploma em apreço estabelece que o subcontratante que, em violação do

---

[34] V. G29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, cit., pp. 8-12.

RGPD, determinar as finalidades e os meios de tratamento, nomeadamente por exceder as instruções conferidas pelo responsável pelo tratamento, "é considerado responsável pelo tratamento no que respeita ao tratamento em questão" (art. 28.º, n.º 10 do RGPD). Mais acresce que o RGPD vem regular especificamente a relação entre responsáveis conjuntos pelo tratamento, prevendo de forma expressa que tais corresponsáveis devem adotar um acordo que defina as funções e responsabilidades de cada um (art. 26.º, n.º 1 e 2 do RGPD) e que, independentemente deste acordo, o titular dos dados pode exercer os seus direitos contra cada um dos responsáveis pelo tratamento (art. 26.º, n.º 3 do RGPD).

A extensão das obrigações e responsabilidades do subcontratante, em conjunto com as pesadas sanções no âmbito do RGPD, são assim suscetíveis de gerar alterações na dinâmica de negociação dos contratos a celebrar entre os responsáveis pelo tratamento e subcontratantes, designadamente no que respeita à transferência de risco e ações de direito de regresso no caso do subcontratante ser sancionado devido a qualquer incumprimento por parte do responsável pelo tratamento[35].

6. A avaliação de impacto sobre a proteção de dados

Às características anteriormente identificadas como relevantes novidades do RGPD deve ainda enfatizar-se, em matéria de responsabilidade e governação, a obrigação da avaliação de impacto sobre a proteção de dados e a consulta prévia.

Deste modo, quando o tratamento de dados pessoais, em particular com recurso a novas tecnologias, é suscetível de implicar um elevado risco para os direitos e liberdades de pessoas singulares, o responsável pelo tratamento encontra-se obrigado, nos termos do RGPD, a conduzir, antes de iniciar o tratamento, uma avaliação de impacto das operações de tratamento sobre a proteção de dados (art. 35.º, n.º 1 do RGPD). Através desta medida, os responsáveis pelo tratamento devem descrever as operações de tratamento

---

[35] A este título, v. Linklaters, *The General Data Protection Regulation – A survival guide*, outubro de 2016, p. 42. Disponível em: <http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf> (acedido a 10/12/2017).

e sua finalidade, assim como ponderar a respetiva necessidade e proporcionalidade, avaliar os riscos para os direitos e liberdades dos titulares dos dados decorrentes desse tratamento e determinar as medidas essenciais para a sua mitigação (art. 35.º, n.º 7 do RGPD). Esta obrigação constitui uma importante ferramenta complementar aos princípios da responsabilidade e *data protection by design* e *by default*. Isto porque, devendo a avaliação ter lugar num momento prévio ao tratamento, visa assegurar que a proteção de dados e privacidade sejam consideradas desde a conceção do processo de tratamento, promovendo, assim, a criação de soluções que assegurem o cumprimento das regras de proteção de dados e constituindo um elemento essencial para demonstrar tal cumprimento[36].

Em consonância com a abordagem baseada no risco adotada no RGPD, a condução de uma avaliação de impacto não é obrigatória para todo o tipo de tratamento de dados pessoais, sendo apenas exigível quando o tratamento "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (art. 35.º, n.º 1 do RGPD).

Desta forma, cumpre desde já salientar que, conforme clarificado pelo G29, a referência aos "direitos e liberdades dos indivíduos" diz respeito, *prima facie*, ao direito à privacidade, mas também envolve outros direitos fundamentais, tais como a liberdade de expressão, liberdade de circulação, proibição de discriminação, direito à liberdade de pensamento e religião[37].

É igualmente importante considerar que os riscos podem resultar não só da ineficiência das medidas de segurança adotadas, mas também de aspetos inerentes à própria natureza do tratamento de dados em questão. Por exemplo, a privacidade é comprometida se informação sobre a vida privada é recolhida e a proibição de discriminação é suscetível de ser afetada quando

---

[36] Neste sentido, v. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN-WP 248, de 4 de abril de 2017, pp. 4 e 13. Disponível em: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_data_protection_impact_assessment_dpia.pdf> (acedido a 10/12/2017).

[37] Ver, a este título, G29, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN-WP 218, de 30 de maio de 2014, para. 8. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> (acedido a 10/12/2017).

os dados recolhidos são referentes à origem racial ou étnica. Deste modo, a avaliação de impacto sobre a proteção de dados não deve por isso cingir-se à avaliação da forma como os dados são recolhidos e conservados. Esta avaliação deverá também ter em conta as operações de tratamento de dados no seu todo. Tal pressuposto obriga a que os responsáveis pelo tratamento tenham em conta um conjunto de considerações éticas no momento de conceção do próprio processo de tratamento, devendo interromper o mesmo, caso os riscos aos direitos e liberdades dos indivíduos inerentes ao processo sejam elevados[38].

Por outro lado, o RGPD veio estabelecer, a título exemplificativo, casos em que o tratamento de dados é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares": (i) "avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada no tratamento automatizado, incluindo a definição de perfis", para servir de base a decisões que produzem efeitos jurídicos na esfera de uma pessoa singular ou que a afetem significativamente[39]; (ii) operações de tratamento em grande escala[40] de categorias especiais de dados ("dados pessoais sensíveis[41]"); ou que (iii) requeiram o "controlo sistemático de zonas acessíveis ao público" (art. 35.º, n.º 3 do RGPD).

---

[38] Neste sentido, Quelle, Claudia. *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing* (November 25, 2015). Disponível em: <https://ssrn.com/abstract=2695398> (acedido a 10/12/2017).

[39] Por exemplo, quando o tratamento é suscetível de conduzir à exclusão ou à discriminação de indivíduos.

[40] O G29 recomenda a adoção dos seguintes critérios para a determinação se um tratamento de dados é conduzido em grande escala: (i) o número de titulares de dados em causa, (ii) o volume dos dados e/ou variedade de tipo de dados que estão a ser tratados, (iii) a duração ou a continuidade da atividade de tratamento dos dados, (iv) o âmbito geográfico da atividade de tratamento. V. G29, *Guidelines on Data Protection Officers ('DPOs')*, 16/EN-WP 243, p. 7. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=43823> (acedido a 10/12/2017).

[41] Dados pessoais sensíveis incluem as categorias especiais de dados previstos no art. 9.º do RGPD (entre outros aí previstos, dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, dados relativos à saúde), bem como os dados pessoais referentes a condenações penais e infrações, conforme previsto no art. 10.º do RGPD.

O G29, com base em várias disposições do RGPD, veio também publicar algumas orientações para determinar se o tratamento é "suscetível de implicar um elevado risco" no âmbito do RGPD[42].

Adicionalmente, nos casos em que a avaliação de impacto indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco, deve ser consultada a autoridade de controlo competente antes do início do tratamento dos dados (art. 36.º, n.º 1 do RGPD). De acordo com o G29, estão em causa casos em que os riscos identificados não podem ser suficientemente endereçados pelo responsável pelo tratamento (*i.e.* quando os riscos residuais se mantêm elevados), como, por exemplo, situações em que os titulares dos dados se podem deparar com consequências significativas ou, até mesmo, irreversíveis, que não podem ultrapassar, e/ou quando parece óbvio que o risco ocorrerá[43].

No caso da autoridade de controlo considerar que o tratamento viola o previsto no RGPD, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deverá, no prazo de oito semanas a contar da receção do pedido de consulta, emitir orientações ao responsável pelo tratamento ou, quando aplicável, ao subcontratante, podendo aplicar uma variedade de medidas para mitigação ou eliminação do risco (art. 36.º, n.º 2 do RGPD), incluindo, por exemplo, a imposição da limitação temporária ou definitiva do tratamento de dados, ou mesmo a respetiva proibição (art. 58.º, n.º 2, alínea f) do RGPD).

Importa ainda salientar que, apesar da obrigação jurídica de avaliação de impacto sobre a proteção de dados incidir sobre o responsável pelo tratamento, no contrato a celebrar com o subcontratante deverá resultar expressamente que este se obriga a prestar todo o suporte necessário e fornecer qualquer informação relevante para a realização da referida avaliação, sempre e quando o tratamento for realizado, no todo ou em parte, pelo subcontratante (art. 28.º, n.º 3, alínea f) do RGPD).

---

[42] V. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, cit., p. 7-11

[43] V. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 19.

7. O registo das atividades de tratamento e notificação de violação de dados pessoais

Não obstante o RGPD suprimir a obrigação de notificação prévia das operações de tratamento de dados pessoais às autoridades de controlo, prevista no art. 18.º da Diretiva 95/46/CE, este diploma vem estabelecer novas obrigações de registo para os responsáveis pelo tratamento de dados e subcontratantes (art. 30.º do RGPD).

Pretende-se, com efeito, que, a fim de comprovar a observância do RGPD, o responsável pelo tratamento ou o subcontratante conserve registos de atividades de tratamento sob a sua responsabilidade[44]. Acresce ainda que os responsáveis pelo tratamento e subcontratantes estarão obrigados a cooperar com a autoridade de controlo, facultando-lhe os referidos registos, sempre que solicitado, para fiscalização dessas operações de tratamento (art. 30.º, n.º 4 do RGPD).

Cumpre também mencionar que, com o intuito de atender às especificidades das micro, pequenas e médias empresas[45], o RGPD prevê uma derrogação da obrigação de conservação deste registo para as organizações com menos de 250 trabalhadores, salvo se o tratamento em apreço implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional, ou abranja os já mencionados "dados pessoais sensíveis" (art. 30.º, n.º 5 do RGPD).

Por outro lado, o responsável pelo tratamento deve notificar à autoridade de controlo a violação de dados pessoais, no prazo máximo de 72 horas após ter tido conhecimento da mesma, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada (art. 33.º do RGPD).

Adicionalmente, se a violação dos dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá notificar o titular dos dados (art. 34.º, n.º 1 do RGPD).

---

[44] V. considerando 82 do RGPD.

[45] V. considerando 13 do RGPD.

Nesta matéria, importa salientar que, de acordo com o RGPD, por violação de dados pessoais deverá entender-se qualquer violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais objeto de tratamento (art. 4.º, alínea 12 do RGPD). Com base na mencionada definição, o G29 identificou três tipos de violação de dados pessoais que poderão observar-se, isolada ou cumulativamente: violação de confidencialidade (divulgação ou acesso não autorizado ou acidental a dados pessoais), violação da disponibilidade dos dados (perda de acesso ou destruição não autorizada ou acidental dos dados pessoais) e violação da integridade dos dados (alteração não autorizada ou acidental de dados pessoais)[46]. Neste âmbito, veio também definir critérios de avaliação do nível de risco[47].

8. O encarregado da proteção de dados

O encarregado da proteção de dados surge no RGPD como um elemento chave no novo modelo de governação das instituições, assumindo um papel crucial no cumprimento por parte destas das disposições legais relativas à proteção de dados pessoais[48].

No âmbito do RGPD, torna-se obrigatória a nomeação de um encarregado da proteção de dados por parte do responsável pelo tratamento e do subcontratante, sempre que um tratamento de dados pessoais for efetuado por uma autoridade ou organismo público[49] (excetuando os tribunais no exercício da sua função jurisdicional), ou nos casos em que as atividades principais do responsável pelo tratamento ou do

---

[46] V. G29, *Guidelines on Personal data breach notification under Regulation 2016/679, 17/EN WP250*, de 3 outubro de 2017, p. 6 e 7. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=47741> (acedido a 10/12/2017).

[47] *Idem*, pp. 19-22.

[48] A designação do encarregado de proteção de dados não constitui em si uma inovação, encontrando-se já prevista, a título facultativo, na atual Diretiva 95/46/CE e constituindo já prática corrente em alguns Estados- Membros, tais como a Alemanha, a França e a Holanda.

[49] De acordo com o G29, o conceito de autoridade ou organismo público deverá ser aferido de acordo com a legislação local. V. G29, *Guidelines on Data Protection Officers (*'DPOs'), cit., p. 6.

subcontratante[50] consistirem em operações de tratamento de dados em grande escala que exijam um controlo regular e sistemático[51] dos titulares dos dados ou o tratamento de dados sensíveis (art. 37.º, n.º 1 do RGPD)[52].

O mencionado encarregado da proteção de dados pode ser um trabalhador do responsável pelo tratamento ou do subcontratante, bem como um prestador de serviços contratado por qualquer um deles (art. 37.º, n.º 6 do RGPD).

Por outro lado, um único encarregado da proteção de dados poderá ser designado para um grupo empresarial ou um conjunto de autoridades ou organismo públicos, desde que seja facilmente acessível a partir de cada estabelecimento (art. 37.º, n.º 2 e 3 do RGPD) e tenha conhecimento especializado no domínio do direito e das práticas aplicáveis em matéria de proteção de dados (art. 37.º, n.º 5 do RGPD).

De forma a assegurar que o encarregado da proteção de dados se encontra acessível, tanto interna como externamente, é importante que os seus contactos estejam publicamente disponíveis (art. 37.º, n.º 7 do RGPD). Por

---

[50] De acordo com considerando 97 do RGPD, as "atividades principais" dizem respeito às "atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar". O G29 veio, contudo, salientar que tal conceito não deverá excluir aquelas atividades em que o tratamento de dados é uma parte indissociável da atividade do responsável pelo tratamento ou subcontratante. Por exemplo, a atividade principal de um hospital é prestar serviços de saúde. Contudo, um hospital não poderá assegurar cuidados de saúde de uma forma segura e eficaz sem o tratamento dos dados de saúde dos pacientes. Desta forma, o tratamento destes dados deverá ser considerado parte integrante das atividades principais do hospital. V. G29, *Guidelines on Data Protection Officers ('DPOs')*, cit., pp. 6 e 7.

[51] A noção de "controlo regular e sistemático" não se encontra definida no RGPD. De acordo com o G29 esta definição inclui todo o tipo de monitorização e definição de perfis na Internet. Contudo, não se restringe apenas ao ambiente on-line. v. G29, *Guidelines on Data Protection Officers ('DPOs')*, pp. 8 e 9.

[52] Da análise do n.º 4 do art. 37.º do RGPD resulta ainda que a UE e/ou os Estados-Membros terão a discricionariedade de fixar outos casos em que seja obrigatória a nomeação de um encarregado da proteção de dados para além das circunstâncias previstas no RGPD, permitindo assim a fixação, a nível dos Estados-Membros, de requisitos ainda mais exigentes no que respeita à nomeação do encarregado da proteção de dados. Adicionalmente, nos casos em que não é legalmente exigível a nomeação de um encarregado da proteção de dados, os responsáveis pelo tratamento, subcontratantes ou as associações e outros organismos que os representam poderão optar voluntariamente por tal designação. Neste caso, deverão ser igualmente aplicáveis os requisitos previstos no RGPD relativamente ao encarregado da proteção de dados.

conseguinte, o encarregado da proteção de dados, com o suporte de uma equipa, se necessário, deverá encontrar-se numa posição que lhe permita comunicar eficazmente com a sua organização, com os titulares dos dados e com as autoridades de controlo. Tal significa que esta comunicação deve ser realizada no idioma (ou idiomas) utilizados por estas entidades[53].

O encarregado da proteção de dados assume assim um papel fundamental na promoção de uma cultura de *compliance* na área de proteção de dados dentro da organização para a qual trabalha. Em especial, incumbe-lhe, nos termos do RGPD, controlar o cumprimento das obrigações legais e políticas internas em matéria de proteção de dados, incluindo assegurar a repartição de responsabilidades, dar formação, sensibilizar, informar e prestar aconselhamento, designadamente sobre as obrigações do responsável pelo tratamento ou do subcontratante, coordenar auditorias, assim como cooperar e ser o ponto de contacto com as autoridades de controlo (art. 39.º do RGPD) e com os titulares dos dados (art. 38.º, n.º 4 do RGPD).

Estas funções deverão ser exercidas com a máxima independência[54]. O próprio RGPD estabelece alguns mecanismos para garantir que o encarregado da proteção de dados exerça as suas funções com um suficiente grau de autonomia dentro da organização: (i) obrigação do responsável pelo tratamento e do subcontratante assegurarem que o encarregado da proteção de dados não recebe instruções relativamente ao exercício das suas funções, (ii) proibição de destituição ou penalização do encarregado da proteção de dados devido ao exercício as suas funções, (iii) proibição de conflito de interesses com outras funções exercidas pelo encarregado da proteção de dados (art. 38.º, n.º 3 e n.º 6 do RGPD). O G29 veio elencar algumas funções que poderão consubstanciar um conflito de interesses com o cargo de encarregado da proteção de dados, tais como funções que tipicamente envolvam a determinação das finalidades e meios de

---

[53] Neste sentido, G29, *Guidelines on Data Protection Officers ('DPOs')*, cit., p. 10.

[54] Neste sentido, veja-se o previsto no considerando 97 do RGPD: "Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência". Sobre boas práticas que ajudam a assegurar a independência do encarregado da proteção de dados ver também Network of Data Protection Officers of the EU Institutions and Bodies, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/20011*, 14 October 2010, pp. 5-7. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf> (acedido a 10/12/2017).

tratamento de dados, como, por exemplo, posições de direção na gestão de negócios, ou funções que envolvam a representação em juízo do responsável pelo tratamento ou subcontratante em ações que envolvam a proteção de dados[55].

É importante salientar que, não obstante o encarregado da proteção de dados seja responsável por zelar pela implementação e cumprimento das regras de proteção de dados, tal não significa, contudo, que seja pessoalmente responsável em caso de incumprimento. Na verdade, ao abrigo do princípio da responsabilidade, a designação do encarregado da proteção de dados não exonera a própria instituição da responsabilidade em assegurar e demonstrar a conformidade com o RGPD[56].

9. Códigos de conduta, certificação e selos de proteção

Por último, cumpre ainda salientar que o RGPD vem também incentivar a criação de códigos de conduta pelas associações ou outras entidades representativas de categorias de responsáveis pelo tratamento ou de subcontratantes (arts. 40.º e 41.º do RGPD).

Os referidos códigos de conduta apresentam-se como mecanismos de autorregulação suscetíveis de conferir orientação sobre a aplicação efetiva das regras de proteção de dados, tendo em conta as especificidades de cada sector e as necessidades das micro, pequenas e médias empresas[57]. Neste sentido, aquando da elaboração dos códigos de conduta, as associações e os demais organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes devem consultar as partes interessadas e procurar ter em conta os contributos recebidos e as opiniões expressas em resposta a essas consultas[58].

Adicionalmente, o RGPD promove ainda a criação de mecanismos de certificação na área da proteção de dados e de selos e marcas de proteção, para efeitos de comprovação da conformidade das operações de tratamento de dados com o próprio Regulamento (arts. 42.º e 43.º do RGPD).

---

[55] V. G 29, *Guidelines on Data Protection Officers ('DPOs')*, p. 24.

[56] *Ibidem*, p. 4.

[57] Neste sentido, v. considerando 98 do RGPD.

[58] Neste sentido, v. considerando 99 do RGPD.

Estes instrumentos, além de constituírem um elemento determinante na demonstração do cumprimento das obrigações do responsável pelo tratamento (art. 24.º, n.º 3 do RGPD), assumem-se como fator atenuante na determinação das coimas a aplicar em caso de violação das regras de proteção de dados (art. 83.º, n.º 2, alínea j) do RGPD).

Conclusões

Face ao exposto, cumpre concluir que o RGPD se apresenta como um instrumento essencial para a modernização e harmonização das regras de proteção de dados na UE, baseando-se, essencialmente, na garantia dos direitos e liberdades fundamentais dos cidadãos, perante os novos desafios da era digital.

As novas tecnologias, a globalização, o fenómeno do *big data* permitem, nos dias de hoje e cada vez mais, a utilização de dados pessoais em larga escala, o que exige um quadro de proteção de dados mais sólido e eficaz, que confira uma maior segurança ao tratamento dos dados pessoais.

Este regulamento tem como principais características a especial ênfase no *compliance*, através da consagração dos princípios da responsabilidade e de *data protection by design* e *by default*, bem como do estabelecimento de novas medidas organizativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes.

A responsabilidade pela verificação prévia do cumprimento das normas de proteção de dados passa, pois, a incidir, essencialmente, sobre os responsáveis pelo tratamento e subcontratantes e não tanto sobre as autoridade de controlo, ficando os primeiros obrigados a implementar mecanismos eficazes que assegurem tal cumprimento, sob pena da aplicação de pesadas sanções, que podem ascender a 20.000.000 EUR ou, tratando-se de uma empresa, até 4% do volume de negócios anual a nível mundial.

Por conseguinte, torna-se fundamental adaptar a estrutura organizacional das empresas e fomentar uma cultura de *compliance*, de molde a promover, internamente, a implementação e a aplicação dos princípios e das novas obrigações desta reforma europeia da proteção de dados, favorecendo o desenvolvimento de uma economia cada vez mais aberta, transparente e responsável.

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?

Inês Oliveira Andrade de Jesus*

Resumo: Volvidos mais de vinte anos desde a aprovação do primeiro instrumento europeu que se dedicou à regulação da proteção de dados pessoais, podemos afirmar que tudo mudou, sendo o *Big Data* a realidade que nos absorve nos dias de hoje. O direito fundamental à proteção de dados pessoais, o combate à criminalidade e o crescimento do comércio internacional têm de andar de mãos dadas. A privacidade é, agora, uma vantagem competitiva para as empresas e uma prova imprescindível para as polícias e autoridades judiciárias, estando investido o legislador na tarefa hercúlea de arquitetar a disciplina aplicável à troca de dados pessoais, (des)equilibrando os interesses ofensivos das empresas e das autoridades públicas e os interesses defensivos dos cidadãos a quem os dados respeitam.

Palavras-chave: *Proteção de dados pessoais; transferências internacionais de dados; Regulamento (UE) 2016/679; Diretiva (UE) 2016/680.*

Abstract: More than 20 years after the adoption of the first European instrument on the regulation of personal data, we can say that everything has changed, with Big Data being a reality that absorbs us today. The fundamental right to personal data protection, the fight against crime and the growth of international trade must go hand in hand. Privacy is now a competitive advantage for companies and an indispensable evidence for the

* Licenciada (2008) e Mestre (2010) em Direito pela Faculdade de Direito da Universidade Nova de Lisboa. Doutoranda (desde 2015) em Administração Pública no Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa. Desempenhou funções no Centro Nacional de Informação e Arbitragem de Conflitos de Consumo (2009) e no Gabinete para a Resolução Alternativa de Litígios/Ministério da Justiça (2010) e foi bolseira de investigação no ISCTE – IUL, na área da proteção de dados pessoais (2011). Atualmente (desde 2013) é Consultora de Política Legislativa na Direção-Geral da Política de Justiça/Ministério da Justiça, sendo representante de Portugal junto da União Europeia para as questões atinentes à proteção de dados pessoais. Foi designada (por despacho de 4 de julho de 2017) encarregada da proteção de dados da Direção-Geral da Política de Justiça do Ministério da Justiça.

police and judicial authorities, being the legislator charged with the Herculean task of designing a discipline applicable to the exchange of personal data, (un) balancing the offensive interests of the companies and public authorities and the defensive interests of the citizens to whom the data respect.

Keywords: *Personal data protection; international data transfer; Regulation (EU) 2016/679; Directive (EU) 2016/680.*

Enquadramento

Tornou-se lugar-comum afirmar que as novas tecnologias facilitam a circulação de informação. Na verdade, neste novo mundo virtual, a informação circula sem constrangimentos temporais ou espaciais, o que proporciona inúmeras vantagens aos próprios indivíduos a quem respeitam. Pense-se, mormente, na simplificação das interações sociais.

No entanto, os cidadãos não são os únicos a beneficiar dos avanços tecnológicos. As empresas, numa economia como a nossa, de consumo, também beneficiam desta nova realidade, que permite, designadamente, a definição de perfis e de estratégias comerciais mais eficientes. Aliás, as trocas de dados integram as operações diárias das empresas, incluindo pequenas e médias, em todos os setores da economia, e não apenas na área das tecnologias de informação, estando esta tendência ainda em crescimento. Note-se que o valor da economia europeia de dados rondou os 272 mil milhões de euros em 2015, prevendo-se que cresça para 643 mil milhões em 2020[1].

A par disso, os organismos públicos e as polícias também não podem prescindir de todas as funcionalidades que as novas tecnologias oferecem, mormente no que tange à prestação de serviços públicos essenciais e à prevenção da criminalidade. Sublinhe-se que as empresas e o próprio Estado necessitam, de forma ímpar, nos nossos dias, de cada vez mais informação para prosseguirem as suas missões.

Ora, atrevemo-nos a antever que este lugar-comum faz, já hoje, parte do passado. Erguem-se agora novos paradigmas no que ao tratamento de

[1] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, Construir uma Economia Europeia dos Dados, COM/2017/09 final, p. 2.

dados respeita. Refiro-me, em concreto, ao *Big Data*, à *Internet of Things* e à *Cloud Computing*. A já aludida necessidade de informação é acompanhada pelo próprio progresso tecnológico, que facilita, cada vez mais, o tratamento de dados, também aqui entendido de forma ampla, tal como a lei o desenha, abrangendo todas as operações que é possível efetuar.

Nestes novos cosmos, complexos e, não raras vezes, obscuros, a criação de valor e o aumento da produtividade caminham a par com a inovação, tornando os setores privado e público ainda mais eficazes e eficientes, metamorfoseando a forma como a sociedade se compreende e organiza. Estamos cientes, aliás, de que hoje em dia se arquitetam cada vez mais bases de dados, contendo cada vez mais informação, bases de dados estas acessíveis a qualquer momento, em qualquer sítio e sem custos, permitindo um controlo total, nomeadamente, das pessoas.

A esta acumulação quase ilimitada de dados soma-se a qualidade dos mesmos, cuja exatidão é surpreendente, adequando-se aos fins prosseguidos pelas empresas e pelo próprio Estado, mas vulnerabilizando as pessoas e a própria sociedade, mormente devido à criação de perfis de personalidade e ao consequente uso para fins abusivos e discriminatórios.

Note-se que grande parte dos dados utilizados são dados pessoais, que espelham as interações humanas e as formas e estilos de vida, cuja análise pode ter impacto direto nas pessoas. Pense-se na identificação de padrões comportamentais e na previsão de comportamentos futuros, que podem resultar em decisões (de empresas ou de entes públicos) potencialmente negativas, levando, nomeadamente, à discriminação dos visados.

Foi neste contexto que a União Europeia aprovou o comummente apelidado Pacote de Proteção de Dados, integrado pelo 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[2] e pela 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

[2] 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.

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[3]. Enquanto a Diretiva 95/46/CE oferece, até aos nossos dias, um quadro legal equilibrado e adequado[4], sendo vista, a nível internacional, como a medida certa de proteção de dados pessoais[5], a Decisão-Quadro 2008/977/JAI não logrou uma tutela equivalente à concedida pela aludida diretiva, mormente porque o seu âmbito de aplicação não abrange nem a Europol nem a Eurojust, não protegendo os cidadãos em todas as situações[6].

A necessidade de rever a Diretiva 95/46/CE e a Decisão-Quadro 2008/977/JAI foi espoletada, mormente, pelo Tratado de Lisboa, visto, para alguns autores, como a oportunidade ideal para revisitar a disciplina jurídica atinente à proteção de dados pessoais na União, modernizando e harmonizando as regras aplicáveis, por um lado, e, por outro, colmatando as lacunas existentes[7].

No recentemente publicado Pacote de Proteção de Dados, a União Europeia parece ter em devida conta as críticas de falta de harmonização do regime, fazendo aprovar, no que concerne ao mercado interno, um instrumento diretamente aplicável, que reforça os direitos das pessoas e responsabiliza as empresas e os organismos públicos, o que contrasta com o domínio da cooperação policial e judiciária em matéria penal, ao qual se aplicará um instrumento distinto, que carece de transposição e que oferece, através dos seus articulados permissivos, larga margem de manobra aos Estados membros, desprotegendo os cidadãos em apreço[8]. Note-se que

---

[3] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

[4] Hijmans, Hielke e Scirocco, Alfonso. "Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?", *Common Market Law Review*, vol. 46, 2009, p. 1485.

[5] De Hert, Paul e Papakonstantinou, Vagelis. "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, vol. 28, 2012, p. 131.

[6] Hijmans, Hielke e Scirocco, Alfonso. "Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?", cit., p. 1493.

[7] De Hert, Paul e Papakonstantinou, Vagelis. "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", cit., p. 131.

[8] *Idem*, p. 132.

esta separação de instrumentos legais, mantida no novo pacote legislativo, mostrou ser, ao longo dos anos, artificial, assistindo-se, cada vez mais, à partilha de dados pessoais entre entidades privadas e públicas[9].

O RGPD é já visto como o modelo a seguir por outros países[10], apesar de se notar, mesmo no presente, uma convergência de regimes, mormente no que toca aos principais princípios, quando comparamos o ordenamento jurídico europeu com os restantes, convergência esta espelhada, em grande medida, pela Diretiva 95/46/CE ainda aplicável. Certo é que esta compatibilidade de regimes facilita a troca de dados e, consequentemente, o comércio, fortalecendo a economia digital global. Note-se que esta compatibilidade de regimes também favorece a cooperação entre autoridades policiais e judiciárias, unidas no combate à criminalidade.

A matéria atinente à proteção de dados pessoais está na ordem do dia, não só na Europa, mas no mundo inteiro. Prova disso é a aprovação, nos últimos anos, de legislação nesta área, levada a efeito por muitos países estrangeiros[11].

O mês de maio de 2018 marcará o início, entre nós, da aplicação do novo regime de proteção de dados pessoais. Porque não nos é permitido abordar todas as matérias, debruçar-nos-emos, em particular, sobre a disciplina jurídica atinente às transferências internacionais de dados pessoais, elencando as continuidades e chamando à colação as inovações do legislador europeu.

1. As transferências internacionais de dados pessoais: regime aplicável no contexto comercial

As transferências de dados pessoais para países terceiros ou organizações internacionais vão ser admissíveis, ao abrigo do RGPD, em variadas situações-tipo, algumas das quais configuram uma continuidade relativamente ao regime ainda em vigor. Vejamos.

---

[9] *Ibidem*.

[10] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM/2017/07 final, pp. 2 e 11.

[11] *Idem*, p. 7.

Em primeiro lugar, continuarão a ser admissíveis as transferências internacionais baseadas numa decisão da Comissão que ateste a adequação do nível de proteção do país terceiro, do território ou de um ou mais setores específicos desse país terceiro, ou da organização internacional, o que dispensa qualquer autorização concreta (art. 45.º).

Em segundo lugar, não tendo sido adotada uma decisão de adequação por parte da Comissão, as transferências internacionais de dados pessoais poderão realizar-se, ainda assim, se forem apresentadas garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (n.º 1 do art. 46.º). O Regulamento elenca dois tipos de garantias adequadas: as que dispensam autorização específica (n.º 2 do art. 46.º) e as que pressupõem autorização da autoridade de controlo competente (n.º 3 do mesmo art.).

Configuram garantias adequadas que dispensam autorização específica os instrumentos juridicamente vinculativos e com força executiva entre autoridades ou organismos públicos, as regras vinculativas aplicáveis às empresas e as cláusulas-tipo adotadas pela Comissão ou por uma autoridade de controlo e aprovadas pela Comissão, bem como os códigos de conduta ou as certificações, como selos e marcas, se acompanhados de compromissos vinculativos e com força executiva. Note-se, porém, que as regras vinculativas aplicáveis às empresas, para serem consideradas garantias adequadas, e não obstante dispensarem autorização específica de uma autoridade de controlo tal como referido, estão sujeitas a aprovação da autoridade de controlo competente (art. 47.º).

Por seu turno, as cláusulas a inserir nos contratos a celebrar entre entes privados ou as disposições a prever nos acordos administrativos entre autoridades e organismos públicos, depois de autorizadas pela autoridade de controlo competente, também legitimam transferências internacionais de dados pessoais.

Em terceiro lugar, as transferências internacionais de dados pessoais poderão realizar-se com base num acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro e a União ou um dos Estados membros (art. 48.º).

Em quarto lugar, na falta de decisão de adequação da Comissão, de garantias adequadas e de acordo internacional, as transferências de dados poderão ainda ser efetuadas com base no consentimento explícito do titular dos dados, após ter sido informado dos possíveis riscos de tais transferências

para si próprio (alínea a) do n.º 1 do art. 49.º). Em alternativa, as transferências poderão realizar-se caso sejam necessárias para a celebração ou execução de contratos ou de diligências prévias pedidas pelo titular dos dados (alíneas b) e c) do preceito citado).

Note-se que as transferências também terão lugar quando forem necessárias por importantes razões de interesse público (alínea d) do n.º 1 do art. 49.º), para a declaração, exercício ou defesa de direitos em processos judiciais (alínea e)), para proteção de interesses vitais do titular dos dados ou de terceiros (alínea f)) e nos casos em que os dados são públicos (alínea g)). Por fim, e ainda ao abrigo do art. 49.º, a transferência de dados será permitida se não for repetitiva, apenas respeitar a um número limitado de titulares e for necessária para efeitos dos interesses legítimos do responsável pelo tratamento, desde que tais interesses se mostrem imperiosos face aos direitos dos titulares dos dados e forem oferecidas garantias adequadas.

Passado em revista o regime substantivo das transferências internacionais de dados pessoais plasmado no RGPD, importa agora sublinhar as principais novidades face à Diretiva 95/46/CE.

É a própria epígrafe do Capítulo V, que acolhe a disciplina jurídica em apreço, que espelha a primeira novidade: o novo regime das transferências de dados pessoais, que se aplicará, como até aqui acontece, a países terceiros, passará a aplicar-se, também, às organizações internacionais.

O alargamento às organizações internacionais, que se afigura claro, também pela leitura do primeiro art. que se dedica a esta temática (art. 44.º), caminha a par com o alargamento das situações em que as transferências serão permitidas. Este alargamento, esparso em várias normas, porventura para efeitos da sua dissimulação, é também ele claro, depois de uma análise aturada das normas em causa.

Na verdade, as transferências internacionais de dados passarão a ser admissíveis, em aditamento às situações até agora permitidas, em outros três casos: quando as autoridades de controlo competentes aprovarem regras vinculativas aplicáveis às empresas; quando houver acordo internacional nesse sentido; e quando a transferência não for repetitiva, apenas respeitar um número limitado de titulares, for para fins de interesse legítimo imperioso do responsável e oferecer garantias adequadas. Certo é que o alargamento das situações-tipo cumpre o propósito da União de oferecer mais oportunidades às empresas, conjugando a necessidade da

troca de dados para efeitos comerciais com os direitos das pessoas visadas, protegendo-se ademais a confiança nos mercados[12].

As novidades não se ficam pelas enunciadas. A subcontratação, neste contexto, surge com nova roupagem. Com efeito, nos termos da alínea a) do n.º 3 do art. 28.º, à obrigatoriedade de celebração de contrato ou de aprovação de outro ato normativo ao abrigo do direito da União ou dos Estados membros, que vincule o subcontratado ao responsável pelo tratamento, soma-se a obrigação, imposta ao subcontratado, de tratar os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento.

Além disso, o subcontratado é obrigado a conservar um registo de todas as categorias de atividades de tratamento realizadas em nome do responsável pelo tratamento, do qual constarão as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, se for o caso, a documentação que comprove a existência das garantias adequadas (alínea c) do n.º 2 do art. 30.º).

Elencadas as novidades no que à subcontratação respeita, importa destacar, por outro lado, o reforço ao nível da tutela do direito à informação dos titulares. Saliente-se, a este propósito, que o titular dos dados passará a ter direito a informação detalhada sobre transferências subsequentes (alínea f) do n.º 1 do art. 13.º e alínea f) do n.º 1 do art. 14.º).

O regime atinente à própria decisão de adequação da Comissão também surge densificado (art. 45.º), estando agora prevista a obrigação da Comissão de publicar no Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e organizações internacionais relativamente aos quais tenha declarado se asseguram ou não um nível de proteção adequado (n.º 8 do art. referido).

Relativamente à avaliação da adequação do nível de proteção, a aferir, nos casos concretos, pela Comissão, importa sublinhar que aos critérios plasmados na Diretiva 95/46/CE o RGPD adita outros, num claro reforço dos direitos dos cidadãos.

Com efeito, às circunstâncias da transferência aludidas pela Diretiva 95/46/CE, em especial, a natureza dos dados, a finalidade, a duração do

---

[12] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM/2017/07 final, p. 3.

tratamento, os países de origem e destino final, as regras de direito, as regras profissionais, as medidas de segurança, a legislação interna e os compromissos internacionais, o RGPD acrescenta o primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a jurisprudência, os direitos dos titulares dos dados efetivos e oponíveis, as vias de recurso administrativas e judiciais e a existência e funcionamento de autoridades de controlo independentes (n.º 2 do art. 45.º). Note-se que a Comissão é obrigada a avaliar periodicamente o nível de adequação, no mínimo de quatro em quatro anos, devendo ter em conta todos os desenvolvimentos pertinentes (n.º 3 do mesmo art.), controlando, de forma continuada, o funcionamento das decisões de adequação (n.º 4) e podendo revogar, alterar ou suspender as referidas decisões, se tal se mostrar necessário (n.º 5).

O art. 45.º acrescenta, no n.º 9, que as decisões adotadas pela Comissão com base na Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o novo Regulamento. Esta norma refere-se, em concreto, às doze decisões de adequação em vigor – respeitantes à Suíça (Decisão da Comissão 2000/518/CE, de 26 de julho de 2000), Canadá (Decisão da Comissãoo 2002/2/CE, de 20 de dezembro de 2001), Argentina (Decisão da Comissão 2003/490/CE, de 30 de junho de 2003), Guernsey (Decisão da Comissão 2003/821/CE, de 21 de novembro de 2003), Ilha de Man (Decisão da Comissão 2004/411/CE, de 28 de abril de 2004), Jersey (Decisão da Comissão 2008/393/CE, de 8 de maio de 2008), Ilhas Faroé (Decisão da Comissão 2010/146/UE, de 5 de março de 2010), Andorra (Decisão da Comissão 2010/625/UE, de 19 de outubro de 2010), Estado de Israel (Decisão da Comissão 2011/61/UE, de 31 de janeiro de 2011), República Oriental do Uruguai (Decisão de Execução da Comissão 2012/484/UE, de 21 de agosto de 2012), Nova Zelândia (Decisão de Execução da Comissão 2013/65/UE, de 19 de dezembro de 2012) e Estados Unidos da América (Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016).

Neste contexto, cumpre dar nota das decisões da Comissão relativas às cláusulas contratuais-tipo em vigor: por um lado, da Decisão da Comissão 2001/497/CE, de 15 de junho de 2001, para países terceiros, e, por outro, da Decisão da Comissão 2010/87/UE, de 5 de fevereiro de 2010, para subcontratantes estabelecidos em países terceiros.

2. O Caso Schrems e o Escudo de Proteção da Privacidade UE-EUA

Adentremo-nos agora no caso particular dos EUA. Antes de mais, abra-se um parêntesis. Os regimes de proteção de dados pessoais nos dois lados do Atlântico têm, até agora, espelhado dois paradigmas distintos. Por um lado, a disciplina jurídica aplicável nos EUA ancora-se em princípios como o da autocertificação e da autorresponsabilização. Por seu turno, na União Europeia, os ordenamentos jurídicos nacionais fundam-se em articulados legais, que preveem obrigações e deveres estritos. No entanto, com a aprovação do RGPD, a ordem jurídica europeia parece aproximar-se da norte-americana. Esta tendência de aproximação, perspetivando alterações de princípio, fundamenta-se, mormente, na substituição da tradicional obrigação de notificação de tratamento à autoridade de controlo (art. 18.º da Diretiva 95/46/CE) pela notificação de uma violação de dados pessoais (art. 33.º do RGPD). Ademais, assistimos à consagração dos princípios da proteção de dados desde a conceção e por defeito (art. 25.º do RGPD), bem como à previsão da obrigação de designação do encarregado da proteção de dados (art. 37.º do Regulamento), que, em conjunto, parecem reforçar a tendência, imprimida nos ordenamentos europeus, de autorresponsabilizar as empresas e os organismos públicos.

Feito este parêntesis, cumpre trazer à colação o comummente apelidado Caso Schrems[13], nos termos do qual o TJ sublinhou que o "nível de proteção adequado" a que alude o n.º 1 do art. 25.º da Diretiva 95/46/CE deve ser interpretado no sentido exigir uma proteção substancialmente equivalente oferecida pelo país terceiro. Na verdade, a proteção conferida por esse país, podendo ser configurada em moldes diferentes do regime aplicável na União, deve ser, não obstante, efetiva, oponível e sujeita a supervisão para ser considerada como adequada.

Ora, chamado a pronunciar-se na sequência da recusa de uma autoridade de controlo em investigar uma queixa atinente às transferências de dados pessoais para os EUA, o TJ, em acórdão de 6 de outubro de 2015 não apreciando o conteúdo dos princípios em causa, concluiu que a Comissão Europeia excedeu os seus poderes ao restringir os poderes das autoridades de controlo nacionais para suspender os fluxos de dados e invalidou a Decisão da Comissão 2000/520/CE, de 26 de julho de 2000.

---

[13] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, de 6 de outubro de 2015.

A invalidação da referida Decisão 2000/520/CE tornou premente a aprovação de nova decisão de adequação, sendo de sublinhar que, mesmo antes do acórdão *Schrems*, a Comissão Europeia tinha reconhecido a necessidade de rever o regime em apreço, nas Comunicações COM (2013) 846 final e COM (2013) 847 final. Nas referidas comunicações, a Comissão, testemunhando o aumento exponencial dos fluxos de dados pessoais, a importância crescente dada aos dados pessoais no contexto da economia transatlântica e o rápido aumento do número de empresas dos EUA que aderiram ao "Porto Seguro", bem como os programas de informações dos EUA, recomendou o reforço dos princípios de proteção da privacidade, da supervisão e controlo pelas autoridades dos EUA e dos mecanismos de resolução de litígios, frisando que a utilização para fins de segurança nacional deve ser proporcional e estritamente necessária.

Voltemos à invalidação da Decisão da Comissão 2000/520/CE: em causa estava o art. 3.º da aludida decisão, nos termos do qual os poderes das autoridades de controlo nacionais para suspender as transferências de dados só podiam ser exercidos em dois casos concretos, a saber, quando as autoridades dos EUA verificassem uma violação dos princípios ou existissem fortes probabilidades para supor que os princípios não estavam a ser respeitados.

No que toca a este ponto, a Decisão de Execução (UE) 2016/1250, que veio substituir a ora invalidada Decisão 2000/520/CE, fazendo cumprir o decidido pelo TJ, preceitua, no art. 3.º, que, sempre que as autoridades competentes dos Estados membros exerçam os seus poderes conducentes à suspensão ou proibição definitiva de fluxos de dados para uma organização nos Estados Unidos que conste da lista do Escudo de Proteção da Privacidade, o Estado membro em causa deve informar a Comissão sem demora, devolvendo todos os poderes às autoridades de controlo nacionais, que não se veem agora sujeitas a quaisquer restrições.

Citado este art. da Decisão de Execução (UE) 2016/1250, façamos uma visita guiada a todo o preceituado no Escudo de Proteção da Privacidade UE-EUA, que, nos termos da referida decisão que o acolhe, assegura o nível de proteção adequado exigido pela Diretiva 95/46/CE.

Preliminarmente, sublinhe-se o que já antes deixámos dito: o sistema em vigor nos EUA baseia-se na autocertificação; ou seja, são as próprias empresas norte-americanas que assumem o compromisso de proteger a

privacidade dos cidadãos europeus, compromisso esse assumido perante o Departamento do Comércio.

Vejamos agora os princípios plasmados no aludido Escudo da Privacidade. Em primeiro lugar, é consagrado o princípio de aviso, que impõe às empresas a prestação de informações aos titulares dos dados sobre as operações de tratamento, sendo imposta, em complemento, a obrigação de indicar os *links* para os sites oficiais das entidades com competência nesta matéria.

Em segundo lugar, é consagrado o princípio basilar, enformador do regime da proteção de dados, da limitação dos fins, que proíbe o tratamento posterior dos dados pessoais para qualquer fim reputado incompatível com a finalidade que legitimou o tratamento primitivo. Este princípio basilar caminha a par com a regra que determina que a conservação dos dados apenas é lícita durante o período temporal em que o tratamento for conforme às finalidades que motivaram a recolha.

O princípio da escolha também se revela de grande importância: relativamente ao tratamento de dados sensíveis, tal só é legítimo nos casos em que o titular tenha dado o seu consentimento expresso nesse sentido (*opt-in*); relativamente ao tratamento de dados não sensíveis, não sendo exigido o consentimento do titular, é-lhe conferido o direito a opor-se a tal tratamento (*opt-out*).

Ao titular é ainda conferido o direito de acesso aos dados, configurado como outro princípio basilar, acesso esse que pode ser exercido sem motivo justificativo e que pressupõe, incluindo, os direitos de retificação e eliminação dos dados. Ao titular dos dados é ainda reconhecido o direito de contestar as decisões automáticas que lhe digam respeito e lhe causem prejuízos. A estes princípios ainda se soma o da segurança dos dados.

A subcontratação, que também é permitida neste contexto, pressupõe a celebração de um contrato, sendo, pois, necessário um acordo entre o subcontratante e o subcontratado. As transferências ulteriores, sendo igualmente permitidas, estão sujeitas a condições, impondo-se que apenas ocorram para fins específicos, mediante a celebração de um contrato e apenas nos casos em que seja oferecido o mesmo nível de proteção.

É agora exigida a elaboração e publicação de uma lista atualizada de todas as empresas autocertificadas, sendo obrigação das empresas renovar a certificação anualmente, passando a ser obrigatória também a disponibilização de um registo atualizado das empresas suprimidas da referida lista

e do motivo da supressão. Note-se que a supervisão do regime plasmado no Escudo da Privacidade cabe ao Departamento do Comércio, à Comissão Federal de Comércio e ao Departamento dos Transportes norte-americanos.

Atentemos agora no novo regime atinente à apresentação de queixa por parte do titular dos dados, sendo de frisar que tal regime é arquitetado segundo uma ordem lógica que é aconselhável seguir (é o próprio preceituado que o refere).

Em primeiro lugar, o titular pode apresentar queixa à empresa que recolheu os seus dados, tendo esta 45 dias para responder ao indivíduo. Em segundo lugar, e estando a empresa obrigada a designar um organismo independente de resolução de litígios, o particular pode queixar-se a esse organismo. Em terceiro lugar, o titular pode recorrer às autoridades de controlo dos Estados membros, sendo a queixa reencaminhada para o Painel informal de autoridades constituído ao abrigo do Escudo da Privacidade. Este Painel dispõe de 60 dias para apreciar a reclamação, podendo, na sequência dessa apreciação, intentar uma ação nos tribunais competentes dos Estados membros. Em quarto lugar, o particular visado pode queixar-se junto do Departamento do Comércio norte-americano, tendo esta entidade 90 dias para responder. Em quinto lugar, o titular dos dados pode solicitar a intervenção da Comissão Federal de Comércio, que pode espoletar a devida ação junto do Tribunal Federal. Em sexto lugar, o titular dos dados pode recorrer ao Comité Arbitral agora criado, podendo, em sétimo e último lugar, recorrer aos tribunais norte-americanos.

Por seu turno, tendo em conta a relevância do regime atinente ao acesso aos dados pessoais por parte das autoridades norte-americanas para fins de segurança nacional, vejamos com detalhe o preceituado quanto a esta temática.

O novo acordo, plasmado no Estudo da Privacidade, distingue a recolha da utilização de dados por parte das autoridades competentes, prevendo limitações para ambos os casos. No que concerne à recolha de dados, é exigido que a mesma se faça apenas ao abrigo de lei ou autorização presidencial e exclusivamente nos casos de espionagem externa ou de contraespionagem, assim como para apoiar missões nacionais e departamentais. A regra estabelecida é que a recolha seja seletiva, isto é, a colheita de dados apenas é legítima mediante a utilização de identificadores associados a um objetivo específico e dos respetivos filtros. No entanto, continua a figurar como exceção a recolha em larga escala, que, não obstante, requer a identificação

de objetivos específicos, como ameaças novas, exigindo-se, igualmente, a utilização de filtros.

Vistas as limitações impostas aquando da recolha dos dados, vejamos agora os limites impostos à utilização dos mesmos. Com efeito, as autoridades norte-americanas só poderão usar os dados nos casos em que tais informações se mostrem pertinentes à deteção e combate a ameaças decorrentes de espionagem, terrorismo e armas de destruição maciça, assim como a ameaças à cibersegurança, para as forças armadas ou pessoal militar e ameaças criminosas transnacionais relacionadas com as ameaças anteriormente referidas. Caso a utilização dos dados se mostre necessária para a deteção e combate das ameaças enumeradas, as autoridades competentes podem conservar as informações em causa durante o período de cinco anos, podendo, em alguns casos, haver retenção continuada.

A utilização dos dados pelas autoridades dos EUA encontra-se sujeita a supervisão do poder executivo e do Congresso, podendo também ser sindicada pelos tribunais norte-americanos. Ao cidadão é conferido o direito de recorrer judicialmente do acesso aos seus dados, podendo, igualmente, pedir uma indemnização pelos danos causados e a supressão dos dados que lhe digam respeito. A par disso, tem ao seu dispor o novo mecanismo da mediação, ora criado.

Por fim, e ainda no que toca ao Escudo da Privacidade, importa sublinhar a obrigatoriedade de reapreciação conjunta anual, sendo atribuídos poderes à Comissão Europeia para suspender, parcial ou totalmente, as transferências de dados, assim como alterar ou revogar a Decisão de Adequação, caso assim o entenda. Quanto ao poder de revogação, saliente-se que o mesmo deve ser exercido nos casos em que se verifique o incumprimento do preceituado, a não resolução de queixas apresentadas pelos particulares ou a falta de cooperação por parte dos EUA.

3. As transferências internacionais de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal: breve alusão

A matéria da transferência de dados pessoais para efeitos de prevenção, investigação, deteção e repressão da criminalidade encontrou regulação, até aos dias de hoje, na Decisão-Quadro 2008/977/JAI. Esta decisão-quadro foi revogada pela Diretiva (UE) 2016/680, revogação que só produz efeitos

a partir de 6 de maio de 2018, dia em que termina o prazo de transposição a levar a respeitar pelos Estados-Membros. No que às transferências de dados respeita, assistimos a diversas continuidades, que importa elencar.

Em primeiro lugar, ao abrigo da Decisão-Quadro 2008/977/JAI, sempre presidiu à transferência o princípio da necessidade, princípio este que continua a imperar na Diretiva (UE) 2016/680. Por outro lado, as transferências continuam a ser efetuadas para as autoridades competentes e com o consentimento prévio do Estado membro detentor dos dados. Aliás, a transferência de dados sem o aludido consentimento prévio apenas pode ser operacionalizada em casos excecionais; a saber, quando está em causa uma ameaça imediata e grave à segurança pública ou um interesse fundamental de um Estado membro, e, em ambos os casos, quando o consentimento não puder ser obtido em tempo útil.

A par disso, e como continuidades, assinale-se que as transferências são e vão continuar a ser permitidas com base na adequação dos ordenamentos jurídicos estrangeiros ou mediante as salvaguardas adequadas. Podem e continuarão a poder ocorrer em situações específicas, designadamente quando estão em causa interesses legítimos do titular ou interesses públicos.

Vistos os pontos paralelos da Decisão-Quadro 2008/977/JAI e da Diretiva (UE) 2016/680, vejamos agora as novidades. A primeira respeita à possibilidade de transferir dados diretamente para os destinatários, transferência esta que é, não obstante, sujeita a determinadas condições. As transferências continuam a ser legítimas, tal como já adiantámos, com base na adequação do ordenamento jurídico estrangeiro em apreço; ora, as novidades residem precisamente na consagração, também nesta sede, das decisões de adequação da Comissão e na obrigatoriedade de disponibilização de uma lista das decisões de adequação em vigor. Além disso, os critérios de avaliação da adequação do nível de proteção são densificados, em prol do fortalecimento dos direitos fundamentais em causa. Recorde-se que a Decisão-Quadro 2008/977/JAI apenas fazia alusão à necessidade de apreciar as circunstâncias da transferência, em concreto, a natureza dos dados, a finalidade, a duração do tratamento, o destinatário, o direito vigente e as medidas de segurança. Por seu turno, a Diretiva (UE) 2016/680 acrescenta os princípios do Estado de direito, aludindo expressamente à legislação, à jurisprudência e aos compromissos internacionais, assim como, sublinhe-se, à existência de uma autoridade de controlo independente.

Outras duas novidades: as transferências passarão a ser permitidas mediante a adoção de garantias adequadas, sendo expressamente reconhecidos os instrumentos juridicamente vinculativos, como os acordos internacionais; são acrescentadas novas situações-tipo que ditam as transferências, passando a ser permitidas também para salvaguardar interesses vitais e em processos judiciais.

Num claro reforço do direito à proteção de dados dos cidadãos, passará a exigir-se autorização expressa para transferências ulteriores, que caminha a par com um regime densificado sobre cooperação internacional e assistência mútua.

Uma referência final ao recente acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais[14] e à intenção da Comissão Europeia de aprovar acordos com outros países[15].

Considerações finais

Stefano Rodotà, a propósito da Diretiva 2006/24/CE[16], atinente ao tratamento de dados no contexto das comunicações eletrónicas, aventou a invasão generalizada da esfera íntima das pessoas, nomeadamente por parte das entidades públicas, e a reestruturação do espaço privado e público dos cidadãos, afirmando que a aludida diretiva não configurava uma exceção para casos específicos e particulares, mas antes a antecipação do futuro, agora presente, sendo a primeira das etapas com vista à profunda alteração dos princípios basilares da proteção de dados pessoais[17]. Aliás, para o autor,

---

[14] Decisão (UE) 2016/2220 do Conselho, de 2 de dezembro de 2016, relativa à celebração, em nome da União Europeia, de um acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais.

[15] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM/2017/07 final, p. 14.

[16] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE.

[17] Rodotà, Stefano. "La conservación de los datos de tráfico en las comunicaciones electrónicas", *Revista de Internet, Derecho y Política*, n.º 3, 2006, pp. 53-59.

a ponderação de interesses pertence ao passado, pelo que assistimos à inadequação das garantias oferecidas aos cidadãos e ao abandono do critério do alto nível de proteção[18].

Na verdade, as empresas e os organismos públicos dispõem, nos dias de hoje, de mais informações e de mais formas de as tratar, e mais sofisticadas, impulsionadas não só pelos avanços tecnológicos, mas também por algumas iniciativas legislativas, que facilitam a recolha e a troca de dados. Aliás, o tratamento de dados pessoais é, hoje, uma prioridade da União Europeia, em prol, principalmente, da segurança das pessoas, com evidentes efeitos negativos no direito à proteção de dados, que é, nos nossos dias, o direito de controlar a informação que nos diz respeito.

Certo é que o legislador da União, visando o justo equilíbrio entre os valores públicos e os interesses particulares em apreço, sempre teve a preocupação de balancear o princípio da livre circulação das pessoas e dos seus dados, o propósito da luta contra o terrorismo e a criminalidade grave e a proteção dos direitos e liberdades fundamentais, nomeadamente a proteção da privacidade e dos dados pessoais. Isso mesmo decorre da generalidade dos considerandos que enquadram os principais diplomas nesta área que hoje nos ocupa.

O Escudo de Proteção da Privacidade UE-EUA a que já aludimos, constante da Decisão de Execução (UE) 2016/1250, não é exceção, destacando, na respetiva introdução, o intuito de equilibrar os valores e direitos em presença. No entanto, muitas dúvidas[19] se colocam acerca deste novo acervo jurídico. Vejamos.

Em primeiro lugar, o ordenamento jurídico norte-americano parece não contemplar a autoridade independente exigida pelo art. 8.º da Carta dos Direitos Fundamentais da União Europeia, enquanto corolário do direito fundamental à proteção de dados. O Escudo de Proteção da Privacidade, arquitetando um complexo esquema de recurso, que segue, aliás, uma ordem lógica, não disponibiliza, para efeito da apreciação das queixas apresentadas pelos cidadãos, um mecanismo de resolução de litígios totalmente imparcial ou uma autoridade independente do poder executivo.

---

[18] *Idem*, p. 57.

[19] No mesmo sentido, Lucas Pires, Martinho. "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado no presente Anuário.

Em segundo lugar, este acordo UE-EUA parece perpetuar a possibilidade de recolha de dados em larga escala pelas autoridades norte-americanas. A recolha em larga escala é, pois, uma recolha em massa, o que viola os direitos fundamentais em presença, tal como já afirmado pelo TJ.

Em terceiro lugar, as autoridades norte-americanas, além de poderem recolher dados pessoais em larga escala, podem conservá-los, em certos casos, por períodos superiores a cinco anos, o que, na prática, permite uma retenção continuada, também atentatória dos direitos das pessoas, tal como interpretados pelo TJ.

Por fim, o mediador criado, cuja missão é apreciar as queixas dos cidadãos europeus relativamente ao tratamento dos seus dados pelas autoridades norte-americanas, suscita-nos as maiores reservas, não ficando claro quem nomeia o aludido mediador e, por conseguinte, não sendo certo que tal mecanismo é independente.

Este enquadramento parece provar que a segurança pesa mais, quando colocada na balança com a liberdade, sendo a utilidade das informações pessoais dada por adquirida nas circunstâncias atuais.

Certo é que a segurança é precondição da liberdade. No entanto, não podemos esvaziar ou desvalorizar o conflito que existe efetivamente entre os valores em causa, que reclamam, a cada novo desafio da sociedade, a ponderação devida. Esta tendência para transmutar valores conflituantes em valores conciliáveis, flexibilizando os discursos políticos, deve ser combatida, dignificando todos e cada um dos direitos humanos. Note-se que, ainda recentemente, a Comissão Europeia afirmou que a livre circulação e a proteção de dados não se excluem mutuamente, reiterando o discurso conciliador[20].

Na verdade, o diálogo político tem sido fortemente influenciado por interesses comerciais e aspirações políticas, faltando, notoriamente, uma consulta genuína aos cidadãos sobre uma matéria que terá um impacto significativo na sociedade[21]. Aliás, um estudo recente sobre a matéria vem concluir que as normas de proteção de dados constantes dos acordos comer-

---

[20] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM/2017/07 final, p. 16.

[21] Ashbourn, Julian. "The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies", *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla: European Commission, 2005.

ciais celebrados pela União Europeia não são suficientes, não se podendo excluir a hipótese de um parceiro comercial intentar ações contra a União Europeia por causa das regras de proteção de dados, mormente a forma como se avalia a adequação pode ser vista como obscura e inconsistente[22].

A Comissão Europeia aprovou, de facto, uma nova decisão de adequação para os EUA, mudando o acervo jurídico aplicável[23]. No entanto, esta mudança não foi acompanhada pelo reforço da proteção dos direitos fundamentais. Na nossa opinião, continuamos a não acautelar o que antes preocupava o TJ e que levou à invalidação do anterior acordo. Salvo melhor opinião, a proteção não viaja com os dados, tal como era propósito da União[24].

Na sequência do acórdão *Schrems*, que espoletou, como já vimos, o aludido Escudo de Proteção da Privacidade celebrado com os EUA, a Comissão prepara-se para alterar as restantes decisões de adequação em vigor, bem como as decisões que aprovam cláusulas contratuais gerais, suprimindo todas as restrições aos poderes das autoridades de controlo nacionais; por outro lado, a Comissão revelou o propósito de aprovar mais decisões de adequação, visando, nomeadamente, o Japão e a Coreia, que adotaram novas regras de proteção de dados recentemente, promovendo, assim, o comércio com estes países[25]. Prevê-se que, posteriormente, sejam adotadas decisões de adequação sobre o nível de proteção conferido na Índia e em alguns países da América Latina[26].

Numa palavra: o direito à proteção de dados pessoais é, hoje, o direito de controlar a informação que nos diz respeito, sendo, por isso, premente

---

[22] Irion, Kristina; Yakovleva, Svetlana e Bartl, Marija. *Trade and privacy: complicated bedfellows?* Institute for Information Law (IViR), 2016. Disponível em: <http://www.ivir.nl/publicaties/download/1807> (acedido a 24/11/2017).

[23] Rodrigues de Oliveira, Ricardo. "What's in a Name? Uma breve análise do nível de protecção adequado no âmbito das transferências de dados pessoais dos cidadãos da UE para países terceiros", publicado no presente Anuário. Concordamos com a crítica à política de negociações da União Europeia, mormente à insuficiente investigação da Comissão Europeia, que assegura a adequação apenas porque confia nas autoridades do Estado terceiro, bem como com a crítica ao legislador europeu, que continua a não definir de forma satisfatória o "nível de proteção adequado".

[24] Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM/2017/07 final, p. 4.

[25] *Idem*, p. 8.

[26] *Ibidem*.

a sensibilização e a escolha informada dos cidadãos, mormente sobre a utilização da Internet.

Sublinhe-se que as funcionalidades oferecidas pelo *Big Data* aumentam exponencialmente os riscos de enviesamento da análise de dados, assim como a subestimação das implicações do uso de dados nos processos de decisão e a marginalização dos indivíduos. Contudo, essas mesmas funcionalidades são poderosos instrumentos económicos, permitindo a análise de dados em grande quantidade. As vantagens são muitas, ditando a flexibilidade de princípios basilares, como o princípio da finalidade, vislumbrando-se como alternativas legitimadoras do tratamento o consentimento dos visados, a anonimização ou o tratamento apenas para fins estatísticos, tratamento este que redunda num *profiling* mascarado[27].

Vivemos numa sociedade que guarda as informações dos seus cidadãos de forma rotineira. Vejam-se as obrigações legais das transportadoras aéreas e das operadoras de telecomunicações de reter dados dos seus clientes e de os fornecer às autoridades. Porém, a nossa segurança não pode significar a devassa total da privacidade. A identidade digital requer, não temos dúvida, o direito à nossa intimidade, mesmo com os ímpetos das medidas securitárias que o mundo de hoje dita.

---

[27] Mayer-Schonberger, Viktor e Padova, Yann. "Regime change? Enabling Big Data through Europe's new Data Protection Regulation", *The Columbia Science & Technology Law Review*, vol. XVII, Spring 2016, pp. 315-335.

Algumas considerações sobre a compatibilidade do sistema de *Privacy Shield* com o direito da União Europeia à luz do acórdão Schrems

Martinho Lucas Pires*

Resumo: O presente artigo tem por objeto a análise crítica dos principais elementos do sistema de *Privacy Shield*, relativo à transferência de dados entre a União Europeia e os Estados Unidos da América. A análise parte dos critérios normativos de direito da União Europeia que devem rodear a apreciação do nível de proteção de dados garantido por um país terceiro, estabelecidos pelo Tribunal de Justiça da União Europeia no acórdão *Schrems*. Tais considerações demonstram que importantes características do *Privacy Shield* suscitam sérias dúvidas de legalidade, colocando em dúvida o futuro de tal sistema a médio e longo prazo.

Palavras-chave: *Direito da União Europeia; Proteção de Dados; Direitos Fundamentais; Relações UE-EUA.*

Abstract: The purpose of this article is to critically analyse the main elements of the Privacy Shield framework on the transfer of data between the European Union and the United States of America. In order to do so, this article shall start from an assessment of the framework in light of the normative criteria of European Union law as set out by the Court of Justice of the European Union in the *Schrems* case. This analysis shows that important characteristics of *Privacy Shield* raise serious questions of legality that cast a shadow over the long-term feature of the framework.

Keywords: *European Union Law; Data Protection; Fundamental rights; Relations EU-USA.*

---

* Licenciado e mestre em Direito pela Faculdade de Direito da Universidade Católica Portuguesa. Doutorando em direito da União Europeia pela Faculdade de Direito da Universidade Nova de Lisboa. Bolseiro da Fundação para a Ciência e Tecnologia. Advogado, com inscrição suspensa por motivos académicos. Assistente convidado da Faculdade de Direito da Universidade Católica Portuguesa. Escreve sobre os temas de Direito Constitucional, Direito da União Europeia, Direito Económico e Protecção de Dados. Este artigo foi escrito com o apoio de uma bolsa da Fundação para a Ciência e Tecnologia.

Introdução

O quadro normativo sobre a recolha, armazenamento, tratamento e transferências de dados pessoais na UE tem sido alvo de grandes e profundas transformações nos últimos anos[1]. Deve-se este facto ao grande desenvolvimento que entretanto se verificou no campo das chamadas tecnologias de informação[2]. A utilização e subscrição de serviços comerciais, de entretenimento, e dos mais variados tipos, através de mecanismos digitais que são facilmente acessíveis através de instrumentos portáteis como um telefone ou um simples relógio tornou-se tão comum que é hoje um comportamento normal e recorrente. Não só da vivência cultural e social mas, sobretudo, económica. Basta um "clique" numa tecla ou um "toque" num ecrã para que uma série de informações possa ser transmitida para um outro aparelho, que pode estar localizado num território não só *distinto* como também bastante *distante* do lugar onde o utilizador se encontra. Esta facilidade de comunicação levou a um aumento exponencial de transferências territoriais de dados, possibilitando o desenvolvimento de vários negócios dedicados somente à economia digital, naquilo que se diz ser o primeiro mercado, pela sua natureza e características, naturalmente global[3].

Esta digitalização de serviços económicos trouxe consigo vários desafios de regulação, tendo em conta a vulnerabilidade a que os mesmos dados estão sujeitos. De facto, os dados não são só facilmente transmissíveis; são igualmente objeto de fácil recolha ou tratamento por parte de entidades privadas (empresas, associações) quer por entidades públicas (administração fiscal ou policial). Tratamento esse que pode ou não ser indevido, se

---

[1] Para uma análise histórica da evolução sobre legislação de protecção de dados na UE, v. Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa "Handbook on European data protection law", 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf> (acedido a 25/10/2017).

[2] V. igualmente, sobre esta evolução e evolução das regulações comerciais, o artigo de 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?", publicado no presente Anuário.

[3] Sobre o impacto económico das transferências internacionais de dados, v. Conferência das Nações Unidas sobre Comércio e Desenvolvimento, "Data protection regulations and international data flows: Implications for trade and development", 2016. Disponível em: <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> (acedido a 25/10/2017).

não for conhecido e autorizado de antemão pelo utilizador. Cabe assim às autoridades políticas estabelecer sistemas de normas e meios práticos que permitam uma proteção eficaz dos direitos de privacidade dos titulares destes dados – sem no entanto afetar em demasia a liberdade de transmissão dos mesmos num mundo global.

Esta fácil mobilidade de dados entre diferentes ordens jurídicas é um dos problemas mais importantes desta nova realidade digital. Isto porque, no caso da UE, muitas das grandes empresas que operam (e, de certa forma, têm uma posição determinante) no seu mercado interno são oriundas dos EUA, como a *Apple*, *Google*, *Facebook*, *Amazon*, entre outras. A estrutura multinacional destas empresas, com certos serviços internos divididos entre vários territórios e continentes, faz com que os dados dos consumidores e utilizadores (e, igualmente, dos trabalhadores) destas empresas sejam passíveis de tratamento em vários locais, com regimes jurídicos diversos. Consequentemente, os utilizadores estarão sujeitos a diferentes níveis de proteção dos seus direitos à privacidade e à intimidade da vida privada, dependendo da ordem jurídica em que se encontrem os seus dados. Coloca-se, deste modo, o desafio de estabelecer mecanismos jurídicos que possam garantir a efetiva proteção de dados a um nível razoavelmente semelhante ao gozado pelos utilizadores no seu território residencial, quando tais dados são transmitidos para territórios terceiros.

O sistema atualmente em vigor quanto à transferência de dados pessoais de cidadãos europeus para empresas sediadas nos EUA é denominado de *Privacy Shield* ou "Escudo de Proteção". Este sistema foi considerado adequado face às normas europeias de proteção de dados pela Decisão de Execução da Comissão número 2016/1250, de 12 de julho de 2016 (doravante "Decisão *Privacy Shield*"). O *Privacy Shield* veio substituir os princípios de *Safe Harbor* que se encontravam em vigor desde há dezassete anos[4], e que em 2015 foram considerados incompatíveis com o direito da União Europeia pelo Tribunal de Justiça no acórdão *Schrems*[5]. O conteúdo desta sentença judicial acabou por afetar a elaboração da Decisão de *Privacy*

[4] Comissão Europeia, Decisão 2000/520 EC com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa ao nível de proteção assegurado pelos princípios de Porto Seguro e Resposta a Questões pelo Departamento de Estado dos EUA, de 26 de julho de 2000.

[5] Acórdão do TJ, C-362/14, *Maximilian Schrems* v. *High Authority*, de 6 de outubro de 2015.

Shield, ao estabelecer de forma contundente critérios normativos que limitam a ação da Comissão ao apreciar a adequação de um sistema jurídico de proteção de direitos de titulares de dados pessoais de um país terceiro com o sistema da UE. Apesar da aprovação de uma decisão de adequação, subsistem ainda sérias dúvidas sobre a compatibilidade do *Privacy Shield* com as normas do direito da UE sobre proteção de dados pessoais. Estas dúvidas foram expressas por autoridades públicas de proteção de dados europeias e nacionais[6] e por órgãos políticos como o Parlamento Europeu[7].

O propósito deste artigo é apresentar algumas considerações relativas quanto ao juízo de compatibilidade do *Privacy Shield* com as normas de direito da UE sobre a transmissão e a proteção de direitos dos titulares de dados pessoais para um país terceiro. Para tal efeito iremos, numa primeira parte, ver quais os requisitos normativos da UE relativos à transmissão de dados para países terceiros. Iremos analisar não só as normas em vigor mas sobretudo a interpretação que lhes foi dada pelo Tribunal de Justiça no acórdão *Schrems*. Em seguida, numa segunda parte, faremos uma breve descrição da Decisão de *Privacy Shield* e de quais os seus traços gerais em termos de forma, estrutura e conteúdo. Na terceira parte olharemos de forma crítica para a Decisão de *Privacy Shield*, tendo por base não só a sua compatibilidade com os requisitos normativos em causa face a certos preceitos analisados em abstrato, mas também considerando a questão da sua aplicação prática por parte das autoridades públicas norte-americanas. Terminaremos com uma breve consideração sobre o futuro do sistema de *Privacy Shield* e das transferências de dados transatlânticas.

---

[6] Autoridade Europeia para a Protecção de Dados, "Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision", de 30 de maio de 2016. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf> (acedido a 25/10/2017); e G29, "Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", adoptada a 13 de abril de 2016. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (acedido a 25/10/2017).

[7] Parlamento Europeu, Proposta de Resolução Comum de 24 de maio de 2016. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P8-RC-2016-0623+0+DOC+PDF+V0//EN> (acedido a 25/10/2017); e Parlamento Europeu, Proposta de Resolução de 29 de março de 2017. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2017-0235+0+DOC+PDF+V0//PT> (acedido a 25/10/2017).

2. Requisitos normativos para transferências de dados da UE para países terceiros

2.1. Requisitos legislativos: Diretiva 95/46/CE

O regime de transferência de dados da UE para países terceiros encontra-se regulado no capítulo IV da Diretiva 95/46/CE do Conselho e do Parlamento (doravante a "Directiva"), mais concretamente nos art. 25.º e 26.º. Dispõe o n.º 1 do primeiro art. que as transferências de dados pessoais para países terceiros só podem ser realizadas caso o país em questão – país recetor – assegure um nível de proteção adequado para os dados, ou caso alguma das exceções estabelecidas na Diretiva ocorra. Quer isto dizer que a transferência de dados da UE para países terceiros é em princípio *proibida* caso não estejam preenchidas as condições previstas na Diretiva.

A averiguação da adequação do nível de proteção de dados do país recetor deverá ser efetuada, de acordo com o n.º 2 do art. 25.º, "em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados". Para o efeito desta avaliação, deve ter-se em conta uma série de critérios, tais como: a natureza dos dados, a razão de ser do tratamento e sua duração, o local de origem dos dados para tratamento e o local de destino após tratamento, o regime jurídico de proteção de dados no país terceiro, e "as regras profissionais e as medidas de segurança" que são respeitadas no território do país recetor. Cabe à Comissão, nos termos do disposto no n.º 6 do mesmo art., após averiguação do preenchimento destes critérios, tomar uma decisão, declarando se o país terceiro oferece ou não um nível de proteção adequada de tratamento de dados pessoais, tendo em conta a respetiva legislação nacional e compromissos internacionais assumidos por esse país recetor.

Como foi mencionado *supra* existem exceções a este regime, estabelecidas nas alíneas a) a f) do art. 26.º n.º 1. A transferência pode ser efetuada independentemente do país terceiro oferecer ou não um nível de proteção adequada nos seguintes casos: se uma pessoa dado o seu consentimento inequívoco à transferência de dados; se a transferência efetuada a partir de um registo público; se a transferência necessária para a celebração de um contrato e efetuada no interesse do titular dos dados, ou se for efetuada para proteger um interesse público, ou para exercer um direito de defesa num processo judicial, ou ainda para proteger os interesses vitais do titular

dos dados. Importa também referir que, nos termos do art. 26.º n.º 2, caso um Estado-Membro ou a Comissão considerem que existem, em concreto, cláusulas contratuais que garantam direitos de proteção da vida privada e condições de exercício desses respetivos direitos, a transferência de dados para um país terceiro que não ofereça um nível de proteção adequado é permitida.

A Diretiva foi recentemente revogada pelo RGPD. Este diploma passará a ser aplicável a partir de 18 de maio de 2018, segundo o seu art. 99.º, pelo que cabe verificar o quadro normativo relativo às transferências de dados para países terceiros[8].

A matéria sobre transferência de dados para países terceiros encontra-se disposta no capítulo V do Regulamento, nos arts. 44.º a 50.º. O nível de regulação é mais desenvolvido do que na Diretiva. A regra geral continua a ser a de que a transferência de dados é proibida a não ser que exista uma decisão de adequação da Comissão que considere o nível de proteção de dados pessoais do país terceiro como sendo adequado. Contudo, o art. 45.º n.º 1 alíneas a) a c) apresenta uma lista reforçada de critérios para avaliação da adequação. Aos critérios do art. 25.º n.º 1 da Diretiva acrescentam-se: a existência do "primado do Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais"; a aplicação e respeito de regras de proteção de dados, nas quais se incluem as que são desenvolvidas por jurisprudência; a existência de "direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência"; e "a existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional" com capacidade coerciva. Deve ter-se igualmente em conta o facto do país recetor estar ou não sob a alçada de instrumentos jurídicos internacionais de carácter vinculativo sobre esta matéria.

Caso não exista uma decisão de adequação, os responsáveis de tratamento de dados só podem transferi-los desde que apresentem garantias adequadas de proteção e que os titulares dos dados disponham de direitos e mecanismos judiciais de reação que sejam eficazes, nos termos do

---

[8] Cabe dizer neste ponto que a elaboração do quadro normativo do Regulamento, em particular quanto aos critérios necessários que a decisão de adequação deve preencher, foi bastante influenciado pelas considerações que o TJ fez no acórdão *Schrems*, como se verificará após a análise do *douto aresto*.

art. 46.º n.º 1. Estas garantias adequadas, nos termos do n.º 2, podem ser previstas através de instrumentos jurídicos vinculativos "e com força executiva entre autoridades ou organismos públicos", regras vinculativas de autoridades nacionais de controlo[9], cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão, códigos de conduta emitidos ao abrigo do art. 40.º ou procedimentos de certificação ao abrigo do art. 42.º. Quanto às derrogações, o regime do art. 49.º transcreve, na prática, o regime do n.º 1 do art. 26.º da Diretiva, acrescentando-se no entanto que, caso uma transferência não tenha por base uma decisão de adequação nem preencha as derrogações dos art. 46.º ou do n.º 1 do art. 49.º, só pode ocorrer se:

> (...) não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais.

Por fim, o art. 50.º do Regulamento estabelece que a Comissão e as autoridades nacionais de controlo devem prosseguir com esforços contínuos de cooperação internacional no domínio de proteção de dados[10].

2.2. Interpretação dos requisitos normativos: o caso Schrems

Como decorre da exposição anterior, a questão principal quanto ao critério para permitir a transferência de dados de forma generalizada

---

[9] Ao abrigo do art. 47.º do Regulamento, as autoridades de controlo podem emitir regras vinculativas relativas ao tratamento e às transferências de dados por empresas ou grupos de empresas. Essas regras devem especificar, nos termos das várias alíneas do n.º 2 do artigo, uma série de elementos, entre os quais os direitos dos titulares e métodos de reação e exercício desses mesmos direitos, bem como procedimentos internos de supervisão do tratamento e de reclamação sobre o mesmo.

[10] Sobre as transferências de dados ao abrigo do Regulamento, v. 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?", publicado no presente Anuário.

prende-se com o entendimento que deve ser dado à expressão "nível de proteção adequado". Existem critérios de averiguação amplos, mas não existe uma definição exata do conceito de adequação. Neste sentido, caberia à Comissão, no âmbito dos poderes que lhe foram atribuídos pela Diretiva, realizar tal juízo dentro dos seus poderes discricionários.

A questão foi discutida no acórdão *Schrems* pelo TJ. O caso em questão tem por base a ação intentada por um cidadão austríaco, Maximilian Schrems, contra o *Data Protection Commissioner*, a autoridade de controlo de proteção de dados da Irlanda. Após as revelações de Edward Snowden – antigo funcionário da NSA, uma agência de segurança e investigação pertencente à administração dos EUA – a vários órgãos de comunicação social internacionais sobre as práticas de vigilância operadas pelos serviços secretos dos EUA, que recolhiam de forma generalizada e indiscriminada dados pessoais armazenados em sistemas de comunicação diversos através da NSA, Schrems fez uma queixa ao *Data Protection Commissioner.* A queixa assentava no facto de a rede social Facebook, da qual Schrems era utilizador, transferir dados de clientes para os EUA, onde poderiam ser alvo de recolha por parte dos serviços secretos norte-americanos. Deste modo, Schrems requeria que as autoridades irlandesas deixassem de autorizar a transferência de dados e investigasse se o Facebook permitia ou não a recolha dos mesmos por parte das autoridades norte-americanas. A autoridade de controlo irlandesa recusou-se a ouvir a queixa por considerar que esta carecia de fundamento, e remeteu para a existência da decisão da Comissão que considerava que o nível de proteção existente nos EUA, assente nos princípios de *Safe Harbor,* era adequado.

Insatisfeito com a decisão, Schrems recorreu judicialmente para a *High Court,* o Supremo Tribunal irlandês. Este órgão jurisdicional, ao contrário do *Data Protection Commissioner,* considerou que os efeitos das revelações Snowden não podiam ser ignorados, e que existiam dúvidas sobre se a decisão de adequação da Comissão face ao sistema de *Safe Harbor* era ou não válida ao abrigo da CDFUE[11]. No entanto, cabia saber se a decisão de adequação impedia ou não as autoridades nacionais de controlo de prosseguir uma queixa individual que lhes fosse colocada, havendo suspeitas de risco de utilização indevida de dados. O Supremo Tribunal Irlandês

[11] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, paras. 30 a 35, de 6 de outubro de 2015.

decidiu questionar o TJ, através do mecanismo de reenvio prejudicial, relativamente ao grau de vinculação que o art. 25.º n.º 1 da Diretiva impõe à autoridade nacional de proteção de dados relativamente à decisão de adequação da Comissão[12].

O TJ tratou prontamente de responder a esta questão, considerando que ao abrigo da Diretiva e da interpretação que lhe deve ser dada segundo os art. 7.º – respeito pela vida privada e familiar – e 8.º – proteção de dados pessoais – da CDFUE, a autoridade nacional de proteção de dados pode investigar queixas relativas ao tratamento de dados em países terceiros, mesmo se existir já uma decisão de adequação prévia[13]. Entender o contrário seria retirar os poderes às autoridades nacionais de proteção de dados e limitar o direito dos particulares a uma proteção judicial efetiva, nos termos do art. 47.º da Carta.

Em seguida, em vez de dar o caso por terminado, o tribunal europeu decidiu debruçar-se sobre a decisão de adequação *per se*. Ou seja, o TJ quis olhar para a validade da decisão face às normas europeias sobre transferências de dados. Para tal, era necessário interpretar o significado de nível proteção adequado à luz dos artigos da CDFUE mencionados *supra*, e no seguimento da recente jurisprudência do TJ consagrada à interpretação destas normas no ordenamento jurídico da UE, mormente no acórdão *Digital Rights*[14].

---

[12] *Idem*, para. 36.

[13] "Atendendo às considerações anteriores, há que responder às questões submetidas que o artigo 25.º, n.º 6, da Diretiva 95/46, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520, através da qual a Comissão 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, 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". Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, para. 66, de 6 de outubro de 2015.

[14] Acórdão do TJ, C-293/12 e C-594/12, *Digital Rights Ireland*, de 8 de abril de 2014, sobre uma análise do caso, v. Granger, Marie-Pierre e Irion, Kristina. "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection", *European Law Review*, vol. 39, n.º 6, 2014, pp. 835-850 e Ramalho, David e Coimbra, José Eduardo. "A declaração de invalidade da

Neste sentido, o TJ afirmou que por nível de proteção adequado deve entender-se que o quadro de proteção de direitos dos titulares de dados do país terceiro é "substancialmente equivalente" ao que é oferecido pela UE[15]. Isto não significa que um país terceiro tenha de ter um sistema exatamente *idêntico* ao da UE mas sim, nas palavras do TJ, que este país deve dispor de meios jurídicos "efetivos, na prática" para proteção dos direitos dos titulares, "para assegurar uma proteção substancialmente equivalente à garantida dentro da União[16]". Apesar de reconhecer o poder de apreciação da Comissão, o TJ alega que este é limitado, dados os requisitos estipulados pelo art. 25.º da Diretiva e os direitos estabelecidos na CDFUE. Deve, portanto, ser aplicado e fiscalizado de forma estrita[17].

O TJ trata então de identificar três características essenciais que o sistema de proteção de direitos dos titulares de dados do país terceiro deve garantir para ser considerado equivalente ao da UE. A primeira característica é a *eficácia* do próprio sistema. A Comissão deve averiguar se os instrumentos jurídicos de proteção dos direitos do respeito pela vida privada e do tratamento de dados em vigor no país terceiro são capazes, na prática, de detetar, responsabilizar e punir de forma completa e real quaisquer infrações aos seus preceitos[18]. Em segundo lugar, só são permitidas interferências na esfera jurídica de proteção dos direitos fundamentais constantes dos art. 7.º e 8.º da CDFUE *de forma excecional*, ou seja, quando tiverem por fim a prossecução de um objetivo de interesse geral ou comum; quando estiverem definidas por regras claras e precisas; quando estabelecerem exigências mínimas de garantias de tratamento de dados; e, por fim, quando forem efetuadas na estreita medida do necessário e segundo um critério de proporcionalidade,

---

Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteçãoo e repressão de crimes graves", *O Direito*, Ano 147.º, IV, 2015, pp. 997-1046.

[15] TJ, C-362/14, ECLI:EU:C:2015:650, *Maximilian*, para.73, de 6 de outubro de 2015.

[16] *Idem*, para. 74.

[17] *Idem*, para. 78 sobre a discricionariedade da Comissão e do seu papel na fundamentação do critério de adequação, v. o artigo de Rodrigues de Oliveira, Ricardo. "'What's in a name? Uma breve análise do nível de proteção adequado no âmbito das transferências de dados pessoais dos cidadãos da UE para países terceiros" publicado no presente Anuário.

[18] TJ, C-362/14, ECLI:EU:C:2015:650, *Maximilian*, para.73, de 6 de outubro de 2015, para. 81.

tal como preconizado anteriormente no acórdão *Digital Rights*[19]. Por fim, a Comissão deve averiguar se existem meios de recurso judicial ao dispor do titular dos dados que lhe garantam *uma forma de reação efetiva* contra as empresas de tratamento. Como afirma o TJ, "uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, tal como é consagrado no art. 47.º [da CDFUE][20]".

Após ter desenvolvido estes três pontos o TJ passou à análise do sistema norte-americano de *Safe Harbor*. O tribunal não colocou, em abstrato, entraves ao facto deste quadro regulatório assentar num regime de auto-certificação[21]. No entanto, considerou que existiam dúvidas sobre a sua fiabilidade pelo facto dos princípios não se aplicarem às autoridades públicas norte-americanas[22] e da decisão da Comissão não apresentar "constatações suficientes" sobre a adequação do nível de proteção garantido pelo ordenamento jurídico norte-americano[23]. Em segundo lugar, o TJ entendeu que a "Decisão 2000/520 consagra o primado dos "requisitos de segurança nacional, interesse público ou [cumprimento da lei]", sendo que sempre que haja uma lei norte-americana sobre matéria de segurança que regule em sentido contrário aos princípios de *Safe Harbor* as empresas de tratamento devem obedecer-lhe em detrimento dos princípios[24]. Esta supremacia do

---

[19] *Idem*, para 91.

[20] *Idem*, para 95.

[21] *Idem*, para 81 quer isto dizer que o sistema norte-americano é baseado numa série de princípios que as empresas de tratamento de dados escolhem adotar e implementar por si mesmos e cujo compromisso é posteriormente comunicado a uma autoridade pública, de modo a poder beneficiar da liberdade transferência de dados ao abrigo. Sobre o sistema de proteção de dados norte-americano, v. Cole, David e Fabbrini, Federico. "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders", *iCourts Working Paper Series*, n.º 33, 2015, pp. 1-19; e Hasty, Robert; Nagel, Trevor W. e Subjally, Mariam. "Data Protection Law in the U.S.A", *Advocates for International Development,* 2013. Disponível em: <https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf> (acedido a 25/10/2017).

[22] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, para. 82, de 6 de outubro de 2015.

[23] *Idem*, para. 83.

[24] *Idem*, paras. 84 e 85.

princípio de segurança nacional face à proteção dos direitos fundamentais dos particulares é, na opinião do TJ, excessiva e desequilibrada, pois a decisão de adequação não apresenta "qualquer referência à existência, nos Estados Unidos, de normas de caráter estatal destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados pessoais sejam transferidos da União para os Estados Unidos, ingerências essas que as autoridades estatais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional[25]". Assim, existe o risco de as interferências, em vez de serem a exceção, poderem ser a regra. O facto de a regulamentação norte-americana autorizar não só a conservação da totalidade dos dados pessoais de forma indiscriminada e arbitrária[26] mas também o acesso de modo generalizado ao conteúdo de comunicações electrónicas[27] faz com que o TJ considere que não é respeitado o princípio de que as ingerências à esfera de proteção dos direitos fundamentais só podem operar na "estrita medida do necessário". Por fim, o tribunal entende que não existem mecanismos administrativos ou judiciais que permitam ao particular aceder aos seus dados e pedir a sua retificação ou supressão, o que viola o direito a uma tutela jurisdicional efetiva estabelecido no art. 47.º da CDFUE[28].

Em suma, o TJ conclui que a Comissão não apresentou de forma fundamentada informações de que os EUA, nos termos do art. 25.º n.º 6 da Diretiva, dispõem de um sistema de regulação que garanta um nível adequado e substancialmente equivalente ao nível que existe na UE. O tribunal não considera necessário olhar em concreto para o conteúdo dos princípios de *Safe Harbor,* visto que o art. 1.º da decisão de adequação não cumpre com os requisitos estabelecidos na Diretiva, interpretados à luz dos direitos fundamentais estabelecidos nos art. 7.º, 8.º e 47.º da CDFUE. Assim, o TJ considerou que o art. 1.º da decisão de adequação é inválido[29]. Finalmente, após análise crítica do art. 3.º da mesma decisão e da invalidade dos limites aí estabelecidos aos poderes das autoridades nacionais para conhecer

[25] *Idem*, para. 88.
[26] *Idem*, para. 93.
[27] *Idem*, para. 94.
[28] *Idem*, para. 95.
[29] *Idem*, para. 98.

de queixas particulares, o TJ acabou por declarar que toda a decisão era inválida face ao ordenamento jurídico da UE[30].

3. Os Princípios de *Privacy Shield*

3.1. Breve história dos princípios de Privacy Shield

Ao anular a decisão de adequação sobre os princípios de *Safe Harbor*, o TJ tornou mais premente a conclusão de um processo que se encontrava em marcha à data do acórdão *Schrems*.

Em 2013 a Comissão Europeia emitiu um comunicado anunciando as suas dúvidas face à efetividade do *Safe Harbor*[31]. Para a Comissão tornava-se necessário reexaminar o sistema não só à luz das alterações contextuais que se verificaram entretanto na sociedade económica, com o "aumento exponencial dos fluxos de dados" e sua importância no desenvolvimento do comércio digital e transatlântico, mas também face às questões sobre o "nível da proteção" efetivamente garantido[32]. As autoridades nacionais dos Estados-Membros da UE notavam que a adesão aos princípios não era muito seguida na práctica, e de que existiam dúvidas sobre qual o verdadeiro grau de interferência de entidades públicas dos EUA, como a NSA, na recolha e tratamento indiscriminado de dados por empresas americanas[33]. A Comissão identificou igualmente problemas na supervisão e aplicação coerciva dos princípios de *Safe Harbor* por parte dos reguladores americanos[34].

---

[30] *Idem*, paras. 105 e 106. Para uma visão mais abrangente das consequências do caso, v. Ojanen, Thomas. "Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union", *in*: David Cole *et al.* (ed.). *Surveillance, Privacy and Transatlantic Relations* Oxford: Hart Publishing, 2017, pp. 13-30.

[31] 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 UE", de 27 de novembro de 2013. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013DC0847&qid=1488287495250&from=PT> (acedido a 25/10/2017). Cabe dizer igualmente que muitos elementos desta comunicação são citados pelo TJ no acórdão *Schrems*.

[32] Comissão Europeia, "Comunicação...", cit, p. 3.

[33] *Idem*, pp. 5-8.

[34] *Idem*, pp. 11-15.

No fundo, a Comissão constatou que existiam graves deficiências práticas no sistema de *Safe Harbor* que permitiam o acesso indiscriminado e arbitrário a dados de cidadãos europeus por parte de autoridades americanas. Constatou-se ainda que as vias de recurso ao dispor dos titulares dos dados para contestar qualquer interferência abusiva contra os seus direitos eram limitadas[35]. A Comissão verificou igualmente que havia problemas de transparência quanto à utilização de derrogações aos princípios de Safe Harbor por parte de empresas americanas[36]. O órgão executivo máximo da UE concluiu deste modo que "o acesso em grande escala pelos serviços de informações a dados transferidos para os EUA por empresas certificadas participantes no sistema de 'porto seguro' levanta novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA[37]".

Perante este cenário a Comissão apresentou várias recomendações[38]. Primeiro, deve-se melhorar a transparência do sistema, ou seja, a exigência de publicação e comunicação por parte de empresas aderentes de todas as políticas de proteção de dados que têm em vigor e seu cumprimento efetivo com os princípios de proteção em vigor. Em segundo lugar, deve-se trabalhar a questão dos meios de reação judicial disponíveis. Entende-se por este ponto que deve procurar-se a instituição de um sistema mais acessível, menos oneroso e mais fiável ao dispor dos particulares para recorrer a mecanismos de resolução de litígios, quer sejam mecanismos de resolução alternativa de litígios ou outras formas. Em terceiro lugar, é necessário que haja maior aplicação de controlos regulatórios por parte das autoridades americanas, em particular quanto à supervisão efetiva de queixas dos particulares face a empresas que não cumpram com os princípios de proteção de dados em vigor. Por fim, e em quarto lugar, o acesso a dados por parte das autoridades norte-americanas ao abrigo das exceções acordadas como o princípio de segurança nacional só pode e deve ser efetuado de forma que respeite critérios de necessidade e proporcionalidade face ao respeito dos direitos de privacidade dos particulares.

---

[35] *Idem*, pp. 18 e 19.

[36] *Idem*, pp. 19 e 20.

[37] *Idem*, p. 20.

[38] *Idem*, pp. 20-22.

Iniciou-se posteriormente a esta comunicação um processo de melhoramento do *Safe Harbor* efetuado em conjunto pelas autoridades americanas e europeias. As negociações tiveram início em 2014, sendo aceleradas a partir de 2015 devido ao acórdão *Schrems*[39]. Apesar da urgência em atingir um acordo, dada à situação de incerteza provocada pela falta de uma decisão (incerteza que afetava negativamente todo o mercado económico de base digital e seus agentes), o processo enfrentou várias dificuldades. Chegou-se a pensar que as discussões poderiam estar irremediavelmente votadas ao fracasso[40]. No entanto, em fevereiro de 2016 a Comissão conseguiu apresentar um projeto de decisão de adequação, tendo por base a existência de um novo sistema para as empresas americanas, chamado *Privacy Shield*. Após consideração das opiniões do G29 onde se reúnem representantes das autoridades de controlo dos Estados-Membros, e da AEPD, a Comissão aprovou a nova decisão de adequação, que foi publicada a 1 de agosto de 2016, dez meses após o acórdão *Schrems*.

3.2. Forma, estrutura e conteúdo do Privacy Shield

O *Privacy Shield*, tal como o *Safe Harbo*r, é um sistema norte-americano de proteção de dados transferidos da UE para os Estados Unidos. A apresentação do sistema e dos seus princípios é acompanhada por uma série de declarações de entidades públicas norte-americanas. Quanto à decisão de adequação, é um ato normativo da UE, de carácter geral mas não legislativo, tomada pela Comissão ao abrigo de uma delegação de poderes consagrada no art. 25.º n.º 6 da Diretiva, permitida pelo art. 290.º TFUE.

A estrutura da Decisão *Privacy Shield* é semelhante à da decisão de adequação do *Safe Harbor.* A decisão contém uma lista de considerandos que versam sobre o contexto, descrição e justificação do ato jurídico, seguido

---

[39] Comissão Europeia, "Decisão de execução da Comissão número 2016/1250, 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", de 12 de julho de 2016, p. 3.

[40] Voss, Gregory W. "The Future of Transatlantic Data Flows: Privacy Shield or Bust", *Journal of Internet Law*, vol. 19, n.º 11, 2016, p. 11.

do conteúdo normativo da decisão *per se*, e de uma lista de anexos. O que difere a Decisão *Privacy Shield* da decisão de adequação do *Safe Harbor* neste aspeto estrutural é a sua extensão[41]. Justifica-se esta maior dimensão com duas situações provocadas pelo acórdão *Schrems*. A primeira tem que ver com a obrigação da Comissão justificar *fundadamente* a adequação do sistema. O TJ foi contundente no acórdão a estabelecer critérios normativos detalhados a que a Comissão deve obedecer para poder decidir se um sistema jurídico de um país terceiro garante ou não um nível de proteção substancialmente equivalente ao da UE. Em segundo lugar, era necessário que os EUA apresentassem maiores garantias, não só do ponto de vista regulatório (nível *micro* de proteção, *vis-à-vis* as empresas), mas também (e em particular) do ponto de vista dos poderes das autoridades nacionais de investigação e segurança (nível *macro* de proteção, *vis-à-vis* o Estado).

Quanto ao conteúdo, as grandes diferenças entre os princípios de *Privacy Shield* e os princípios de *Safe Harbor* verificam-se no maior desenvolvimento e precisão das normas e do aumento das obrigações para as empresas, de garantias de supervisão e de meios de recursos para os cidadãos europeus. O *Privacy Shield* procura assim não só responder às dúvidas da Comissão face as aparentes deficiências do *Safe Harbor*, mas também às críticas do TJ no acórdão *Schrems*, intenção declarada de forma explícita nos considerandos 4 a 13 da decisão.

Mantêm-se o sistema de autocertificação, pelo que cabe às empresas americanas apresentar às entidades reguladoras (DOC e FTC) a sua adesão aos princípios e o cumprimento efetivo dos mesmos. Mantêm-se igualmente os princípios do *Safe Harbor* – a saber: aviso, escolha, responsabilização pela transferência ulterior, segurança, integridade dos dados e limitação dos objetivos, acesso e recurso, aplicação e responsabilidade – embora mais trabalhados e desenvolvidos quanto ao alcance das obrigações para as empresas[42]. Destacam-se igualmente a existência de novas obrigações de informação das empresas perante os titulares de dados, relativamente não só às políticas de recolha e de tratamento, mas também aos meios de

---

[41] A decisão de adequação do *Safe Harbor* tinha 47 páginas, com 11 considerandos, 4 artigos e 7 anexos. A Decisão *Privacy Shield*, por seu turno, tem 112 páginas, com 155 considerandos, 6 artigos e 7 anexos.

[42] Comissão Europeia, "Decisão de execução...", Anexo II, pp. 48-52.

reação internos (dentro da estrutura da empresa) e externos (recurso a meios de resolução alternativa) que os particulares dispõem para poder aceder ou reagir contra o tratamento a que os seus dados estão sujeitos. Foi adicionada igualmente uma lista de princípios suplementares que estabelece novas obrigações e que complementam e consolidam os sete princípios iniciais[43], como por exemplo ao nível de proteção do tratamento de dados que se deve verificar em grupos de empresas, ou quanto à proteção a ter relativamente a situações sectoriais específicas (dados relativos a informação médica, laboral, jornalística, etc).

Destacam-se igualmente novos mecanismos de recurso, podendo o particular escolher reagir diretamente perante a empresa, uma autoridade de controlo nacional ou um organismo independente de resolução de litígios (que podem apresentar queixas ao DOC e à FTC), perante o recém-criado Comité do Escudo de Proteção da Privacidade (iniciando uma arbitragem vinculativa) e, por fim, através da reação para os tribunais norte-americanos[44]. A grande novidade foi a criação de um Mediador para receber queixas interpostas por autoridades de controlo nacionais da UE em nome de cidadãos particulares quanto à prática de serviços de espionagem pelos EUA[45]. Este Mediador fará parte da estrutura administrativa do Governo dos EUA, respondendo perante o Secretário de Estado.

Por fim, para além de renovadas declarações relativas à supervisão da aplicação dos princípios por parte de autoridades como o DOC, a FTC e o *Department of Transportation*[46], foi acrescentada uma carta do *Director of National Intelligence*, que explica e presta garantias quanto ao modo de recolha de dados para efeitos de segurança nacional, ao abrigo de regras proporcionais quanto ao nível de interferência nos direitos dos particulares, e os direitos e meios de reação dos particulares nessas situações[47].

---

[43] *Idem*, pp. 52-67.

[44] *Idem*, pp. 9-12.

[45] Comissão Europeia, "Decisão de execução...", Anexo III, pp. 71-77.

[46] Comissão Europeia, "Decisão de execução...", Anexos IV e V, pp. 78-90.

[47] Comissão Europeia, "Decisão de execução...", Anexo VI, pp. 91-108.

4. Os princípios de *Privacy Shield* face ao direito da União Europeia

4.1. A compatibilidade do Privacy Shield *face aos critérios do acórdão* Schrems

Na secção II analisámos o quadro normativo de normas fundamentais e secundárias que se aplicam à proteção de dados. Vimos que, fora certas exceções, a regra geral é a de que só podem ser autorizadas transferências de dados para países terceiros desde que tais países disponham de um nível de proteção adequado. Deve entender-se por adequado, segundo o TJ, que o país terceiro em causa garanta um *quadro de proteção substancialmente equivalente* ao da UE. Esta avaliação sobre a adequação deve ser efetuada tendo em conta não só as normas abstratas aplicáveis mas, principalmente, a sua efetivação prática. O TJ considerou ainda que para um sistema jurídico garantir um nível de proteção substancialmente equivalente ao da UE deve preencher três critérios. Em primeiro lugar, o sistema deve ser eficaz, ou seja, estabelecer um nível de coerção suficiente que obrigue os seus aderentes à sua observação estrita. Em segundo lugar, o sistema deve ter como objetivo principal a proteção dos direitos de privacidade dos titulares de dados, sendo qualquer derrogação a este princípio excecional e exercida segundo requisitos de necessidade e de proporcionalidade. Em terceiro lugar, o sistema deve estabelecer meios judiciais de reação ao dispor dos titulares contra possíveis violações dos seus direitos.

Vimos igualmente que o TJ considerou no acórdão *Schrems* que estes critérios não estavam a ser preenchidos pois existiam demasiadas derrogações possíveis face a uma primazia do princípio de segurança nacional. Além do mais, o TJ entendeu que não existiam garantias jurídicas suficientes que impedissem uma recolha e um tratamento generalizado de dados. Desta forma, tal tratamento não obedecia a critérios de estrita proporcionalidade e necessidade. O TJ também considerou que os particulares não tinham direito, na prática, a uma tutela jurídica efetiva face a estas interferências de autoridades públicas. Assim, parece que a questão que mais preocupa o TJ não é tanto o tratamento *per se* de dados por empresas privadas, mas sim o seu tratamento pelas autoridades públicas norte-americanas, em especial as agências de informação e de segurança nacional. Também vimos que previamente ao acórdão *Schrems* existiu uma comunicação da Comissão Europeia que identificou deficiências no *Safe Harbor* e apresentou

recomendações. No entanto, a possibilidade de acesso a dados por parte de entidades públicas americanas não era alvo de tanto destaque como no julgamento do TJ. As principais preocupações da Comissão tinham que ver mais com a adesão de empresas ao regime de *Safe Harbor* e com a efetiva supervisão das autoridades norte-americanos quanto ao cumprimento desses princípios e aos meios de reação ao dispor dos particulares.

Na nossa análise geral ao sistema de *Privacy Shield* vimos que foram introduzidos novos princípios e obrigações para as empresas, em especial quanto às questões de transparência e de recurso[48]. Neste sentido, parece que as preocupações da Comissão, face ao nível de proteção *micro* (perante as empresas) foram salvaguardas. Cabe-nos no entanto verificar se as preocupações do TJ, quanto ao nível de proteção *macro* (perante o Estado), e essas sim decisivas quanto à interpretação a dar às normas da Diretiva sobre os limites do juízo de adequação, foram ou não objeto de resposta no *Privacy Shield*.

Comecemos por verificar o primeiro critério, relativo à eficácia. O *Privacy Shield* estabelece em várias disposições o compromisso das autoridades regulatórias norte-americanas, mormente o DOC, de supervisionar de forma estrita o cumprimento dos princípios e obrigações das empresas[49]. No entanto, nenhum destes compromissos refere qualquer poder efetivo destas entidades regulatórias face a possíveis interferências de outras entidades públicas, em particular de índole militar ou informativa. É verdade que se verifica um esforço na Decisão *Privacy Shield* de fundamentar de forma desenvolvida e aprofundada as capacidades do ordenamento jurídico norte-americano de regular eficazmente a aplicação dos novos princípios. É preciso relembrar, no entanto, que o sistema norte-americano continua assente na autocertificação, pelo que cabe ainda às empresas aderir e adotar políticas

---

[48] Para uma análise mais extensa do Privacy Shield, v. Monteleone, Shara e Puccio, Laura. "From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules, *European Parliament Research Service*, 2017, pp. 1-36.

V. igualmente a contribuição de 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?" e, em particular, pela análise crítica do valor normativo do *Privacy Shield*, de Rodrigues de Oliveira, Ricardo. "What's in a name? Uma breve análise do nível de protecção adequado no âmbito das transferências de dados pessoais dos cidadãos da UE para países terceiros", publicado neste Anuário.

[49] Comissão Europeia, "Decisão de execução...", pp. 40-44.

de proteção de dados, sem interferências das autoridades reguladoras. Ou seja, só será possível verificar o critério da eficácia em concreto após a entrada em vigor do sistema. Assim, apesar de existirem declarações de que existirá uma supervisão e aplicação mais eficaz do *Privacy Shield* do que houve do *Safe Harbor*, essas não passam de meras expressões de intenções de conduta. Neste sentido, coloca-se a dúvida sobre se a preocupação expressa pelo TJ no acórdão *Schrems* quanto à existência de um sistema de proteção eficaz estará completamente resolvida. Tal preocupação, parece-nos, só poderá ser resolvida através de uma análise concreta dessa supervisão, na prática.

Passemos para o segundo critério. O *Privacy Shield* continua a manter *ipsis verbis* as derrogações aos seus princípios para fins de segurança nacional. Assim, a adesão aos mesmos:

> [P]ode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal, b) por legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas, desde que, no exercício de tal autorização, uma organização possa demonstrar que o seu incumprimento dos princípios se limita ao necessário para respeitar os legítimos interesses superiores avançados por essa autorização, ou c) por exceção ou derrogação prevista na diretiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas exceções ou derrogações ocorra em contextos comparáveis[50].

A questão continua a colocar-se quanto ao carácter excecional destas derrogações e da necessidade e proporcionalidade na sua aplicação. Há um esforço grande no *Privacy Shield*, particularmente expresso no anexo VI na carta do *Director of National Intelligence*, para descrever e informar sobre todos os direitos e regras dos titulares de dados tratados pelas agências de investigação, bem como sobre os meios de fiscalização política de tal atividade e da proporcionalidade dos mecanismos utilizados. A Comissão vem acrescentar que considera que desde 2013 este quadro jurídico de "proteção eficaz de dados contra a ingerência ilegal e o risco de abuso" foi bastante reforçado[51]. Este reforço verifica-se, na opinião da Comissão, com a aprovação da PPD-28 de 2014, que estabelece vários deveres que os

[50] *Idem*, p. 49.
[51] *Idem*, p. 13.

serviços de informação americanos devem cumprir quando tratam dados[52]. Chama-se igualmente a atenção para o facto de ter sido aprovado o *USA Freedom Act* em 2015, que veio alterar legislação sobre segurança nacional e combate ao terrorismo (*Patriot Act* e o FISA) no que respeita à eliminação da recolha massificada de dados.

Apesar destes esforços, mantém-se ainda a dúvida sobre se estes compromissos são suficientes ou não para satisfazer os critérios normativos estabelecidos pelo TJ. Existem três elementos que continuam a suscitar preocupações. O primeiro tem que ver com a recolha de informação de forma generalizada. Diz a Comissão que ao abrigo da legislação norte-americana "as informações de origem eletromagnética podem ser recolhidas exclusivamente nos casos em que exista um objetivo de espionagem externa ou de contra-espionagem ou para apoiar missões nacionais e departamentais[53]", e não para qualquer outro fim. Nesse âmbito, os serviços de informação "devem [ao abrigo da PPD-28], por vezes recolher informação de origem eletromagnética em larga escala em determinadas circunstâncias, por exemplo, para identificar e avaliar ameaças novas ou emergentes", embora tenham de dar prioridade a métodos alternativos de recolha seletiva[54]. A recolha alargada só pode ser efetuada por falta de meios técnicos ou operacionais que impeçam a recolha individualizada. Ora tal descrição da PPD-28 não parece estabelecer, de forma clara, certa e precisa, que a recolha generalizada de dados só será utilizada em casos altamente excecionais. Os serviços de informação devem dar prioridade a meios menos lesivos, mas isso não exclui a possibilidade de, em certos casos (cuja excecionalidade assenta somente em meios técnicos) poderem recorrer à recolha dados de forma massificada e generalizada. A legislação americana (quer o FISA, o programa *PRISM* e o *American Freedom Act*) também não é clara quanto aos limites e alcance dos poderes das autoridades americanas neste ponto.

O segundo elemento tem que ver com a questão do período de retenção de dados. Segundo as declarações que compõem o Privacy Shield, é possível que os serviços de informação possam reter os dados por um período máximo de cinco anos, sem qualquer aparente motivo[55]. Ora, isto vai contra aquilo

---

[52] *Idem*, p. 14.

[53] *Ibidem*.

[54] *Idem*, p. 15.

[55] *Idem*, p. 19.

que é considerado como sendo proporcional pelo TJ. Segundo a opinião do douto tribunal no acórdão *Digital Rights*, a retenção de dados por um período largo tem de obedecer a um "critério objetivo por modo a assegurar que está limitado ao que é estritamente necessário[56]". No entanto, não há qualquer menção na Decisão *Privacy Shield* a critérios que justifiquem a retenção por tal período de tempo. Assim, falta claridade e precisão numa matéria de especial importância. A Comissão considera que "esta prática [dos EUA] está conforme à norma fixada pelo Tribunal de Justiça no acórdão *Schrems*, segundo o qual uma legislação que envolva uma ingerência nos direitos fundamentais garantidos pelos art. 7.º e 8.º da Carta deve impor 'um mínimo de exigências". Mas temos dúvidas que assim seja, visto que ainda existe um elevado grau de dúvida e de imprecisão relativamente às possibilidades de interferência dos serviços secretos norte-americanos nos direitos dos particulares, em particular quanto à recolha generalizada de dados, o seu tratamento e acesso e à sua preservação. Aliás, apesar da abertura e disponibilidade para maiores explicações, a importância detalhada de questões relacionadas com atividades de serviços de informação no *Privacy Shield* parece indicar o quão importante é este princípio para os norte-americanos. Tal é que a AEPD vem, no seu parecer, questionar se a centralização deste princípio de segurança nacional na Decisão *Privacy Shield* não vem antes "legitimar a rotina" de recolha e de investigação, mesmo que estabeleça alguns limites à atividades de investigação e recolha de dados[57]. Ou seja, coloca-se a questão de saber se a exceção de segurança nacional não se torna, no *Privacy Shield*, na regra, e a proteção de direitos de privacidade na exceção, a contrário daquilo que é prescrito no acórdão *Schrems*.

O terceiro e último elemento tem que ver com o problema da tutela judicial efetiva. Os princípios de *Privacy Shield* estabelecem uma série de mecanismos de recurso ao dispor dos particulares. No entanto, todos estes mecanismos, exceto o último de acesso aos tribunais nacionais norte-americanos, dizem respeito à reação contra o tratamento de dados por empresas aderentes ao *Privacy Shield* e preconizam como meio principal a arbitragem. Como refere a AEPD, não há a possibilidade de intentar uma ação em solo europeu, o que garantiria uma tutela judicial dos particulares

---

[56] Casos C-293/12 e C-594/12, *Digital Rights Ireland*, paras. 63 e 64.

[57] Autoridade Europeia para a Proteção de Dados, "Opinion 4/2016...", cit., p. 7.

mais efetiva[58]. Mas mais problemático é o facto, mais uma vez, do sistema norte-americano não conter nenhum mecanismo claro e preciso ao dispor dos particulares para reagir contra o possível acesso aos dados por parte de autoridades públicas norte-americanas. Como diz a AEPD, "parecem existir vários instrumentos de recurso no direito norte-americano mas nenhum cobre de forma adequada todas as instâncias em que o governo pode aceder a dados pessoais[59]". Parece-nos que neste caso cabe aos particulares utilizar uma de duas vias: ou os tribunais norte-americanos, ou recorrer ao Mediador de proteção de dados, estabelecido ao abrigo do Anexo (III) da Decisão *Privacy Shield*. Mas esta situação também é problemática. Por um lado, a utilização de tribunais nacionais norte-americanos implica um custo para os cidadãos europeus que pode ser incomportável, dado o facto de se terem de deslocar e contratar serviços jurídicos para conseguir reagir num sistema forense bastante diferente do europeu. Por outro lado, o mediador é uma entidade que se encontra dentro da estrutura administrativa da Secretaria de Estado norte-americana. Ou seja, é nomeado pelo Secretário de Estado, que é um órgão executivo e que tem competência para tratar da política externa dos EUA. Não parece que estejam assim preenchidos os mínimos requisitos de independência e imparcialidade do Mediador face ao poder executivo norte-americano, ao qual pertencem as agências de informação. É um mecanismo meramente administrativo, que precisaria de mais desenvolvimentos para garantir a eficaz tutela judicial dos particulares de forma equivalente ao prescrito no art. 47.º da CDFUE[60].

4.2. O problema da avaliação efetiva do Privacy Shield

A análise anterior sobre o sistema de *Privacy Shield* centrou-se em normas jurídicas e sua consideração em abstrato. No entanto, como vimos no acórdão *Schrems*, a decisão de adequação tem de ter em conta um critério de eficácia, que considera em especial a execução e aplicação prática do sistema de proteção de dados pessoais do país terceiro. Este juízo é mais

---

[58] *Idem*.

[59] *Ibidem* (tradução do autor).

[60] *Idem*, "Opinion 4/2016...", p. 8; G29, "Opinion 01/2016", cit., p. 57.

complicado de fazer de momento, do ponto de vista científico, pois não existem ainda dados suficientes sobre a aplicação do *Privacy Shield* durante o seu curto período de vigência. Um juízo sobre a eficácia do sistema feito neste momento será necessariamente uma prognose, baseada simplesmente nos diplomas normativos e numa análise contextual e histórica sobre qual poderá ser a verdadeira capacidade de execução destas normas. No entanto, estamos em crer que quer os dados disponíveis por via da decisão de adequação e do contexto jurídico-político atual (e neste sentido, devido a algumas ações concretas do Governo norte-americano) proporcionam algumas informações para conseguir projetar pelo menos alguns desafios à execução do sistema, com uma margem suficientemente legítima de dúvida que pode ter efeitos importantes na capacidade de sucesso do *Privacy Shield*.

A decisão de adequação da Comissão considera que os EUA oferecem um sistema de proteção substancialmente equivalente com base numa análise do seu sistema jurídico de proteção de dados. Esta análise é fundamentada não só por referência a legislação americana e outros atos normativos de cariz executivo-administrativo, como a PPD-28, mas igualmente devido às comunicações em anexo dos diretores das entidades públicas norte-americanas. 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[61]. 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.

Estas declarações pertencem a órgãos executivos que seguiam uma determinada estratégia política definida por uma administração norte-americana liderada por um membro do Partido Democrata, Barack Obama. O programa e agenda política deste Presidente evidenciava uma postura

[61] *Idem*, p. 7.

pró-globalização, aberta à cooperação internacional e económica. Cerca de três meses após a aprovação da Decisão *Privacy Shield* houve eleições nos EUA, sendo o vencedor das eleições um candidato do Partido Republicano, Donald Trump. Enquanto candidato o Presidente Trump defendeu posições políticas completamente contrárias às do seu antecessor Barack Obama, advogando um maior protecionismo económico, uma visão mais nacionalista e anti-globalização. Neste sentido, tem procurado tomar medidas para combater a entrada de cidadãos estrangeiros nos EUA, medidas essas que levantam muitas dúvidas quanto a possíveis discriminações religiosas ou étnicas[62]. Apesar de tais tentativas terem sido bloqueadas pelos tribunais[63], não é seguro que a atividade das agências de informação para recolher dados de imigrantes e cidadãos estrangeiros não aumente com esta nova postura protecionista da administração Trump. Ao mesmo tempo têm sido preparadas medidas pelo Congresso norte-americano para eliminar regulação de práticas comerciais privadas, com importantes incidências nos direitos de proteção de dados dos cidadãos[64]. Coloca-se desta forma a dúvida de saber se as declarações de *Privacy Shield* serão ou não cumpridas na prática pelas autoridades norte-americanas.

Conclusão

Os requisitos estabelecidos pelo TJ no acórdão *Schrems* sobre qual o entendimento jurídico a dar ao conceito de "nível de proteção adequado" acabam por delimitar a adoção de decisões de adequação sobre países que não garantam, na prática, a proteção dos direitos dos particulares da

---

[62] Presidente dos Estados Unidos da América, "Executive Order Protecting The Nation From Foreign Terrorist Entry Into The United States. Disponível em: <https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states> (acedido a 25/10/2017).

[63] *BBC*, "Trump travel ban: Hawaii judge places indefinite hold", de 30 de março de 2017. Disponível em: <http://www.bbc.com/news/world-us-canada-39439595> (acedido a 25/10/2017).

[64] *The Independent*, "US Senate votes to allow sale of people's browsing history without consent", de 23 de março de 2017. Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/us-senate-internet-privacy-bill-vote-sell-consumer-data-browsing-history-a7646981.html> (acedido a 25/10/ 2017).

mesma forma que na UE[65]. A Decisão de *Privacy Shield* procura demonstrar que o novo sistema de princípios acordado com os EUA preenche todos os critérios e que se trata de uma proteção substancialmente equivalente à que os particulares gozam na UE. Existe, de facto, uma nova precisão e desenvolvimento quer ao nível dos princípios que as empresas devem seguir, quer ao nível dos controlos que as entidades de supervisão vão exercer. No entanto, existem elementos importantes da Decisão de *Privacy Shield* que continuam a ser problemáticos e a conflituar com o entendimento do TJ em *Schrems* e, assim, com o direito da UE. Ainda se estabelece um primado do princípio de segurança nacional face ao primado do respeito pela intimidade privada, ainda existe a possibilidade de recolha generalizada de dados, e não existem ainda mecanismos de reação suficientemente adequados ao dispor dos particulares perante interferências estatais. Parece-nos, deste modo, que a Decisão de *Privacy Shield*, mais do que cumprir com os requisitos delineados no acórdão *Schrems* procura resolver as questões levantadas pela Comissão na sua Comunicação.

Cabe aqui dizer que o problema do juízo de compatibilidade do *Privacy Shield* com o direito da União (já) não é apenas uma questão a ter em conta em abstrato. Isto porque em setembro e outubro de 2016 foram intentadas duas ações de anulação junto do TG para avaliar da validade do sistema face ao direito da União Europeia[66]. A primeira ação foi apresentada pela organização não-governamental Digital Rights Ireland[67], e a segunda pela

---

[65] Há quem questione não só a interpretação do TJ mas também as consequências da mesma. v. a discussão entre Richard Epstein e Martin Scheinin na European Constitutional Law Review. Epstein, Richard A. "The ECJ's Fatal Imbalance Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sound Commercial Practices" e Scheinin, Martin. "Towards Evidence-Based Discussion on Surveillance: A Rejoinder to Richard A. Epstein", *European Constitutional Law Review,* vol. 12, n.º 2, 2016, pp. 330-348.

[66] *Politico*, "Privacy shield data agreement challenged before EU court", de 27 de outubro de 2016. Disponível em: <http://www.politico.eu/article/privacy-shield-data-agreement--challenged-before-ecj/> (acedido a 24/04/2017); EurActiv, "EU-US Privacy Shield pact faces second legal challenge", de 3 de novembro de 2016. Disponível em: <http://www.euractiv.com/section/digital/news/eu-us-privacy-shield-pact-faces-second-legal-challenge/> (acedido a 25/10/2017).

[67] Recurso interposto em 16 de setembro de 2016 – Digital Rights Ireland/Comissão, Processo T-670/16. A acção foi julgada inadmissível pelo TJ a 22 de novembro de 2017. V. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=19714

organização não-governamental La Quadrature du Net[68]. Acrescente-se a isto os desenvolvimentos que a aplicação de políticas aguerridas de segurança nacional e de desregularização de proteções de utilizadores de dados por parte da Administração Trump e é difícil de prever o futuro do *Privacy Shield* para lá de uma grande nuvem de incerteza, apesar de ser o sistema que está atualmente em prática[69].

O problema de uma regulação transfronteiriça de proteção de dados é tentar satisfazer quatro preocupações. Por um lado, é preciso salvaguardar as liberdades económicas e de desenvolvimento empresarial, mas garantindo um nível de proteção adequado para os direitos de intimidade privada dos particulares, bem como uma proteção da segurança nacional e, com tudo isto, manter boas relações diplomáticas e comerciais com países terceiros, em especial com grandes potências internacionais que partilham na sua base constitucional e democrática o compromisso liberal e cosmopolita de proteção dos direitos fundamentais[70]. Resolver esta quadratura do círculo é o grande desafio desta área, ao qual o *Privacy Shield*, perante o entendimento do TJ sobre a primazia dos direitos individuais face aos outros interesses, parece não conseguir dar resposta.

1&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=812481> (acedido a 20/12/2017).

[68] Recurso interposto em 25 de outubro de 2016 – La Quadrature du Net e o./Comissão, Processo T-738/16.

[69] Apesar da incerteza, o Privacy Shield passou na primeira revisão anual efetuada pela Comissão. v. Directorate General of Justice and Consumers, "First Annual Review of the EU-U.S. Privacy Shield". Disponível em: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> (acedido a 25/10/2017). No entanto, apesar do relatório ser favorável e à melhor supervisão por parte das autoridades regulatórias, foram identificadas situações que precisam de maior definição, relativamente a procedimentos internos de investigação e vigilância. O facto de não ter sido ainda nomeado um Mediador foi igualmente considerado problemático. A Comissão disse que continuaria a analisar de perto a situação. v. Comissão Europeia"Report From the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield". Disponível em: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> (acedido a 25/10/2017).

[70] Sobre este ponto, v. Lucas Pires, Martinho, "The shortcomings of the EU framework for transnational data transfers and the need for an internationalist approach", LUISS School of Governance Working Paper Series 43/2017. Disponível em: <http://sog.luiss.it/sites/sog.luiss.it/files/SOG%20Working%20Papers%20WP43%20-%202017%20Pires_0.pdf>. (acedido a 20/12/2017).

What´s in a Name?
Uma Breve Análise do Nível de Protecção Adequado no Âmbito das Transferências de Dados Pessoais dos Cidadãos da União Europeia para Países Terceiros

Ricardo Rodrigues de Oliveira*

Resumo: O presente texto pretende questionar o efeito útil aparentemente decorrente do desenvolvimento pelo legislador europeu das cláusulas relativas ao nível de protecção para as transferências de dados pessoais de cidadãos da União Europeia para países terceiros. A Directiva 95/46/CE foi substituída pelo Regulamento (UE) 2016/679, assim se mudando, em parte, o paradigma anterior, visto que este é mais desenvolvido no que respeita aos critérios para a tomada de decisões pela Comissão. No entanto, deveria era ter sido modificada a política de negociações, especialmente com os EUA, para garantir uma protecção efectiva, tanto *de iure* como de facto.

Palavras-chave: *Directiva 95/46/CE; Nível de Protecção Adequado; Regulamento (UE) 2016/679; Schrems.*

Abstract: The present text aims at questioning the 'effet utile' apparently resulting from the development by the European legislator of the clauses relative to the level of protection for the transference of EU citizens' personal data to third countries. The Directive 95/46/EC was replaced by the Regulation (EU) 2016/679, thus partially changing the previous paradigm, as the latter is more developed regarding the decision-making criteria by the Commission. However, the negotiating policy is what should have been modified, especially with the USA, to guarantee an effective protection, both de iure as de facto.

Keyword: *Adequate Level of Protection; Directive 95/46/EC; Regulation (EU) 2016/679; Schrems.*

---

* Doutorando no Instituto Universitário Europeu (EUI), Investigador do Centro de Investigação em Direito Público da Faculdade de Direito da Universidade de Lisboa (FDUL) e Investigador da Jurisnova da Faculdade de Direito da Universidade Nova de Lisboa (FDUNL).

Introdução

A relação dos cidadãos e dos poderes públicos com a transferência e processamento de dados pessoais, bem como a sua protecção, está a mudar rapidamente no mundo electronicamente globalizado dos tempos contemporâneos. São cada vez mais os estudos[1] e a literatura que atestam as diferentes exigências que rodeiam as deslocações de informação dos cidadãos, tanto intra como inter-jurisdições. Eles revelam uma tensão crescente entre os direitos à privacidade e à intimidade[2] e as potenciais utilizações que a compilação de dados em grandes quantidades oferece.

Desde a criação mais básica de perfis comerciais até ao complexo entrecruzamento de dados de geolocalização para efeitos de investigação criminal ou de contra-terrorismo, há uma rede global de entidades e plataformas, privadas, públicas e sob regimes mistos de cooperação e interoperabilidade, que gerem bases de dados com dimensões, as mais das vezes, verdadeiramente *orwellianas*. A nível europeu, as instituições, com a Comissão à cabeça, têm vindo a desempenhar um papel cada vez mais activo, em conjunto com os Estados-Membros, na cumplicidade administrativa de, por um lado, recorrer à compilação massiva de dados que permitem identificar os indivíduos e localizá-los geográfica e temporalmente, para os mais diversos fins, e, por outro, tentar limitar a disseminação, acesso e consequente usos abusivos destes elementos.

A situação torna-se mais melindrosa quando os dados correm o risco de serem vertidos para meios de comunicação e espaços de armazenamento que não garantem uma isenção e garantias de protecção contra utilizações distintas daquelas consentidas originalmente pelos titulares dos dados. Com as aberturas permitidas pela internet das coisas, a certeza e segurança jurídicas do resguardo das informações só podem ser mantidas em condições relativamente estritas. Nomeadamente, com as garantias de que os controladores e administradores de sistemas não as libertem; de que não

---

[1] V. a título ilustrativo, a página electrónica da Comissão Europeia sobre os estudos mais recentes relativos à protecção de dados, bem como os diversos documentos e ligações acessíveis a partir desta plataforma. Disponível em: <http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm> (acedido a 29/07/2017).

[2] V. Herrán Ortiz, Ana. "El derecho a la protección de datos personales en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, n.º 26, 2003, pp. 9-92.

haja entidades a imiscuir livremente nas bases de dados, mesmo se forem autoridades públicas; e de que existam meios processuais ao alcance dos particulares para defesa dos seus interesses, direitos e liberdades, a par de um conjunto efectivo de sanções.

O tema desta investigação recai, precisamente, sobre um aspecto da actualidade da transmissão de dados no âmbito das relações externas da UE. Desde 1995, que o legislador europeu tem baseado a transferência de dados dos cidadãos do espaço eurocomunitário para o exterior em decisões de adequação, a determinar pela Comissão em cooperação com os Estados-Membros. Mediante negociações bilaterais, a instituição tem vindo a declarar que determinadas jurisdições externas apresentam garantias suficientes nos seus ordenamentos para que sejam consideradas como destinos 'seguros', facilitando o desenvolvimento das relações comerciais.

O presente trabalho é uma excursão simplificada pelo conceito de nível de protecção adequado na legislação eurocomunitária relativamente às transferências transnacionais de dados pessoais, *i.e.*, envio de informações dos cidadãos da União para bases de dados localizadas em países terceiros. O objectivo que subjaz é evidenciar a falta de proposição normativa a definir o conceito na evolução legislativa, deixando em aberto potenciais conclusões a este respeito, e, de outro tanto, demonstrar a prática negocial da Comissão nos acordos "porto seguro" e "escudo de protecção" estabelecidos com os EUA quanto a este assunto.

A inexistência de um conceito formalizado e alguma 'nebulosidade' dos trechos legais poderão explicar, em parte, a insuficiente investigação que a instituição insiste em levar a cabo de cada vez que dialoga com os EUA, preferindo confiar, sem exercício de eficaz ou notório contraditório, nas cartas e declarações de princípios que representantes institucionais de alguns sectores de actividade enviam para a Europa. A escolha deste exemplo deve-se a um conjunto de razões, como a importância norte-americana nas relações políticas, comerciais e económicas europeias com o exterior; a maior publicidade dos documentos negociais; a especificidade dos acordos UE-EUA por oposição aos demais países; e a toda a celeuma decorrente do caso *Wikileaks*.

Aparte esta introdução e as notas conclusivas, o artigo está dividido em 4 secções. A primeira e a terceira, mais breves, dão conta dos enunciados legais de 1995 e de 2016, focando-se na consagração do conceito de nível de protecção adequado, muito embora somente o primeiro informe

actualmente os procedimentos de adequação. A segunda e a quarta, mais extensas, debruçam-se sobre a insuficiente atenção executiva dada ao conceito, quer na primeira decisão de adequação da Comissão, designada por "porto seguro", e no desenvolvimento posterior no caso *Schrems*, quer na segunda decisão, mais recente e aprovada no âmbito da renovação legislativa europeia em matéria de protecção de dados, designada por "escudo de protecção de privacidade".

1. A Directiva 95/46/CE

A Directiva 95/46/CE de 24 de Outubro de 1995[3] criou, pela primeira vez, um regime relativo à transferência de dados pessoais dos cidadãos das Comunidades Europeias para países terceiros. Nos termos do n.º 1 do art. 25.º, os Estados-Membros deveriam cuidar que as transferências só fossem concretizadas para países que assegurassem um nível de protecção adequado relativamente ao tratamento e manutenção destas informações.

O legislador europeu não definiu o que deveria ser entendido por este patamar de adequação em 1995[4-5], tal como não o vai fazer em 2016. Apenas

---

[3] Directiva 95/46/CE 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 281/31, 23.11.1995). Tal como o actual pacote legislativo relativo à protecção de dados, a Directiva demorou algum tempo a ser elaborada e aprovada pelo seu cariz inovador e pela complexidade técnica. Este documento resulta de uma proposta da Comissão apresentada a 27 de Julho de 1990 e que depois foi adaptada pelo Conselho (COM (90) 314 final — SYN 287, 90/C 277/03), e alterada subsequentemente (92/C 311/04, 27.11.1992).

[4] Sendo que tal vai gerar diferentes preocupações de ambos os lados do Atlântico quanto ao que poderá significar, visto que os EUA nunca acabaram por importar verdadeiramente o conceito, segundo Estadella-Yuste, Olga. *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid: Tecnos, 1995, p. 117. Para uma perspectiva norte-americana do problema da EU como uma *norm-giver* que pode cair na tentação da 'estandardização' das normas aplicáveis fora do seu território, v. Goldsmith, Jack e Wu, Tim. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press, 2006, pp. 173 e ss.

[5] Aliás, Herrán Ortiz, Ana. "El derecho a la protección de datos personales en la sociedad de la información", cit., p. 40, reflecte, ironicamente, que mais parece que se deve estabelecer qual o nível desadequado para se saber mais facilmente se o país terceiro oferece garantias suficientes para a transmissão de dados. Aquele seria o patamar abaixo do qual

referiu os critérios segundo os quais o nível de protecção teria de ser apreciado. Segundo o n.º 2, deveriam ser tidas em conta todas as circunstâncias relativas às transferências, singular ou colectivamente consideradas, nomeadamente "a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país".

Esta situação de indefinição do conceito levou a que o trecho fosse criticado por ambíguo[6] e por se assemelhar a outras disposições legais[7], criando alguma incerteza jurídica. Donde, não parece ser de partilhar a 'leveza' com que certa doutrina encara a regra como um conceito jurídico indeterminado, uma norma em branco, que, pela sua flexibilidade, se ajusta excepcionalmente bem ao colorido de situações às quais se aplica o seu modelo de estandardização[8].

À luz do n.º 6 do art. 25.º desta Directiva, caberia à Comissão constatar, segundo o procedimento de comitologia previsto nos termos do n.º 2 do art. 31.º, que países assegurariam esse tal *standard* de protecção adequado, tanto pela primeira vez como no caso de algum país que tivesse deixado de assegurar este limiar e a 'confiança' tivesse que ser reposta após negociações com os decisores europeus. A instituição apreciava, com base neste amplo critério e de forma casuística[9], como o vai fazer em 2016, a presença dos

---

ainda se produziriam efeitos negativos para os interessados quanto à protecção dos seus dados pessoais.

[6] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, n.º XXXVI, 2011, p. 335.

[7] Como, por exemplo, a expressão "protecção equivalente" da alínea a) do n.º 3 do art. 12.º da Convenção 108 do Conselho da Europa, de 28 de Janeiro de 1981, para a protecção dos indivíduos relativamente ao tratamento automatizado dos dados de carácter pessoal, ou a locução "garantias comparáveis" da Organização das Nações Unidas, *Guidelines for the Regulation of Computerized Personal Data Files*, A/RES/45/95, de 14 de Dezembro de 1990 (68.ª sessão plenária), para. 9.

[8] Heredero Higueras, Manuel. *La Directiva comunitaria de protección de datos de carácter personal*. Madrid: Aranzadi, 1997, p. 188.

[9] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", cit., p. 336.

mencionados critérios "em virtude da sua legislação interna ou dos seus compromissos internacionais", sempre no sentido de acautelar a protecção do direito à vida privada e dos direitos e liberdades fundamentais dos cidadãos[10].

Foram muito poucos (e, na maioria dos casos, pouco relevantes) os países a gozar de uma decisão de adequação. Contam-se Andorra[11], a Argentina[12], o Canadá (mas somente no que respeita as suas organizações comerciais)[13], as Ilhas Faroé[14], Guernsey[15], Israel[16], a Ilha de

---

[10] Importa mencionar que alguns documentos não legislativos ajudaram a compreender a leitura que deveria ser feita do nível de adequação pela falta de definição expressa. Através da flexibilização dos critérios interpretativos, tem sido possível, no entender de algumas entidades, contornar a inexistência de uma consagração cristalizada do conceito e adaptar as normas europeias às realidades externas para se determinar, como mencionado, de forma *ad hoc*, se dado país assegura o referido nível. Entre alguns destes textos, contam-se: *G29, First orientations on transfers of personal data to third countries – Possible ways forward in assessing adequacy*, XV D/5020/97-EN final WP4, de 26 de Junho de 1997. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf> (acedido a 3/12/2017), ou G29, *Working document. Transfers of personal data to third countries: Applying articles 25 and 26 of the EU Data Protection Directive*, DG XV D/5025/98 WP 12, de 24 de Julho de 1998. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf> (acedido a 7/12/2017).

[11] 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 de dados pessoais em Andorra (JO L 277, 21.10.2010).

[12] 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 de dados pessoais na Argentina (JO L 168, 05.7.2003).

[13] 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, 4.1.2002).

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

[15] Decisão da Comissão de 21 de Novembro de 2003 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais em Guernsey (JO L 308, 25.11.2003).

[16] 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, 1.2.2011).

Man[17], Jersey[18], a Nova Zelândia[19], a Suíça[20] e o Uruguai[21]. Nas diversas decisões, o legislador comunitário apenas decidia que a jurisdição assegurava um nível de protecção adequado, sem explorar o conceito.

2. A Decisão 2000/520/CE e o caso *Schrems*

Para além destes países, também os EUA gozaram de uma decisão a considerar o país como adequado para receber os dados pessoais dos cidadãos das Comunidades, embora através de um sistema algo diferente dos demais[22]. Pela sua importância económica e capacidade de diálogo político, os EUA conseguiram uma posição negocial de vantagem, baseada em compromissos, princípios gerais e questões mais frequentes[23]. É, sem dúvida, o país sobre cujos documentos de negociação mais se conhece publicamente, mas, precisamente por isso, é também a chave para compreender como é

---

[17] 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, 30.4.2003).

[18] 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, 28.5.2008).

[19] Decisão da Comissão de 19 de Dezembro de 2012 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pela Nova Zelândia (JO L 28, 30.1.2013).

[20] 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, 25.8.2000).

[21] Decisão de execução da Comissão de 21 de Agosto de 2012 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de protecção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 227, 23.08.2012).

[22] Decisão 2000/520/CE 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 25.08. 2000).

[23] Levando a uma consequente tendência de aproximação das legislações europeia e norte-americana, nas palavras de 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 qe nos dizem respeito?", publicado neste Anuário.

que deverá ter sido levada a cabo a 'investigação' que a Comissão fez para verificar o nível de adequação.

Logo no art. 1.º da Decisão 2000/520/CE, se percebe que a constatação das circunstâncias relativas às transferências de dados feita pela Comissão da legislação interna e dos compromissos internacionais dos EUA se baseou não numa indagação de facto, mas no recebimento de documentos com promessas de natureza política e princípios de aplicabilidade comercial e na consequente expectativa europeia de que todas as instituições norte-americanas, dentro ou fora do sector, os cumprissem. Sem haver qualquer definição do que seja o nível adequado, nos termos do n.º 1 do art. 1.º, a protecção proporcionada aos dados pessoais dos europeus derivava dos princípios da privacidade em "porto seguro" e das linhas de orientação publicadas pelo DOC, a 21 de Julho de 2000[24], segundo os 'compromissos' assumidos em 4 documentos anexos à Decisão: um memorando a explicar a autoridade e funções da FTC; um outro com uma clarificação sumária da legislação norte-americana quanto a danos por violação das regras de protecção da vida privada e autorizações explícitas no que respeita ao uso de informações pessoais de forma contrária aos princípios de "porto seguro"; uma carta de Robert Pitofsky, da FTC, dirigida a John Mogg, Diretor-geral do Mercado Interno da Comissão, respondendo às dúvidas deste relativamente à jurisdição da FTC sobre "protecção da vida privada na área das comunicações em linha"; e um outro ofício, desta feita da parte de Samuel Podberesky, Conselheiro-Geral Adjunto da secção de *Aviation Enforcement and Proceeding* do *Department of Transportation* (DOT), ao mesmo John Mogg, no sentido de explicar as funções desta entidade no âmbito da "protecção da privacidade dos consumidores relativamente às informações por estes facultadas às companhias de transportes aéreos".

À altura, e como vieram a revelar o escândalo *Wikileaks* espoletado por Julian Assange e as acções de Edward Snowden, antigo analista e administrador de sistemas da CIA e da NSA, já as agências de segurança dos EUA recolhiam e tratavam em "larga escala e de forma indiferenciada[25]"

---

[24] V. Disponível em: <https://build.export.gov/main/safeharbor/eu/eg_main_018475> (acedido a 23/07/2017).

[25] Para. 45 das Conclusões do Advogado-Geral Yves Bot, apresentadas em 23 de Setembro de 2015, no âmbito do Processo C-362/14 relativo ao pedido de decisão prejudicial apresentado pela *High Court* (Irlanda) ao Tribunal de Justiça no processo *Schrems*.

big data para efeitos de vigilância. Isto, tanto sobre cidadãos e entidades em território nacional como no estrangeiro, nomeadamente residentes ou com sede em território europeu, mesmo que não pudessem vir a interagir com os EUA.

Isto era conhecido da União, pelo menos, nas verificações periódicas que a Comissão levou a cabo, já que os EUA implementaram o programa PRISM por volta de 2007[26], tendo assim permitido que entidades como a NSA acedessem de forma quase livre a dados pessoais que estejam armazenados em servidores localizados nos territórios dos EUA[27]. Ou seja, a Comissão tinha conhecimento de que esta política poderia contrariar directamente quaisquer garantias estabelecidas nos princípios do "porto seguro" e de que ia para além de qualquer controlo que pudesse exercer *overseas*, mas preferiu manter a decisão de adequação[28].

---

[26] Greenwald, Glenn e Macaskill, Ewen. *NSA Prism program taps in to user data of Apple, Google and others*, the Guardian, de 7 de Junho de 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (acedido a 28/06/2017).

[27] Para. 49 das Conclusões do Advogado-Geral Yves Bot no Processo C-362/14.

[28] A Comissão sabia deste programa, pelo menos, desde a avaliação periódica realizada em 2013, segundo a Comunicação ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE (COM(2013) 847 final, 27.11.2013). Não obstante ter conhecimento da gravidade da intromissão das entidades de segurança norte-americanas nos dados pessoais europeus e da desproporcionalidade, falta de transparência e utilização das informações para além do estritamente necessário em termos de segurança nacional, a Comissão decidiu manter o nível de adequação dos EUA. Aliás, curiosamente, somente o escândalo *Wikileaks* na base do caso *Schrems* teve a suficiente dimensão para pressionar as instituições europeias no sentido de alterarem a legislação e as práticas relativas aos níveis de adequação. Embora o acesso quase indiscriminado das agências aos dados recolhidos por empresas certificadas tivesse aparentemente levantado "novas questões graves sobre a continuidade dos direitos dos cidadãos europeus em matéria de proteção de dados quando os seus dados pessoais são transferidos para os EUA", a verdade é que as duas recomendações institucionais relativas ao acesso pelas autoridades dos EUA apenas vão num sentido 'informativo' de que "[a]s políticas de proteção da vida privada adotadas pelas empresas autocertificadas devem incluir informações sobre a medida em que a legislação dos EUA permite às autoridades públicas recolher e tratar dados transmitidos no âmbito do sistema de «porto seguro». Em especial, as empresas devem ser incentivadas a indicar, nas suas políticas de proteção da vida privada, se aplicam exceções ao sistema de «porto seguro» para observar requisitos de segurança nacional, interesse público ou execução legal" (recomendação 12); e que "[é] importante que a exceção por motivos de segurança nacional prevista na Decisão «porto seguro» seja utilizada apenas de forma

Donde, em primeiro lugar, o que quiçá importaria saber é se os membros da Comissão responsáveis pela 'investigação' das circunstâncias demonstrativas da adequação sabiam ou poderiam ter descoberto da (potencial) violação desse patamar mínimo por parte de algumas autoridades de vigilância e segurança, em virtude das suas atribuições e competências. E, em segundo lugar, se, assim sendo, deveriam ter incluído outro nível de compromissos nos acordos para acesso e processamento dos dados europeus.

Não é possível aferir se, no sentido de cumprir com o enunciado no n.º 2 do art. 25.º da Directiva 95/46/CE, foi sequer ponderada esta última hipótese, visto que a apreciação da adequação estava, de alguma forma, constrangida por dever ser levada a cabo em "função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados" (que seriam de foro estritamente comercial), e não imediatamente tendo em vista prospectivas 'rebuscadas' de utilização dos dados em investigações, de certo modo, secretas.

No entanto, segundo o mesmo enunciado, não só as regras gerais de Direito deveriam ser ponderadas como também as "medidas de segurança que são respeitadas" no país em questão, o que levanta dúvidas mais sobre a execução da lei pela Comissão e da ponderação de valores nas negociações do que propriamente sobre a suficiência do articulado de 1995. Por isso mesmo, aliás, não é de partilhar a opinião de doutrina como Olga Estadella-Yuste quando diz que a Directiva 95/46/CE não especifica se o *standard* de adequação se aplica à globalidade das leis de protecção da privacidade do país terceiro, a um sector, ou inclusivamente apenas às regras sobre o tipo de dados objecto das transferências propostas[29]. Parece ser claro que o nível de protecção só deveria ser definido com base no apuramento de todas as proposições normativas relevantes.

Um aspecto importante, relacionando as falhas no conceito e a concreta Decisão 2000/520/CE, é o que fica a descoberto relativamente ao balanço de competências entre os Estados-Membros e a Comissão quanto

---

proporcional e na medida em que for estritamente necessária" (recomendação 13) – algo que jamais seria, como a Comissão bem sabia, ou pelo menos deveria suspeitar.

[29] Estadella-Yuste, Olga. "Spain is on the road to implementing EU Directive 95/46", *International Review of Law, Computers & Technology*, vol. 11, issue 1, 1997, p. 40.

à fiscalização da adequação, no entendimento que parecia prevalecer ao nível institucional europeu antes do Acórdão *Schrems*[30].

Apesar de o n.º 3 do art. 25.º da Directiva 95/46/CE prever que os Estados-Membros e a Comissão se deveriam mutuamente informar quando considerassem que dado país terceiro não pareceria assegurar uma protecção adequada face ao manuseamento e tratamento dos dados pessoais, os números seguintes poderiam sugerir uma desconstrução de aparência da paridade. Segundo o n.º 4, somente a Comissão é que poderia "verificar" que dado país não asseguraria um nível de protecção adequado, na acepção feita no n.º 2[31]. Em consequência, os Estados-Membros deveriam proibir as transferências de dados daquela natureza para esse território e a Comissão, nos termos do n.º 5, deveria negociar com a jurisdição em causa para atender a este problema. Tal levaria a que ou o país fosse considerado como 'desadequado' a receber os dados pessoais dos cidadãos ou que a Comissão mantivesse a permissão para as transferências ao constatar que o país protegia a privacidade e as liberdades e direitos fundamentais de forma bastante, nos termos da sua "legislação interna ou dos seus compromissos internacionais".

Parece que o Comissário que respondeu a *Maximillian Schrems* aquando da sua queixa pela transferência de dados pessoais da *Facebook Ireland* para a *Facebook US*, interpretou o texto da Directiva 95/46/CE no sentido de que os Estados-Membros tinham, precisamente, um papel meramente informativo, quiçá mesmo acessório, na consideração do que seriam as medidas adequadas e suficientes a garantir a protecção dos dados pessoais fora das Comunidades. Aliás, à luz do desequilíbrio, o Comissário nem sequer terá interpretado o texto de forma exaustiva, visto que entendeu que uma investigação estaria imediatamente enviesada pelo facto de haver uma prévia decisão de adequação[32].

---

[30] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, de 6 de Outubro de 2015.

[31] Na verdade, pelo facto de o n.º 2 não consignar uma definição do nível de protecção mas somente os critérios para aferir da sua existência, as remissões dos n.os 3, 4 e 6 e a linguagem, em geral, utilizada neste artigo, tornam-se algo difíceis de compreender.

[32] Para. 50 das conclusões do Advogado-Geral Yves Bot no Processo C-362/14. Levantam-se, porém, algumas dúvidas quanto ao entendimento do Comissário e, quiçá, de toda a Comissão quanto aos deveres necessários para manter a certeza e segurança jurídicas e o princípio do primado do Direito no ordenamento eurocomunitário perante esta resistência institucional

Apesar da capacidade técnica de algumas autoridades nacionais a este respeito, a decisão de adequação da Comissão, por mais contestada que fosse, marcaria o derradeiro entendimento sobre a adequação de protecção de dado país terceiro. Desta forma, o legislador europeu centralizaria a função, assegurando a necessária certeza jurídica. Mas, por outro lado, pareceria desnivelar de forma excessiva o contributo das APDs nacionais no âmbito da declaração e manutenção das decisões de adequação *vis-à-vis* os poderes da Comissão Europeia[33-34].

---

a investigar uma queixa, como se as decisões da Comissão não fossem, por exemplo, democraticamente passíveis de crítica.

[33] Aliás, no Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 78, de 6 de Outubro de 2015, o Tribunal de Justiça da União Europeia sublinhou que, ponderando a relevância da protecção de dados pessoais no âmbito do direito fundamental ao respeito pela vida privada e o número potencialmente elevado de pessoas afectadas na sua intimidade caso o país terceiro não assegurasse uma adequada protecção, como acabou por suceder, a Comissão teria um poder de apreciação reduzido, muito possivelmente devido às suas competências e aos recursos de que dispõe, para averiguar estas situações. Assim sendo, o recurso às ADPs e a todas as ferramentas dos Estados aplicáveis é mais do que desejável – é verdadeiramente essencial no cumprimento da legislação europeia pela complexidade e volume das exigências decorrentes do art. 25.º da Directiva 95/46/CE, entre outras disposições, nomeadamente as do pacote legislativo de 2016.

[34] Também o Advogado-Geral Yves Bot obviou esta situação mas acabou por ler de forma diferente o texto do n.º 6 do art. 25.º da Directiva 95/46/CE, ao dizer que "é possível interpretar a Diretiva 95/46, e nomeadamente o seu artigo 25.º, n.º 6, bem como a Decisão 2000/520 num sentido que permita às autoridades nacionais conduzir as suas próprias investigações para estabelecer se a transferência de dados pessoais para um país terceiro satisfaz as exigências que decorrem dos artigos 7.º e 8.º da Carta", segundo o para. 46 das suas Conclusões ao Processo C-362/14. Igualmente no para. 86 virá reforçar o seu entendimento ao dizer que resultaria da economia do art. 25.º que a constatação em causa poderia ser levada a cabo quer pelos Estados-Membros quer pela Comissão. Assim sendo, numa importante análise *de iure*, tratar-se-ia de uma competência partilhada entre os Estados e as instituições. E, no para. 89, vai continuar, na mesma linha de pensamento, ao escrever que o artigo não acaba por atribuir à Comissão qualquer exclusividade em matéria de constatação do nível adequado quanto à proteção dos dados pessoais transferidos. Como antes, a economia do preceito demonstraria que os países também têm um papel relevante a desempenhar nesta matéria. Por fim, afere o Advogado-Geral que "uma decisão da Comissão desempenha, é certo, um papel importante na uniformização das condições de transferência válidas nos Estados-Membros. No entanto, essa uniformização só pode perdurar enquanto a constatação não for posta em causa", avançando, inclusivamente, com a ideia de que a avaliação da adequação poderá resultar de uma cooperação entre a Comissão e os Estados-Membros, no para. 91 das suas Conclusões.

Esta situação explica o entendimento do Tribunal de Justiça no caso *Schrems*[35]. Desde logo, o TJ avançou com a preocupação que subjaz a este trabalho, afirmando que:

> É certo que nem o artigo 25.º, n.º 2, nem nenhuma outra disposição da Diretiva 95/46 contêm uma definição do conceito de nível de proteção adequado. Em particular, o artigo 25.º, n.º 2, da referida diretiva limita-se a indicar que a adequação do nível de proteção oferecido por um país terceiro «será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados», e enumera, de modo não exaustivo, as circunstâncias que devem ser tomadas em conta ao proceder a tal apreciação[36].

O Tribunal também não avança com uma definição, mas continua a discorrer, nos trechos seguintes, sobre o nível de adequação. No para. 71 indica que, mesmo não havendo uma acepção *ex lata* do que seja o tal patamar, o n.º 6 do art. 25.º da Directiva impõe que os países terceiros o assegurem através da sua legislação, bem como dos compromissos internacionais de que sejam parte. Seguidamente, foca-se no elemento finalístico desta cláusula. A adequação deverá ser entendida e investigada tendo em vista o cumprimento da política expressa de protecção de dados pessoais à qual a União está obrigada, nos termos do n.º 1 do art. 8.º da CDFUE. E essa adequação deverá ser mantida pelo país terceiro, tal como se se aplicassem no seu território as disposições da Carta (para. 72)[37].

O termo 'adequado' indica, no entendimento do Tribunal, somente uma suficiência de protecção e não necessariamente um idêntico nível àquele garantido pela ordem jurídica da União. No entanto, igualmente na esteira do entendimento perfilhado pelo Advogado-Geral[38], isto deve

---

[35] Para um aprofundamento desta decisão, veja-se Lucas Pires, Martinho, "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

[36] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 70, de 6 de Outubro de 2015.

[37] Também no para. 139 das Conclusões, Bot refere que o objectivo do artigo será o de "assegurar a continuidade da proteção conferida" em caso de transferência de dados pessoais para um país terceiro.

[38] No para. 141 das Conclusões, o Advogado-Geral refere que a avaliação do nível de adequação deverá ser feita nos termos do Direito e da prática do país em causa. Aquele será pronunciado dependendo da verificação de uma equivalência substancial de protecção à

significar que o país assegure efectivamente um resguardo "das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União (...). Com efeito, na falta de uma exigência desta natureza, o objetivo [de assegurar a continuidade do nível elevado dessa protecção em caso de transferência de dados pessoais para um país terceiro] seria ignorado[39]", tornando-se o processamento dos dados fora da União um modo de fugir à lei.

O Tribunal chegou ao ponto de deixar inclusivamente claro que a Comissão deveria verificar que a protecção dos dados pessoais é assegurada de forma holística e efectiva em todo o sistema jurídico do país terceiro considerado, independentemente de que meios utilize para o fazer na prática[40], algo que parece estar na base da mudança que o legislador europeu operou quanto a esta matéria em 2016. De facto, por detrás desta linguagem do TJ parece estar a crítica (e simultaneamente aviso para o futuro) de que havia a obrigação jurídica pendente sobre a Comissão de descobrir todas as alternativas possíveis à utilização dos dados pelas autoridades norte-americanas para lá do óbvio e imediato uso pelo DOC ou pelo DOT, fosse por que meios fosse, e de assegurar a substancial não ingerência nos dados para lá dos objectivos da Directiva, antes, durante e depois das negociações com os EUA.

Certamente que é preciso reconhecer que esta posição, em jeito *ex post*, é mais fácil e avisada do que à altura quiçá fosse previsível, no meio das negociações e muito antes da intrincada verdade verter para fora do controlo dos serviços secretos e de segurança dos EUA. Não obstante, a Comissão não é uma simples entidade qualquer, tem uma posição privilegiada que pode e deve usar no sentido de promover o interesse geral da União, *inter alia*, pelo controlo da aplicação do direito da União Europeia[41] (onde quer que ele deva ser aplicado, mesmo que externamente); e tem acesso, ou tem capacidade para ter acesso, a informações bem mais profundas e completas do que aquelas que pareceram satisfazê-la à altura – e até, mais tarde, nas periódicas análises da situação que lhe incumbem, a si e aos Estados, como

---

conferida pelas normas da União, independentemente dos meios pelos quais se processe e aplique a legislação estrangeira.

[39] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 73, de 6 de Outubro de 2015.

[40] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, paras. 74 e 75, de 6 de Outubro de 2015.

[41] N.º 1 do art. 17.º do Tratado da União Europeia (TUE).

garantia do efeito útil nos termos dos n.os 1 a 3 do art. 25.º, conforme exige o n.º 6, da Directiva 95/46/CE, e como relembram o para. 76 deste Acórdão e os paras. 146 e 160 das Conclusões do Advogado-Geral[42].

Além disso, convém sublinhar paralelamente que o Tribunal de Justiça está, nestes parágrafos, a discutir a validade da Decisão 2000/520 e nunca a da Directiva 95/46/CE. São o direito e as práticas dos EUA que não asseguram um nível de protecção adequado na acepção do art. 25.º e não este trecho legal que é insuficiente, inválido ou que, na sua clareza e simplicidade, protege ineficazmente os direitos dos cidadãos europeus.

3. O Regulamento (UE) 2016/679

O RGPD[43] faz parte do mais recente pacote legislativo derivado da União Europeia relativamente à protecção de dados pessoais[44]. O texto vem afastar a Directiva 95/46/CE e propor um novo entendimento sobre o nível de protecção adequado que os países terceiros devem demonstrar para terem uma decisão de adequação por parte da Comissão. A inovação do n.º 1 do art. 45.º será no sentido de incluir as organizações internacionais a par com os países terceiros; além do esclarecimento de que, com uma decisão de adequação 'genérica', não serão necessárias autorizações específicas de cada vez que haja uma transferência de dados pessoais para esses destinatários.

---

[42] Uma obrigação contínua, *i.e.*, que se mantenha no tempo para lá da decisão inicial, de manutenção da adequação, segundo refere o Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, para. 147, de 6 de Outubro de 2015.

[43] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (RGPD).

[44] A ele juntam-se a Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, e a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (9091/17 [2017/0002 (COD)], 24.05.2017).

Como dito, o legislador europeu não define o que entende por nível de protecção adequado e somente enuncia de forma não exaustiva os critérios que a Comissão deverá ter em conta na sua avaliação. Aqui, a inovação é substancial. Estamos, aliás, perante um caso excepcional de verborreia jurídica europeia cujos efeitos nas negociações da UE com os EUA em termos de capacidade de verificação dos compromissos deverão ser, na melhor das hipóteses, inexistentes. Nos termos do n.º 2 do art. 45.º do Regulamento, há agora que ponderar:

a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

Como se pode verificar, este texto é bastante mais minucioso que o n.º 2 do art. 25.º da Directiva 95/46/CE. Não parece, porém, que este 'labor

legislativo' vá provocar um cuidado extra nas investigações periódicas encetadas pela Comissão ou uma sinceridade excepcional na definição das garantias de correcta utilização e protecção dos dados pessoais pelos países terceiros, muito menos os EUA.

4. O *Privacy Shield*

A Comissão não proferiu decisões típicas de adequação em 2000 nem em 2016 para as transferências de dados pessoais para os EUA, ambas à luz da Directiva 95/46/CE. Convém assim indagar porque é que este país terá o privilégio exclusivo de desenvolver, actualmente, um acordo para a transferência de dados que, não só já padece da singular falta de contrapartida, ou *trade-off*, que a UE imprimiu a esta legislação desde 1995 – visto que os países terceiros contratantes não têm de transferir os dados pessoais dos seus cidadãos para a União –, como mantém as regras de auto-certificação e se baseia no mesmo tipo de compromissos políticos e institucionais que permitiram a intromissão dos serviços de segurança nos dados pessoais dos cidadãos europeus. Se o sistema de "porto seguro" foi criticado por assentar em boa medida numa espécie de autoavaliação pelas empresas que participam voluntariamente neste sistema e por não ser acompanhado de garantias adequadas e de um mecanismo de fiscalização suficiente, o "escudo de protecção" poderá vir a ser alvo de semelhantes comentários por não se distinguir de forma significativa do acordo anterior, ao menos, neste aspecto[45].

Apesar de vir tentar responder às insuficiências do regime anterior, apontadas tanto pelo braço executivo como judiciário da União[46], não parece que seja o 'excesso linguísitco' adoptado pelo legislador europeu para o novo pacote de protecção de dados que vá garantir um efeito útil

---

[45] V. o seu funcionamento nos paras. introdutórios 30 e ss da Decisão de Execução (UE) 2016/1250 da Comissão de 12 de Julho de 2016 relativa ao nível de protecção assegurado pelo Escudo de Protecção da Privacidade UE-EUA, com fundamento na Directiva 95/46/CE do Parlamento Europeu e do Conselho (JO L 207, 1.8.2016).

[46] Lucas Pires, Martinho. "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

de não ingerência nas informações pessoais dos cidadãos por agências de segurança de países terceiros, com os EUA à cabeça, ou que não surja, quiçá de forma bastante apropriada, um *Schrems II*[47].

A Comissão não modificou o seu *modus operandi* – ou, pelo menos, não anunciou nada a esse respeito – quanto à investigação que deveria legalmente fazer para assegurar que os interesses económicos e políticos não se sobrepõem à privacidade dos dados individuais, que, pelo menos por ora, ainda é um valor premente no quadro jurídico europeu, tanto primário como derivado.

A decisão de adequação da Comissão em relação aos EUA, à sombra da Directiva 95/46/CE, esclarecia sobre os compromissos e os textos norte-americanos sobre práticas comerciais e sobre as entidades que deverão tomar medidas contra práticas comerciais desleais e enganosas[48]. Mas não havia qualquer compromisso quanto à utilização dos dados fora do âmbito comercial, nomeadamente a proibição da sua utilização no seio de investigações criminais. Isto é, de certa forma, de estranhar pois que o nível de adequação só deve ser declarado se o país terceiro revelar todas as suas intenções relativamente ao uso dos dados, desde logo para efeitos de controlo e vigilância no combate ao terrorismo, criminalidade e situações afins.

Ora, a nova legislação europeia vem, e aí correctamente, elucidar os EUA (e talvez o próprio executivo europeu) que quando se fala em regras de direito gerais no presente contexto se quer dizer todas as regras que possam levar à utilização daqueles dados por uma qualquer entidade e para qualquer efeito, através de um exercício de 'exemplificação' e 'adjectivação' jurídicas. Como se lê na alínea a) do n.º 2 do art. 45.º acima citado, essas regras compreendem toda a "legislação *pertinente* em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal" (itálico adicionado). Assim sendo, consagrou o legislador europeu que os futuros compromissos com Estados

---

[47] Existindo já acções pendentes que poderão resultar nessa situação. V. Rücker, Daniel e Dienst, Sebastian, *Action for annulment against the EU-US Privacy Shield and coordinated review by German data protection authorities*, Noerr, de 10 de Novembro de 2016. Disponível em: <https://www.noerr.com/en/newsroom/News/action-for-annulment-against-the-eu-us-privacy-shield-and-coordinated-review-by-the-german-data-protection-authorities.aspx> (acedido a 16/10/2017).

[48] Anexo VII da Decisão 2000/520/CE.

terceiros não devem somente respeitar a abusos na utilização dos dados no âmbito de más práticas comerciais, mas também compreender todo o fenómeno de utilização desses dados, independentemente do seu fim.

É difícil que os autores da Directiva 95/46/CE previssem a utilização dos dados pessoais no âmbito da vigilância secreta pelos Estados. Não havia, aliás, uma atenção especial ao tratamento de dados por meios informáticos à altura. Mas, em bom rigor, não só a Directiva referia já, em 1995, as "regras de direito, gerais e sectoriais", como o fenómeno do uso de dados dos cidadãos no combate ao terrorismo e à criminalidade já estava consolidado. Será realmente necessário este desenvolvimento legislativo tão detalhado no art. 45.º do RGPD ou será sintomático de uma fraca capacidade de tratar do problema de forma eficaz, a nível executivo? E, mesmo existindo, será que vai surtir algum efeito, nomeadamente na conduta futura dos EUA?

Em defesa da União é possível dizer que não será uma tarefa fácil fazer com que países sem preocupações de protecção dos dados pessoais dos cidadãos como as presentes na legislação da União acabem por cumprir os diversos compromissos políticos e comerciais, *inter alia*, que originalmente estipulam nas conversações com os negociadores europeus. Vários factores explicam (embora não justifiquem) a dificuldade em manter o mesmo *standard* e a consequente utilização abusiva de dados alheios pelo controlo, real ou extrapolado, que isso permite às entidades de segurança e aos próprios governos. Basta pensar no clima de combate ao terrorismo a nível global através de meios intrusivos que incutem no público a ideia de que os governos estão, de facto, a fazer algo no sentido de dirimir ou diminuir a ameaça; na disponibilidade e quantidade de bases de dados comerciais com conteúdos e meta-informações variados e altamente detalhados; na prática estabelecida de vigilância interna sobre os próprios cidadãos da parte de certos Estados, que assim veem como necessários e naturalmente complementares o acesso e *profiling* dos dados de utilizadores externos de serviços, físicos ou electrónicos, nacionalmente localizados, entre outros.

A confiança política, económica e relativa a matérias de segurança do espaço europeu deveria ter saído, não obstante, seriamente fragilizada com a descoberta da utilização abusiva dos dados por parte dos EUA, tanto nas investigações de 2013 como no seguimento do fenómento *Wikileaks*. Donde, como agir em seguida? A Comissão decidiu esmiuçar até à exaustão somente os critérios de adequação e esperar que os novos compromissos de auto-certificação e as renovadas promessas tenham um efeito de externalidade

positiva sobre todas as instituições que podem processar ou imiscuir-se nos dados pessoais. Parece pouco salutar.

No acordo *privacy shield*[49], os compromissos norte-americanos acabam, desta vez, por passar igualmente pelo DOJ. Segundo o para. introdutório 125 da Decisão de Execução (UE) 2016/1250, o governo dos EUA terá apresentado determinadas garantias relativas a limitações e salvaguardas que, no sentido da avaliação da Comissão Europeia, devem demonstrar um nível de protecção adequado.

O documento não apresenta qualquer definição do que seja este patamar[50], à semelhança da legislação europeia, tanto nos parágrafos introdutórios

---

[49] Relembre-se que a Decisão de Execução (UE) 2016/1250 é ainda baseada no n.º 2 do art. 25.º da Directiva 95/46/CE e não no RGPD. É passível de discussão o conjunto de razões que terão levado a Comissão a não esperar pela entrada em vigor da nova legislação europeia em matéria de protecção de dados para basear o "escudo de protecção", especialmente quando algumas das preocupações do art. 45.º do Regulamento (UE) 2016/679 espelham, de uma forma quase inversa ao que seria normal de um ponto de vista da construção de um ordenamento jurídico, o que foi decidido entre a Comissão e as autoridades norte-americanas. No entanto, considerando que as apreciações periódicas ao acordo deverão ser feitas sobre este novo enquadramento e serão tanto o RGPD como a legislação conexa de 2016 a ditar os parâmetros para as futuras decisões sobre o nível de adequação dos países terceiros, assim se justifica a inclusão na secção anterior do novo trecho legal sobre transferências de dados pessoais de cidadãos da União Europeia para fora. Aliás, o G29 vem obviar igualmente esta situação ao dizer que, à luz do facto do *privacy shield* ter sido adoptado com base na Directiva de 1995, terá de ser consistente com o novo enquadramento europeu em termos de protecção de dados, tanto em finalidade como em escopo. O G29 sugeriu até, na Opinião 1/2016, adoptada a 13 de Abril de 2016 (16/EN, WP 238), 3, 15 e 58, que uma revisão seja encetada pouco depois da entrada em vigor do RGPD, no sentido de garantir que o elevado nível de protecção garantido nesse documento seja seguida pela decisão de adequação da Comissão. Algum tempo volvido, igualmente a AEPD veio reforçar esta linha de argumentação na sua Opinião 4/2016, adoptada a 30 de Maio de 2016, ao dizer que o art. 45.º do RGPD veio, de facto, criar novos requisitos para as transferências de dados baseadas numa decisão de adequação, como a Decisão de Execução (UE) 2016/1250.

[50] Infelizmente, o G29 não parece encontrar necessidade, nas suas conclusões relativas às clarificações recomendadas ao esboço da Decisão de Execução (UE) 2016/1250, nos termos da Opinião 01/2016, 57, de esclarecer o próprio conceito de nível de protecção adequado. Se o tivesse feito, talvez seria mais claro o conjunto de exigências da União nesta matéria de relações externas, visto que uma noção completa e legalmente bem construída seria mais adequada, clara e indicativa do que referências às circunstâncias em que decorrem as transferências de dados pessoais. Também na secção 4.3, designada "rumo a seguir", da Comunicação ao Parlamento Europeu e ao Conselho sobre a transferência transatlântica de dados: restaurar a

como no articulado. Não obstante, nos termos dos paras. introdutórios 126 e ss., é demonstrado como a Quarta Emenda à Constituição dos EUA[51] irá garantir a privacidade, dignidade e a protecção "contra atos arbitrários e invasivos por parte de funcionários do governo[52]". E muito embora as proposições constitucionais não recaiam sobre cidadãos estrangeiros, como as empresas que detêm os dados estão localizadas em território ou estão sob a alçada do direito norte-americano, aqueles beneficiarão de uma protecção indirecta[53].

Ademais, as "autoridades com funções coercivas [deverão] em qualquer caso obter autorização judicial (ou pelo menos respeitar o requisito de razoabilidade)", bem como respeitar as orientações do DOJ que limitem o acesso aos dados por motivos equivalentes aos critérios europeus de necessidade e proporcionalidade, como o uso dos "métodos de investigação menos invasivos possíveis", *vis-à-vis* o seu efeito sobre a privacidade e as demais liberdades cívicas dos titulares dos dados[54].

Ora, difícil é saber se este requisito de 'razoabilidade' irá suster a adequação da protecção perante a tenacidade das agências de segurança em obter grandes quantidades de informações pessoais, a qual é especialmente

---

confiança através de garantias sólidas (COM (2016) 117 final, 29.02.2016), a Comissão parece considerar que, embora se encarregue de encontrar e rever o nível adequado de protecção dos dados pessoais num ambiente dinâmico e vivo, por oposição ao paradigma estático que perpassava no "porto seguro", encontrar uma definição do que seja o nível de adequação não é uma componente essencial dessa adaptação às mudanças legislativas.

[51] Nos termos desta proposição constitucional, os cidadãos norte-americanos terão direito à inviolabilidade das suas pessoas, casas, documentos e outros bens pessoais contra buscas e apreensões não razoáveis. Ademais, ainda se consagra que não deverão ser emitidos mandatos a não ser sob causa provável, apoiada por juramento ou declaração, e com uma descrição específica do local sob investigação, bem como das pessoas ou coisas a serem apreendidas. V. a versão original com anotações e referências detalhadas. Disponível em: <http://uscode.house.gov/view.xhtml?path=/frontmatter/organiclaws/constitution&edition=prelim> (acedido a 29/6/2017).

[52] Para. introdutório 126 da Decisão de Execução (UE) 2016/1250.

[53] Muito embora, sejam de referir as dúvidas que o G29 avança nesta matéria. Diz o Grupo, na Opinião 01/2016, 55, que, mesmo que a protecção fosse efectiva, tal não significa que os meios de defesa dos interesses dos cidadãos estejam, de facto, ao alcance dos particulares, visto que o sujeito do direito a uma compensação efectiva neste cenário parece ser a companhia que recebe o pedido de acesso e não o(s) indivíduo(s) cujos dados estão em causa.

[54] Para. introdutório 127 da Decisão de Execução (UE) 2016/1250.

voraz se os dados ainda estiverem num estado quase cru, *i.e.*, pouco ou nada editados por intermediários. Nesta secção da Decisão, a Comissão demonstra até ter conhecimento de práticas norte-americanas que, não obstante a actualização do texto europeu, poderão continuar a perigar a protecção e secretismo dos dados pessoais[55]. Por outro lado, é interessante constatar que, apesar de "um certo número de vias de recurso judiciais para as pessoas singulares" (apresentados nos paras. introdutórios 130 a 132)[56], a Comissão conforta-se com factos como:

> [A]o abrigo da *Freedom of Information Act* (FOIA 5 U.S.C. § 552), qualquer pessoa tem o direito de obter acesso aos registos de uma agência federal e, após o esgotamento das soluções administrativas, de fazer valer esse direito em tribunal, exceto na medida em que esses registos sejam protegidos de divulgação pública por uma isenção ou uma exclusão especial decorrente do exercício de funções coercivas.

Somando à excepção referida no final deste parágrafo, é mister relembrar que as agências de segurança retiram as informações pessoais de forma,

---

[55] Disso são exemplo as excepcionais, mas existentes, buscas sem mandato. No para. introdutório 180 da Decisão de Execução (UE) 2016/1250, a Comissão enumera alguns dos casos de jurisprudência em que tal tenha sucedido, nomeadamente *Johnson c. Estados Unidos*, 333 U.S. 10, 14 (1948); *McDonald*, 335 U.S. 451, 453 (1948); *Camara c. Municipal Court*, 387 U.S. 523, 528 (1967); ou *G.M. Leasing Corp. c. Estados Unidos*, 429 U.S. 338, 352-53, 355 (1977). Por outro lado, o Supremo Tribunal de Justiça, alega a Comissão, tem periodicamente reforçado a ideia de que buscas realizadas fora de um processo judicial ou sem autorização prévia de um magistrado não tendem a ser razoáveis *per se*, na acepção constitucional. Mas, retomando, o para. introdutório 189 reforça as preocupações europeias ao dizer que, segundo as informações que a Comissão recebeu do governo norte-americano, há diversas situações que não necessitam de mandatos judiciais, como a actuação das autoridades no âmbito do *Electronic Communications Privacy Act* relativamente a "informações básicas sobre os assinantes, as sessões e a faturação (18 U.S.C. § 2703(c)(1), (2) (...) e [a] pedidos de acesso ao conteúdo de mensagens de correio eletrónico com mais de 180 dias (18 U.S.C. § 2703(b)", e as intimações administrativas, que estão fora desta exigência processual, muito embora sejam limitadas a casos concretos e, alegadamente, objecto de controlo jurisdicional independente, caso se executem em tribunal.

[56] V. as dificuldades relativas ao princípio da tutela jurisdicional efectiva em Lucas Pires, Martinho. "Algumas considerações sobre a compatibilidade do sistema de Privacy Shield com o direito da União Europeia à luz do acórdão Schrems", publicado neste Anuário.

obviamente, secreta e o acesso às suas bases de dados é, até agora, inédito, especialmente por cidadãos singulares, estrangeiros e fora do âmbito de um processo judicial. Assim sendo, torna-se difícil compreender quão adequada poderá realmente ser, na prática, esta garantia ao nível do patamar, nunca definido, de protecção de dados pessoais. Quiçá as reapreciações periódicas da verificação de adequação demonstrarão que o nível é suficiente, ou não[57]. Para já, os Estados Unidos comprometeram-se a informar a Comissão da evolução da legislação norte-americana, particularmente se se apresentar discordante do "escudo de protecção", tanto no domínio da protecção dos dados pessoais como no das limitações e garantias ao acesso das autoridades públicas a essas informações[58].

Numa nota positiva, convém referir que os anexos à Decisão de Execução (UE) 2016/1250 relativos aos compromissos dos EUA são bastante mais abrangentes, nomeadamente envolvendo mais entidades do sistema jurídico norte-americano na elaboração das garantias relativas à protecção dos dados pessoais e não se limitando aos princípios de aplicabilidade comercial, como sucedia previamente com a Decisão 2000/520/CE. Embora não avancem com quaisquer definições do nível de adequação e, de novo, fosse aconselhável que a Comissão tivesse levado a cabo um trabalho de campo, uma investigação de facto, que culminasse numa lista analisando toda a legislação interna e os compromissos internacionais dos EUA[59], os anexos consistem em: uma carta de Penny Pritzker, Secretária do Comércio, contendo um pacote de materiais que explicam tanto o funcionamento do *privacy shield* como o envolvimento e limitações das diversas autoridades[60]; um escrito

---

[57] Especialmente tendo sublinhado a Comissão de que as revisões não podem ser exercícios formais sem consequências e que as decisões de adequação não podem ser letra morta, na sua Comunicação (COM (2016) 117 final, 29.02.2016), 10. Numa curiosa formulação, a instituição disse ainda que as "*U.S. companies and authorities have to breathe life into the framework and continuously sustain it by living up to their commitments*" – infelizmente a tradução em Português está longe de correcta ou de carregar o mesmo impacto semântico ao dizer que "as empresas e as autoridades americanas têm de contribuir positivamente para o novo quadro e apoiar continuamente o seu funcionamento mediante o respeito dos seus compromissos".

[58] V. o para. introdutório 146 da Decisão de Execução (UE) 2016/1250.

[59] Eventualmente contando até com formas de acesso aos dados fora do âmbito estrito de vigilância e segurança nacionais, nos termos da Opinião 01/2016 do G29, 12.

[60] Neste pacote estão incluídos uma carta de Edith Ramirez, Presidente da FTC, que descreve a aplicação do "escudo de protecção", com um apêndice com uma descrição ampla

de Ken Hyatt, Subsecretário interino para as questões do comércio internacional, que, em representação da *International Trade Administration* (ITA), narra a melhoria da protecção dos dados pessoais que o quadro do *privacy shield* irá proporcionar, bem como os diversos compromissos que o DOC assumiu para a aplicação eficaz do acordo[61]; um desenvolvimento exaustivo dos princípios do quadro do "escudo de protecção de privacidade" (muito embora se assemelhe ao texto produzido anteriormente), baseado nas noções de adequação e razoabilidade; e uma carta de John Kerry, Secretário de Estado dos EUA à altura, felicitando o entendimento alcançado.

Por fim, a Comissão acabou por concluir que o ordenamento jurídico dos EUA consagra normas em vigor que limitam as ingerências, para efeitos coercivos ou outros de interesse público, aos direitos fundamentais dos cidadãos europeus cujos dados pessoais sejam transferidos da União ao abrigo do "escudo de protecção", no limite do necessário para a prossecução dos objectivos legítimos de investigação que levarem a cabo e dentro da protecção e certeza jurídicas legalmente exigidas[62]. Será a conclusão certa ou será antes a conclusão 'necessária' para os negócios europeus?

---

do sistema jurídico dos EUA em matéria de protecção da privacidade e da segurança; um ofício do DOT, assinado por Anthony Foxx, Secretário dos Transportes, semelhante ao texto anterior; duas missivas elaboradas pelo Conselheiro-Geral Robert Litt, do *Office of the Director of National Intelligence*, relativamente às garantias e limitações aplicáveis aos serviços de segurança nacional dos EUA na intromissão nos dados pessoais dos cidadãos europeus; uma outra carta e memorando em anexo do *Department of State*, informando do seu compromisso em instituir um novo Mediador para o Escudo de Protecção da Privacidade tendo em vista a apresentação de questões sobre as práticas norte-americanas de recolha de informação de origem eletromagnética; e um outro documento, desta feita subscrito por Bruce Swartz, Vice-Procurador-Geral Adjunto e Conselheiro para os Assuntos Internacionais, em representação do DOJ, sobre as garantias e limitações de acesso do governo dos EUA no exercício de funções coercivas e de interesse público pelos seus agentes e representantes públicos. Na missiva, a Secretária Pritzker sublinha ainda, com a seriedade possível, que a Comissária Věra Jourová, responsável da UE pela Justiça, Consumidores e Igualdade de Género "[p]ode ter a certeza de que os Estados Unidos da América encaram estes compromissos com seriedade".

[61] Entre os quais, merece destaque a resolução de cooperação com as APDs europeias na investigação e resolução de queixas.

[62] Paras. introdutórios 135 e ss. da Decisão de Execução (UE) 2016/1250.

Notas conclusivas

Os fluxos crescentes de dados pessoais a nível mundial impõem a adopção de medidas multilaterais que aproximem legislações, entidades, serviços e pessoas no sentido de se provocar um duplo, embora frágil, efeito. Por um lado, deve ser garantido um nível adequado de protecção para todos os titulares dos dados e, por outro, é mister acautelar para que não se levantem barreiras desnecessárias à livre circulação da informação, tanto pelos efeitos económicos[63] como pelas consequências sociais.

Não parece que a recente política legislativa europeia em matéria de transmissão de dados pessoais para países terceiros tenha, neste sentido, seguido a vereda mais eficaz. Especialmente em matérias complexas, propensas já de si a redundâncias e inutilidades técnico-linguísticas, a simplicidade da legislação é, das mais das vezes, a melhor escolha. Aliada a mecanismos *de iure*, mas também *de facto*, de verificação do cumprimento das normas, tanto melhor quanto mais descentralizados forem, a legislação não deve ser inutilmente prolixa na expectativa de que os destinatários e todos os demais afectados pelas normas percebam uma qualquer 'dica implícita de bom comportamento'.

É verdade que não é inteiramente seguro, ou sequer óbvio, que haja uma relação directa de efeito útil entre a consagração de um conceito de forma expressa e balizada e os problemas decorrentes de conseguintes decisões executivas (e administrativas) menos avisadas, baseadas na leitura e interpretação desse trecho legal que, não consagrando o conceito, se debruça sobre a sua essência. As decisões institucionais analisadas neste estudo basearam-se, segundo alguns autores, num conceito indeterminado ou flexível que, assim, melhor abrangeria as diferenças dos sistemas jurídicos dos países terceiros aquando das decisões de adequação. Mas a verdade é que esta 'insuficiência' legislativa tão gritante parece ter levado a alguma incerteza na elaboração dessas decisões e ter permitido a atitude subsequente dos EUA. Em suma, parece que esta 'abertura' do sistema não teve os efeitos que poderiam ter sido avistados originalmente.

O legislador europeu teve uma segunda oportunidade nesta matéria após o julgamento *Schrems*. Infelizmente, não teve a difícil, mas frutuosa,

---

[63] Cerda Silva, Alberto. "El «nivel adecuado de protección» para las transferencias internacionales de datos personales desde la Unión Europea", cit., p. 353.

postura de não subjugação à diplomacia da força e dos interesses. Não é criando normas jurídicas que quase escapam às exigências de abstracção e de generalidade e tomando decisões de execução não baseadas em investigações *de facto* e em compromissos holísticos e executivos, que a União vai conseguir impedir que os países terceiros imiscuam e utilizem os dados pessoais dos cidadãos da União para efeitos de investigações criminais e de contra-terrorismo, explícita ou secretamente.

É possível indagar se não será o próprio conceito de privacidade, como a União Europeia o tem vindo a conceber e defender[64], que estará algo desactualizado ou mesmo desadequado perante o crescente cruzamento de dados pessoais e o consentimento pessoal tácito e generalizado 'à base de um *click*'. Os governos, em sentido lato, são, hoje em dia, receptáculos e processadores em massa de informações pessoais. Aliás, a crescente conectividade, dentro e fora da União, faz com que dados recolhidos por uma dada administração nacional, possam vir a ser transferidos e utilizados por outras entidades e autoridades, nacionais e regionais, bem como pelas instituições, órgãos, organismos e agências europeias, para os mais diversos fins. E a somar a esta utilização pública, há que considerar a rede ainda mais complexa, densa e interoperável que subsiste a nível de *profiling* por agentes privados.

O acompanhamento que o Direito pode fazer da realidade, tanto física como virtual, ficará sempre aquém das expectativas mais básicas de justiça encontradas em cada ser humano. No entanto, cabe ao legislador, tanto nacional como europeu, recorrer a todas as ferramentas disponíveis, e inclusivamente a outras áreas do saber, para que construa um ordenamento jurídico claro, descomplicado e suficientemente corajoso para cumprir com os princípios axiológicos que o informam. O desenvolvimento social, especialmente perante a consolidação da sociedade da informação, exige respostas jurídicas precisas e adequadas aos novos fenómenos sociais[65]. A consagração de conceitos com os quais os aplicadores do direito podem

---

[64] No sentido de se apoiar num "justo equilíbrio entre os valores públicos e os interesses particulares em apreço" para 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?", publicado neste Anuário.

[65] Herrán Ortiz, Ana. "El derecho a la protección de datos personales en la sociedad de la información", cit., p. 13.

melhor trabalhar e assim corresponder às disposições legais das quais dependem é uma parte crucial de todo este processo. Assim como o é também todo o conjunto de esforços que conduza à manutenção desses princípios fundacionais presentes em todas as boas ideias, entre as quais se conta a própria União Europeia.

O *Passanger Name Record* e a Proteção de Dados Pessoais: Uma análise sobre a transferência da informação dos passageiros aos Estados

Emellin de Oliveira*

Resumo: Em 27 de abril de 2016, foi aprovada a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, sobre a utilização dos dados dos registos de identificação dos passageiros (PNR ou *Passenger Name Record*) como instrumento de combate ao terrorismo e à criminalidade grave. A Diretiva estabelece a obrigação de as transportadoras aéreas transferirem para os Estados-Membros as informações do PNR relativas aos voos provenientes/destinados a/de países terceiros. Neste contexto, analisaremos de forma crítica o conteúdo da Diretiva UE-PNR face às normas do Regulamento de Proteção de Dados Pessoais de 2016, com vista a averiguar as convergências e incongruências entre os dois atos legislativos.

Palavras-Chave: *Proteção de Dados; Transferência de dados; Terrorismo; Criminalidade Grave.*

Abstract: On the 27th April 2016, the Directive 2016/681 (EU) of the European Parliament and of the Council was approved, regulating the use of Passenger Name Record (PNR) data as an instrument to combat terrorism and serious crimes. The Directive lays down an obligation for air carriers to transfer PNR information of flights to/from third countries to Member States. In this context, the research's aim is to critically analyse the content of the EU-PNR Directive in relation to the 2016 rules of the Personal Data Protection Regulation, in order to ascertain the convergences and inconsistencies between the two legislative acts.

Keywords: *Data Protection; Data Transfer; Terrorism and Serious Crimes.*

---

* Emellin de Oliveira é Doutoranda em Direito na Universidade Nova de Lisboa (FDUNL), Investigadora no Centro de I&D em Direito e Sociedade (CEDIS) e Bolseira de Doutoramento da Fundação para a Ciência e a Tecnologia (FCT). É Mestre em Migrações Internacionais pelo Instituto Universitário de Lisboa (ISCTE-IUL), Especialista em Estudos da Paz e da Segurança pela Universidade de Coimbra (FEUC) e Licenciada em Direito pela Universidade Federal do Ceará (UFC-CE, Brasil).

Introdução

De acordo com o art. 13.º da Convenção de Aviação Civil Internacional (Convenção de Chicago de 1944), as leis e os regulamentos de um Estado contratante devem ser cumpridos pelos passageiros, tripulação e seu representante aquando da entrada ou saída do seu território. Diante desta determinação da ICAO (*International Civil Aviation Organization*) e com o intuito de adotar medidas contra o terrorismo e a criminalidade grave, no dia 14 de abril, o Parlamento Europeu aprovou uma Resolução Legislativa[1], a respeito do tratamento de dados contidos no PNR. Aquela resolução estabelece para as companhias aéreas, especificamente as transportadoras, a obrigação de fornecer as informações relativas ao registo dos seus passageiros nos voos com proveniência e/ou destino países terceiros, extra-UE.

Posteriormente, no dia 27 de abril de 2016, foi aprovada a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, cuja publicação ocorreu no dia 24 de maio, determinando que a transposição das regras inerentes ao documento citado seja realizada até 25 de maio de 2018. Ainda, a Diretiva prevê uma data para o reexame dos termos aprovados e a formulação de um relatório pela Comissão a ser apresentado ao Parlamento e ao Conselho em 2020.

Apesar de a Diretiva ir ao encontro das medidas de caráter securitário desenvolvidas na União Europeia com a finalidade de combater a imigração ilegal, a criminalidade grave e detetar infrações terroristas, algumas preocupações surgiram com o texto legislativo apresentado. Diana Dimitrova[2], aquando da Comunicação[3] da Comissão Europeia a propor a Diretiva UE-PNR ao Parlamento e ao Conselho, destacava a problemática

---

[1] Resolução legislativa do Parlamento Europeu (P8_TA-PROV (2016) 0127), de 14 de abril de 2016, COM (2011) 0032 – C7-0039/2011 – 2011/0023 (COD), sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

[2] Dimitrova, D. "Passenger Name Records and data protection issues: busting some myths", *Media Policy Project Blog*, de 19 de maio de 2015. Disponível em: <http://blogs.lse.ac.uk/mediapolicyproject/2015/05/19/passenger-name-records-and-data-protection-issues-busting-some-myths/> (acedido a 12/12/2017).

[3] Proposta de Diretiva do Parlamento Europeu e do Conselho, COM (2011) 32 final da Comissão, de 2 de fevereiro de 2011, relativa à utilização dos dados dos registos de identificação

que se gerava em volta da vigilância proposta a todos os indivíduos. A autora menciona como questões a refletir: a precisão e o tratamento dos dados transferidos pelas companhias aéreas; a inexatidão da eficácia, proporcionalidade e necessidade da transmissão de informações; além da possível violação de princípios consagrados em documentos comunitários e internacionais, entre os quais se encontra a proteção de dados pessoais[4].

Tendo em conta a aprovação do Regulamento[5] sobre a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades, é necessário abordar o tema do PNR no contexto da proteção de dados pessoais na União Europeia.

Posto isto, o presente artigo visa, na sua primeira secção, analisar o conteúdo da Diretiva UE-PNR. Na segunda secção, um quadro comparativo será desenhado de modo a destacar as convergências e incongruências entre a Diretiva UE-PNR e o Regulamento de Proteção de Dados. Na terceira secção, apreciamos a prática das companhias aéreas no que diz respeito à obtenção das informações dos passageiros e ao tratamento dado àquelas, para que se possa perceber o impacto das obrigações contidas na Diretiva do PNR. Por fim, pretende-se criticamente averiguar a aplicabilidade e a eficácia no combate ao terrorismo e à criminalidade grave desses atos legislativos face ao imposto às transportadoras.

Para fins de limitação do objeto de estudo, o presente artigo assumirá a definição dos dados do PNR como descrita pelo Parlamento Europeu, que seria a informação fornecida pelos passageiros e coletada pelas transportadoras aéreas durante os procedimentos de reserva e *check-in*[6].

---

dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave (2011/0023 (COD) C7-0039/11).

[4] Dimitrova, D. "Passenger Name Records and data protection issues: busting some myths", cit.

[5] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[6] Parlamento Europeu, *EU Passenger Name Record (PNR) directive: an overview*, de 1 de junho de 2016. Disponível em: <http://www.europarl.europa.eu/news/pt/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview> (acedido a 5/12/2016).

1. A Diretiva UE-PNR e a transferência de informações dos passageiros

A compreensão da motivação e do objetivo da Diretiva UE-PNR, pressupõe o conhecimento das razões de sua origem, daí o breve historial que se passa resumidamente a traçar.

I. Em novembro de 2001, entre uma das medidas securitárias desenvolvidas pelos Estados Unidos em resposta aos atentados terroristas de setembro do mesmo ano, o governo norte-americano passou a exigir das companhias aéreas o acesso eletrónico aos dados contidos nos registos de passageiros.

Em resposta ao requerimento, a Comissão Europeia, em junho de 2002, comunicou aos EUA que aquela exigência poderia gerar conflitos com as legislações, da União Europeia e dos seus Estados-Membros, em matéria de proteção de dados, nomeadamente no que toca à extensão desta obrigação às transportadoras com base operacional na UE. No entanto, em fevereiro de 2003, os EUA e a UE emitiram conjuntamente uma declaração em que assumiam o compromisso de continuar a negociar a respeito da comunicabilidade dos dados do PNR à alfândega norte-americana.

A administração dos EUA, impaciente com os diversos adiamentos por parte da UE à efetivação da transmissão das informações, impôs às transportadoras aéreas penalidades caso o acesso ao PNR dos passageiros não fosse disponibilizado a partir de 5 de março de 2003[7].

---

[7] Sobre este tema, o Parlamento Europeu emitiu a Resolução P5_TA (2003) 0429, cujo seguinte excerto se destaca: "3. Convida, por conseguinte, a Comissão a: A) Determinar de imediato, com base nos limites delineados pelo grupo de trabalho criado pela Directiva 95/46/CE, quais os dados que podem legitimamente ser transmitidos pelas companhias aéreas e/ou pelos sistemas informatizados de informações a terceiros, e em que condições, desde que: não exista discriminação contra passageiros não nacionais dos EUA e os dados não sejam retidos para além do período de estada do passageiro em território dos EUA; os passageiros sejam informados plenamente e com precisão antes da aquisição do seu bilhete e dêem o seu consentimento informado no que se refere à transmissão dos dados em causa para os EUA; os passageiros tenham acesso a um procedimento de recurso rápido e eficaz, na eventualidade de qualquer problema. B) Proibir às companhias aéreas e aos sistemas de reserva informatizados qualquer acesso e/ou transmissão que não respeite os princípios estabelecidos na alínea a) ou caso as mesmas companhias e sistemas estejam em aparente violação das obrigações decorrentes da Directiva 95/46/CE e do Regulamento (CEE) n.º 2299/89".

II. Ainda, em dezembro do ano de 2003, a Comissão publicou um Comunicado[8] ao Conselho e ao Parlamento Europeu, com as ideias de base consideradas como "uma abordagem global da UE" relativamente à transferência de dados do PNR. Ao defender uma abordagem equilibrada e abrangente, as componentes do plano europeu sobre a transmissão de informações dos passageiros aos EUA seriam: um quadro jurídico para as transferências existentes de dados dos PNR para os EUA; o fornecimento de informações completas, exatas e oportunas aos passageiros, a fim de que estes consentissem na transferência dos seus dados; a substituição do método de extração direta dos dados pelo governo norte-americano, "método *pull*", pelo método de exportação, "método *push*", no qual se poderia usar filtros que impedissem a transmissão de informações por outros canais[9]; o desenvolvimento de uma posição da UE sobre a utilização dos dados dos passageiros para a segurança da aviação e das fronteiras; a criação de um quadro multilateral para a transferência de dados dos PNR's no âmbito da Organização Internacional da Aviação Civil[10].

Da análise dos documentos referidos, é notória a preocupação da UE sobre a transferência de dados do PNR. Visa-se estabelecer um modelo jurídico da União que permita autorizar as companhias aéreas a transferir as informações dos passageiros para os EUA, como uma obrigação legal e, ao mesmo tempo, garantir que cidadãos europeus sob investigação do governo norte-americano sejam sujeitos a um processo legal justo, com respeito pelos seus direitos fundamentais.

Esta preocupação também se encontra na Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras. Apesar desta Diretiva

---

[8] Comunicação da Comissão ao Conselho e ao Parlamento Europeu sobre a transferência de dados contidos nos registos de identificação dos passageiros aéreos, COM (2003) 826 final, de 16 de dezembro de 2003, (PNR – *Passenger Name Record*): uma abordagem global da UE, Bruxelas.

[9] Sobre esses métodos, destaca-se o que veio delineado na Proposta de Decisão-Quadro do Conselho, COM (2007) 654 final, de 6 de novembro de 2007, p. 5: "(...) A principal diferença entre os dois métodos reside no facto de, no método de transferência por exportação, os dados serem enviados pela transportadora à autoridade nacional, enquanto nos métodos de transferência por extracção a autoridade nacional obter acesso ao sistema de reservas da transportadora aérea e extrair os dados".

[10] COM (2003) 826 final, cit., pp. 10 e 11.

estabelecer como legítimo o processamento dos dados do PNR para controlo fronteiriço e a utilização dessas informações como meio de prova em ações judiciais, estipula que "qualquer tratamento de algum modo incompatível com esta finalidade é contrário ao princípio enunciado na alínea b) do n.º 1 do art. 6.º da Directiva 95/46/CE[11-12].

Neste sentido, as companhias aéreas passaram a ter como obrigação legal a transmissão, até ao final do registo do embarque, das "Informações Prévias sobre Passageiros" (*Advance Passanger Information* – API). Entre as informações a comunicar encontram-se, nomeadamente: o número e tipo de documento de viagem utilizado; a nacionalidade; o nome completo; a data de nascimento; o ponto de passagem da fronteira à entrada no território dos Estados-Membros; o código do transporte; a hora de partida e de chegada do transporte; o número total de passageiros incluídos nesse transporte; o ponto inicial do embarque. No entanto, por ser uma transcrição das informações contidas no passaporte e/ou Bilhete de Identidade, o API apenas permite a identificação de suspeitos de terrorismo e crime organizado já conhecidos pelas autoridades.

III. No sentido de colmatar esta lacuna, em novembro de 2007, o Conselho comunicou uma Proposta de Decisão-Quadro[13] sobre a utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) pelos Estados-Membros da União Europeia. Na proposta, destacava-se que seriam necessários "uma cooperação e um maior intercâmbio de informações entre os Estados-Membros e os seus serviços, bem como com a Europol" a fim de que se pudesse enfrentar o caráter transnacional adquirido pelo terrorismo e pela criminalidade organizada. Para o Conselho, a recolha e a análise dessas informações dos passageiros permitiriam às autoridades estatais competentes identificar pessoas consideradas

---

[11] Directiva 95/46/CE, alínea b) do n.º 1 do art. 6.º: "Recolhidos para finalidades determinadas, explícitas e legitimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas".

[12] Directiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação dos dados dos passageiros pelas transportadoras.

[13] Proposta de Decisão-Quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (UE – PNR) para efeitos de aplicação da lei, COM (2007) 654 final, de 6 de novembro de 2007.

de alto risco e tomar medidas adequadas antecipadamente, usando como exemplos positivos as iniciativas já materializadas nos EUA, Canadá e Reino Unido.

Assim, a base jurídica da proposta ancorava-se no art. 29.º, na alínea b) do n.º 1 do art. 30.º e na alínea b) do n.º 2 do art. 34.º, do Tratado da União Europeia, bem como nos princípios da subsidiariedade, no que toca à harmonização das obrigações jurídicas que recaem sobre todas as companhias aéreas operadoras de voos da/para União Europeia, e da proporcionalidade, relativamente ao objeto de harmonização, pois o uso e o tratamento dos dados deverão restringir-se ao estritamente necessário.

Ao verificar que a proposta do Conselho não havia avançado e que ainda se mantinham as discussões entre a UE e os EUA a respeito da transmissão das informações relativas ao registo de passageiros, o Conselho Europeu relembrou a questão do PNR no "Programa de Estocolmo – Uma Europa aberta e segura que sirva e proteja os cidadãos", projeto apresentado pela Presidência em outubro de 2009. No Programa, o Conselho solicitava à Comissão a proposta de adoção de uma medida por parte da UE no âmbito do PNR que garanta um elevado nível de proteção de dados[14].

Assim, findo o período de negociação com os EUA sobre a transferência de dados do PNR e assinado um acordo para tal efeito, que foi repetido com o Canadá e a Austrália, a UE, por via do Comunicado[15] da Comissão em setembro de 2010, retomou o discurso em prol de uma abordagem global relativa à transferência dos dados do PNR para países terceiros. Nesta comunicação, ressalta-se o PNR como uma importante ferramenta em matéria de informações criminais, servindo mais do que um sistema de verificação de identidade – como ocorre com o API – e podendo ser utilizado de modo: "reativo", em investigações iniciadas após a prática do

---

[14] Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos, Jornal Oficial da União Europeia, 2010/C 115/01, p. 9: "Com base nos debates realizados no Conselho e no Parlamento Europeu tendo em vista a criação na União de um sistema de registo de identificação dos passageiros (PNR), o Conselho Europeu exorta a Comissão a: — propor a adopção de uma medida da União, que garanta um elevado nível de protecção de dados, no domínio do PNR no intuito de prevenir, detectar, investigar e reprimir infracções terroristas e formas graves de criminalidade com base numa avaliação de impacto".

[15] Comunicação da Comissão Europeia sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros, COM (2010) 492 final, de 21 de novembro de 2010.

crime; "real", quando um crime está a ser cometido ou na iminência de ocorrer, em que se se pode evitar a conclusão do ato ilícito; e "pró-ativo", possibilitando a criação de padrões de viagem e de comportamento, o que facilitaria a identificação de perfis criminosos.

IV. Não obstante a clara e explícita intenção em criar-se uma legislação específica sobre PNR para a UE, a Comissão deparou-se com um óbice prático: a possibilidade de requisição de reciprocidade na transmissão de dados de PNR por Estados terceiros que aceitarem fornecer estas informações à União Europeia. Tal preocupação subjaz no arcabouço legislativo da União, especificamente no relativo à proteção de dados. Isto porque a transferência de dados de passageiros a países terceiros só pode ocorrer caso estes assegurem garantias adequadas para a proteção das informações disponibilizadas.

Neste sentido, ainda no Comunicado da Comissão, estabeleceu-se quais seriam os princípios básicos em matéria de proteção de dados que deveriam ser aplicados pelo país terceiro que requeira reciprocidade na transmissão dos dados do PNR, designadamente: finalidade clara e objetiva da utilização dos dados do PNR; intercâmbio de dados em caráter mínimo e proporcional à finalidade; dados sensíveis não devem ser utilizados, salvo face à uma ameaça iminente e sob garantias de adequação à finalidade original; proteção contra a utilização incorreta e o acesso ilegal; sistema de fiscalização sobre as autoridades que tratam os dados do PNR; transparência e comunicação do uso e do tratamento dos dados; possibilidade de acesso, retificações e supressão dos dados de PNR; via de recurso efetiva para os indivíduos que entenderem ter seus direitos violados; decisões individuais de caráter não-automatizado; conservação dos dados apenas no tempo estritamente necessário para a finalidade; restrições às transferência dos dados a outras autoridades que não tenham competência em matéria de luta contra o terrorismo e a criminalidade grave; e restrições a transferências ulteriores para países terceiros.

Dando continuidade à abordagem global relativa à transferência dos dados do PNR, em 11 novembro de 2010, o Parlamento Europeu lança a "Estratégia externa da UE relativamente aos dados dos registos de identificação dos passageiros (PNR)". Nesta estratégia, o Parlamento relembra a importância em combater o terrorismo e a criminalidade transnacional, mas sem mitigar a proteção das liberdades cívicas e dos direitos fundamentais.

Neste contexto, é chamada a atenção para que fossem respeitados os arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia e o art. 8.º da Convenção Europeia dos Direitos Humanos, apontando ainda a base jurídica da legislação europeia a ser criada nesta matéria, designadamente o art. 16.º do Tratado de Funcionamento da União Europeia, cujo texto remete para o art. 39.º do Tratado da União Europeia. Ainda, ressalta que a necessidade e a proporcionalidade são princípios que devam estar consagrados nos acordos, bem como medidas políticas em matéria de proteção de dados, mostrando-se contrário a ações que utilizem as informações transmitidas no sentido de "prospeção de dados" ou "determinação de perfis".

V. Apesar de todos os avanços legislativos e estratégicos desenvolvidos no ano de 2010, apenas a 14 de abril de 2016 é que foi aprovada, com emendas, a Resolução Legislativa do Parlamento Europeu sobre a "Utilização dos Dados dos Registos de Identificação dos Passageiros (PNR)[16]". A Diretiva UE-PNR 2016/681, do Parlamento Europeu e do Conselho, foi publicada em 27 de abril de 2016, sobre a utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

No Considerando (7) da Diretiva mencionada, defende-se que o resultado da avaliação dos dados do PNR permite a identificação de suspeitos de infrações terroristas ou criminalidade grave antes que pratiquem o ato. Daí a importância do uso deste método para fins policiais. No entanto, o uso dos dados do PNR para identificar indivíduos para fins deteção e repressão ao terrorismo e à criminalidade grave não poderá ultrapassar os objetivos da Diretiva.

Assim, no art. 1.º prevê-se que as transportadoras aéreas deverão transmitir os dados do PNR de voos extra-UE e que estes dados serão recolhidos, tratados, utilizados e conservados pelos Estados-Membros, que deverão trocar entre si informações dos resultados obtidos. Importa ainda verificar que, no art. 2.º, a Diretiva não afasta a obrigação de transferência de dados

---

[16] Resolução legislativa do Parlamento Europeu, sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, P8_TA-PROV (2016) 0127, de 14 de junho de 2016.

do PNR também de voos intra-UE, sob notificação prévia por escrito dos Estados-Membros à Comissão.

Nos termos do art. 4.º, estabelece-se que cada Estado-Membro deverá criar ou designar uma autoridade capaz de cumprir com os objetivos da Diretiva, a qual será nomeada de "Unidade de Informações de Passageiros" (UIP). A constituição da UIP, que poderá representar um ou mais EM, deverá ser notificada à Comissão no prazo de um mês após a sua constituição. Um responsável de proteção de dados será designado pela UIP, tendo como competência o controlo do tratamento dos dados do PNR e a aplicação das salvaguardas relevantes durante a atuação da Unidade. No caso de considerar que os dados do PNR não estão a ser tratados em conformidade com a lei, o citado responsável pela proteção de dados poderá informar a autoridade nacional de controlo.

O art. 9.º da Diretiva, por sua vez, estabelece em que termos ocorrerá a troca de informações entre os Estados-Membros. Tendo por base o disposto no n.º 6 do art. 6.º, os Estados-Membros ficam obrigados a transmitir às UIP's dos outros Estados os dados de PNR, ou o resultado do tratamento destes, sobre as pessoas já identificadas como prováveis terroristas ou criminosos de elevada gravidade, a fim de que as autoridades competentes nacionais possam ser informadas pelas Unidades sobre estes indivíduos. Contudo, tal ação apenas pode ser realizada após análise individualizada e não automatizada dos dados, de forma a assegurar o respeito pelas pessoas que se encontrem identificadas devido à suspeita das atividades criminosas objeto da Diretiva.

Outrossim, a UIP de um Estado-Membro poderá solicitar acesso aos dados do PNR ainda não encriptados a outras UIP's, mediante pedido fundamentado em um caso específico, com o fim de que encontrar maiores indícios no âmbito de uma investigação que vise prevenir, detetar ou repreender infrações terroristas ou de criminalidade grave. As autoridades competentes nacionais não estão completamente impedidas de realizar a requisição de dados de PNR diretamente às UIP's de outros Estados-Membros, mas apenas poderão fazê-lo em caso de emergência, sendo a UIP nacional informada do pedido direto por meio de uma cópia do requerimento. Apesar de deixar claro que o procedimento normal será requerer o acesso das informações de passageiros à UIP nacional, que fará o papel de mediadora com as suas congéneres nos outros Estados-Membros, a

Diretiva não esclarece o que seriam os chamados "casos de emergência", deixando esta tarefa ao legislador nacional.

A Agência da União Europeia responsável por garantir o cumprimento da lei, conhecida pela abreviação "Europol", está também habilitada a requerer diretamente às UIP's dados de PNR, nos termos do art. 10.º da Diretiva. Este requerimento deverá ser fundamentado e claro, de modo a evidenciar o "contributo substancial" das informações do PNR à prevenção, deteção ou investigação de uma infração a ser inspecionada pela Agência, nos limites de sua competência. A Europol, no entanto, está obrigada a comunicar ao responsável pela proteção de dados do Estado-Membro da UIP que contactar a fim de obter dados de um PNR.

Vale destacar que as transferências de dados de PNR efetuadas pelas companhias aéreas, conforme estabelece o art. 16.º, devem ocorrer por via eletrónica e oferecer garantias suficientes de segurança. Inclusive, em caso de avarias, a modalidade de envio poderá alterar-se, mas as garantias de seguranças devem permanecer. Contudo, está prevista a adoção de protolocos a respeito dos formatos de dados que serão reconhecidos para a transferência de todos os dados de PNR após um ano da data que a Comissão vier a adotar. Novamente, caberá ao Estado-Membro viabilizar os meios para que os protocolos sejam implementados e utilizados.

VI. Antes de passarmos a uma análise da transferência destes dados face à proteção de dados pessoais, importa trazer à baila a disposições finais constantes na Diretiva UE-PNR, de 27 de abril de 2016. O prazo para os Estados-Membros transporem a Diretiva para o seu direito interno é até 25 de maio de 2018. É previsto um reexame de todos os elementos da Diretiva é 25 de maio de 2020 pela Comissão, que apresentará um relatório ao Parlamento Europeu e ao Conselho com base nas informações prestadas pelos Estados-Membros anualmente, os quais comunicam as estatísticas sobre os dados de PNR comunicados às UIP's.

Especificamente sobre o Relatório da Comissão, é relevante mencionar que o reexame, nos termos do n.º 2 do art. 19.º, deve ter atenção especial ao cumprimento das normas aplicáveis de proteção de dados pessoais; à necessidade e proporcionalidade da recolha e do tratamento dos dados de PNR; à duração do prazo de conservação dos dados; à eficácia do intercâmbio de informações com os Estados-Membros; e, à qualidade das avaliações, nomeadamente as estatísticas fornecidas.

No que toca à relação da Diretiva UE-PNR com outros instrumentos, o art. 21.º estabelece que os Estados-Membros podem continuar a aplicar acordo e/ou convénios que façam parte em matéria de intercâmbio de informações entre si e/ou com Estados-terceiros. Não obstante, ressalva que a aplicação de tais instrumentos não pode prejudicar o que está previsto em matéria de proteção de dados pessoais. Este tema será abordado com mais detalhes no tópico que se segue.

2. A Diretiva UE-PNR e o Regulamento de Proteção de Dados Pessoais: convergências e incongruências

Desde que os dados do PNR passaram a ser usados como fonte de informação para prevenir, detetar e investigar eventuais suspeitos de terrorismo ou criminalidade grave, já se evidenciava a violação do direito de proteção de dados pessoais dos passageiros cujas informações seriam transferidas aos Estados. De facto, esta foi uma das razões – talvez a principal – que motivou o adiamento de um ato legislativo europeu sobre o PNR, mas que acabou por efetivar-se em prol de um almejado ambiente de segurança no ELSJ.

Segundo Niovi Vavoula[17], a Diretiva relativa a dados de identificação dos registos de identificação dos passageiros, mesmo antes da sua aplicação, já esbarra em dois direitos: respeito pela vida privada e familiar e a proteção dos dados pessoais. O primeiro direito encontra-se no art. 7.º da Carta dos Direitos Fundamentais da União Europeia e no art. 8.º da Convenção Europeia dos Direitos Humanos, encontrando-se nesta última a exceção na qual se vislumbra a interferência de autoridade pública quando estabelecido por lei e na defesa da segurança nacional, segurança pública e no bem-estar económico do Estado[18].

---

[17] Vavoula, Niovi. "I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive", *EU Immigration and Asylum Law and Policy*, 2016. Disponível em: <http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/> (acedido a 5/12/2017).

[18] CEDH, Convenção Europeia dos Direitos Humanos, n.º 2 do art. 8.º. "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".

No entanto, a mencionada autora chama a atenção para o facto de que as informações a disponibilizar pelas companhias aéreas permitirão às autoridades traçar um perfil de cada viajante e de sua família apenas sob suspeita de eventual ligação com atividades ligadas ao terrorismo e à criminalidade grave. Por isso, não parece que a segunda parte do artigo citado venha a justificar de uma forma clara e objetiva esta atuação europeia.

Trazendo ao debate o considerando (1) do Regulamento de Proteção de Dados, deste dispositivo consta que a "proteção de dados de pessoas singulares relativamente ao tratamento de dados pessoas é um direito fundamental". Ainda, o mesmo Regulamento estabelece no considerando (2) que esse direito subsiste e aplica-se "independentemente da nacionalidade ou do local de residência dessas pessoas".

Neste sentido, a Diretiva UE-PNR enuncia, nos termos do n.º 1 do art. 13.º, que os Estados-Membros devam assegurar a todos os passageiros "o mesmo direito à proteção dos seus dados pessoais, os direitos de acesso, retificação, apagamento e limitação". Os Estados-Membros também estão obrigados a garantir o respeito pela confidencialidade e pela segurança dos dados e do tratamento dos mesmos, devendo evitar que indivíduos sejam discriminados devido à sua origem étnica, opiniões políticas, religião, convicção filosófica, filiação sindical, saúde, vida ou orientação sexual.

Ainda, devem os Estados executar medidas que garantam a manutenção e a sistematização do trabalho desenvolvido pelas suas respetivas UIP's, de modo a reter a documentação sobre, nos termos das alíneas do n.º 5 do art. 13.º: o nome e os contactos da organização e do pessoal da UIP a quem confiar o tratamento de dados dos PNR, bem como os diferentes níveis de acesso; os pedidos apresentados pelas autoridades competentes e pelas UIP's de outros Estados-Membros; e, todos os pedidos e transferências de dados PNR para um país terceiro.

É de salientar que a UIP poderá disponibilizar, se requerido, a documentação à autoridade de controlo nacional. Ainda, cabe aos Estados-Membros assegurar que, face a uma violação de dados pessoais de elevado risco para a proteção de dados pessoais ou dano para a privacidade do titular dos dados, as UIP's deverão comunicar àquele e à autoridade de controlo o ocorrido.

Nos termos do art. 11.º, os Estados-Membros apenas poderão enviar os dados de PNR, ou o resultado do seu tratamento, a países terceiros desde que, segundo a alínea a) do n.º 1 do art. indicado, preencham as seguintes condições estabelecidas no art. 13.º da Decisão-Quadro 2008/977/JAI, de

28 de novembro: tal seja necessário para a prevenção, investigação, deteção ou repressão de infrações penais ou para a execução de sanções penais; a autoridade recetora no Estado terceiro ou o organismo internacional de receção seja responsável pela prevenção investigação, deteção ou repressão de infrações penais ou pela execução de sanções penais; o Estado-Membro que forneceu os dados tenha consentido na transferência, de acordo com a sua legislação nacional; e que o Estado terceiro ou o organismo internacional em causa assegurem um nível de proteção adequado para o tratamento previsto dos dados.

Somam-se a estas condições, a necessidade de que a transferência de dados de PNR se coadune com o objetivo da Diretiva UE-PNR e o compromisso de que o país terceiro recetor das informações apenas transmitirá os dados recebidos para um outro Estado, caso seja estritamente necessário e mediante notificação do Estado-Membro europeu que lhe tenha transmitido os dados de PNR. É possível, todavia, que seja realizada a transferência de informações para um Estado terceiro diferente daquele que recebeu os dados de PNR sem autorização prévia do Estado-Membro que facultou as tais informações, desde que esta transferência seja essencial para responder a uma ameaça específica e concreta no que toca a infrações terroristas ou a criminalidade grave ou porque não foi possível obter em tempo útil tal autorização.

Em todo o caso, deverá sempre o responsável pela proteção de dados da UIP do Estado-Membro ser informado sobre as transferências de dados de PNR, sejam as que ocorrem entre Estados-Membros, sejam as destinadas a países terceiros, bem como as que são transferidas de países terceiros a outros interessados.

No caso específico dos Estados-Membros da UE, as transferências devem observar o Capítulo V do Regulamento de Dados Pessoais, que trata das transferências de dados pessoais para países terceiros ou organizações internacionais. De acordo com este capítulo, as transferências devem ter por base uma decisão de adequação, que constate o nível de proteção dos dados enviados, ou poderá ser sujeita a outras garantias consideradas adequadas, nomeadamente um instrumento juridicamente vinculativo e com força executiva, entre outras garantias citadas no n.º 2 do art. 46.º.

O Regulamento de Proteção de Dados também chama atenção para o consentimento necessário ao tratamento de dados de crianças. Contudo, a questão securitária parece ainda prevalecer e o consentimento expresso

parece sucumbir à obrigação de que todos os dados de PNR nas rotas indicadas na Diretiva devem ser enviados às UIP's.

Importa ainda indicar que no Plano de Implementação da Diretiva[19], sobre a transposição da Diretiva UE-PNR, prevê-se que um dos desafios na implementação das normas relativas à transferência de dados de PNR é a experiência seja dos Estados-Membros, seja de Estados-terceiros, no que toca aos recursos, tempo e complexidade técnica para adaptação dos sistemas de PNR. Por isso, além da própria transferência, há dificuldades relativas à introdução e ao uso dos sistemas pelas autoridades responsáveis.

Outro artigo da Diretiva UE-PNR que merece destaque é o 12.º, designadamente o prazo de conservação e anonimização dos dados do PNR. As UIP's dos Estados-Membros devem conservar nas suas bases de dados as informações recebidas das companhias aéreas por um prazo máximo de cinco anos, a contar da data em que a transferência foi recebida pela UIP. No entanto, seis meses após o recebimento dos dados de PNR, esses deverão ser anonimizados, através do mascarar de algumas das informações constantes nos dados recebidos, tais como: nome, morada, contactos, forma e dados de pagamentos, número de passageiro frequente, eventuais dados de API e observações que permitam identificar o passageiro.

Tenha-se em mente que não é totalmente vedado o acesso às informações integrais do PNR após o decurso dos seis meses, mas para tanto será necessária uma motivação razoável, bem como uma autorização, que poderá ser emitida por autoridade judiciária ou por outra autoridade nacional competente. Neste último caso, também será obrigatório informar o responsável de proteção de dados sobre o referido acesso, a fim de que este possa realizar uma verificação *ex post* da situação.

Decorridos os cinco anos, as informações do PNR deverão ser apagadas definitivamente do banco de dados das UIP's.

Sublinhe-se novamente o art. 13.º, que liga expressamente a Diretiva UE-PNR ao Regulamento de Proteção de Dados Pessoais, referindo a obrigação dos Estados-Membros em assegurar a igualdade no tratamento de dados de todos os passageiros, assim como os direitos advindos do uso de tais dados, tal como a proteção dos dados pessoais, o acesso, a retificação, apagamento e limitação. Este artigo estabelece que fica a cargo também

[19] Commission Staff Working Document SWD (2016) 426 final, de 28 de novembro de 2016.

dos Estados-Membros estabelecer uma autoridade nacional de controlo que terá como responsabilidade aconselhar e monitorar a aplicação das normas nacionais provenientes da Diretiva UE-PNR. Caberá a esta autoridade, nos termos do n.º 3 do art. 15.º, as seguintes funções, entre outras: analisar as reclamações apresentadas por qualquer titular de dados, verificar a legalidade no tratamento dos dados e proceder a auditorias, nos termos nas legislações nacionais.

O que não parece claro é quais serão os meios a utilizar para garantir os tais níveis de segurança adequados aquando das transferências de dados de PNR, em especial para países terceiros. VanWasshnova[20] aborda esta questão quando compara os conflitos que emergem em matéria de proteção de entre os Estados Unidos e a União Europeia. Destaca o autor que enquanto a UE tenta limitar a quantidade de informações a serem transmitidas a fim de garantir a proteção dos dados pessoais, os EUA requerem uma transferência irrestrita. No entanto, a limitação da informação recebida pela UE e pelos seus Estados-Membros não garante a proteção completa destes dados, muito menos a criação de perfis, visto que apenas o nome de um passageiro e o trajeto de sua viagem poderão implicar, por si sós, em um perfil, indo de encontro ao estabelecido no art. 22.º do Regulamento de Proteção de Dados.

Nesta mesma perspetiva, Gavin Robinson[21] critica o uso de dados do PNR para os fins supra identificados, pois permitem criar perfis e aplicar processos de *data mining*, que não identificam criminosos ou terroristas, mas apenas antecipam possíveis ações criminosas, que podem não ter relação com o terrorismo ou a criminalidade grave. No que se refere ao equilíbrio entre privacidade e segurança, Georgio Nouskalis[22] chama a atenção para

---

[20] Vanwasshnova, Mattheew R. "Data Protection Conflicts between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange", *Case Western Reserve Journal of International Law (JIL),* vol. 39, 2008, p. 827.

[21] Robinson, Gavin. "Data protection reform, passenger name record and telecommunications data retention: – Mass Surveillance Measures in the E. U. and the Need for a Comprehensive Legal Framework", *Critical Quarterly for Legislation and Law/Revue critique trimestrielle de jurisprudence et de législation,* vol. 95, n.º 4, 2012, pp. 394-416.

[22] Nouskalis, Georgio. "Biometrics, e-identity, and the balance between security and privacy: case study of the passenger name record (PNR) system", *ScientificWorldJournal*, n.º 11, 2011 march 1, pp. 474-477.

a mitigação do princípio da presunção de inocência, analisando o facto de que a partir da Diretiva UE-PNR a maioria das pessoas poderia ser considerada suspeita de crimes, o que permitirá um contínuo Estado de Exceção, cujo fundamento seria a luta contra o terrorismo.

Soma-se à questão do uso de dados de PNR como método de prevenção do terrorismo e da criminalidade grave outro problema: e quando uma pessoa tem os seus dados pessoais utilizados para a compra de bilhetes sem a sua autorização prévia, como nos casos de fraudes a cartões de crédito ou *hacking*? Domingues & Al.[23], apresentaram um estudo sobre o Sistema de Distribuição Global (GDS – *Global Distribution System*), uma plataforma bastante avançada para criação e gestão de reservas de viagem, ambiente em que se criam os PNR's. Os autores afirmam que, mesmo diante dos avanços referentes aos sistemas de segurança e informação, ainda hoje a plataforma GDS não está imune a ações fraudulentas, que buscam obter informações indevida ou mesmo alterar informações constantes no sistema.

Por fim, deve-se ter em conta não apenas os aspetos relativos ao Estado e aos titulares dos dados, mas também o impacto que a Diretiva em análise terá na prática laboral das companhias aéreas, sendo este tópico analisado de seguida.

3. As companhias aéreas e a transferência de dados dos passageiros: o que mudará na prática?

Nos termos do art. 3.º da Diretiva UE-PNR, transportadora aérea é "uma empresa de transporte aéreo titular de uma licença de exploração válida ou equivalente que lhe permite transportar passageiros por via aérea".

No mercado da aviação civil, todavia, nem sempre a transportadora aérea é a companhia responsável pela venda do bilhete. A transportadora é aquela responsável pelo cumprimento do objeto do contrato de transporte, ou seja, a viagem. No entanto, por uma questão comercial, as companhias

---

[23] Domingues, Rémi *et al*. An application of unsupervised fraud detection to Passenger Name Records", *46th Annual Conference IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, 2016. Disponível em: <http://www.eurecom.fr/fr/publication/5058/download/data-publi-5058.pdf> (acedido a 28/11/2017).

unem-se e fazem contratos entre si, que podem ser bilaterais ou em aliança com diversas transportadoras. Assim, uma companhia aérea poderá vender um bilhete cujo voo não operará por si mesma ou com a sua tripulação, sendo o agente comercial de venda do transporte aéreo, por isso é nomeada de *Market Carrier.*

Esta explanação serve para indicar que a companhia aérea que vender o bilhete deverá ser a responsável por obter todos os dados pessoais do passageiro, visto que, mesmo não operando o voo, será aquela que criará o PNR no sistema, sendo a detentora das informações até ao embarque. No entanto, nos termos do art. 8.º da Diretiva, caberá à companhia que opera o voo informar os dados que constam do Anexo II. Tal informação poderá ser feita até o momento do *check-in*, mas não se pode deixar de assinalar que a possibilidade de atuar preventivamente para detetar eventuais criminosos poderá ser comprometida, tendo em consideração que o registo para embarque poderá ser feito alguns minutos antes do voo, diretamente no aeroporto.

Assim, será na transposição das regras europeias para as legislações nacionais que se poderá verificar o momento exato em que a obrigação de informar os dados de PNR deverão ser realizadas pelas companhias operadoras, devendo o legislador nacional ter conta os óbices técnicos e temporais para que as informações sejam enviadas em tempo útil. Isto especialmente na expectativa de que os dados do PNR serão efetivamente utilizados para prevenir o terrorismo e a criminalidade grave, evitando ferir e/ou denegrir a reputação de indivíduos por uma avaliação rápida e destoante da realidade das verdadeiras intenções de uma viagem.

Neste contexto, a Diretiva traçou prazos mais exatos para evitar diferenças temporais consideráveis referentes à obrigação de transmissão dos dados dos passageiros. Nos termos do n.º 3 do art. 8.º, as transportadoras transferem os dados do PNR, sob "um nível adequado de segurança": a) 24 a 48 horas antes da hora programada da partida do voo; e b) imediatamente após o encerramento do voo. Entretanto, nos termos do direito nacional, as companhias aéreas poderão enviar informações de dados de PNR noutro momento e não apenas as especificadas anteriormente, "caso a caso e mediante pedido apresentado por uma UIP".

Importa verificar ainda, neste momento anterior à data limite para a transposição, que nos termos do art. 7.º, os Estados-Membros devem adotar

uma lista na qual designarão quais as autoridades habilitadas a solicitar das UIP's e receber destas informações sobre os dados de PNR ou os resultados advindos do tratamento dos mesmos. Assim, as companhias aéreas deixam de ter a obrigação de fornecer diretamente às autoridades competentes as informações necessárias a fundamentar um procedimento policial ou investigatório. A obrigação subjaz, portanto, em transmitir os dados de PNR à UIP, que será a responsável por analisar e conservar os dados, atuando como base das informações relativas aos passageiros.

Deve-se salientar, no entanto, que tal obrigação não prejudica a competência das autoridades policiais e judiciárias, designadamente de atuação face a indícios de outras infrações, que não o terrorismo e a criminalidade grave.

Outra questão que se deve ter em atenção é a existência de, até ao momento, seis tipos diferentes de programas de reservas, sendo alguns incompatíveis entre si. Nos aeroportos, os computadores costumam funcionar com um programa universal que tenta convergir as informações dos passageiros. Contudo, a criação de vários departamentos com diversas pessoas a utilizar este mecanismo é um investimento vultuoso para as companhias aéreas. Tendo em consideração este alto investimento e procurando evitar o incumprimento das companhias sob esta fundamentação, a Diretiva, de acordo com enunciado no n.º 1 do art. 8.º, prevê que os Estados-Membros devem adotar as medidas consideradas necessárias para que as companhias sejam capazes de transferir pelo método de exportação os dados do PNR às UIP's e, em combinação com o previsto no Considerando n.º 14, os Estados-Membros deverão suportar os custos da utilização, conservação e do intercâmbio de dados de PNR.

Relativamente à transferência de dados para as UIP's, merece também destaque que os voos que incluam escalas na sua rota obrigam as companhias aéreas a transferir os dados de todos os passageiros a todas as UIP's dos Estados-Membros por onde o passageiro passará. O mesmo será aplicável aos voos intra-UE, no caso dos Estados-Membros que exigirão também receber informações referentes a este tipo de viagem.

Diga-se também que as sanções relativas a não ou má-aplicação das regras nacionais, após transposta a Diretiva UE-PNR, serão estabelecidas pelos Estados-Membros, que também se obrigam a assegurar a aplicação das normas. Conforme estabelecido no texto do art. 14.º, "as sanções previstas devem ser efetivas, proporcionadas e dissuasivas".

Relativamente a este ponto, a Associação das Companhias Aéreas Regionais Europeias[24] esclareceu, por meio de um comunicado, que os dados de API e de PNR estão localizados em diferentes sistemas. Por esta razão, a exportação desses dados pode demorar de 3 a 6 meses para um pedido das informações de um API, e de 6 a 12 meses transferência de um PNR. Portanto, além dos custos associados, a rapidez não é apenas uma questão de vontade ou não em aplicar as normas, mas também do desenvolvimento tecnológico que vá ao encontro das expectativas criadas relativas aos sistemas de reserva de viagens.

Avizinham-se outras questões técnicas e económicas ligadas às transferências de dados de PNR após as transposições. A título de ilustração, podem-se citar eventuais falhas nas transferências dos dados, ocasionando a chegada de informações incompletos à UIP, bem como a fechamento ou falência de companhias aéreas de pequeno porte que não consigam arcar com o investimento tecnológico e humano para transferir dados de PNR para a UIP. Uma nova análise sobre o impacto à prática laboral das companhias aéreas será certamente um tópico que importará uma nova análise no futuro.

Considerações Finais

A escolha dos dados PNR's transferidos, em detrimento dos API, já demonstra a quantidade de informação que se pode aferir a partir desses dados. Contudo, é verdade também que a transferência das informações de PNR obtidas pelas companhias aéreas não garante que tais dados sejam corretos e idóneos.

Destacam-se, portanto, duas questões que foram debatidas no presente texto: a capacidade de identificar e prevenir terroristas, sem que tal constitua uma discriminação de grupos ou indivíduos; e a garantia do tratamento adequado dos dados, seja pela companhia, seja pelos Estados-Membros, seja ainda pelos países terceiros.

---

[24] ERA, European Regions Airlines Association, API-PNR, de 14 de dezembro de 2016. Disponível em: <http://www.eraa.org/policy/security/advance-passenger-information-api--and-passenger-notifications-records-pnr> (acedido a 3/12/2017).

A possibilidade de que inocentes sejam identificados erroneamente como eventuais criminosos ou terroristas é um facto já reconhecido pela Diretiva UE-PNR, bem como a abertura a que outros Estados requeiram reciprocidade no tratamento de dados. No entanto, o que ainda não é evidente é se a transposição e a aplicação das normas contidas na Diretiva em análise serão realizadas em conformidade e respeito pelo Regulamento de Proteção de Dados, que se coaduna com as normas de direitos fundamentais referidas ulteriormente.

A certeza, por agora, é que as companhias aéreas poderão incorrer diversas vezes em sanções, de carácter primordialmente pecuniário, para que cumpram normas que, até ao momento, não se sabe se serão transpostas a tempo e com a mesma ordem que foi estabelecida pelo ato legislativo europeu, a Diretiva UE-PNR.

Ademais, a validade da Diretiva poderá ser objeto de apreciação pelo Tribunal de Justiça da União Europeia, o qual já se pronunciou anteriormente, aquando da análise da Diretiva de Retenção de Dados[25], que a prevenção ao terrorismo não seria suficiente para mitigar a proteção e a inviolabilidade dos dados pessoais. Destaca-se ainda que, em 26 de julho 2017, o TJ proferiu parecer[26] no sentido de considerar a incompatibilidade do acordo entre o Canadá e a UE, sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros, com os arts 7.º, 8.º, 21.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia "na medida em que não exclui a transferência de dados sensíveis da União Europeia para o Canadá nem a utilização e a conservação desses dados".

Por fim, apesar de a data limite para a transposição da Diretiva UE-PNR aos direitos nacionais ser 25 de maio de 2018, pouco debate sobre o tema tem ocorrido nos meios sociais e comerciais. Contudo, é percetível a relevante preocupação nestes meios no que toca ao Regulamento de Proteção de Dados, que será aplicável a partir da mesma data limite para a transposição da Diretiva UE-PNR.

---

[25] Acórdão do TJ, C-293/12, *Digital Rights Ireland*, de 8 de abril de 2014 e processos apensos C-293/12 e C-594/12.

[26] Acórdão do TJ, 2017/C 309/03, "Projeto de acordo entre o Canadá e a União Europeia", Parecer 1/15 (Grande Secção), de 26 de julho 2017.

Índice Geral

O Anuário do Direito da Proteção de Dados Pessoais é uma revista jurídica de livre acesso, disponível em linha no sítio http://protecaodedadosue.cedis.fd.unl.pt/, que pretende divulgar estudos doutrinários sobre o direito à proteção de dados pessoais. O Anuário é editado pelo Observatório para a Proteção de Dados Pessoais, grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa. Aberto a qualquer interessado, o Observatório integra atualmente oito investigadores (dois doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

A edição de 2018 do Anuário do Direito da Proteção de Dados Pessoais reúne, no essencial, textos apresentados no Workshop "O novo regulamento de proteção de dados pessoais", realizado na Faculdade de Direito da Universidade Nova de Lisboa a 15 de dezembro de 2016.

Jurisnova
Associação da Faculdade de Direito da Universidade Nova de Lisboa

SRS ADVOGADOS

visionware
we secure your assets