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.