DOI 10.5380/rfdufpr.v61i3.48085

DO DIREITO A ESTAR SÓ AO DIREITO AO ESQUECIMENTO. CONSIDERAÇÕES SOBRE A PROTEÇÃO DE DADOS PESSOAIS INFORMATIZADOS NO DIREITO DA UNIÃO EUROPEIA: SENTIDO, EVOLUÇÃO E REFORMA LEGISLATIVA

FROM THE RIGHT TO BE LET ALONE TO THE RIGHT TO BE FORGOTTEN. CONSIDERATIONS ON THE PROTECTION OF COMPUTERIZED PERSONAL DATA IN THE EUROPEAN UNION LAW: MEANING, EVOLUTION, AND LEGISLATIVE REFORM

Alessandra Silveira[*]
João Marques[**]

RESUMO
O direito à privacidade (originariamente reconhecido como o direito a estar só) sofreu consideráveis desenvolvimentos desde as suas primeiras referências doutrinárias nos EUA do séc. XIX – e já não se compadece integralmente com as necessidades de proteção de internautas que definitivamente não querem estar sós, mas querem ter o direito a ser esquecidos. O tratamento de dados pessoais e sua livre circulação no espaço da União Europeia é regulado pela Diretiva 95/46, de 24 de outubro de 1995. Este ato jurídico europeu *i*) obriga os Estados-Membros à adoção de garantias semelhantes em todo o espaço da União e *ii*) estipula procedimentos-regra quanto ao fluxo de dados pessoais para países terceiros. Foi, sem dúvida, uma referência mundial naquela matéria, especialmente por ter entrado em vigor num período em que os riscos associados às tecnologias da informação ainda não eram evidentes. Contudo, o crescente recurso a meios eletrónicos desatualizou as garantias entretanto previstas contra o tratamento e a utilização abusiva de dados pessoais informatizados. Por isso, a partir de 2018, a matéria da proteção de dados pessoais será disciplinada noutros termos na União Europeia. O presente texto procura *i*) captar o sentido e a evolução do direito à proteção de dados pessoais informatizados no direito da União, sobretudo a partir da jurisprudência do Tribunal de Justiça da União Europeia, assim como *ii*) perspectivar as principais alterações decorrentes da aplicação do novo pacote legislativo de proteção de dados pessoais no espaço da União e, nesta medida, o futuro daquele direito fundamental na Europa.

PALAVRAS-CHAVE
Dados pessoais informatizados. Internet. União Europeia. Direitos fundamentais. Tribunal de Justiça da União Europeia.

ABSTRACT
The right to privacy (originally known as the right to be let alone) was subject to considerable developments since the first legal writings in the USA of the 19th century – and can no longer respond fully to the protection needs of the Internet users who definitely do not want to be let alone but want to have the right to be forgotten. The processing and free movement of personal data in the European Union are regulated by Directive 95/46, of October, 24, 1995. This European legal act *i*) obliges the

[*] Diretora do Centro de Estudos em Direito da União Europeia (CEDU), Universidade do Minho (Braga, Portugal). Titular da Cátedra Jean Monnet em Direito da União Europeia (concedida pela Comissão Europeia, Bruxelas). *E-mail*: asilveira@direito.uminho.pt
[**] Advogado e Vogal da Comissão Nacional (Portuguesa) de Protecção de Dados (Lisboa, Portugal). *E-mail*: joao.marques@cnpd.pt

Member-States to adopt similar safeguards across the entire area of the European Union and *ii*) stipulates the same procedures related to the flow of personal data to third counties. It was, without doubt, a world reference in that domain, especially since it has entered into force when the risks associated to the information technology were not obvious. However, the increasing use of electronic facilities outdated the safeguards laid down by the law against the treatment and misuse of the computerized personal data. For this reason, from 2018 the personal data protection will be regulated on the basis of other terms in the European Union. This text aims to *i*) grasp the meaning and evolution of the protection of computerized personal data in the EU law, especially through the case-law of the Court of Justice of the European Union, as well as *ii*) address the main changes resulting of the application of the new legislative package on personal data protection in the European Union and, to this extent, the future of that fundamental right in Europe.

KEYWORDS
Computerized personal data. Internet. European Union. Fundamental rights. Court of Justice of the European Union.

INTRODUÇÃO. COMPETÊNCIA REGULATÓRIA DA UNIÃO EUROPEIA E NATUREZA JUSFUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS

A competência da União Europeia (UE) para regular a matéria relativa à proteção de dados de carácter pessoal está patente no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e relaciona-se com o adequado funcionamento do mercado interno. Ou seja, a competência para o estabelecimento de normas relativas à proteção de dados decorre da necessidade de fazer circular informações pessoais entre os Estados-Membros, sendo uma consequência do bom funcionamento de um mercado interno e do aumento do fluxo transfronteiriço de dados – que acompanha a livre circulação de pessoas, mercadorias, serviços e capitais. Nos termos do artigo 16.º, n.º 1, do TFUE, "Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito." E decorre do artigo 16.º, n.º 2, do TFUE, que o Parlamento Europeu e o Conselho estabelecem normas relativas à proteção das pessoas singulares no que diz respeito *i*) ao tratamento de dados pessoais pelas instituições, órgãos e organismos da UE, bem como pelos Estados-Membros em aplicação do direito da União[1] e *ii*) à livre circulação desses dados entre os Estados-Membros e à garantia de um nível de proteção adequado para a transferência de dados pessoais para países terceiros.

Trata-se de uma competência partilhada com os Estados-Membros no domínio do mercado

[1] Com exceção da matéria relativa à política externa e de segurança comum (PESC) que, nos termos do artigo 39.º do Tratado da União Europeia, admite normas próprias *no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros*, constituindo uma base jurídica especial relativamente à base jurídica geral do artigo 16.º do TFUE. Em derrogação do processo legislativo ordinário, no domínio da PESC o Conselho adota, por unanimidade, normas relativas ao tratamento de dados pessoais pelos Estados-Membros, tendo em conta a reserva tradicional que preside às práticas diplomáticas nacionais.

interno [artigo 4.º, n.º 2, alínea *a)*, do TFUE] cujo exercício, tal como resulta do artigo 2.º, n.º 2, do TFUE, preclude/inibe a iniciativa legislativa dos Estados-Membros. Assim, no âmbito de competências partilhadas entre a UE e os seus Estados-Membros, ambos podem legislar e adotar atos juridicamente vinculativos naquele domínio – porém os Estados-Membros só exercem a sua competência na medida em que a UE não tenha exercido a sua, e só voltam a exercê-la na medida em que a UE decida deixar de exercer a sua. Ora, como a UE exerceu (e exerce, cada vez mais) a sua competência no domínio do tratamento de dados pessoais e da sua circulação, a proteção de dados no espaço da UE é regulada pelo direito da União. As normas nacionais que hoje (ainda) disciplinam a proteção de dados nos distintos Estados-Membros da UE (no caso português, a Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto – Lei da Proteção de Dados Pessoais, doravante LPDP) são normas de transposição de diretivas europeias – que devem ser interpretadas e aplicadas segundo critérios definidos pelo direito da União.

Contudo, como veremos no decorrer deste texto, a partir de 25 de maio de 2018, e por conta da entrada em vigor de um pacote legislativo recentemente publicado no Jornal Oficial da União Europeia, a matéria que nos ocupa será disciplinada noutros termos, sobretudo por meio de um distinto instrumento normativo europeu – o regulamento. No âmbito das suas competências partilhadas, a UE adota regulamentos e diretivas (atos jurídicos europeus previstos no artigo 288.º do TFUE), residindo a diferença entre ambos no facto de que as diretivas apenas harmonizam as normas aplicáveis nos distintos Estados-Membros da UE, enquanto os regulamentos uniformizam o direito aplicável num dado domínio, sem necessidade de intermediação legislativa das autoridades nacionais. Não é propriamente árduo perceber que só uma proteção equivalente em todos os Estados-Membros, garantida por uma legislação inicialmente harmonizada (e agora tendencialmente uniformizada) em todos os Estados-Membros, poderia assegurar a livre circulação de dados no mercado interno.

Ora, a Diretiva 95/46 (que regula o tratamento de dados pessoais e a sua circulação no espaço da UE até que as novas normas sejam aplicáveis em maio de 2018) veio responder a esta necessidade ao *i*) obrigar os Estados-Membros à adoção de garantias semelhantes em todo o espaço da UE no domínio da proteção de dados pessoais e *ii*) estipular procedimentos-regra quanto ao fluxo de dados pessoais para países terceiros – tendo sido uma referência mundial naquela matéria, especialmente por ter entrado em vigor num período em que os riscos associados às tecnologias da informação ainda não eram evidentes. O âmbito material da Diretiva 95/46 é limitado ao mercado interno, não se aplicando ao domínio da cooperação judiciária e policial em matéria penal (artigos 82.º e seguintes do TFUE), e por isso a Decisão-Quadro 2008/97/JAI completa a referida diretiva em matéria penal. Como a diretiva é endereçada aos Estados-Membros, foi adotado o Regulamento 45/2001, que

protege os dados pessoais relativamente ao uso que as instituições, órgãos e organismos da UE deles fazem, tendo sido inclusivamente criada uma Autoridade Europeia para Proteção de Dados. Para além da Diretiva 95/46 foram ainda adotadas diretivas sectoriais que a desenvolvem, designadamente a Diretiva 2002/22/CE (relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas), a Diretiva 2002/58 (relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas) – ambas alteradas pela Diretiva 2009/136 –, além da Diretiva 2003/31 (relativa ao comércio electrónico, dispondo inclusivamente sobre o correio eletrónico não solicitado – *spam*).

A propósito da competência da UE no domínio da proteção de dados pessoais há ainda um relevante elemento a considerar, qual seja, aquele que se prende com a força juridicamente vinculativa da Carta dos Direitos Fundamentais da União Europeia (CDFUE), em vigor desde dezembro de 2009. Teoricamente, as disposições da CDFUE não alargam as competências da UE tal como definidas nos Tratados, mas as disposições da Carta obrigam as instituições europeias e os Estados-Membros a respeitar e promover a aplicação dos direitos fundamentais nela previstos (artigo 51.º, n.º 1, da CDFUE). Seria, portanto, ingénuo pretender que a entrada em vigor da CDFUE não afeta o exercício das competências da UE. E a novidade, neste contexto, é que a CDFUE autonomiza o direito à proteção de dados pessoais (artigo 8.º) relativamente ao direito à proteção da vida privada (artigo 7.º). Para o direito da União, nem todos os dados pessoais são susceptíveis, pela sua natureza, de causar prejuízo à vida privada da pessoa em causa – mas devem ser igualmente protegidos.

Ora, isso traduz a relevância atribuída pelo direito da União ao direito fundamental à proteção de dados pessoais – como um direito distinto ou autónomo relativamente àquele da proteção da vida privada. O direito à privacidade (*privacy*), originariamente reconhecido como o direito a estar só (*the right to be let alone*), sofreu consideráveis desenvolvimentos desde as suas primeiras referências doutrinárias nos EUA do séc. XIX (WARREN; BRANDEIS, 1890) – e já não se compadece integralmente com as necessidades de proteção de internautas que definitivamente não querem estar sós, mas querem ter o direito a ser esquecidos. Por conseguinte, a CDFUE dá um passo adiante em relação a várias Constituições dos Estados-Membros da UE e em relação à Convenção Europeia dos Direitos do Homem (CEDH) no domínio da proteção de dados, na medida em que consagra um direito fundamental que protege dados que não têm de ser privados e muito menos íntimos – basta que sejam pessoais.

Ainda quanto aos direitos fundamentais, importa ressaltar algumas particularidades que envolvem a sua aplicação num contexto de interconstitucionalidade (SILVEIRA, 2016) como é aquele da UE. O modelo de proteção dos direitos fundamentais da UE baseia-se no seu

reconhecimento como princípios gerais do direito da União e no apelo a normas jusfundamentais de distintas fontes: normas de proveniência europeia (constantes dos Tratados constitutivos, e especialmente a CDFUE), normas de proveniência nacional (constantes das Constituições dos Estados-Membros e correspondentes às suas tradições constitucionais comuns) e normas de proveniência internacional relativas à proteção dos direitos humanos (sobretudo a CEDH que funciona, desde a década de 1970, como quadro de referência para a proteção dos direitos fundamentais na UE). Nada disso é alterado pela entrada em vigor da CDFUE – que agora se acrescenta, enquanto direito primário da União, à proteção existente. Nesse sentido, do artigo 6.º, n.º 3, do Tratado da União Europeia (TUE) deriva que do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a CEDH e como resultam das tradições constitucionais comuns aos Estados-Membros. Assim, quando uma situação jurídica é regida pelo direito da União, o padrão de jusfundamentalidade aplicável é o da UE. Mas o direito da União, por força do disposto no artigo 53.º da CDFUE, manda aplicar o nível de proteção mais elevado de entre os vários mobilizáveis para resolver a situação jusfundamental concreta. E é por isso que a proteção de dados pessoais, enquanto direito fundamental protegido também pelas Constituições dos Estados-Membros e pela CEDH, releva para a correta aplicação do direito da União[2].

Contudo, passados vinte anos da publicação da Diretiva 95/46 – durante os quais a dimensão jusfundamental da proteção de dados pessoais desenvolveu-se nos termos descritos –, fez-se necessário reequacionar o enquadramento legislativo da matéria. O desenvolvimento dos meios tecnológicos e o crescente recurso a meios eletrónicos desatualizaram as garantias previstas contra o tratamento e a utilização abusiva de dados pessoais informatizados. A reforma recentemente publicada, e amplamente discutida desde 2012, baseia-se em duas propostas legislativas da Comissão Europeia: *i*) um regulamento que estabelece o enquadramento geral da proteção de dados na UE e revoga a Diretiva 95/46 e *ii*) uma diretiva que estabelece normas sobre proteção de dados pessoais em matéria penal (relacionados com prevenção/investigação/detenção/prossecução/ execução penal) e que revoga a Decisão-Quadro 2008/97/JAI. Por isso o presente texto procura, num primeiro momento, *i*) captar o sentido e a evolução do direito à proteção de dados pessoais informatizados no direito da UE, sobretudo a partir da interpretação das disposições da Diretiva 95/46 pelo Tribunal de Justiça da União Europeia (TJUE) via incidente processual do reenvio prejudicial (artigo 267.º do

[2] Sobre o feixe de direitos que tende a densificar o moderno direito à autodeterminação informacional, previsto de forma pioneira no artigo 35.º da Constituição da República Portuguesa, cf. CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Constituição da República Portuguesa Anotada*, vol. I. Coimbra: Coimbra Editora, 2007.

TFUE), e, seguidamente, *ii*) perspectivar as principais alterações decorrentes da aplicação do novo pacote legislativo de proteção de dados pessoais, designadamente no que se refere ao Regulamento UE 2016/679, de 27 de abril de 2016 (Regulamento Geral sobre Proteção de Dados), que revoga a Diretiva 95/46, de modo a captar o futuro do regime jurídico da proteção de dados na Europa.

1 SENTIDO E EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS INFORMATIZADOS NO DIREITO DA UNIÃO À LUZ DA JURISPRUDÊNCIA DO TJUE

Decorre da jurisprudência assente do TJUE que a expressão *dados de carácter pessoal* corresponderia, no direito da União, a qualquer informação relativa a uma pessoa singular[3], identificada ou identificável, direta ou indiretamente. Ou seja, dados pessoais não são apenas aqueles que de forma direta possibilitam a identificação de uma pessoa (como seria o caso do número de identificação pessoal, do nome e do endereço), mas também aqueles dados que permitam chegar a essa identificação por associação de conceitos e conteúdos, mesmo que não se faça uma referência direta [como seria o caso do endereço IP (*Internet Protocol*) do computador com que se acede à rede] ou da matrícula de um veículo. Portanto, a título meramente exemplificativo, a doutrina identifica como dados pessoais o número de cliente de um estabelecimento comercial, o valor de uma retribuição, o som da voz registada para permitir o acesso a uma conta bancária, as classificações escolares, o *curriculum vitae*, a história clínica, as dívidas e os créditos, o registo de compras que alguém efetua, o registo dos meios de pagamento que utiliza, etc. – desde que, por estarem associados a uma pessoa, permitam identificá-la (CASTRO, 2013, p. 122).

Ora bem, esses dados pessoais são objeto de proteção quando sujeitos a qualquer operação ou tratamento efetuados com ou sem meios automatizados – até pode ser manual, desde que exista um ficheiro. O direito da União apenas exclui o tratamento de dados realizados por pessoas singulares no exercício de atividades domésticas, como seja uma lista de endereços para fins de correspondência (a lista de destinatários de cartões de Natal, por exemplo). O tratamento desses dados implica a sua recolha, registo, organização, conservação, adaptação, alteração, consulta, difusão (ou qualquer outra forma de disponibilização), bem como o bloqueio, o apagamento ou a destruição dos mesmos. E sempre independentemente da tecnologia utilizada – técnica de captação, transmissão, manipulação de dados (de som e imagem), etc. A obrigação de respeitar e garantir o exercício das várias dimensões

[3] Importa notar que no acórdão *Lindqvist*, de 6 de novembro de 2003, proc. C-101/01, considerando 98, o TJUE afirma que: "nada se opõe a que um Estado-Membro alargue o alcance da legislação nacional que procede à transposição da Diretiva 95/46 a domínios não incluídos no seu campo de aplicação, desde que nenhuma outra disposição do direito comunitário a tal obste". Ademais, algumas disposições constantes de diretivas sectoriais, como a Diretiva 2002/58, aplicam-se explicitamente à proteção de dados relativos a pessoas coletivas.

que integram o direito à proteção de dados pessoais impende sobre o responsável pelo tratamento dos dados – ou seja, a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que determina as finalidades e os meios de tratamento dos dados pessoais. E a fiscalização do cumprimento das normas em matéria de proteção de dados é realizada por uma autoridade independente, instituída em cada Estado-Membro, com poderes efetivos de intervenção (podendo ordenar o bloqueio, apagamento ou destruição de dados; proibir temporária ou definitivamente o tratamento; dirigir uma advertência ao responsável pelo tratamento; intervir em processos judiciais).

Quanto aos direitos daqueles cujos dados são objeto de tratamento, decorre da Diretiva 95/46 que seriam basicamente os seguintes:

i) direito de acesso aos dados objeto de tratamento (o titular dos dados tem direito à comunicação das informações tratadas para que as possa conhecer ainda que por mera curiosidade);

ii) direito à informação (o titular dos dados tem direito a saber da finalidade do tratamento, das condições em que o mesmo foi realizado, e se existe comunicação dos dados a outras entidades);

iii) direito ao apagamento (o titular dos dados tem direito a que os mesmos sejam conservados apenas por um certo período de tempo, exigindo-se o seu apagamento a partir de um prazo adequado às finalidades do tratamento; se porventura fins históricos, científicos os estatísticos o justifiquem, o alargamento do prazo é permitido, desde que não seja incompatível com os fins do tratamento original);

iv) direito à retificação de dados inexatos ou incompletos bem como à atualização dos mesmos (e isto independentemente da iniciativa do titular dos dados, tratando-se de um dever que impende sobre o responsável pelo tratamento dos dados);

v) direito à não sujeição a uma decisão individual automatizada (o titular dos dados tem direito a uma decisão que não seja exclusivamente tomada com base na avaliação automatizada de certos aspetos, como seja a solvabilidade na concessão de crédito bancário, por forma a garantir o contraditório e a consideração de circunstâncias específicas);

vi) direito de oposição ao tratamento dos dados (seja com base em razões preponderantes e legítimas relacionadas com a situação particular do titular, ou independentemente de qualquer razões, gratuitamente e em qualquer momento no caso de tratamento de dados para fins de *marketing* direto);

vii) direito ao não tratamento de dados sensíveis (como filiação sindical e partidária, orientação sexual, raça, dados de saúde e confissão religiosa, afastando-se todavia a proibição mediante o consentimento explícito do interessado, ou quando o tratamento for necessário para proteger os interesses vitais da pessoa em causa, ou ainda para efeitos de diagnóstico médico, prestação de cuidados de saúde, ou gestão de serviços de saúde – caso de cirurgias no âmbito da

telemedicina que implicam a recolha de imagens).

O âmbito de proteção dos direitos suprarreferidos (ou seja, o que protegem, o que proíbem) foi desenvolvido pela jurisprudência do TJUE ao longo do tempo, sobretudo mediante o mecanismo de diálogo entre os tribunais nacionais e o TJUE conhecido por reenvio prejudicial (artigo 267.º do TFUE). Por meio deste incidente processual, o juiz nacional que tem em mãos um processo regido pelo direito da União pode (e em certas circunstâncias deve) submeter ao TJUE questões de interpretação de disposições europeias ou de validade de atos jurídicos europeus que relevem para a boa decisão da causa. Por isso a referência a alguns dos acórdãos emblemáticos do TJUE em matéria de proteção de dados resulta indispensável para a compreensão da reforma legislativa de que trataremos a seguir, nomeadamente os acórdãos *Lindqvist*, *Scarlet*, *Google*, *Digital Rights e Schrems*.

1.1 ACÓRDÃO *LINDQVIST*

O primeiro acórdão do TJUE que aplicou a Diretiva 95/46 ao tratamento de dados na Internet foi o acórdão *Lindqvist* de 2003[4]. As questões prejudiciais foram colocadas por um tribunal sueco no âmbito de um processo penal contra a Sr.ª Lindqvist – que era acusada de violar a legislação sueca que transpunha a Diretiva 95/46 por publicitar dados de carácter pessoal numa página da Internet relativos a um determinado grupo de pessoas que com ela trabalhavam a título gratuito como catequistas numa paróquia protestante. Pensando na utilidade que daí advinha para a comunidade, a acusada disponibilizou dados dos seus dezoito colegas (os nomes completos, a situação familiar, as funções que exerciam, os *hobbies*, os números de telefone, etc. – e em relação a uma colega inclusivamente indicou que estava de baixa por conta de uma lesão no pé). Ocorre que a Sr.ª Lindqvist não informou os seus colegas sobre a criação da página, não obteve o consentimento dos mesmos para a introdução dos seus dados pessoais, nem declarou a sua atuação à autoridade sueca de proteção de dados transmitidos por via informática. Por isso foi acusada pelo Ministério Público sueco de ter procedido ao tratamento de dados pessoais sem comunicação à correspondente autoridade de controlo, de ter procedido ao tratamento de dados sensíveis, assim como de os ter transferido para países terceiros sem o consentimento dos titulares dos dados. Logo que tomou conhecimento de que alguns colegas não apreciaram a página em causa, Lindqvist suprimiu as informações, mas negou ter cometido qualquer infracção. Foi, todavia, condenada ao pagamento de uma sanção pecuniária.

O tribunal nacional que apreciou o caso em sede de recurso reenviou ao TJUE a fim de saber se a operação levada a efeito por Lindqvist constituía ou não um tratamento de dados pessoais na

[4] Acórdão *Lindqvist*, de 6 de novembro de 2003, proc. C-101/01.

acepção do artigo 3.º da Diretiva 95/46. O TJUE entendeu que a criação de uma página na Internet, a sua instalação num servidor, bem como a introdução de informações pessoais disponíveis a todos quantos se conectem à Internet constituía sim um tratamento de dados pessoais por meios automatizados na acepção da diretiva. O TJUE ainda entendeu que o tratamento em causa não constituía o exercício de uma atividade exclusivamente pessoal ou doméstica excecionalizada pela diretiva, pois tal exceção teria por objeto as atividades que se inserem no âmbito da vida privada e familiar, o que manifestamente não seria o caso do tratamento de dados pessoais disponibilizados via Internet a um número indeterminado de pessoas. Contrariamente ao que sustentava o advogado de Lindqvist, o TJUE entendeu que o âmbito de aplicação da diretiva não se limita ao exercício de uma atividade económica, pois disciplina a circulação de dados pessoais também no exercício de atividades sociais, no contexto mais amplo de uma integração europeia orientada pela proteção de direitos fundamentais. Ademais, a indicação de que uma das catequistas lesionou o pé constituía um dado pessoal relativo à saúde cuja divulgação demandaria o consentimento explícito do interessado, ou seja, a manifestação de vontade livre, específica e informada, por tratar-se de um dado sensível. De qualquer forma, o TJUE entendeu que a operação em causa não constituía (em si mesma) uma transferência de dados do território de um Estado-Membro para um país terceiro na acepção do artigo 25.º da diretiva. Se cada carregamento de dados pessoais na Internet fosse considerado uma transferência de dados para um país terceiro, então os Estados-Membros estariam obrigados a prevenir que nenhum dado pessoal fosse introduzido *online*, pois poderiam ser acessíveis em países terceiros que não asseguram o nível exigido pela diretiva – o que seria impraticável.

1.2 ACÓRDÃO *SCARLET*

Já no acórdão *Scarlet*, de 2011[5], o TJUE foi chamado a interpretar as disposições não só da Diretiva 95/46, mas também da Diretiva 2000/31 (relativa ao comércio eletrónico), da Diretiva 2001/29 (relativa aos direitos de autor e direitos conexos na sociedade da informação), da Diretiva 2002/58 (relativa ao tratamento de dados pessoais no sector das comunicações eletrónicas) e da Diretiva 2004/48 (relativa aos direitos de propriedade intelectual). O pedido foi apresentado no âmbito de um litígio que opunha a Scarlet (um fornecedor belga de acesso à Internet – FAI) à SABAM (uma sociedade de gestão belga que representa autores, compositores e editores de obras musicais, autorizando a utilização, por terceiros, das suas obras protegidas). O mote da discórdia devia-se ao facto de a SABAM ter concluído que os internautas que utilizam os serviços da Scarlet

[5] Acórdão *Scarlet*, de 24 de novembro de 2011, proc. C-70/10.

teledescarregavam na Internet, sem autorização e sem pagar direitos, obras constantes do seu catálogo, por meio de um *software peer-to-peer* (meio de partilha de conteúdos independente e munido de funções de busca e de teledescarga avançadas). Por conta disso a SABAM demandou judicialmente a Scarlet por entender que, enquanto FAI, estaria nas melhores condições para tomar medidas tendentes a fazer cessar as violações de direito de autor cometidas pelos seus clientes. O processo principal prendia-se, portanto, com recusa da Scarlet em instalar um sistema de filtragem de todas as comunicações eletrónicas que transitam pelos seus serviços, aplicado indistintamente a toda a sua clientela, com carácter preventivo, exclusivamente a expensas suas e sem limitação no tempo, a fim de impedir o intercâmbio de ficheiros que violassem direitos de autor.

O TJUE considerou que a medida inibitória não assegurava o justo equilíbrio entre, por um lado, a proteção do direito à propriedade intelectual de que gozam os autores (artigo 17.º da CDFUE), e, por outro, a liberdade de empresa de que beneficiam os operadores como os FAI (artigo 16.º da CDFUE), na medida em que tal inibição imporia uma vigilância ativa de todos os dados pessoais dos clientes, obrigando o FAI a instalar um sistema informático complexo, oneroso, permanente. Ademais, não assegurava o justo equilíbrio entre, por um lado, a proteção da propriedade intelectual dos autores, e, por outro, a proteção dos dados pessoais (artigo 8.º da CDFUE) e da liberdade de receber e transmitir informações ou ideias (artigo 11.º da CDFUE) dos clientes, pois a medida inibitória implicaria a análise sistemática de todos os conteúdos e a recolha/identificação dos endereços IP dos utilizadores que estão na origem do envio de conteúdos ilícitos – e estes endereços estão protegidos por permitirem a identificação precisa dos utilizadores. Ademais, a medida poderia violar a liberdade de informação, na medida em que o sistema pode não distinguir um conteúdo lícito de um ilícito e o seu acionamento poderia provocar o bloqueio de comunicações de conteúdo lícito. Logo, as disposições das referidas diretivas, lidas conjuntamente e interpretadas à luz das exigências resultantes da proteção dos direitos fundamentais aplicáveis, devem ser consideradas no sentido de que se opõem a uma medida inibitória que ordena a um FAI a instalação de um sistema de filtragem como o que estava em causa no processo principal.

1.3 ACÓRDÃO *GOOGLE*

No acórdão *Google*, de 2014[6], o TJUE reconheceu o direito ao esquecimento de dados pessoais constantes de *sites* terceiros, mas acessíveis por motores de busca – um direito fundamental que se sobrepõe aos interesses económicos do operador e ao interesse público da informação. O litígio

[6] Acórdão *Google*, de 13 de maio de 2014, proc. C-131/12.

principal opunha, por um lado, a Google Spain e a Google Inc., e, por outro, a Agencia Española de Protección de Datos, por conta de uma decisão da referida agência que deferiu a pretensão do Sr. Mario Costeja, ordenando que a Google adotasse as medidas necessárias para retirar os dados pessoais do requerente do seu índice e impossibilitar o futuro acesso aos seus dados. A reclamação baseava-se no facto de que, quando um internauta inseria o nome de Mario Costeja no motor de busca da Google, obtinha ligações a duas páginas do jornal La Vanguardia, ambas de 1998, nos quais figurava um anúncio de venda de imóveis em hasta pública, decorrente de um arresto com vista à recuperação de dívidas à Segurança Social que envolvia Mario Costeja. Com essa reclamação o requerente pedia que se ordenasse *i*) que o jornal suprimisse ou alterasse as referidas páginas, para que o seu nome deixasse de aparecer, e *ii*) que a Google suprimisse ou ocultasse os seus dados pessoais para que deixassem de aparecer nos resultados de pesquisa – isso porque, segundo o requerente, o arresto tinha sido completamente resolvido há anos e a sua referência carecia atualmente de pertinência. A agência espanhola indeferiu a reclamação na parte que dizia respeito ao jornal por considerar que a publicação das informações estava legalmente justificada – mas deferiu a reclamação na parte que dizia respeito à Google por concluir que o motor de busca realiza um tratamento de dados pelo qual é responsável e que prossegue objetivos distintos dos do jornal. Insatisfeita, a Google questionou judicialmente a decisão da Agencia Española e o competente tribunal nacional reenviou para o TJUE, a fim de saber que obrigações incumbem aos operadores de motores de busca para efeitos de proteção de dados pessoais.

Importava, portanto, desvendar *i*) se a normativa europeia de proteção de dados se aplica a um organismo cuja sede social está nos EUA, *ii*) se os operadores de motores de busca (como Google, Bing, Ask, etc.) são responsáveis (e em que circunstâncias) pelo suposto tratamento de dados na sua atividade, e *iii*) qual o alcance dos direitos em causa. A Google rejeitava a aplicação do direito da União dado que a sua sede matriz encontra-se nos EUA, e eximia-se de qualquer responsabilidade por entender que, ao indexar informações, não estaria a tratar dados de forma individual. O TJUE considerou que a diretiva do tratamento de dados seria aplicável à Google porque *i*) as buscas se realizavam por meio de uma página *web* sediada em Espanha (mediante uma sucursal destinada à promoção e venda de espaços publicitários), *ii*) com efeitos vinculativos em Espanha e *iii*) relativamente a cidadãos situados fisicamente em Espanha. Na medida em que a Google ordena a informação publicada e posta na Internet por terceiros, armazena-a temporariamente e a disponibiliza aos internautas, está a realizar uma operação de tratamento de dados. É, por isso, responsável pelo tratamento na acepção da Diretiva 95/46, pois determina os meios e a finalidade da atividade. Trata-se de um tratamento distinto daquele levado a efeito pelo editor, pois o lesado não se vai dirigir ao

jornal pedindo que não indexe a informação – tem de o requerer ao operador do motor de busca, por isso está-se em presença de um direito posterior ante dados já existentes. Assim, o direito ao esquecimento se exerce em relação ao operador que deve eliminar a conexão dos resultados da busca. Por meio do direito ao esquecimento o afetado reclama proteção contra lesões produzidas pela difusão de dados pessoais que não deseja que sejam conhecidos – e que são processados/propagados e se tornam acessíveis mediante motores de busca. O direito ao esquecimento não elimina dados de carácter pessoal de nenhuma página web, mas sim impõe que o motor de busca deixe de indexar/conectar o internauta àqueles dados pessoais, ou seja, que deixe de conectar dados a pessoas concretas.

Assim, a resposta do TJUE foi suficientemente clara quanto *i*) à existência de um tratamento de dados pessoais por parte do operador do motor de busca; *ii*) à responsabilidade do operador do motor de busca; *iii*) ao elemento de conexão entre o tratamento de dados e o responsável pelo tratamento, quando este não possua a sua sede no espaço da União Europeia; *iv*) à obrigação do operador do motor de busca proceder à desassociação de resultados aquando do pedido do titular dos dados; e *v*) à extensão, alcance e limites dos direitos do titular dos dados. O TJUE reconheceu que cada pessoa tem o direito a que informações sobre si disponíveis na Internet deixem de ser associadas ao seu nome por meio de uma lista de resultados exibida na sequência de uma pesquisa efetuada em motores de busca, sem que, todavia, a constatação desse direito pressuponha que tal associação cause prejuízo à pessoa em causa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° (proteção da vida privada) e 8.° (proteção de dados pessoais) da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão numa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca, mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão[7].

1.4 ACÓRDÃO *DIGITAL RIGHTS IRELAND*

No acórdão *Digital Rights* de 2014[8] o pedido de decisão prejudicial tinha por objeto a

[7] Cf. acórdão *Google*, *cit*., considerando 99.
[8] Acórdão *Digital Rights Ireland*, de 8 de abril de 2014, processos apensos C-293/12 e C-594/12.

validade da Diretiva 2006/24/CE (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 não regulava o tratamento de dados pelas autoridades públicas ou policiais dos Estados-Membros, mas sim a retenção de dados pessoais por fornecedores de serviços de comunicações eletrónicas. Isto é, a conservação de dados pessoais por empresas privadas no exercício de atividades económicas, tendo em vista a disponibilização desses dados para efeitos de investigação, de deteção e de repressão de infrações graves. Os dados em causa seriam os necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de uma comunicação, além do equipamento de comunicação dos utilizadores – dados entre os quais figuram o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário, e também um endereço IP para os serviços Internet. Estes dados permitem saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou, e por qual meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada (informações conhecidas por metadados). Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas, durante um determinado período. A diretiva seria aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas, não sendo todavia aplicável ao conteúdo das comunicações eletrónicas, incluindo as informações consultadas utilizando uma rede de comunicações eletrónicas. De qualquer forma, os Estados-Membros deviam assegurar que os dados fossem conservados por períodos não inferiores a seis meses e não superiores a dois anos, a contar da data da comunicação, de modo que tais dados pudessem ser transmitidos imediatamente, mediante pedido, às autoridades competentes.

Por ser proprietária de um telefone móvel que utilizava regularmente, a Digital Rights interpôs um recurso na *High Court* irlandesa *i*) pondo em causa a legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas e *ii*) pedindo ao órgão jurisdicional de reenvio que declarasse a nulidade da Diretiva 2006/24. O busílis residia no facto de que a diretiva abrangia todas as pessoas que utilizassem serviços de comunicações eletrónicas na Europa (vigilância generalizada), sem que as pessoas cujos dados são conservados se encontrassem numa situação suscetível de dar lugar a ações penais. Além disso, a diretiva não previa nenhuma exceção, pelo que era aplicável mesmo a pessoas cujas comunicações estão sujeitas ao segredo profissional. A esta ausência geral de limites acresce que a Diretiva 2006/24 não estabelecia um critério objetivo que permitisse delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior. Ademais a diretiva não impunha que os dados em

causa fossem conservados no território da União, pelo que não se podia considerar que estivesse plenamente garantida a fiscalização por uma entidade independente. O TJUE foi então chamado a apreciar a validade da Diretiva 2006/24 à luz dos artigos 7.° (proteção da vida privada) e 8.° (proteção de dados pessoais) da CDFUE. E concluiu que a Diretiva 2006/24 não estabelecia regras claras e precisas que regulassem o alcance da ingerência nos referidos direitos fundamentais de modo a limitá-la ao estritamente necessário. Ao adotar a Diretiva 2006/24 o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da CDFUE – razão pela qual o TJUE declarou a invalidade integral da diretiva com efeitos retroativos (*ex tunc*), ou seja, desde a sua entrada em vigor.

1.5 ACÓRDÃO *SCHREMS*

No acórdão *Schrems*[9] a questão prejudicial foi apresentada pela *High Court* irlandesa no âmbito de um litígio principal que opunha M. Schrems ao *Data Protection Commissioner* (comissário irlandês para a proteção de dados). O pomo da discórdia residia no facto de a autoridade administrativa ter-se recusado a investigar uma queixa apresentada pelo requerente que acusava a Facebook Ireland de transferir dados pessoais dos seus utilizadores para os EUA, onde seriam tratados e conservados. O Commissioner entendia que qualquer questão relativa ao caráter adequado da proteção dos dados pessoais nos EUA devia ser decidida em conformidade com a Decisão 2000/520, pois nesta decisão a Comissão Europeia tinha constatado que os EUA asseguravam um nível de proteção adequado. Na medida em que M. Schrems questionava judicialmente a legalidade do regime de "porto seguro" estabelecido pela Decisão 2000/520, importava saber se, de acordo com o disposto na Diretiva 95/46, a autoridade irlandesa estava vinculada pela constatação da Comissão Europeia, ou se, pelo contrário, a CDFUE autorizava o Commissioner a afastar-se dessa constatação. O TJUE foi então confrontado com a questão de saber se, e em que medida, o artigo 25.°, n.° 6, da Diretiva 95/46 – lido à luz dos artigos 7.° (proteção da vida privada), 8.° (proteção de dados pessoais) e 47.° (tutela jurisdicional efetiva) da CDFUE –, devia ser interpretado no sentido de que uma decisão adotada nos termos daquela disposição (como a Decisão 2000/520) obsta a que uma autoridade de controlo de um Estado-Membro examine um pedido relativo à transferência de dados pessoais para um país terceiro quando o interessado alega que o direito e as práticas então em vigor não asseguram um nível de proteção adequado.

O TJUE considerou que o termo "adequado" que figura no artigo 25.°, n.° 6, da Diretiva

[9] Acórdão *Schrems*, de 6 de outubro de 2015, proc. C- 362/14.

95/46 não exige que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da União – mas exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção dos direitos fundamentais substancialmente equivalente ao conferido pela União. Para controlar as transferências de dados pessoais para países terceiros, o artigo 25.° da Diretiva 95/46 impõe uma série de obrigações aos Estados-Membros e à Comissão. Resulta deste artigo que a constatação de que um país terceiro assegura ou não um nível de proteção adequado pode ser feita quer pelos Estados-Membros quer pela Comissão. E que a Comissão pode, com base no artigo 25.°, n.° 6, da Diretiva 95/46, adotar uma decisão que constate que um país terceiro assegura um nível de proteção adequado. Tal decisão terá como destinatários os Estados-Membros, que devem tomar as medidas necessárias para dar-lhe cumprimento. Assim, enquanto a decisão da Comissão não for declarada inválida pelo TJUE, os Estados-Membros e os seus órgãos, entre os quais se encontram as autoridades de controlo independentes, não podem adotar medidas contrárias a essa decisão, como sejam atos destinados a constatar, com efeitos vinculativos, que o país terceiro visado pela referida decisão não assegura um nível de proteção adequado.

Ocorre que, com fundamento na segurança nacional, no interesse público ou na legislação interna dos EUA, a Decisão 2000/520 permitia ingerências nos direitos fundamentais dos indivíduos cujos dados pessoais fossem ou pudessem ser transferidos da União para os EUA – e não continha qualquer referência à existência de normas destinadas a limitar ingerências que prosseguissem objetivos legítimos ou relativas à proteção jurídica eficaz contra as mesmas. Nesta medida, entendeu o TJUE que não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais transferidos da União para os EUA *i*) sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e *ii*) sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos – leia-se estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam. Em particular, uma regulamentação que permita às autoridades públicas aceder de modo generalizado ao conteúdo das comunicações eletrónicas deve ser considerada lesiva do conteúdo essencial do direito fundamental ao respeito da vida privada, tal como é garantido pelo artigo 7.° da CDFUE. De igual modo, 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 artigo 47.° da CDFUE.

Ora, nos termos do artigo 28.° da Diretiva 95/46, lido à luz do artigo 8.° da CDFUE (proteção de dados pessoais), as autoridades nacionais de controlo devem poder examinar, com total independência, qualquer pedido relativo à proteção dos direitos e liberdades de uma pessoa no que diz respeito ao tratamento dos seus dados. Assim é, em particular, quando tal pedido questiona a compatibilidade de uma decisão da Comissão Europeia adotada nos termos do artigo 25.°, n.° 6, da referida diretiva com a proteção dos direitos fundamentais protegidos pela UE. Todavia, o artigo 3.°, n.° 1, primeiro §, da Decisão 2000/520 prevê uma regulamentação específica quanto aos poderes de que dispõem as autoridades nacionais de controlo perante uma constatação efetuada pela Comissão Europeia relativamente ao nível de proteção adequado previsto no artigo 25.° da Diretiva 95/46 – ou seja, tal disposição da Decisão 2000/520 priva as autoridades nacionais de controlo dos poderes que lhes são conferidos pelo artigo 28.° da Diretiva 95/46. Ora, o poder de execução atribuído pelo legislador da União à Comissão Europeia no artigo 25.°, n.° 6, da Diretiva 95/46 não confere a esta instituição competência para limitar os poderes das autoridades nacionais de controlo – razão pela qual a Comissão Europeia teria ultrapassado a competência que lhe é atribuída. Neste pressuposto, e atendendo a todas as considerações precedentes, o TJUE concluiu que a Decisão 2000/520 era inválida, cumprindo ao tribunal nacional do reenvio dar provimento à pretensão do requerente.

2 O NOVO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS – REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 27 DE ABRIL DE 2016

Com a publicação do novo regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados, que revoga a Diretiva 95/46), abre-se espaço a um novo paradigma no tratamento comum dos vários Estados-Membros da UE. Como já foi assinalado, a clara distinção no alcance dos instrumentos jurídicos em questão – antes uma diretiva, agora um regulamento – implica necessariamente uma maior coerência (ao menos formal) na resposta que cada um dos Estados que compõem a UE podem e devem dar às matérias relacionadas com a proteção de dados.

O considerando 9 do regulamento bem traduz o que se visou combater:

> Os objetivos e os princípios da Diretiva 95/46 continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados

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

Vemos que, por um lado, se quis dar resposta à questão ligada à "fragmentação da aplicação da proteção dos dados ao nível da União", elemento disruptor do próprio conceito em que assenta o contrato social a que aderiram todos os povos participantes do projeto político da UE, sem que, por outro lado, se desmereça a dimensão da livre circulação dos dados que representa igualmente a concretização, neste domínio, de uma das prerrogativas basilares do seu funcionamento e existência[10]. A este propósito, importa sublinhar que já a Diretiva 95/46 propugnava, lapidarmente, no seu considerando 8, que

> […] para eliminar os obstáculos à circulação de dados pessoais, o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-Membros; [ora] a realização deste objectivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-Membros.

É, portanto, na uniformização, imposta pela figura do regulamento, que se funda a primeira grande alteração introduzida no quadro da proteção de dados na UE. Com ela pretende-se eliminar eventuais contradições na aplicação do direito entre os vários Estados-Membros, desde logo ao nível das (agora denominadas) Autoridades de Controlo, entidades responsáveis pela fiscalização da aplicação do regulamento, do direito europeu e do direito interno aplicáveis a esta matéria.

Com efeito, a liberdade conferida na transposição das diretivas para o direito interno dos diversos Estados-Membros, ainda que longe de irrestrita[11], permite a instituição de soluções nem sempre coincidentes, a consagração de exceções eventualmente equívocas e também a previsão de restrições/condições não partilhadas pelas restantes nações. A este título, observe-se o que vinha disposto no artigo 5.º da Diretiva 95/46: "Os Estados-Membros especificarão, dentro dos limites do disposto no presente capítulo, as condições em que é lícito o tratamento de dados pessoais". Ora, a licitude do tratamento depende do respeito por um conjunto de princípios fundamentais inscritos no artigo 6.º da diretiva, complementados pelas específicas condições em que os tratamentos de dados pessoais são admitidos (estes chamados de "fundamentos de legitimidade") e que se preveem nos

[10] Tal como descrito no artigo 3.º, n.º 2, do TUE, "A União proporciona aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, em que seja assegurada a livre circulação de pessoas, em conjugação com medidas adequadas em matéria de controlos na fronteira externa, de asilo e imigração, bem como de prevenção da criminalidade e combate a este fenómeno".

[11] Veja-se, quanto aos limites da transposição da Diretiva 95/46, o recente Acórdão Patrick Breyer, de 19 de outubro de 2016, proc. C- 582/14.

artigos 7.º e 8.º da diretiva. Ao permitir a conformação das "condições em que é lícito o tratamento de dados pessoais" por parte dos Estados-Membros, a diretiva deu azo a algumas particularidades que distanciam os ordenamentos jurídicos nacionais – e, consequentemente, os cidadãos – no que respeita à proteção dos seus dados pessoais.

Atente-se, como exemplo, no que vem prescrito na LPDP, mais precisamente no seu artigo 7.º, n.º 1, pelo qual se proíbem os tratamentos de dados pessoais ditos sensíveis ("categorias específicas de dados", na terminologia da diretiva), que se prendem com a origem racial, com convicções religiosas ou filosóficas, com a saúde – entre outros. Ao contrário da diretiva, há uma categoria de dados que a lei portuguesa proíbe e à qual aquela não faz referência – que é a da "vida privada". Este conceito, ainda hoje controverso, sustenta-se na previsão do artigo 35.º, n.º 3, da Constituição da República Portuguesa (CRP), decalcando, praticamente *ipsis verbis*, o teor daquela disposição. Aí se limita o tratamento de dados referentes à "vida privada" do seu titular aos casos em que exista "consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis". O artigo 7.º, n.º 2, da LPDP vem concretizar esse mandamento constitucional, permitindo o tratamento dos dados sensíveis, mediante disposição legal ou autorização da Comissão Nacional de Proteção de dados (CNPD)[12], quando por motivos de interesse público esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento – em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º. Essa especificidade do direito português semicerrou a porta a muitos tratamentos de dados que, por força do conceito de "vida privada", acabam por obrigar a que apenas mediante lei ou autorização da CNPD, quando obtido o consentimento expresso do titular dos dados, se possa proceder aos referidos tratamentos. Assim não acontece, por exemplo, na legislação espanhola, o que facilita a existência destes tratamentos de dados e suscita naturais dúvidas e questões aos responsáveis pelos tratamentos que operem nos dois países.

É certo que, com a aplicação do novo regulamento, a discussão sobre tais particularidades nacionais dos regimes de proteção de dados pessoais não terá necessariamente que acabar, uma vez que ele próprio prevê um espaço de conformação e responsabilidade do legislador nacional[13]. Ademais, no caso citado, o imperativo constitucional português, na medida em que oferece um nível

[12] A CNPD, criada pelo artigo 21.º da LPDP, e por imperativo constitucional (artigo 35.º, n.º 2, da CRP), "é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei", de acordo com o artigo 22.º, n.º 1, da LPDP.

[13] Veja-se, a este propósito, o disposto quanto à matéria das sanções no artigo 84.º do Regulamento.

mais elevado de proteção dos direitos dos cidadãos, não deverá merecer reparo por parte da jurisprudência europeia, mas o que se visa alcançar com este passo em frente é a garantia de um denominador mínimo (quando não mesmo máximo) comum em matéria de proteção de dados pessoais – e essa é uma garantia que apenas o regulamento pode viabilizar sem excessivas discrepâncias.

Igualmente relevante, no domínio das novidades, é o que se prevê relativamente ao âmbito de aplicação do regulamento. Desde logo, a existência de uma diretiva específica estabelecendo normas sobre proteção de dados pessoais em matéria penal (relacionados com prevenção/investigação/detenção/prossecução/execução penal) afasta a aplicação do regulamento neste âmbito – mas se tal não fosse bastante, o artigo 2.º, n.º 2, é suficientemente explícito. Ainda mais relevante, porém, é o disposto no artigo 3.º, quanto ao âmbito de aplicação territorial:

> 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União; 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União. 3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

Ora, são patentes os reflexos de acórdãos estruturantes em matéria de proteção de dados nas soluções aqui presentes. A nitidez com que agora se afirma que o regulamento se aplica aos tratamentos levados a cabo por responsáveis/subcontratantes situados no território da União, independentemente de o tratamento de situar dentro ou fora da União, remete-nos para o teor do acórdão *Google* (no que respeita aos conceitos de estabelecimento), mas também para o acórdão *Schrems* (quanto à questão de o tratamento se situar dentro ou fora do espaço da União). Por outro lado, o alargamento do âmbito de aplicação do regulamento a responsáveis/subcontratantes não estabelecidos na União, se bem que potencialmente polémico na aplicação e alcance, representa um avanço importante para a proteção dos dados pessoais dos cidadãos da UE, onde quer que tal tratamento ocorra.

Se a isto acrescentarmos a possibilidade de sancionamento dos responsáveis com coimas de valor elevado (até €10.000.000 ou 2% do volume de negócios anual mundial da empresa), previsto no artigo 83.º, n.º 4, alínea *a)*, teremos assegurada uma vontade, séria e inscrita na lei, de velar pela

integridade dos tratamentos de dados pessoais dos cidadãos da UE, ainda que se anteveja como difícil a aplicação dessas coimas a entidades que não tenham representantes no território da União. Esta possibilidade liga-se a mais uma das novidades deste regulamento, qual seja, a da obrigatoriedade de os responsáveis por tratamentos de dados pessoais que não tenham estabelecimento na UE [14] designarem "por escrito" um representante (artigo 27.º), a fim de que se possam fazer cumprir todas as suas obrigações e, bem assim, respeitar todos os direitos reconhecidos aos titulares dos dados.

Em termos estruturais, no que aos princípios relativos à proteção de dados pessoais respeita, não existem novidades de monta. Mantêm-se como válidos os pressupostos inscritos na Diretiva 95/46, sendo obrigatório que o princípio da licitude, o princípio da finalidade, o princípio da qualidade dos dados, o princípio do tratamento leal e o princípio da responsabilidade sejam respeitados integralmente. Alteração relevante é aquela que respeita às crianças e ao respeito pela sua especial vulnerabilidade neste contexto. Saúdam-se as menções particulares às condições de licitude do tratamento [artigo 6.º, n.º 1, alínea *f)*], bem como as reforçadas exigências relativas ao consentimento prestado por crianças – seja quanto à idade mínima para esse consentimento ser prestado de forma válida, seja quanto ao caráter explícito e apreensibilidade da informação prestada (artigo 8.º).

No domínio dos direitos dos titulares dos dados são consagradas algumas novidades – como o direito de portabilidade, pelo qual o titular dos dados passa a poder, num claro movimento de facilitação do controlo dos dados,

> […] receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e 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.

Este direito tem uma dimensão simbólica de relevo, dado que, porventura pela primeira vez, o titular dos dados terá por corpórea uma realidade até aqui intangível. Ora, a capacidade de qualquer titular dos dados percecionar, com algum grau de precisão, a quantidade e qualidade de dados tratados que lhe pertencem, é diminuta. Dificilmente estará ao alcance do cidadão médio perceber a exata medida da dimensão e do grau de intrusão à sua privacidade que representa a informação que sobre si é recolhida e processada. Neste quadro, a possibilidade de requerer e obter, num formato legível, essa mesma informação, seja para transmiti-la a um outro responsável pelo tratamento de dados ou

[14] Sem prejuízo do que já ficou estabelecido quanto a esta matéria pelo TJUE no acórdão *Google*, interessa levar em linha de conta o teor do considerando 22, a fim de perceber a que se refere o regulamento quando menciona o conceito de estabelecimento: "O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto".

subcontratante, seja apenas para o exercício de um direito que deve caber a qualquer cidadão (o de conhecer e/ou reclamar a entrega, de forma legítima, dos seus próprios dados), representará um avanço no sentido da transparência sobre todas as operações de tratamento de dados e, nessa medida, um acréscimo sensível da consciencialização e responsabilização dos cidadãos pela forma como cedem os seus dados pessoais.

O agora célebre "direito ao esquecimento" passa a ter honras de novo direito – o que em muito se deve às conclusões do acórdão *Google*. Em boa verdade, o direito ao apagamento dos dados fazia já parte do catálogo dos chamados direitos ARCO[15] (artigos 12.º e 14.º da Diretiva 95/46), mas o direito ao esquecimento surge agora, sem dúvida por força da mediatização daquele acórdão, como parte integrante (e autonomizada) da epígrafe do artigo 17.º. De qualquer forma, são dois direitos com âmbitos de proteção distintos. Por meio do direito ao esquecimento o afetado reclama proteção contra a difusão de dados pessoais que são processados/propagados e se tornam acessíveis por intermédio de motores de busca – ou seja, um direito originariamente concebido para ser exercido *online*. Nessa medida, o direito ao esquecimento se distingue do direito ao apagamento originariamente previsto na Diretiva 95/46 para ser exercido *offline*, pois o último implica que os dados pessoais sejam conservados apenas por um certo período de tempo, exigindo-se o seu apagamento a partir de um prazo adequado às finalidades do tratamento.

Por fim, a obrigação de *notificar* a autoridade de controlo (artigo 33.º) e, em certos casos, o próprio titular (artigo 34.º) quando ocorra uma violação de dados pessoais, representa um avanço em matéria de obrigação de informação por parte do responsável pelo tratamento dos dados. É compreensível que a divulgação de uma violação de dados pessoais cause prejuízos económicos e reputacionais à entidade que o divulga – muitas vezes sem que se lhe possa assacar diretamente responsabilidades fundadas em dolo ou mesmo mera negligência. Todavia, a condição de que essa comunicação se faça apenas nos casos em que "seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares" – e, no caso dos titulares dos dados, apenas quando tal violação seja "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" –, limita de forma incompreensível o direito (quando não o dever, no caso das autoridades de controlo) a saber que tipo de violações ocorreram e avaliar a existência ou não dos referidos riscos. Ao devolver aos responsáveis pelo tratamento de dados pessoais a avaliação do risco que a violação suscitou, privatiza-se uma função que deveria caber exclusivamente à autoridade de controlo, além de

[15] Acrónimo anglo-saxónico para *Access* (acesso), *Rectification* (retificação), *Cancellation* (apagamento) e *Opposition* (oposição).

sobrecarregar as entidades que realizam o tratamento de dados sem que se anteveja qualquer vantagem para os direitos dos cidadãos.

No domínio dos conceitos, importa assinalar que as novas definições constantes do artigo 4.º, como "definição de perfis" (artigo 4.º, n.º 4), "pseudonimização" (artigo 4.º, n.º 5) e "dados genéticos" (artigo 4.º, n.º 13) representam a preocupação do legislador europeu com os novos desafios com que se depara o mundo atual, no qual emergem realidades complexas tão eivadas de potencial como de risco. As possibilidades infinitas que permitem o *Big data* ou a *Internet das coisas* relativamente ao tratamento de dados, à criação de perfis e à limitação da liberdade de ação/reação dos cidadãos, exigem uma correspondente e proporcionada resposta por parte do legislador no sentido de impedir os abusos que a facilidade por vezes autoriza. Tanto mais que o que se enfrenta nestes casos é o risco do dano perpétuo na reputação, na imagem, na liberdade e na autoestima pessoal e, portanto, no livre desenvolvimento da personalidade de cada um.

Uma nota especial deve ser dada às novidades introduzidas no conceito de "consentimento" (artigo 4.º, n.º 11). Até agora a Diretiva 95/46 se bastava com "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento" [artigo 2.º, alínea *h)*] permitindo, por exemplo, que o consentimento fosse prestado de forma tácita (com exceção do consentimento relativo às categorias específicas de dados). Todavia, o regulamento contrai significativamente as possibilidades para a prestação do consentimento, limitando-as a "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". O caráter explícito da declaração de consentimento obriga a uma ação (declaração ou ato positivo inequívoco) do titular dos dados que demonstre esse consentimento, sendo inadmissível a obtenção do consentimento por meio de presunções ou omissões.

Verdadeiramente revolucionária é a modificação do papel atribuído às "autoridades de controlo" (artigo 4.º, n.º 21). Relembre-se que a Diretiva 95/46, no seu artigo 18.º, previa a obrigação de notificação à autoridade de controlo "antes da realização de um tratamento ou conjunto de tratamentos". Ademais, o artigo 20.º estabelecia a necessidade de controlo prévio do tratamento, por parte da autoridade de controlo, quando se estivesse perante tratamentos que pudessem representar riscos específicos para os direitos e liberdades das pessoas em causa. Estávamos num período em que o modelo de regulação jurídica de atividades privadas ainda assentava no controlo administrativo prévio tendente a verificar se do seu desenvolvimento não resultaria a violação de interesses públicos ou a violação insuportável dos direitos dos indivíduos (CALVÃO, 2015).

Ora, foi esse modelo de supervisão que a Diretiva 95/46 assumiu em relação aos tratamentos de dados que apresentavam maiores riscos para o direito à proteção de dados pessoais – e que foi consagrado na generalidade dos diplomas legais que procederam à sua transposição para a ordem jurídica dos Estados-Membros da UE. Todavia, com o novo regulamento prescinde-se do modelo das notificações prévias[16] em favor de um modelo de autorregulação, no qual se inscrevem as novas obrigações a que os responsáveis pelo tratamento estão vinculados. Desde logo, estabelece-se a necessidade de avaliação de impacto da privacidade quando um certo tipo de tratamento – em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades – for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares (artigo 35.º).

Paradigmática desta nova opção do legislador europeu é a previsão da figura do "encarregado de proteção de dados" (artigo 37.º) que representa, em si mesmo, a transferência operacional da atividade de controlo prévio para uma figura estranha ao universo da regulação destas atividades, embora já conhecida de muitas entidades privadas, tanto na UE como nos EUA. O encarregado de proteção de dados é obrigatório no caso de o tratamento ser efetuado por "uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional" [artigo 37.º, n.º 1, alínea *a)*] ou quando "as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala" [alínea *b)* do mesmo artigo], ou ainda quando "as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º" [alínea *c)* do mesmo artigo].

A ele cabem as funções previstas no artigo 39.º, das quais se destacam o controlo da

> […] conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes [art.º 39.º, nº 1, alínea *b)*].

[16] Embora com alguns casos excecionais, como parece ser o das categorias de dados especiais, previstas no artigo 9.º. No seu n.º 4, surgem como possíveis a manutenção ou imposição de "novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde", em que se poderá inscrever a obrigação de controlo prévio. De forma idêntica, veja-se o previsto no artigo 36.º, n.º 5, quanto "ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública".

Compete-lhe ainda cooperar com a autoridade de controlo, sendo o ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º [art.º 39.º, nº 1, alíneas *d)* e *e)*]. Para cumprir este papel que corresponde, no fundo, ao de autoridade de controlo interna dos responsáveis pelos tratamentos ou subcontratantes, exigem-se garantias de independência traduzidas no seu posicionamento e nível de acesso dentro da empresa. Segundo o artigo 39.º, n.º 3, o encarregado não pode ser destituído nem penalizado, pelo responsável pelo tratamento ou pelo subcontratante, pelo facto de exercer as suas funções.

Numa lógica de estruturação interna do cumprimento das obrigações do regulamento, os responsáveis pelo tratamento e os subcontratantes são incentivados a adotar códigos de conduta destinados a contribuir para a correta aplicação do regulamento (artigo 40.º), bem como a certificar (artigo 42.º), por meio de selos e marcas de proteção de dados, a conformidade das operações de tratamento por si levadas a cabo. Esta transformação – que, como se disse, externaliza as funções de controlo e coloca sobre os responsáveis pelo tratamento e subcontratantes a responsabilidade de velar pelo cumprimento das obrigações de proteção de dados pessoais – vem acoplada a um sério agravamento da moldura das sanções abstratamente aplicáveis, em que agora se preveem coimas que podem chegar aos €20.000.000,00 ou 4% do volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior (artigo 83.º, n.º 5 e n.º 6). Uma moldura que alguns doutrinadores portugueses, alicerçados em acórdãos do Tribunal Constitucional, anteveem de difícil admissibilidade (MOUTINHO; RAMALHO, 2015).

Para as autoridades de controlo sobram, no campo dos poderes prévios, a responsabilidade de aprovar listas de tratamentos sujeitos a avaliações de impacto da privacidade, dar parecer e aprovar os códigos de conduta, aprovar os critérios de certificação a acreditação de entidades certificadoras, a possibilidade de emitir orientações ou aprovar cláusulas contratuais (artigo 57.º, n.º 1). Quanto aos poderes de intervenção *ex post* sobressaem duas categorias: poderes de investigação (artigo 58.º, n.º 1) e de correção (artigo 58.º, n.º 2). Nos primeiros, assinalam-se os poderes relativos à realização de investigações sob a forma de auditorias sobre a proteção de dados [artigo 58.º, n.º 1, alínea *b)*], e, nos segundos, destaca-se a possibilidade de impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição [artigo 58.º, n.º 2, alínea *f)*].

Este elenco de poderes serve, sobretudo, para também neste domínio terminar com a desarticulação europeia, em que coabitavam autoridades de controlo investidas dos mais amplos poderes de atuação e outras destituídas de prerrogativas de fiscalização e aplicação de sanções. Refira-se que a articulação pretendida ultrapassa, em muito, a mera consignação de poderes idênticos. Pretende-se lutar contra o fenómeno do *forum shopping* e evitar que os responsáveis pelo tratamento

de dados optem por localizar o seu estabelecimento principal onde a legislação nacional seja mais permissiva ou menos exigente no que respeita quer às condições dos tratamentos de dados, quer à capacidade de reação das autoridades de controlo para punir eventuais abusos.

A instituição do mecanismo de cooperação (artigo 60.º) e do mecanismo de coerência (artigo 63.º) são dois passos adiante no sentido da uniformização da resposta das autoridades de controlo a fenómenos de violação do novo regulamento. Pelo primeiro, prescreve-se que "as autoridades de controlo prestam entre si informações úteis e assistência mútua a fim de executar e aplicar o presente regulamento de forma coerente, e tomam as medidas para cooperar eficazmente entre si" (artigo 61.º, n.º 1), estando, inclusive, prevista a possibilidade de se realizarem operações conjuntas (artigo 62.º).

Neste campo da cooperação sobressai a novidade introduzida com o conceito de "autoridade de controlo principal" (considerando 124)[17] e do "mecanismo de balcão único" (considerando 127 e artigo 56.º). Mediante estes conceitos pretende-se obviar não somente às queixas dos titulares dos dados – cujas consequências se disseminem por todo o espaço europeu, mas que devam ser investigadas pela autoridade de controlo do Estado-Membro onde o responsável pelo tratamento detém o seu estabelecimento principal –, como também à possibilidade de os titulares dos dados verem efetivada a tutela dos seus direitos onde quer que se encontrem e independentemente da sua distância em relação ao responsável pelo tratamento. A intenção do legislador é a de não deixar o cidadão à mercê do poderio económico de grandes empresas ou grupos de empresas que, para evitarem a fiscalização das suas atividades, poderiam esquivar-se à fiscalização da autoridade de controlo do país onde efetivamente ocorreu a violação das regras do regulamento, bastando-lhe para tanto alegar que seria no país onde se encontra o seu estabelecimento principal que o titular dos dados deveria ter apresentado a sua queixa.

Contudo, percebendo-se a intenção do legislador, o certo é que a operação de comunicação entre autoridades de controlo interessadas e a autoridade de controlo principal preconizada suscitará porventura dificuldades procedimentais (como se efetua a comunicação e com que meios?), logísticas (em caso de necessidade de tradução de documentos, quem deverá assegurar que a mesma se efetive?) e até financeiras (quando estão em causa operações conjuntas, quem paga os custos das cooperações e como é repartido o produto das coimas?), que não serão facilmente ultrapassadas – exigindo, desde já, e como está a acontecer, aturadas conversações no seio do Grupo de Trabalho do Artigo 29.º da

[17] Segundo o qual, quando o responsável pelo tratamento ou o subcontratante esteja estabelecido em vários Estados-Membros, ou quando o tratamento no contexto das atividades de um único estabelecimento afete (ou seja suscetível de afetar) titulares de dados em diversos Estados-Membros, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante deverá agir na qualidade de autoridade de controlo principal.

Diretiva 95/46. De resto, o mecanismo de coerência visa precisamente evitar desconformidades na aplicação do regulamento entre as autoridades de controlo. Em determinadas matérias, será chamado à liça o Comité Europeu para a Proteção de Dados[18], seja para a emissão de parecer, tal como previsto no artigo 64.º, n.º 1, seja para a resolução de litígios a que alude o artigo 65.º, n.º 1.

3 CONCLUSÃO. PERSPECTIVAS FUTURAS DA PROTEÇÃO DE DADOS INFORMATIZADOS NA UNIÃO

O quadro normativo da União Europeia em matéria de proteção de dados, pela sua pertinência, pelo grau de maturação e pela densificação dogmática e jurisprudencial de que dispõe, constitui-se como um padrão globalmente respeitado e, por isso mesmo, replicado em vários pontos do mundo. O passo em frente dado pela reforma dessa legislação representa igualmente um "salto de fé", na medida em que o paradigma da avaliação prévia e externa da licitude dos tratamentos dá lugar ao autocontrolo dessa mesma licitude ou adequação, sobrando aos cidadãos o credo na novel figura do encarregado de proteção de dados e, bem assim, no papel de contenção protocolar dos códigos de conduta e mecanismos de certificação.

Esta é uma opção do legislador da União que demonstra uma certa tendência pela "americanização" do regime europeu de proteção de dados pessoais, porquanto o modelo americano desde sempre caracterizou-se por um maior pendor autorregulatório, sustentado na crença quase-metafísica na credibilidade empresarial enquanto bastião da privacidade da clientela. Dir-se-á que a transferência deste poder-dever para as mãos dos privados mimetiza o modelo americano – todavia, no polo inverso, é renovado o papel das autoridades de controlo que se mantêm como uma realidade incontornável e até reforçada do modelo europeu. A prescrição, agora expressa e abrangendo todos os países da União, de poderes suficientes para que tais autoridades possam corresponder às responsabilidades fiscalizadoras que lhes cabem, contraria eventuais alegações sobre derivas mercantilistas. Esta nota continua a afastar claramente o modelo europeu do modelo americano, sobretudo em face da manutenção do critério da independência das autoridades de controlo, em vez do que sucede com a governamentalizada *Federal Trade Commission*.

O que ressalta deste novo tratamento sistémico à problemática da proteção de dados pessoais é a genuína preocupação com o incremento dos direitos dos cidadãos, com o facilitar da percepção e compreensão desses direitos, ao mesmo tempo que se alivia a "carga burocrática" dos responsáveis

[18] Previsto no artigo 68.º, este organismo da União está dotado de personalidade jurídica e visa substituir o Grupo de Trabalho do Artigo 29.º da Diretiva 95/46, em que estarão igualmente congregados representantes das várias autoridades de controlo da União.

pelo tratamento, tudo isto gizado num instrumento verdadeiramente uniformizador como é o regulamento. Os desafios são certamente muitos e complexos: começa pela aplicação concreta do regulamento e pela assunção, por parte dos distintos responsáveis pelo tratamento de dados, das novas responsabilidades que lhes cabem; mas passa também pela consciencialização cívica dos cidadãos para a nova realidade regulatória, terminando na consecução da exigente arquitetura de ação conjunta que se impõe às distintas autoridades de controlo europeias.

Sem embargo das dificuldades antecipáveis e dos necessários ajustes práticos que a realidade venha a exigir, o certo é que o Regulamento 2016/679 representa um passo de vanguarda no esforço europeu de consolidação de um espaço de referência na proteção de dados pessoais. É discutível se o grau de ambição do legislador da União nesta reforma foi o bastante para acomodar os diferentes interesses em jogo. De qualquer forma, em nenhum outro lugar do mundo se conhece uma preocupação tão palpável e uma ação tão consistente quanto à proteção de dados pessoais como na União Europeia. Se no mundo digital as garantias jurídicas são tanto mais ténues quanto mais se fragmente a aplicação das regras que as sustentam, resulta indiscutível que a União Europeia lança para o debate internacional uma reflexão séria e um exemplo concreto do que é possível fazer para garantir um denominador comum (mínimo ou máximo) que sirva à proteção de direitos que ainda se continuam a refletir, simples e eloquentemente, no primordial *right to be let alone.*

REFERÊNCIAS

CALVÃO, Filipa. O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento. In: *Revista Forum de Proteção de Dados*, n.º 1, julho 2015.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Constituição da República Portuguesa Anotada*, v. I. Coimbra: Coimbra Editora, 2007.

CASTRO, Catarina Sarmento e. Comentário ao artigo 8.º. In: SILVEIRA, Alessandra; CANOTILHO, Mariana (Coord.). *Carta dos Direitos Fundamentais da União Europeia Comentada*. Coimbra: Almedina, 2013.

MARQUES, João. And [they] built a crooked h[arbour] – the Schrems ruling and what it means for the future of data transfers between the EU and US. In: *UNIO* – EU Law Journal, n. 2, June/2016 (https://goo.gl/K2qUkO).

MOUTINHO, José Lobo; RAMALHO, David Silva. Notas sobre o regime sancionatório da proposta de regulamento geral sobre a proteção de dados do Parlamento Europeu e do Conselho. In: *Revista Forum de Proteção de Dados*, n. 1, julho 2015.

SILVEIRA, Alessandra. Cidadania e direitos fundamentais. In: SILVEIRA, Alessandra; CANOTILHO, Mariana; FROUFE, Pedro (Coord.). *Direito da União Europeia*. Elementos de direito

e políticas da União. Coimbra: Almedina, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. In: *Harvard Law Review*, n. 5, December 15, 1890 (https://goo.gl/FTWM).

FROM THE RIGHT TO BE LET ALONE TO THE RIGHT TO BE FORGOTTEN. CONSIDERATIONS ON THE PROTECTION OF COMPUTERIZED PERSONAL DATA IN THE EUROPEAN UNION LAW: MEANING, EVOLUTION, AND LEGISLATIVE REFORM

ABSTRACT

The right to privacy (originally known as the right to be let alone) was subject to considerable developments since the first legal writings in the USA of the 19th century – and can no longer respond fully to the protection needs of the Internet users who definitely do not want to be let alone but want to have the right to be forgotten. The processing and free movement of personal data in the European Union are regulated by Directive 95/46, of October, 24, 1995. This European legal act *i*) obliges the Member-States to adopt similar safeguards across the entire area of the European Union and *ii*) stipulates the same procedures related to the flow of personal data to third counties. It was, without doubt, a world reference in that domain, especially since it has entered into force when the risks associated to the information technology were not obvious. However, the increasing use of electronic facilities outdated the safeguards laid down by the law against the treatment and misuse of the computerized personal data. For this reason, from 2018 the personal data protection will be regulated on the basis of other terms in the European Union. This text aims to *i*) grasp the meaning and evolution of the protection of computerized personal data in the EU law, especially through the case-law of the Court of Justice of the European Union, as well as *ii*) address the main changes resulting of the application of the new legislative package on personal data protection in the European Union and, to this extent, the future of that fundamental right in Europe.

KEYWORDS

Computerized personal data. Internet. European Union. Fundamental rights. Court of Justice of the European Union.

Recebido: 15 de agosto de 2016

Aprovado: 11 de novembro de 2016