BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA»: A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)

ALEXANDRE LIBÓRIO. DIAS PEREIRA*

Professor Auxiliar da Faculdade de Direito da Universidade de Coimbra

Resumo: Este trabalho analisa a proteção dos dados pessoais segundo a lei portuguesa, à luz do direito da União Europeia, tendo em conta a jurisprudência do Tribunal de Justiça e as alterações introduzidas pelo Regulamento Geral (GDPR), em especial enfoque nos dados de saúde. Percorre tópicos como as noções de dados pessoais e tratamento, o âmbito de aplicação da lei, os princípios fundamentais do tratamento de dados, os direitos do titular, as obrigações do responsável pelo tratamento, e a transferência de dados para outros países e a liberdade de circulação de dados na EU.

Palavras-chave: dados pessoais – direitos do titular – princípios do tratamento – obrigações do responsável – liberdade de circulação – dados de saúde - RGPD

Abstract: This paper analyzes the protection of personal data under Portuguese law, in the light of European Union law, taking into account the case law of the Court of Justice and the changes introduced by the General Regulation (GDPR), in particular focusing on health data. It covers topics such as notions of personal data and treatment, the scope of application, fundamental principles of data processing, individual rights, the controller's duties, transfers of data to other countries and freedom of movement of data in the EU.

Keywords: personal data - rights of the holder - principles of treatment - obligations of the person in charge - freedom of movement - health data - GDPR

I. ORIGEM E EVOLUÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS

A proteção dos dados pessoais é uma matéria com crescente atualidade e interesse no âmbito da utilização da informática, especialmente em rede. A legislação regula o

* *Lex Medicinae – Revista Portuguesa de Direito da Saúde*, n.º 29 (2018).

Texto elaborado para as Jornadas sobre Proteção de Dados Pessoais, realizadas no âmbito do projeto de investigação «Privacidad y redes sociales», na Faculdade de Direito da Universidade de Salamanca, em Espanha.

tratamento destes dados e as empresas desenvolvem políticas de privacidade que visam conformar a utilização dos seus serviços com as normas legais.

Os dados pessoais de saúde são protegidos pela Lei 67/98, de 2 de outubro.[1] A partir de 25 de maio de 2018 aplica-se o Regulamento Geral de Proteção de Dados na União Europeia.[2] Para além de outros aspetos, este Regulamento Geral codifica jurisprudência do Tribunal de Justiça da União Europeia (TJUE) relativa à interpretação de normas da Diretiva 95/46, nomeadamente o chamado "direito a ser esquecido" (artigo 17.º).3 Ainda ao nível da União Europeia, a proteção dos dados pessoais está consagrada na Carta de Direitos Fundamentais da União Europeia (artigo 8.º) como o direito de todas as pessoas a que os seus dados pessoais sejam objeto de tratamento leal, para fins específicos e autorizado pela pessoa interessada ou com fundamento legítimo

[1] Lei da Proteção de Dados, alterada mais recentemente pela Lei 103/2015, de 24 de agosto. Transpõe para a ordem jurídica portuguesa a 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 dos dados pessoais e à livre circulação desses dados. Revogou a Lei 10/91, de 29 de abril, alterada pela Lei 28/94, de 29 de agosto. É por isso a segunda geração de leis de proteção de dados pessoais. A Lei 10/91 aprovou a Lei da Proteção de Dados Pessoais face à Informática e criou a Comissão Nacional de Proteção de Dados Pessoais Informatizados. Estabeleceu a disciplina legal da utilização da informática prevista no artigo 35 da Constituição da República Portuguesa, consagrado logo no texto originário de 1976 e objeto de alterações e aditamentos em diversas revisões constitucionais. Sobre a proteção de dados pessoais na bibliografia portuguesa ver, por ex., GARCIA MARQUES & LOURENÇO MARTINS, *Direito da Informática*, 2.ª ed., Almedina, Coimbra, 2006, p. 129-313, 422-442, 330-391; MONIZ, M.H., «Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde», *Revista Portuguesa de Ciência Criminal*, 7/2 (1997), p. 231-298; GONÇALVES, M.E., *Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2.ª ed., Almedina, Coimbra, 2003, p. 82-111, 173-183; SARMENTO E CASTRO, C., *Direito da informática, privacidade e dados pessoais*, Almedina, Coimbra, 2005; SOUSA PINHEIRO, A., *Privacy e protecção de dados pessoais*, AAFDL, Lisboa, 2015. Para o direito espanhol vide APARÍCIO VAQUERO, J.P. e BATUECAS CALETRÍO, A. (coord,), En torno a la privacidad y la protección de datos en la sociedad de la información, Granada. Comares, 2015, ROMEO CASABONA, C.M. (dir), *Enciclopedia de Bioderecho y Bioética*, Ed. Cátedra Interuniversitaria de Derecho y Genoma Humano – Comares y Instituto Roche, Bilbao-Granada, 2011 (disponível em <http://enciclopedia-bioderecho.com/voces/91>), esta última sugerida pelo revisor anónimo deste trabalho, que agradecemos, bem como a informação de que, no país vizinho, o Conselho de Ministros aprovou no dia 10 de novembro de 2017 o *Proyecto de Ley Orgánica de Protección de Datos* a fim de adaptar o ordenamento jurídico espanhol ao RGPD, e que substituirá a atual *Ley Orgánica* 15/1999, de 13 de dezembro, Protección de *Datos* de Carácter Personal, em vigor, tal como o RGPD, até 25 de maio de 2018 - <http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF>. Sobre este projeto *vide* GRUPO DE INVESTIGACIÓN BIGDATIUS (Uso de datos clínicos ante nuevos retos tecnológicos y científicos BigData. Implicaciones jurídicas. MINECO/FEDER. España), *Informe. Conclusiones y recomendaciones Seminario Bigdatius 30 de mayo 2017* (disponível em <http://www.bigdatius.com/conclusiones-y-recomendaciones-del-seminario-uso-de-datos-clinicos-ante-nuevos-escenarios-tecnologicos-y-cientificos-bigdata-oportunidades-e-implicaciones-juridicas/>). Ainda na bibliografia espanhola sobre o RGPD, LÓPEZ CALVO, J., *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin, 2017.

[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (artigo 99/2).

[3] Acórdão de 13 de maio de 2014, proc. C-131/12, *Google Spain SL e Google Inc c. Associação Espanhola de Dados Pessoais (AEPD)* c. *Mário Costeja Gonzalez* (pedido de decisão prejudicial apresentado pela Audiencia Nacional). ECLI:EU:C:2014:317.

legalmente previsto, e o direito de lhes aceder e de os retificar, ficando a fiscalização desta disciplina a cargo de uma autoridade independente.

Apoiada inicialmente na tutela de bens da personalidade, como o nome, a imagem ou a reserva da vida privada, prevista em diversos instrumentos de direito internacional4 e no Código Civil Português de 1966 (artigo 70 e seg.), a proteção dos dados pessoais ganhou vida própria com o desenvolvimento da informática. A lei de 30 de setembro de 1970, da Land Hesse, da República Federal da Alemanha, seria a primeira lei de proteção de dados pessoais. No direito internacional várias organizações estabeleceram regras, nomeadamente as Diretrizes sobre a política internacional em matéria de proteção da privacidade e dos fluxos transfronteiriços de dados pessoais publicada pela OCDE em 1980 e, posteriormente, a Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal (1981), as Orientações da ONU sobre a regulação de ficheiros de dados pessoais informatizados (1990)5, e normas do Acordo geral de comércio e serviços de 15 de Abril de 1994 (artigo XIV, 1, c), iii).

No que respeita à proteção constitucional dos dados pessoais na utilização da informática, o artigo 35 da CRP prevê como direito fundamental de cada cidadão o acesso aos respetivos dados informativos, bem como a retificação, a atualização, e ao conhecimento da finalidade a que se destinam, nos termos da lei, para a qual se remete igualmente a definição do conceito de dados pessoais, das condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e da sua proteção, designadamente através de entidade administrativa independente (n.º 2). Além disso, a CRP estabelece algumas linhas vermelhas em sede de tratamento informáticos de dados[6], proibindo a sua utilização para o "tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis" (nº 3), bem como "o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei" (nº 4); garante, por outro lado, o acesso universal e livre às redes informáticas de uso público, cabendo à lei definir o

[4] Artigo 12.º da Declaração Universal dos Direitos Humanos (1948), artigo 8.º da Convenção Europeia do Direitos do Homem e das Liberdades Fundamentais (1950), artigo 17 do Pacto Internacional dos Direitos Civis e Políticos (1966).

[5] <https://www.privacycommission.be/en/united-nations>

[6] Aos dados pessoais constantes de ficheiros manuais é garantida legalmente proteção idêntica (art. 35/7 CRP).

regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional (nº 6).

Na jurisprudência afirma-se a proteção dos dados pessoais como projeção do direito fundamental à "autodeterminação informacional"7. Todavia, o regime dos dados

[7] Acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1, Rel. Cons. Helena Moniz, in <www.dgsi.pt>. A designação «direito à autodeterminação informativa» foi utilizada pelo tribunal federal constitucional alemão no âmbito de um processo relativo a informações pessoais coletadas durante o censo de 1983. O BFGH considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelos direitos gerais das pessoas garantidos na constituição alemã. Este direito fundamental garante, a este respeito, a capacidade do indivíduo para determinar, em princípio, a divulgação e o uso de seus dados pessoais. As limitações a esta autodeterminação informacional só são permitidas em caso de interesse público primordial (BVerGE, Acórdão de 15 de dezembro de 1983: «Recht auf informationelle Selbstbestimmung», *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, org. Leonardo Martins, Montevideo, 2005, <http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf>).

A figura foi recebida pela doutrina portuguesa: o "direito à autodeterminação informativa previsto no art. 35.º, da CRP, (…) protege uma amplitude de direitos fundamentais para lá do direito à privacidade (…) dá 'a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»'" (GOMES CANOTILHO, J.J., MOREIRA, V., *Constituição da República Portuguesa Anotada*, vol. 1, 4.ª ed., Coimbra Editora, 2007, p. 551, também citado no referido acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014). Por seu turno, Joaquim Sousa Ribeiro considera que este direito «impede que o 'eu' seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga -se o *direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um *direito à reserva* (proibição de revelação)» (SOUSA RIBEIRO, J., «A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas», in *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho,* vol. III, Coimbra Editora, p. 853).

Por seu turno, o Tribunal Constitucional, considerou que «Por autodeterminação informativa poderá entender-se o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada» (Acórdão do TC n° 442/2007, de 14 agosto de 2007). Em um outro acórdão, em processo relativo à conservação de dados no SIRP, julgou que o direito à reserva sobre a intimidade da vida privada faz parte do núcleo do direito ao livre desenvolvimento da personalidade previsto no art. 26 da CRP e inclui, como diferentes manifestações, o *direito à solidão*, o *direito ao anonimato* e o *direito à autodeterminação informativa* (Acórdão do TC n.º 403/2015, proc. 773/15).

A figura seria consagrada pela jurisprudência em vários acórdãos, que se reúnem em grupos de casos. Para começar, existem casos sobre «justa causa» de levantamento de sigilo bancário em processo de divórcio para apurar o património do casal, pronunciando-se os tribunais pela prevalência do interesse público da administração de justiça sobre o segredo bancário protegido nos termos dos artigos 78 e 79 do RGIC - Regime Geral de Instituições de Crédito – vide acórdão do TC nº 278/95, de 31 de maio de 1995 ("o segredo bancário não é um direito absoluto, antes pode sofrer restrições impostas pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos. (…) Assim sucede com os artigos 135°, 181° e 182° do atual Código de Processo Penal, os quais procuram consagrar uma articulação ponderada e harmoniosa do sigilo bancário com o interesse constitucionalmente protegido da investigação criminal, reservando ao juiz a competência para ordenar apreensões e exames em estabelecimentos bancários"); acórdão do TC n° 442/2007, de 14 agosto de 2007 (o sigilo bancário não integra a esfera íntima da vida privada); acórdão do STJ de Uniformização de Jurisprudência nº 2/08, de 13 de fevereiro de 2008; acórdão do Tribunal da Relação de Coimbra, de 6 de abril de 2010, proc. 120-C/2000.C1; acórdão do Tribunal da Relação de Évora, de 14/9/2017, proc. 2829/16.9T8PTM-B.E1).

Um outro grupo de casos diz respeito ao ressarcimento de danos morais traduzidos em humilhação, vergonha, embaraço causados pela utilização de dados pessoais sobre nomeações político-partidários. Considerando que subjacente à proteção de dados está o "direito à autodeterminação informativa" e a proteção da privacidade, o STJ considerou que o facto de os referidos dados serem públicos não

pessoais é marcado igualmente por exigências de bom funcionamento do mercado interno. Com efeito, a Diretiva 95/46 afirma a liberdade de circulação de dados como ferramenta das quatro liberdades do mercado interno (pessoas, mercadorias, serviços e capitais), respeitando os direitos fundamentais das pessoas segundo o princípio do "elevado nível de proteção". A proteção da vida privada a nível nacional deixa de ser justificação bastante para impedir a circulação transfronteiriça dos dados pessoais, uma vez que a proteção em cada Estado-membro fica condicionada às exigências do mercado interno. Não obstante – *et pour cause* -, o tratamento de dados pessoais efetuado por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (por exemplo correspondência ou listas de endereços, como refere o considerando 12 da Diretiva 95/4) é excluído do âmbito de aplicação do regime legal.

II. PANORAMA DA LEI PORTUGUESA DOS DADOS PESSOAIS

1. Noções operativas (dados pessoais, tratamento) e âmbito de aplicação (pessoal, material e geográfico)

Em transposição da Dir. 95/46, a Lei 67/98 define o seu âmbito de aplicação, no sentido de reger, designadamente, o tratamento de dados pessoais por meios total ou parcialmente automatizados, e o tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados (artigo 4/1). Quanto ao âmbito geográfico, aplica-se a prestador estabelecido em Portugal independentemente

---

autorizaria o seu tratamento em termos de afixação de um mapa de pessoal com os nomes e os respetivos vencimentos, filiação partidária e contratação por concurso ou por nomeação (Acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1).

O «direito à autodeterminação informativa» é também referido na jurisprudência a propósito de um sistema de registo informatizado das idas ao WC numa empresa, tendo sido julgado que tal não constituiria devassa por meio informático para efeitos do artigo 193 Código Penal, em razão de ser um sistema aceite pela CNPD destinado a controlar a produtividade dos trabalhadores e não a sua vida privada, já que o sistema não registaria a atividade no interior do WC mas apenas o número de vezes de utilização e o tempo aí passado pelo trabalhador (Acórdão do Tribunal da Relação do Porto, de 31 de maio de 2006, proc. 0111584).

Finalmente, encontram-se ainda acórdãos sobre o tema no domínio sensível dos dados pessoais de saúde. O sigilo médico é objeto de proteção legal (Lei 12/2015, CDOM, LADAR), todavia o Código de Processo Penal prevê a possibilidade de dispensa de sigilo, estabelecendo no artigo 135º/2 que "Havendo dúvidas fundadas sobre a legitimidade da escusa, a autoridade judiciária perante a qual o incidente se tiver suscitado procede às averiguações necessárias. Se, após estas, concluir pela ilegitimidade da escusa, ordena, ou requer ao tribunal que ordene, a prestação do depoimento". Com base nisto, o Tribunal da Relação do Porto considerou que o sigilo profissional médico pode ser dispensado em processo de burla tributária (Acórdão do Tribunal da Relação do Porto, de 13 de março de 2013, proc. 605/10.1T3AVR-A.P1, Des. Álvaro Melo). Todavia, o mesmo tribunal, citando o Acórdão do TC nº 155/2007, decidiu que pode ser feita recolha de saliva através de zaragatoa bucal para obter prova, mas essa diligência tem que ser ordenada por juiz e não pelo MP (Acórdão Tribunal da Relação do Porto acórdão de 10 de julho de 2013, proc. 1728/12.8JAPRT.P1, Des. Joaquim Gomes).

da origem e do destino dos dados. Quanto aos destinatários, abrange tanto empresas como organismos públicos, com exclusão de atividades puramente domésticas ou particulares.

Dados pessoais são, para efeitos desta lei, "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados')", isto é, uma "pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" (art. 4/a).

A noção de dados pessoais é ampla, abrangendo "seguramente, o nome de uma pessoa a par do seu contacto telefónico ou de informações relativas às suas condições de trabalho ou aos seus passatempos"8, incluindo os dados de IP na medida em que tornam identificável a pessoa (Dir. 95/46, considerando 26). Uma categoria especial de dados, para efeitos de regime, é composta pelos chamados dados sensíveis, incluindo filiação sindical, dados de saúde (físicos ou psíquicos), dados genéticos, vida privada (por ex. orientação sexual, consumo de drogas), raça e etnia, etc.

São titulares de dados pessoais apenas as pessoas singulares. Pese embora as pessoas coletivas poderem ter direitos de personalidade que não sejam indissociáveis da personalidade singular9, o regime dos dados pessoais é limitado às pessoas singulares.

A noção de tratamento de dados pessoais abrange quaisquer operações (automáticas ou manuais) de recolha, registo, organização, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer forma de colocação à disposição do público, com comparação ou interconexão, bem como bloqueio, apagamento ou destruição. Com efeito, o tratamento de dados pessoais consiste em "qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a

---

[8] Acórdão do Tribunal de Justiça de 6 de novembro de 2003, proc. C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596.

[9] Tal como decidiu o Tribunal de Constitucional no seu acórdão nº 198/95 a propósito da preservação de uma esfera de sigilo para as pessoas coletivas, em especial para os segredos de negócios, no sentido de que o direito ao sigilo da correspondência não é incompatível com a natureza das pessoas coletivas. Todavia, posteriormente, a jurisprudência do TC mostrou-se mais restritiva, pronunciando-se no sentido de que "Não existe no nosso sistema uma equiparação ou presunção de igualdade entre personalidade singular e personalidade coletiva" (acórdão nº 569/98, proc. 505/96). Na doutrina, GOMES CANOTILHO, J.J. & MOREIRA, V., *Constituição da República Portuguesa Anotada*, 3ª edição revista, Almedina, Coimbra, 1993.

utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" (artigo 3/b).

A lei abrange tratamentos efetuados

a) No âmbito de atividades de estabelecimento do responsável do tratamento situado em território português, entendendo-se por responsável "a pessoa singular ou coletiva, a autoridade publica, os serviços ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais" (artigo 3-d); pela negativa, a lei só não se aplica ao tratamento efetuado por pessoa singular no âmbito de atividades exclusivamente pessoais ou domésticas (artigo 4/2).

b) Fora do território nacional em local onde a legislação portuguesa seja aplicável por força do direito internacional,

c) Por responsável estabelecido fora da União Europeia, mas que recorra a meios situados no território português (salvo se foram apenas utilizados para trânsito através do território da EU), devendo neste caso designar um representante estabelecido em Portugal.[10]

d) Videovigilância e outras formas de captação, tratamento e difusão de sons e imagens contendo dados pessoais se o responsável estiver domiciliado em Portugal ou utilizar um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português.

Em suma, a lei regula o tratamento de dados pessoais efetuado no âmbito das atividades de estabelecimento do responsável do tratamento situado em território português ou por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia (art. 4/3-a/c), e, em certas condições, à videovigilância (artigo 4/4).[11]

---

[10] Nos termos do acórdão *Google Spain*, para efeitos do art. 4/1-a da Dir. 95/47, "é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, […] quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro."

[11] A videovigilância e outros tratamentos de imagem estão sujeitos a notificação e eventual autorização quando identifiquem ou tornem identificável a pessoa. Excluem-se os sistemas de vigilância privada do domicílio particular, salvo se permitirem captar imagens de vizinhos ou nos condomínios.

No acórdão *Google Spain*12, o Tribunal de Justiça pronunciou-se no sentido de que "a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», […] quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado «responsável» pelo dito tratamento".

2. Princípios fundamentais do tratamento de dados

O tratamento de dados pessoais obedece a um conjunto de princípios fundamentais, designadamente a transparência, a finalidade, e a qualidade dos dados (licitude e lealdade; adequação, pertinência e proporcionalidade; exatidão e atualização). A licitude do tratamento significa que tratamento de dados pessoais será lícito se houver (1) consentimento do titular dos dados; (2) execução de contrato ou diligências prévias à sua formação ou declaração de vontade negocial do titular de dados; (3) cumprimento de obrigação legal a cargo responsável do tratamento; (4) proteção de interesses vitais do titular dos dados, se este estiver incapaz de consentir; (5) execução de missão de interesse público ou exercício de autoridade pública; (6) prossecução de interesses legítimos do responsável ou de terceiro a quem os dados sejam comunicados (desde que não devam prevalecer os interesses ou direitos do titular dos dados). Todavia, tratando-se de dados sensíveis, rege uma proibição geral de tratamento sujeita a algumas exceções, nomeadamente (a) consentimento do titular ou autorização legal específica, (b) a cláusula geral do art. 7º/3, e (c) a situação específica do tratamento de dados de saúde.

Em suma, o tratamento de dados pessoais deve observar princípios fundamentais como a qualidade dos dados apurada nomeadamente em função da finalidade do

---

Todavia, em certos casos, a lei impõe a obrigatoriedade de sistemas de videovigilância privada, por ex. em casinos, bancos e outros estabelecimentos comerciais (*vide*, por ex., Decreto-Lei n.º 28/2004, de 4 de fevereiro, com alterações posteriores). Além disso, o art. 7º/3 da Lei 67/98 autoriza o tratamento de dados sensíveis, nomeadamente para fins de exercício ou defesa de um direito em processo judicial e se for efetuado exclusivamente com essa finalidade, hipótese que segundo o Supremo Tribunal de Justiça, abrangerá os postos de combustíveis (acórdão de 20 de junho de 2001). De igual modo, os trabalhadores podem estar sujeitos a videovigilância "sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem", cabendo ao empregador informar "o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados" (artigo 20/2-3 do Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com alterações posteriores).

[12] *Google Spain*, para. 41 e conclusão 1)

tratamento (artigo 5) e a legitimidade do seu tratamento, que depende de consentimento do seu titular13 ou de autorização legal (artigo 6).

3. Direitos do titular e obrigações do responsável pelo tratamento

Ao titular é reconhecido um leque de direitos sobre os seus dados pessoais, como sejam o direito ao esquecimento (nomeadamente em termos de prazo máximo de conservação), o direito de informação (art. 10º), o direito de acesso, retificação e atualização, apagamento ou bloqueio, o direito a não sujeição a decisão individual automatizada, o direito de oposição (em especial no marketing direto)[14], e o direito ao não tratamento de dados sensíveis (requisitos do consentimento)

Por seu turno, o responsável pelo tratamento tem um conjunto de obrigações que passam por garantir a segurança do tratamento de dados, a confidencialidade (dever de sigilo) dos dados, e um dever de colaboração (prestando informações, permitindo a realização de inspeções, facultando documentos).

4. Transferência de dados para outros países e a liberdade de circulação de dados na UE

Em matéria de transferência de dados pessoais para outros países, rege o princípio da liberdade de circulação de dados entre Estados-Membros da EU (art. 18º). Já para um país terceiro[15], a situação depende de apreciação caso a caso. Se a Comissão considerar

[13] Isto é, "qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento" (artigo 3-h).

[14] No que respeita à proteção da privacidade nas comunicações eletrónicas (dados de tráfego, anonimização e de conservação, comunicações não solicitadas, dados de localização, listas de assinantes) rege a Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012 de 29 de agosto, transpondo respetivamente a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, e a Diretiva n.º 2009/136/CE, na parte que a altera, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas. A Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, 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 (transposta pela Lei n.º 32/2008 de 17 de julho, artigo 6), que estabelecia o período de conservação de 1 ano foi julgada inválida pelo Tribunal de Justiça no acórdão de 8 de abril de 2014, procs. apensos C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238. No Brasil a "Lei Marco Civil da Internet" (Lei nº 12.965, de 23 de abril de 2014) prevê 1 ano como prazo de conservação de dados a cargo do provedor de conexão (artigo 13). Sobre esta Lei, *vide* DIAS PEREIRA, A.L., «Marco Civil da Internet" e seus Reflexos no Direito da União Europeia», *Revista da ABPI*, 142 (2016), p. 2-21.

[15] O conceito de transferência de dados para um país terceiro foi interpretado pelo TJUE, para efeitos do artigo 25 da Diretiva 95/46, no sentido de abranger "quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, de uma pessoa singular ou coletiva que alberga o sítio Internet no qual a página pode ser consultada e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, dados de carácter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros - acórdão de 6 de novembro de 2003, proc. C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596

que o país terceiro oferece um nível de proteção adequado, a transferência é permitida.16 Caso contrário, a transferência é proibida, salva nas situações legalmente previstas.

A circulação de dados pessoais entre Estados-Membros da União Europeia é livre (artigo 18). Este aliás é um dos objetivos primordiais da Dir. 95/46/CE, tendo em conta a importância da informação para o mercado interno. Pelo contrário, só é permitida a transferência de dados para países terceiros que assegurem um nível de proteção adequado (artigo 19/1). O que, na ausência de determinação da Comissão Europeia, compete à CNPD apurar, tendo em conta nomeadamente a natureza dos dados, a finalidade e a duração do tratamento, os países de origem e de destino final, as regras legais e deontológicas aplicáveis nesse Estado, e as medidas de segurança aí aplicáveis, cabendo-lhe depois comunicar à Comissão Europeia as deliberações negativas (artigo 19/2-5). Mesmo que se conclua que um Estado terceiro não assegura um nível de proteção adequado a CNPD pode autorizar a transferência se for (a) inequivocamente consentida pelo titular dos dados ou necessária para certos fins (responsabilidade contratual, interesse público, exercício de direitos, proteção de interesses vitais do titular) ou (b) realizada a partir de um registo público aberto à consulta do público ou de qualquer pessoa que possa provar um interesse legítimo (artigo 20/1; ver também o 27/4), ou (c) se o responsável pelo tratamento assegurar, mediante cláusulas contratuais adequadas – em especial cláusulas tipo aprovadas pela Comissão Europeia -, mecanismos suficientes de garantia de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do seu exercício.

---

[16] Era o que sucedia, por exemplo, com o protocolo de *Safe Harbor* de transferência de dados da União Europeia para os EUA, o qual todavia foi declarado inválido pelo TJUE no acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*: "1) O art. 25.°, n.º 6, da Diretiva 95/46/CE (…) lido à luz dos art.s 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Department of Commerce dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um Estado-Membro, na aceção do art. 28.° desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado. 2) A Decisão 2000/520 é inválida."

Em fevereiro de 2016, a União Europeia e os EUA chegaram a um acordo sobre a transferência de dados pessoais, denominado "*Privacy Shield*" (Escudo de Privacidade), tendo sido adotada posteriormente a Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

5. Entidade reguladora

As consequências da violação das regras de proteção de dados pessoais incluem sanções administrativas, sanções criminais e outras. A entidade reguladora é a CNPD - Comissão Nacional de Proteção de Dados, cuja natureza, atribuições, competências, composição e funcionamento estão previstas nos artigos 21 a 26 da Lei 67/98 (vide www.cnpd.pt).

III. OS DADOS DE SAÚDE

1. Noção de dados de saúde

Os dados de saúde relevam enquanto dados pessoais. Segundo o TJUE, a noção de dados de saúde deve ser interpretada em termos amplos de modo a abranger informação sobre todos os aspetos, tanto físicos como psíquicos, da saúde de uma pessoa.[17]

O grupo de trabalho sobre proteção de dados, previsto no artigo 29 da Dir. 95/47, desenvolveu a interpretação deste conceito recomendando que os dados de saúde deveriam abranger: (a) quaisquer dados pessoais estritamente relacionados com o estado de saúde da pessoa, tais como dados genéticos ou dados sobre o consumo de medicamentos, álcool e drogas e (b) quaisquer outros dados contidos nos ficheiros clínicos sobre o tratamento de um paciente, incluindo dados administrativos (numero de segurança social, data de admissão no hospital, etc.), de modo a que qualquer dado que não seja relevante para o tratamento do paciente não seja inserido nos ficheiros médicos.18

2. Licitude de tratamento de dados de saúde

Os dados de saúde, incluindo os dados genéticos, são considerados dados sensíveis. Nessa medida, são objeto de proteção reforçada (artigo 7/1-3).19 O tratamento de dados

[17] *Bodil Lindqvist*, para. 50 (concluindo no para. 51 que "a indicação do facto de uma pessoa se ter lesionado num pé e estar com baixa por doença a meio tempo constitui um dado de carácter pessoal relativo à saúde" na aceção do artigo 8/1 da Diretiva 95/46).

[18] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (EHR), 2007. Sobre as questões suscitadas pelo processo clínico eletrónico, regulado nos EUA pela *Health Insurance Portability and Accountability Act* de 1996 (Public Law 104-191), RAPOSO, V.L., «O Fim da 'Letra De Médico': Problemas Suscitados pelo Processo Clínico Eletrónico em Sede de Responsabilidade Médica», *Lex Medicinae,* nº 19 (2013), p. 51-78.

[19] A propósito da noção de interesses legítimos do responsável pelo tratamento, o TJUE decidiu no acórdão de 19 de outubro de 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, que um prestador de serviços de meios de comunicação em linha poderá recolher e utilizar dados pessoais

de saúde é legalmente permitido, juntamente com os relativos à vida sexual, se for (artigo 7/4):

a) necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde.

b) efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional20

c) notificado à CNPD, nos termos do artigo 27º21, devendo o pedido conter as informações previstas no artigo 29, incluindo o tempo de conservação dos dados pessoais.

d) realizado com medidas adequadas de segurança da informação.

Efetuado nessas condições, o tratamento de dados de saúde não está sujeito a autorização da CNPD, ao contrário da sua interconexão22, que deve ser solicitada pelo responsável pelo tratamento, exceto quando legalmente prevista (artigo 9).

3. Direitos do titular dos dados

Ao titular de dados de saúde, enquanto dados pessoais, são reconhecidos diversos direitos. Para começar, o direito de informação sobre a identidade do responsável, as finalidades do tratamento, e outras informações nomeadamente sobre os destinatários dos dados (artigo 10/1).23 Depois, o direito de acesso, i.e., saber se os dados foram tratados, por e para quem e para que fins, a lógica de tratamento automatizado (artigo

---

de um utilizador desses serviços (no caso concreto, o número de IP) sem o consentimento deste na medida em que sejam necessárias para permitir e faturar a utilização concreta dos referidos serviços por esse utilizador, bem como utilizar os referidos dados após o termo de uma sessão de consulta desses meios de comunicação para garantir o funcionamento geral desses mesmos serviços. De notar que as leis de autorização de tratamento de outras categorias de dados sensíveis devem indicar obrigatoriamente os elementos previstos no artigo 30.

[20] Ver também o regime do segredo médico no novo Código Deontológico da Ordem dos Médicos, aprovado pelo Regulamento n.º 707/2016, de 21 de julho, artigos 29 a 38. O respeito pela confidencialidade dos dados de saúde é uma das condições da telemedicina, nos termos deste Código. Sobre o tema, DIAS PEREIRA, A.L., «Telemedicina e farmácia online: aspetos jurídicos da eHealth», *Revista da Ordem dos Advogados*, Ano 75, I/II (2015), p. 55-78.

[21] A CNPD autoriza a simplificação ou isenção de notificação para determinadas categorias de acordos (artigo 27/1-2). Alguns tipos de tratamentos estão isentos da obrigação de notificação à CNPD, em virtude de autorizações concedidas, por exemplo, para o processamento de salários, distribuição de lucros, gestão de utentes de bibliotecas e arquivos, gestão e faturação de contactos com clientes, fornecedores e prestadores de serviços, etc. São excluídos por outro lado os tratamentos de dados pessoais efetuados por pessoa singular no âmbito de atividades exclusivamente pessoais ou domésticas (e.g. listas particulares de contactos). *Vide* <https://www.cnpd.pt/bin/legal/isencoes.htm>

[22] I.e. "qualquer forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade" (artigo 3-i).

[23] Na recolha de dados em redes abertas o titular dos dados tem direito a ser informado sobre a possibilidade de os seus dados circularem na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados (artigo 10/4).

11/1-a-c). O direito de acesso abrange ainda o direito de retificação, apagamento ou bloqueio de dados objeto de tratamento ilegal, nomeadamente quando sejam incompletos ou inexatos (artigo 11/1-d), e o direito de "atualização", i.e., de notificar a retificação, o apagamento ou o bloqueio aos terceiros a quem os dados tenham sido comunicados (artigo 11/1-e). De notar que são excluídos do direito de informação certos tratamentos de dados, nomeadamente para fins de segurança de Estado, investigação criminal, jornalísticos ou de expressão artística ou literária (artigo 10/5-6). Nestes casos, o direito de acesso (incluindo retificação e atualização) exerce-se através da CNPD, podendo esta limitar-se a informar o titular dos dados sobre as diligências efetuadas quando a comunicação dos dados ao titular puder prejudicar as referidas finalidades (artigo 11/2-4). Relativamente aos dados de saúde, incluindo os dados genéticos, o exercício do direito de acesso não é livre, uma vez que, nos termos da lei, cabe ao médico escolhido pelo titular dos dados (artigo 11/5).

Por outro lado, o titular tem o direito de oposição, em qualquer altura, justificada por razões ponderosas e legítimas relacionadas com a situação particular do titular dos dados, e o direito de oposição ao tratamento de dados pessoais para fins de marketing direto (artigo 12).

Finalmente, o direito de não ser objeto de decisões individuais automatizadas baseadas exclusivamente numa avaliação da sua personalidade (por ex. em termos de capacidade profissional, crédito, confiança ou comportamento), salvo no âmbito de um contrato por si solicitado[24] ou mediante autorização da CNPD (artigo 13/1-2-3). Assim, em princípio, a pessoa tem o direito de não ser tratada com base em decisões automatizadas tomadas por robots ou outros sistemas de IA com base na análise dos seus dados de saúde.

4. Deveres do responsável pelo tratamento dos dados

O responsável pelo tratamento de dados tem, para começar, um dever especial de segurança e confidencialidade do tratamento. Cabe-lhe adotar medidas técnicas e organizativas para proteger os dados contra tratamentos ilícitos, nomeadamente contra a destruição, perda, alteração, difusão ou acesso não autorizados, em especial quando envolva a transmissão dos dados por rede, e assegurar um nível de segurança adequado, tendo em conta os conhecimentos técnicos disponíveis, os custos de aplicação, os riscos

[24] Por ex., uma empresa de crédito ao consumo condiciona a celebração de contratos a um tratamento automatizado do perfil do cliente no *Facebook*.

do tratamento, e a natureza dos dados (artigo 14/1). No caso de subcontratação, o responsável pelo tratamento não fica exonerado de responsabilidade pelo cumprimento do dever de segurança, mas o subcontratante fica corresponsável (artigo 14/2-4).

O responsável pelo tratamento de dados de saúde, enquanto dados sensíveis, deve adotar medidas especiais de segurança adequada ao controlo: a) da entrada nas instalações, b) dos suportes de dados, c) da inserção, d) da utilização, e) de acesso, f) da transmissão, g) da introdução (o quê, quando e por quem), h) do transporte (artigo 15/1).

Os dados de saúde e da vida sexual, incluindo os genéticos, devem ser logicamente separados dos restantes dados pessoais, ou seja, devem ser objeto de um ficheiro próprio (HMR) (artigo 15/3). Além disso a CNPD pode exigir que a transmissão em rede seja cifrada quando a circulação em rede de dados sensíveis possa perigar direitos, liberdades e garantias (artigo 15/4).

Finalmente, os responsáveis pelo tratamento, bem como quaisquer pessoas incluindo membros e pessoal da CNPD, que, no exercício das suas funções, tenham conhecimento de dados pessoais tratados, ficam obrigado a sigilo profissional, mesmo após o termo das suas funções (artigo 17).

5. A lei da informação pessoal de saúde e genética, o regime de acesso aos documentos administrativos e o Código Deontológico da Ordem dos Médicos

Além da lei dos dados pessoais a proteção dos dados se saúde é ainda objeto da lei da informação pessoal de saúde e genética, da lei de acesso aos documentos administrativos[25], e do Código Deontológico dos Médicos.

A Lei 12/2005 estabelece igualmente que o acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento, é feito através de médico, com habilitação própria, escolhido pelo titular da informação (art. 3/3). A informação de saúde pertence à pessoa a que diz respeito, sendo as unidades do sistema de saúde seus depositários, e só pode ser utilizada para fins de prestação de cuidados e investigação

[25] Apontando criticamente a "bicefalia de regimes", consoante a natureza pública ou privada do prestador de serviços (articulando a Lei 67/98 com a Lei 12/2005 de 26 de janeiro, e a Lei 46/2007, de 24 de agosto), DIAS PEREIRA, A.G., «Dever de documentação, acesso ao processo clínico e sua propriedade: uma perspectiva europeia», *Revista Portuguesa do Dano Corporal*, nº 16 (2006), e, do mesmo Autor, *Direitos dos pacientes e responsabilidade médica*, Coimbra Editora, 2015 (caps. 3 e 4 da parte III, sobre o direito à documentação e ao acesso à informação pessoal de saúde e sobre o direito à reserva da intimidade da vida privada (os dados de saúde), com referência à problemática do processo clínico eletrónico); BARBOSA, C., «Aspectos Jurídicos do Acesso ao Processo Clínico», *Lex Medicinae*, nº 7 (2010), p. 107-140.

em saúde e outros estabelecidos pela lei (art. 3º/1). Quando aos fins de investigação, o acesso à informação de saúde pode ser facultado se for anonimizada (art. 4/3). O titular da informação tem direito ao conhecimento de todo o processo clínico que lhe diga respeito, salvo circunstâncias excecionais devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial, ou de o fazer comunicar a quem seja por si indicado (art. 3/2). O processo clínico abrange qualquer registo, informatizado ou não, que contenha informação de saúde sobre doentes ou seus familiares, devendo conter toda a informação médica disponível que diga respeito à pessoa (art. 5/2-3). Sendo que a consulta e a edição do processo clínico cabem apenas ao médico ou sob sua supervisão a outro profissional igualmente sujeito ao dever de sigilo (art. 5/4-5).

O responsável da unidade de saúde pelo tratamento da informação de saúde está sujeito a determinados deveres, no que respeita à confidencialidade, à segurança das instalações e dos equipamentos, ao controlo do acesso à informação, e tem ainda um dever reforçado de sigilo e de educação deontológica dos profissionais (art. 4º/1). É proibido o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, e são exigidos níveis de segurança que evitem nomeadamente a sua destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação (art. 4º/2). Além disso, a gestão dos sistemas de informação deve assegurar a realização regular e frequente de cópias de segurança da informação de saúde (art. 4º/6).[26]

Por seu turno, a Lei 46/2007 estabelecia que o acesso a documentos nominativos que incluam dados de saúde podia ser efetuado pelo titular da informação ou por terceiro autorizado por escrito pelo titular ou por quem demonstre um interesse direto, pessoal e legítimo, suficientemente relevante segundo o princípio da proporcionalidade (artigos 2/3 e 6/5). Ao contrário da lei dos dados pessoais e da lei da informação pessoal de saúde, que exigem a mediação do médico no acesso aos dados, no âmbito da LADAR a comunicação de dados de saúde seria feita por intermédio de médico apenas se o requerente o solicitasse (artigo 7). Ao abrigo desta lei, o acesso –não abrangendo notas pessoais, esboços, apontamentos e outros registos de natureza semelhante, excluídos da

[26] A este respeito, note-se que o Regulamento (UE) 611/2013 da Comissão de 24 de junho de 2013 impõe um dever de notificação em caso de violação de dados pessoais.

noção de documento administrativo (artigo 3/2-a) - poderia ser facultado a terceiro parecendo poder dispensar-se a mediação do médico.

Entretanto a Lei 46/2007 foi revogada e substituída pela Lei 26/2016, de 22 de agosto, a qual, embora ressalve o disposto na lei dos dados pessoais e remeta para a Lei 12/2005, parece manter a bicefalia uma vez que contempla a possibilidade de ser dado acesso a terceiro, "que demonstre ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido na informação", sendo a intervenção do médico apenas estritamente necessária quando não se possa apurar a vontade do titular da informação (interpretação conjugada dos artigos 3/3 e 7).

Finalmente, cumpre ainda referir que o novo Código Deontológico da Ordem dos Médicos, aprovado em 2016, regula o tratamento da informação de saúde no artigo 37. Em suma, a informação de saúde só pode ser utilizada pelo sistema de saúde nas condições expressas em autorização escrita do seu titular ou de quem o represente (nº 3), embora o acesso a informação de saúde possa ser facultado para fins de investigação, desde que anonimizada (nº 4). Compete à gestão dos sistemas que organizam a informação de saúde garantir, por um lado, a separação entre a informação de saúde e genética e a restante informação pessoal, designadamente através da definição de diversos níveis de acesso, e por outro, o processamento regular e frequente de cópias de segurança da informação de saúde, salvaguardadas as garantias de confidencialidade estabelecidas por lei (nº 4). Além disso, este preceito corrobora o dever dos responsáveis pelo tratamento da informação de saúde de tomar as providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais (nº 1). Cabe às unidades do sistema de saúde impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, incluindo as respetivas cópias de segurança, assegurando os níveis de segurança apropriados e cumprindo as exigências estabelecidas pela legislação que regula a proteção de dados pessoais, nomeadamente para evitar a sua destruição, acidental ou ilícita, a alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação (nº 2).

IV. O "DIREITO AO ESQUECIMENTO" E O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

1. O acórdão *Google Spain*

No acórdão *Google Spain*27, o Tribunal de Justiça pronunciou-se sobre o chamado "direito ao esquecimento" nos termos da Dir. 95/46. Esta diretiva garante às pessoas em causa o direito de obterem do responsável pelo tratamento, consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o regime nela estabelecido, nomeadamente devido ao carácter incompleto ou inexato desses dados (artigo 12/b). No caso em concreto, o nome do cidadão espanhol aparecia numa lista de resultados de pesquisa do Google no âmbito de um processo antigo de dívidas ao fisco. O cidadão espanhol solicitou a remoção desse resultado, que considerava ofensivo da sua hora e bom nome, mas a empresa Google alegou que não tinha o dever de proceder a esse bloqueio, desde logo por não estar estabelecida na União Europeia, tendo aí apenas uma sucursal que geria o negócio da publicidade.

O Tribunal de Justiça considerou, relativamente ao âmbito de aplicação territorial da Diretiva, que um único operador económico deve ser tratado como uma única entidade jurídica. Sendo a publicidade, feita pela filial espanhola, o *core business* da norte-americana *Google Inc.*, que processa os dados, então devem ser tratadas como uma mesma entidade para efeitos da lei de dados pessoais. O Advogado-Geral, cuja opinião não foi seguida pelo Tribunal, alegou o caso *Lindqvist*, no qual o Tribunal considerara que o carregamento de informação numa página web não seria uma transferência de dados para fora da EU. Mais alegou que o tratamento de dados é passivo, que a Google apenas fornece um instrumento de localização sem controlar os resultados, e, além disso, que seria excessivamente oneroso obrigar as empresas a, caso a caso, proceder à limpeza dos resultados de pesquisa.

Todavia, o Tribunal de Justiça foi de outro entendimento, decidindo que a Google teria que remover as referências a *Costeja González* da sua lista de resultados e impedir o motor de pesquisa da Google de apresentar a página de origem onde a informação está disponível. O Tribunal julgou que "o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que

[27] Acórdão de 13 de maio de 2014, proc. C-131/12, ECLI:EU:C:2014:317.

contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita."

No entender do Tribunal, a pessoa em causa tem o direito de que a informação em questão sobre si "deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7° e 8° da Carta de Direitos Fundamentais da União, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa 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."[28]

Quanto ao âmbito de proteção do direito ao apagamento de dados ilegalmente tratados, o Tribunal considera que abrange o direito a ser esquecido. Todavia, os deveres do operador do motor de pesquisa são limitados à sua esfera de controlo, i.e.,

[28] Sobre o acórdão *Google Spain*, *vide* JONES, J., «Control-alter-delete: the 'right to be forgotten'», *European Intellectual Property Review (*2014), p. 595-601; CROWTHER, «Remember to forget me: The recent ruling in Google v AEDP and Costeja", *Computer and Telecommunications Law Review*, 20 (2014), p. 163-165; KELSEY, K., «Google Spain and Google Inc. v-. AEPD and Mario Costeja Gonzalez: protection of personal data, freedom of information and the 'right to be forgotten», *European Human Rights Law Review* (2014), p. 395-400; WIEBE, A., «Data protection and the internet: irreconcilable interests? The UE Data Protection Reform Package and CJEU case law», *Journal of Intellectual Property Law* (2015), p. 64-68; SPIECKER, I., «A new framework for information markets: Google Spain», *Common Market Law Review,* 52 (2015), p. 1033-1058; CASIMIRO, S.V., «O direito a ser esquecido pelos motores de busca: o Acórdão Costeja», *Revista de Direito Intelectual*, 2014/2, p. 307-353; CALVÃO, F.U., «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual,* 2015/2, p. 67-84 (preferindo falar em "direito à desassociação"); DE HERT, P. / PAPAKONSTANTINOU, V., «Google Spain: Addressing Critiques and Misunderstanding One Year Later», *Maastricht Journal of European and Comparative Law*, Vol. 22, Nº 4 (2015), p. 624-638; SARRIÓN ESTEVE, J. «El alcance territorial de una sentencia que no tenemos derecho a olvidar: una particular aproximación a Google Spain», *CEF Legal: revista práctica de derecho. Comentarios y casos prácticos*, Nº 184 (2016), p. 53-72.

aos seus algoritmos e resultados de pesquisa, não abrangendo terceiros. Por outro lado, os motores de pesquisa não seriam protegidos pelos "media privileges".29

Embora conhecido pela consagração do chamado direito ao esquecimento considera-se que o alcance deste acórdão é especialmente significativo na definição do âmbito territorial, falando-se a propósito no princípio da territorialidade alargado ('principle of territoriality extended').30 A *Google Inc.* atribuiu à *Google Spain* o papel de agente comercial de promoção e venda em linha de produtos e serviços publicitários, sem estar envolvido no trabalho do motor de pesquisa.31

Contra uma interpretação restritiva o Tribunal entendeu não ser importante a forma jurídica do responsável pelo tratamento na medida em que a filial atua de modo estável e efetivo. Ou seja, a atuação não tem que ser diretamente realizada pelo estabelecimento, mas antes apenas no contexto das atividades do estabelecimento. Deste modo, o Tribunal deitou por terra a estratégia das empresas que estabelecem sucursais na União Europeia para tratar dos assuntos comerciais enquanto o tratamento dos dados pessoais é efetuado pelas casas-mãe nos EUA (por ex. *Google*, *Facebook*).

O tribunal considera, à luz de casos anteriores (*Lindqvist*, C-101/01; *Satamedia*, C-73/07) que há tratamento de dados na atividade de encontrar dados na internet, indexá-los automaticamente, armazena-los ainda que temporariamente e finalmente disponibilizá-los na internet aos utilizadores a seu pedido segundo uma ordem de preferência determinada pelo motor de pesquisa. Acrescenta que o mero escanear (scanning) de informação já é tratamento de dados. O operador do motor de pesquisa é considerado o responsável pelo tratamento, isto é, a pessoa que determina os fins e os meios da atividade relevante dos dados mesmo que não seja a entidade fonte dessa informação. Na opinião do Tribunal, o responsável pelo tratamento tem um dever de controlo ativo, no sentido de lhe caber o apagamento dos dados ilegalmente tratados mesmo que as pessoas afetadas não tomem medidas nesse sentido.[32]

Quanto a saber se o Tribunal terá ponderado devidamente os interesses relevantes, nos termos do artigo 7º (o chamado "retângulo de interesses"), para aferir a licitude do tratamento, ao lado dos interesses do titular dos dados (privacidade) existem os

[29] SPIECKER, I., «A new framework for information markets: Google Spain Spiecker», *cit.,* p. 1040-1 (com referência ao acórdão *Satamedia*, C-73/07, EU:C:2008:727).

[30] Indra SPIECKER, «A new framework for information markets: Google Spain Spiecker», *cit.,* p. 1041 ("Probably the most spectacular finding of the ECJ is the extension of the Data Protection Directive so as to apply to both the subsidiary and the US-based parent.").

[31] Cf. o artigo 4º da Diretiva 95/46, sobre o direito nacional aplicável.

[32] *Google Spain*, para. 70-72

interesses da empresa que opera o motor de pesquisa enquanto intermediário que processa a informação, os interesses de terceiros na liberdade de expressão e de informação, e ainda os interesses do público na receção de informação. Ora, todos estes grupos de interesses são relevantes e afetados, mas na opinião do Tribunal a proteção de dados e da privacidade sobrepõe-se aos demais[33]. Para o efeito, o Tribunal invoca o princípio da interpretação da Diretiva em conformidade com a Carta de Direitos Fundamentais (CDFU), em particular o direito à vida privada consagrado no artigo 8[34], comentando-se, a propósito, que o Tribunal de Justiça se tornou num tribunal constitucional de proteção dos direitos humanos, o que de resto seria consequência do desenvolvimento da União Europeia35.

O Tribunal realça o risco que os motores de pesquisa representam para os dados pessoais e a vida privada, organizando e agregando dados automaticamente a partir de todas as fontes disponíveis. Sendo que a legalidade do armazenamento original dos dados não afasta a ilegalidade do tratamento efetuado pelos motores de pesquisa[36]. Em termos económicos, este acórdão levaria ao aumento dos custos de processamento de dados, com possível repercussão no modelo de negócio dos motores de pesquisa.

O Tribunal torna claro que nem toda a publicação de informação em páginas web beneficia das isenções destinadas aos media, deixando assim a porta aberta para a distinção entre publicações editadas, como a *Wikipedia*, mais próximas do jornalismo, dos motores de pesquisa que se limitam a apresentar resultados de forma automática. Embora reconheça o possível interesse público da informação, considera todavia ser necessário ter em conta a natureza da informação, o papel dos dados da pessoa na vida pública, etc., embora não tenha ido ao ponto de desenvolver uma teoria geral dos limites ao direito de imagem, o que terá sido um sinal de "wise self-restraint"37

Todavia, na medida em que parece remeter para o operador do motor de pesquisa a decisão de retirar a informação, sem estabelecer medidas de autoproteção, tal poderia ser "entregar os gansos à guarda da raposa"38. Além disso, entende-se que a decisão

[33] *Google Spain*, para. 81.

[34] *Google Spain*, para. 68-69.

[35] SPIECKER, I., «A new framework for information markets: Google Spain », *cit.,* p. 1055 ("The European court has become a constitutional court protecting individual human rights by further defining the protective width of a provision, the level of infringement and the tests for balancing interests. […] This development towards a human rights court is a consequence of the development of the EU.").

[36] *Google Spain*, para. 83.

[37] SPIECKER, I., «A new framework for information markets: Google Spain Spiecker», *cit.,* p. 1050.

[38] SPIECKER, I., «A new framework for information markets: Google Spain Spiecker», *cit.,* p. 1053 ("This concept thus sets the fox to keep the geese.").

pode colocar as pequenas e médias empresas em maiores dificuldades na concorrência em virtude dos investimentos que serão necessários em pessoal qualificado.

Podemos perguntar, não obstante, se o direito de autorização prévia não é transformado em direito de retirada. O que parece confrontar o princípio, tanto mais que se afirma não estar cumprida a exceção.

2. Aspetos do Regulamento Geral de Proteção de Dados (RGPD) no setor da saúde

O RGPD[39] aplica-se diretamente a partir de 25 de maio de 2018. Terá um impacto significativo no setor da saúde[40], e procura responder a desafios lançados pela Nuvem.[41]

Consagra uma noção de dados relativos à saúde como os "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde" (artigo 4/15). O considerando (35) acrescenta "no passado, no presente ou no futuro". O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, a essa pessoa singular, como (a) qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde, (b) as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e (c) quaisquer

[39] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[40] Sobre o impacto do RGPD no comércio eletrónico vide WEIGL, M., «The EU General Data Protection Regulation's Impact on Website Operators and eCommerce», *Computerrecht-international* 4 (2016), p. 102-108.

[41] Ver, a este propósito, as Recomendações do Article 29 Working Party *Opinion 05/2012 on Cloud Computing*, 2012, e do Cloud Standards Consumer Council, *Impact of Cloud Computing on Healthcare*, 2012. Entre os principais riscos da Nuvem apontam-se: as falhas de segurança de informação, como quebras de confidencialidade, integridade ou disponibilidade de dados pessoais, não detetadas pelo responsável pelo tratamento (a); a transferência de dados para países sem proteção adequada de dados pessoais (b); termos de serviços que permitem ao operador da nuvem tratar os dados em desconformidade com as instruções do responsável (c); a utilização dos dados por parte dos servidores de nuvem ou terceiros associados para os seus próprios fins sem o conhecimento ou a autorização do responsável (d); a responsabilidade evanescente dos subcontratados (e); perda de controlo dos dados e do seu tratamento e incapacidade de controlar as atividades do provedor de Nuvem (f); impossibilidade de fiscalização por parte das autoridades de proteção de dados relativamente ao tratamento dos dados pelo responsável ou pelo provedor de nuvem (g) - Berlin International Working Group on Data Protection in Telecommunications, *Working Paper on Cloud Computing - Privacy and data protection issues* ("Sopot Memorandum"), 2014. Para uma análise do pioneiro sistema Kanta finlandês ver LINDQVIST, C., *Access management and control in eHealth systems*, University of Helsinki, 2013 <http://www.cs.helsinki.fi/u/carolili/ehealth/ehealth.pdf>

informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro.

O RGPD prevê como princípios relativos ao tratamento de dados pessoais a licitude, a lealdade e transparência, a limitação das finalidades, a minimização dos dados, a exatidão, a limitação da conservação, a integridade e confidencialidade, e a responsabilidade pelo tratamento. Estabelece a proibição geral de tratamento de dados pessoais relativos à saúde (artigo 9/1), exceto se for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva de determinadas condições e garantias. Mais se permite o tratamento de dados de saúde se for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.[42]

[42] O preâmbulo contém extensos considerandos sobre estas derrogações à proibição geral de tratamento de dados. Assim, o considerando (52) indica que são justificadas derrogações nomeadamente "para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde." Mais acrescenta que "Essas derrogações poderão ser previstas por *motivos sanitários*, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos."

Para além de dados de saúde o tratamento de outras categorias especiais de dados poderá ter justificação "para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública" (considerando 53). Mais acrescenta este considerando que "Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições,

Ao titular de dados é reconhecido um leque de direitos, como o direito de informação na recolha de dados (artigos 13 e 14), o direito de acesso (artigo 15)[43], o direito de retificação (artigo 16), o direito ao apagamento dos dados («direito a ser esquecido») (artigo 17), o direito à limitação do tratamento (artigo 18), o direito de portabilidade dos dados (artigo 20), o direito de oposição a definição de perfis e decisões automatizadas (artigo 21).

O RGPD regula por outro lado a responsabilidade do responsável pelo tratamento e do subcontratante, e estabelece um conjunto de deveres a seu cargo, como o dever de segurança de tratamento, o dever de notificação de uma violação de dados pessoais à autoridade de controlo e de comunicação da violação ao titular dos dados (artigos 32 e 33).

Por outro lado, o Regulamento cria a categoria do *encarregado* da proteção de dados (artigo 37 e seguintes) e prevê a elaboração de Códigos de conduta e certificação (artigo 40 e seguintes) com o Selo Europeu de Proteção de Dados, e organismos de certificação (ISO). As transferências de dados pessoais para países terceiros ou organizações internacionais são feitas com base numa decisão de adequação, e são sujeitas a garantias adequadas. Prevê-se um esquema de trabalho em rede e de cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas. Para efeitos da aplicação efetiva do RGPD é instituído um Comité europeu para a proteção de dados e uma Autoridade Europeia para a Proteção de Dados.[44]

---

incluindo limitações, no que diz respeito ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados pessoais na União, quando essas condições se aplicam ao tratamento transfronteiriço desses dados."

A saúde pública justifica o tratamento de dados sensíveis sem o consentimento do respetivo titular indicando o considerando 54 que são aí abrangidos "todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade. Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, *como os empregadores ou as companhias de seguros e entidades bancárias*." (*itálico nosso*)

[43] A propósito do direito de acesso aos dados pessoais por parte dos seus titulares diz o considerando (63) "Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados."

[44] https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt

V. CONCLUSÃO

A proteção de dados na União Europeia e em Portugal entra na terceira geração de instrumentos legais com o Regulamento Geral, que se aplica a partir de 25 de maio de 2018. Até lá vigora a Dir. 95/46 e, no direito, interno, a Lei 67/98 complementada por legislação especial, em especial a lei de informação pessoal e genética (Lei 12/2005) e a lei de acesso aos documentos da administração e à sua reutilização (Lei 26/2016). Na evolução da proteção jurídica dos dados pessoais o Tribunal de Justiça da União Europeia tem desempenhado um papel hermenêutico muito importante, em diversos acórdãos (e.g. *Lindqvist*, *Google Spain*) fixando jurisprudência de interpretação dos conceitos normativos da Dir. 95/46.

O RGPD codifica essa jurisprudência e, em termos práticos, (1) reforça o dever de informação aos titulares de dados, no âmbito da sua recolha (incluindo a indicação da base legal do tratamento, o prazo de conservação dos dados, detalhes das transferências internacionais, possibilidade de apresentar queixa junto da CNPD), (2) revê os procedimentos para exercício dos direitos dos titulares de dados, que passam a incluir os direitos à limitação do tratamento e à portabilidade e novos requisitos sobre a eliminação ou retificação dos dados, (3) regula a forma e as condições do consentimento dos titulares dos dados, quando é condição de licitude do tratamento, (4) estabelece novas exigências quanto aos dados sensíveis, que passam a abranger os dados biométricos, em especial a exigência de designação de um encarregado de proteção de dados, (5) impõe obrigações de documentação e registo de atividades de tratamento, incluindo quanto efetuadas por subcontratantes, (6) disciplina aspetos dos contratos de subcontratação, exigindo nomeadamente que incluam um conjunto de elementos de informação, (7) impõe a designação do encarregado de proteção de dados, com funções especificadas no RGPD, nomeadamente para as entidades públicas, (8) exige medidas técnicas e organizativas de segurança do tratamento, exigindo a revisão das políticas de privacidade, (9) estabelece a proteção de dados desde a conceção juntamente com uma avaliação de impacto do tratamento (em termos de serem implementadas medidas como a pseudonimização, a minimização dos dados, o cumprimento de prazos de conservação, a acessibilidade dos dados), (10) exige a documentação e notificação de violações de segurança suscetíveis de acarretar riscos para os titulares.

O novo regime é acompanhado por sanções que incluem coimas que podem atingir valores significativos (semelhantes ao direito da concorrência), e no plano institucional cria a Autoridade Europeia de Proteção de Dados.

Oxalá o novo regime contribua para a proteção dos dados pessoais, em especial no setor da saúde, sem impor custos de transação que prejudiquem o bom funcionamento do mercado interno. Como refere Indra Spiecker a propósito do acórdão Google Spain,

"What is present there, happens – what remains outside their indexes, does not exist. […] In consequence, the Court raises the cost of personal data and may thus create new prices in market that so far has not included the data subjects in price models. Search might once more become costly in time and resources"[45]

De resto, a Internet é, por natureza, uma rede global não devendo a proteção de dados servir apenas de pretexto para a construção de uma Grande Muralha técnico-digital da Europa.

REFERÊNCIAS

APARÍCIO VAQUERO, Juan Pablo, BATUECAS CALETRÍO, Alfredo (coord,), *En torno a la privacidad y la protección de datos en la sociedad de la información*, Granada. Comares, 2015

Article 29 Working Party Opinion 05/2012 on Cloud Computing, 2012

Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (EHR), 2007

BARBOSA, Carla, «Aspectos Jurídicos do Acesso ao Processo Clínico», *Lex Medicinae*, nº 7 (2010), p. 107-140

Berlin International Working Group on Data Protection in Telecommunications, *Working Paper on Cloud Computing - Privacy and data protection issues* ("Sopot Memorandum"), 2014

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

CASIMIRO, Sofia Vasconcelos, «O direito a ser esquecido pelos motores de busca: o Acórdão Costeja», *Revista de Direito Intelectual*, 2014/2, p. 307-353

[45] SPIECKER, I., «A new framework for information markets: Google Spain Spiecker», *cit.,* p. 1049.

Cloud Standards Consumer Council, *Impact of Cloud Computing on Healthcare*, 2012

CROWTHER, «Remember to forget me: The recent ruling in Google v AEDP and Costeja", *Computer and Telecommunications Law Review*, 20 (2014), p. 163-165

DE HERT, P. / PAPAKONSTANTINOU, V., «Google Spain: Addressing Critiques and Misunderstanding One Year Later», *Maastricht Journal of European and Comparative Law*, Vol. 22, Nº 4, 2015, p. 624-638

DIAS PEREIRA, Alexandre Libório, «Marco Civil da Internet" e seus Reflexos no Direito da União Europeia», *Revista da ABPI*, 142 (2016), p. 2-21.

DIAS PEREIRA, Alexandre Libório, «Telemedicina e farmácia online: aspetos jurídicos da eHealth», *Revista da Ordem dos Advogados*, Ano 75, I/II (2015), p. 55-78

DIAS PEREIRA, André Gonçalo, «Dever de documentação, acesso ao processo clínico e sua propriedade: uma perspectiva europeia*», Revista Portuguesa do Dano Corporal*, nº 16, 2006

DIAS PEREIRA, André Gonçalo, *Direitos dos pacientes e responsabilidade médica*, Coimbra Editora, Coimbra, 2015

GARCIA MARQUES & LOURENÇO MARTINS, *Direito da Informática*, 2.ª ed., Almedina, Coimbra, 2006

LÓPEZ CALVO, José, *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin, 2017.

MARTINS, Leonardo (Org.), «Recht auf informationelle Selbstbestimmung», *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, Montevideo, 2005 <http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf >

GOMES CANOTILHO, J.J. & MOREIRA, V., *Constituição da República Portuguesa Anotada*, 4ª edição revista, Almedina, Coimbra, 2007

GONÇALVES, Maria Eduarda, *Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2.ª ed., Almedina, Coimbra, 2003

JONES, J., «Control-alter-delete: the 'right to be forgotten'», *European Intellectual Property Review* (2014), p. 595-601

KELSEY, K., «Google Spain Sl and Google Inc. v-. AEPD and Mario Costeja Gonzalez: protection of personal data, freedom of information and the 'right to be forgotten», *European Human Rights Law Review* (2014), p. 395-400

LINDQVIST, C., *Access management and control in eHealth systems*, University of Helsinki, 2013 (http://www.cs.helsinki.fi/u/carolili/ehealth/ehealth.pdf)

MONIZ, Maria Helena, «Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde», *Revista Portuguesa de Ciência Criminal*, Vol. 7, Nº 2 (1997), p. 231-298

RAPOSO, Vera Lúcia, «O Fim da 'Letra De Médico': Problemas Suscitados pelo Processo Clínico Eletrónico em Sede de Responsabilidade Médica», *Lex Medicinae,* nº 19 (2013), p. 51-78

SARMENTO E CASTRO, Catarina, *Direito da informática, privacidade e dados pessoais*, Almedina, Coimbra, 2005

SARRIÓN ESTEVE, J. «El alcance territorial de una sentencia que no tenemos derecho a olvidar: una particular aproximación a Google Spain», *CEF Legal: revista práctica de derecho. Comentarios y casos prácticos*, Nº 184 (2016), p. 53-72

SOUSA PINHEIRO, A., *Privacy e protecção de dados pessoais*, AAFDL, Lisboa, 2015

SOUSA RIBEIRO, J., «A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas», in *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho,* vol. III, Coimbra Editora, Coimbra, p. 853

SPIECKER, I., «A new framework for information markets: Google Spain», *Common Market Law Review,* 52 (2015), p. 1033-1058

STJ - Supremo Tribunal de Justiça, Acórdão de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1, in <www.dgsi.pt>

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

TJUE – Tribunal de Justiça da União Europeia, Acórdão de 8 de abril de 2014, procs. apensos C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238

TJUE – Tribunal de Justiça da União Europeia, Acórdão de 13 de maio de 2014, proc. C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

TJUE – Tribunal de Justiça da União Europeia, Acórdão de 19 de outubro de 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779

TJUE – Tribunal de Justiça da União Europeia, Acórdão de 6 de novembro de 2003, proc. C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596.

WEIGL, M., «The EU General Data Protection Regulation's Impact on Website Operators and eCommerce», *Computerrecht-international* 4 (2016), p. 102-108.

WIEBE, A., «Data protection and the internet: irreconcilable interests? The UE Data Protection Reform Package and CJEU case law», *Journal of Intellectual Property Law*, (2015), p. 64-68

LEGISLAÇÃO PRINCIPAL

Artigo 35 da Constituição Portuguesa

Artigo 8 da Carta de Direitos Fundamentais da União

Lei 67/98, de 26 de outubro (Lei de Proteção de Dados, alterada recentemente pela Lei 103/2015, de 24 de agosto). Transpõe para a ordem jurídica portuguesa a 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 dos dados pessoais e à livre circulação desses dados.

Regulamento (UE) 611/2013 da Comissão de 24 de junho de 2013

Lei 12/2005, de 26 de janeiro (LIPG)

Lei 26/2016, de 22 de agosto (LADAR)

Código Deontológico da Ordem dos Médicos, aprovado pelo Regulamento n.º 707/2016, de 21 de julho

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 (Regulamento Geral)