· U C · FDUC FACULDADE DE DIREITO
UNIVERSIDADE DE COIMBRA

DIREITO DA INFORMÁTICA

(ESTUDOS)

Vol. III

ALEXANDRE DIAS PEREIRA

Introdução

O volume III reúne alguns estudos recentes sobre «Direito da Informática». Trata de problemas relacionados com a utilização, em especial pelas empresas, das novas tecnologias da informação e da comunicação em rede, face aos novos desafios da chamada "Internet das Coisas (IoT), da inteligência artificial (IA) e da robótica, em especial no contexto do mercado interno digital. A quarta revolução industrial está em curso, com a chamada indústria 4.0. O Direito da Informática é centrado nos desafios jurídicos que se colocam às empresas num contexto de inovações tecnológicas disruptivas, num mercado dominado à escala mundial por 5 gigantes norte-americanas ("Amazon", "Apple", "Facebook", "Google", "Microsoft"), e às quais só a "Grande Muralha da China" parece resistir. Especial atenção é dada às pequenas e médias empresas (PME), uma vez que os regimes legais de dados pessoais, segurança informática, propriedade intelectual e proteção do consumidor discriminam positivamente estas empresas de modo a não barrar a sua entrada no mercado com regulamentações tão "pesadas" como as previstas para as grandes empresas do setor.

A problemática é praticamente inesgotável, não se confinando às ciências jurídico-empresariais, nem sequer ao direito privado em geral. Pelo contrário, o impacto das novas tecnologias é igualmente muito forte no direito constitucional (por ex. o impacto das redes sociais na democracia, com informação, discussão e votação eletrónica à distância), no direito administrativo (com uma administração pública cada vez mais online, das finanças à saúde passando pela educação e a contratação pública) e até no direito penal (com o emergente "panótico digital", o grande olho que tudo vê tornado realidade) e no direito fiscal (de novo o panótico digital, assistido por software cada vez mais "inteligente", e o problema da tributação "privilegiada" das grandes empresas da internet). Além disso, mesmo no âmbito das ciências jurídico-empresariais, a aplicação empresarial das novas tecnologias coloca problemas específicos ao nível do direito do trabalho, que só por si exigiriam uma linha de investigação autónoma (e.g. a qualificação da relação entre a Uber e plataformas similares e os seus colaboradores, o teletrabalho, que aliás o Código do Trabalho já regula, definindo-o como "a prestação laboral realizada com subordinação jurídica, habitualmente fora da empresa e através do recurso a tecnologias de informação e de comunicação" – art. 165.º).

Nestes estudos são tratados problemas fundamentais do Direito da Informática como sejam:

1.º - A caraterização das novas empresas e dos novos modelos de negócios na economia digital e a migração das empresas "tradicionais" para o ambiente online, e compreender o sentido e os limites da liberdade de empresa no mercado interno digital, em especial o significado do "princípio do país de origem" no comércio eletrónico e suas exceções, nomeadamente por razões de proteção da saúde pública (por ex. a venda medicamentos pela internet), e ainda o bom funcionamento do mercado interno online em termos de direito da concorrência (por ex. restrições verticais às vendas em linha, abusos de posição dominante nos serviços de pesquisa);

2.º - O sentido e os limites do princípio da liberdade contratual na negociação por via eletrónica, a equivalência do documento eletrónico ao documento escrito, as assinaturas digitais e serviços de confiança (incluindo a problemática do "Blockchain" e dos "criptocontratos" ou "chamados inteligentes"), e a proteção do consumidor no comércio eletrónico na contratação à distância face à legislação em vigor e às novas Diretivas sobre vendas em linha e conteúdos digitais;

3.º - A proteção da privacidade e dos dados pessoais, designadamente dos consumidores e dos trabalhadores, em contexto empresarial, focando em especial à luz do Regulamento Geral

de Proteção de Dados, os deveres do responsável pelo tratamento de dados, como sejam, designadamente, o respeito pelos direitos dos titulares de dados (por ex. o "direito a ser esquecido"), a designação de representante na União Europeia quando não estiver estabelecido na EU, a aplicação de medidas técnicas e organizativas adequadas para proteger os dados desde a conceção e por defeito, a avaliação de impacto e a designação de encarregado de proteção de dados, a adoção de códigos de conduta ou certificação da "data compliance"; de igual modo, interessa estudar as derrogações para fins jornalísticos, expressão literária, artística ou científica, aquivo de interesse público, investigação científica ou histórica, ou estatísticos;

4.º - A proteção da propriedade intelectual (e.g. direitos de autor, marcas), em especial contra a pirataria online, impondo neste domínio especial atenção à transposição da nova diretiva da União Europeia sobre direitos de autor no mercado único digital, que regula as plataformas de partilha de conteúdos sujeitando-as a licenciamento e a deveres de controlo dos conteúdos carregados pelos seus utilizadores, excluindo todavia desta noção entidades como as microempresas e as pequenas empresas na aceção do título I do anexo da Recomendação 2003/361/CE da Comissão e as empresas que atuam sem fins comerciais. A Diretiva dos direitos de autor no mercado digital tem ainda impacto ao nível das exceções aos direitos de autor, estabelecendo como utilizações livres como a prospeção de textos e dados para fins de investigação científica, a utilização de obras através de rede eletrónica segura acessível apenas por alunos, estudantes e pessoal docente do estabelecimento, e a conservação do património cultural pelas instituições responsáveis pelo património cultural, como bibliotecas ou museus acessíveis ao público, arquivos, instituições responsáveis pelo património cinematográfico ou sonoro.

5.º - A segurança informática e a responsabilidade pela utilização de "agentes inteligentes" nas empresas, focando os deveres de segurança impostos pela diretiva da segurança informática, transposta pela Lei da cibersegurança, sobre os operadores de serviços essenciais (empresas de energia, transportes, banca e bolsas, hospitais e clínicas privadas, fornecedores de água potável, e infraestruturas digitais) e ainda os prestadores de serviços digitais (mercados em linha, motores de pesquisa em linha, e serviços de computação em nuvem), e que passam pela adoção de *medidas técnicas e organizativas* adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços, pela realização de *auditorias de segurança* pela autoridade competente ou por um auditor qualificado e, em especial, pela *notificação dos incidentes de segurança*, i.e., eventos com um efeito adverso real na segurança das redes e da informação. Neste passo, estudar brevemente a tipologia legal do cibercrime e a investigação criminal em meio digital.

A adaptação do direito às novas tecnologias digitais não é propriamente uma novidade, remontando, pelo menos, à década de 70 do século XX. O aparecimento do computador data de 1946, com o chamado ENIAC (*Electronic Numeric Integrator And Calculator*), e o posterior desenvolvimento das ciências de computação por Turing e Neumann, entre outros. O impacto da informática nas empresas não foi imediato, embora uma gigante do setor, como a IBM (*International Business Machines*), seja anterior à II Guerra Mundial. Gradualmente as empresas começaram a utilizar computadores, cada vez mais potentes e sofisticados, depois interligados em redes, culminando na atual internet, fruto da digitalização e da convergência multimédia das telecomunicações e do audiovisual, e em especial da criação do *World Wide Web* por Tim Berners-Lee.

Até ao virar do milénio, destacam-se já mundialmente algumas empresas informáticas, como a "Microsoft" e a "Apple". O computador vai substituir a máquina de escrever, a calculadora e a

folha de cálculo, os livros em papel, o arquivo físico, o cesto de papeis, os álbuns de fotografias e de filmes, o telefone e o fax, os jornais, as revistas, os livros, o gira-discos, o leitor de vídeos e respetivas cassetes, os jogos de tabuleiro (xadrez), o relógio com cronómetro e alarme, o calendário, o gravador de voz e de imagem, etc. Estas "ferramentas" são agora produzidas e comercializadas também como "aplicações" informáticas.

Depois, com a internet, a informática funciona em rede e, em boa parte, na nuvem, através de servidores superpotentes operados por utilizadores a partir de terminais no lugar e no momento individualmente escolhidos. Surge o motor de pesquisa e outros serviços da "Google", como a plataforma de partilha de vídeos "YouTube"; o "Facebook" afirma-se como a principal rede social, uma espécie de internet dentro da internet. Simultaneamente as empresas migram para o digital, não apenas em termos de acesso remoto pelos seus colaboradores, mas igualmente abrindo lojas online, desde vestuário a mobiliário até medicamentos e telemóveis, passando por bancos, seguradoras e apostas desportivas. De tudo um pouco de se vende na Internet e, sem surpresa, o fundador e dono da "Amazon" aparece no primeiro lugar da lista dos mais ricos do mundo da revista *Forbes*, cujo top 20 inclui 7 bilionários ligados às chamadas empresas "GAFA+".

Os Estados Unidos da América, em especial o famoso Vale do Silício na Califórnia (como antes sucedera com Hollywood, literalmente "bosque de azevinho", na indústria cinematográfica), são a pátria dos gigantes da informática, aos quais se juntam mais recentemente alguns chineses ("Alibaba Group", "Tencent"), e que dominam mundialmente a economia digital, incluindo na Europa. Inicialmente o domínio das gigantes americanas no setor dos programas de computador e das bases de dados fez-se sentir, juridicamente, com a aprovação de leis de direitos de autor feitas à imagem e semelhança do copyright norte-americano, privilegiando os interesses das empresas de software na relação com os criadores e com os utilizadores das tecnologias.

Esse domínio foi construído e consolidado num quadro de vazio jurídico, alegadamente. Aliás, aquando da gestação do ciberespaço ("cyberspace"), termo cunhado por Gibson no seu livro *Neuromancer* (1984), tecnólogos como Katsch[1] questionaram a competência do Direito para regular este novo espaço, vista a rede mundial de computadores como um sistema descentrado (*centerless system*). Os códigos informáticos e os mecanismos alternativos de resolução de litígios (*soft law*) teriam primazia sobre as leis e os tribunais do Estado (*hard law*). A Internet cresceu e desenvolveu-se caoticamente em ambiente de *Woodstock* eletrónico, qual *Wild West Story* à escala global. Não existiria um poder estadual capaz de impor as suas leis através dos seus órgãos judiciários e administrativos, nem sequer fronteiras territoriais[2]. Por natureza a-espacial, o ciberespaço seria uma *no man's land*, um "sexto continente", à espera de ser descoberto e conquistado. Preservar o *estado de natureza* do ciberespaço contra a sua *colonização* pelos códigos do Estado e do Direito, eis o ideal proclamado na *Declaration of Independence of Cyberspace* de John Perry Barlow (1996). A nova ordem faria tábua-rasa dos direitos pré-cibernéticos, como o direito à privacidade, por serem incompatíveis com as exigências do *Ser Digital* proclamado por Nicholas Negroponte (1995).

Todavia, logo se percebeu que o ciberespaço enquanto modo de vida com os outros não é axiologicamente neutro. Perdeu-se a inocência do estado de natureza ao tomar-se consciência, contra a falácia do saber-poder tecnológico, que a revolução eletrónica carregava no seu ventre

[1] E.g. ETHAN KATSCH, *Law in a Digital World*, Oxford University Press, 1995, p. 243.

[2] J.J. GOMES CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7ª ed., Coimbra, 2006, p. 1350.

a distopia orwelliana, o "panótico global" e da "sociedade de controlo", na expressão do filósofo Deleuze (1990).

Os juristas reagiram contra a regulação do ciberespaço apenas pelo código informático, recordando a existência de outras leis e defendendo a sua vigência no mundo digital. Como escreveu então Lessig, no seu *Code*: "*The values of free speech, privacy, due process, and equality define who we are. If there is no government to insist on these values, who will do it?*"[1] Com efeito, depois de uma primeira fase revolucionária e eufórica, o Direito foi chamado a dar respostas aos problemas jurídicos da Internet. Foram as questões da pirataria e da contrafação em sede de propriedade intelectual, do exercício de atividades económicas pela internet (por ex. novos serviços de publicidade, venda de medicamentos, apostas desportivas, etc.), da proteção do consumidor no comércio eletrónico, da cibersegurança e do cibercrime, e também da proteção da vida privada e dos dados pessoais.

Neste processo, a União Europeia emergiu como a primeira fonte de produção normativa dos seus Estados-Membros, em nome do bom funcionamento do mercado interno e da sociedade da informação.[2] Ao invés de cada Estado-Membro legislar isoladamente sobre o digital, é a União Europeia que responde primeiro aos desafios da digitalização, afirmando aí um espaço de competências. O acervo jurídico da União sobre sociedade da informação, comércio eletrónico e mercado digital é composto por vários instrumentos de natureza legislativa, complementados por jurisprudência proferida pelo Tribunal de Justiça da União Europeia. Deste modo, estudar o Direito da Informática é, desde logo, estudar o acervo de direito da União Europeia em sede de serviços da sociedade da informação ou comércio eletrónico. Dos instrumentos atualmente em vigor destacamos, com referência igualmente, sendo caso disso, aos diplomas de transposição para a ordem jurídica interna:

- Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (JO L 178 de 17.7.2000, p. 1-16); Decreto-Lei n.º 7/2004, de 7 de janeiro (alterado), e diplomas setoriais, como o Decreto-Lei n.º 307/2007, de 31 de agosto (alterado) e a Portaria nº 1427/2007, de 2 de novembro (venda medicamentos pela internet), o Decreto-Lei n.º 66/2015, de 29 de abril (apostas desportivas) e a Lei n.º 45/2018, de 10 de agosto (regime jurídico da atividade de transporte individual e remunerado de passageiros em veículos descaracterizados a partir de plataforma eletrónica);

- Diretiva (UE) 2015/1535 do Parlamento e do Conselho, de 9 de setembro, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação; vigora ainda o Decreto-Lei n.º 58/2000, de 18 de abril;

- Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (eIDAS);

- Diretiva n.º 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores; Decreto-Lei n.º 24/2014, de 14 de fevereiro (alterado);

- Diretiva n.º 2002/65/CE, do Parlamento Europeu e do Conselho, de 23 de setembro, relativa à comercialização à distância de serviços financeiros prestados a consumidores; Decreto-Lei n.º 95/2006, de 29 de maio (alterado);

- Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais; Diretiva (UE)

[1] LAWRENCE LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, 1999, p. 220.

[2] J. OLIVEIRA ASCENSÃO, «Direito cibernético: a situação em Portugal», *Direito & Justiça* 25/2 (2001) p. 9-26.

2019/771 do Parlamento Europeu e do Conselho, de 20 de maio, relativa a certos aspetos dos contratos de compra e venda de bens;

- 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), e o artigo 8º da Carta de Direitos Fundamentais da EU; foi recentemente aprovada no Parlamento uma lei regulamentar do Regulamento, aguarda publicação;

- Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (alterada pela Diretiva n.º 2009/136/CE); Lei 41/2004, de 18 de agosto (alterada);

- Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativa aos direitos de autor e direitos conexos no mercado único digital e que altera a Diretiva 96/9/CE sobre proteção de bases de dados e a Diretiva 2001/29/CE sobre direito de autor e direitos conexos na sociedade da informação; a acervo relevante sobre direitos de autor inclui outras diretivas como, por ex., a Diretiva 2009/24/CE do Parlamento Europeu e do Conselho, de 23 de abril de 2009, relativa à proteção jurídica dos programas de computador (JO L 111 de 5.5.2009, p. 16-22), a Diretiva 2014/26/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à gestão coletiva dos direitos de autor e direitos conexos e à concessão de licenças multiterritoriais de direitos sobre obras musicais para utilização em linha no mercado interno (JO L 84 de 20.3.2014, p.72-98), a Diretiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade intelectual (JO L 195 de 2.6.2004, p. 16-25) (IPRED), bem como o Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno (JO L 168, 30.6.2017, p. 1-11). as diretivas têm sido transpostas alterando o Código do Direito de Autor e dos Direitos Conexos, exceto no que respeita aos programas de computador (Decreto-Lei n.º 252/94, de 20 de outubro, alterado) e às bases de dados (Decreto-Lei n.º 122/2000, de 4 de julho);

- Diretiva (UE) 2015/2436 do Parlamento Europeu e do Conselho de 16 de dezembro de 2015 que aproxima as legislações dos Estados-Membros em matéria de marcas, e a Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais); no direito interno, veja-se o novo Código da Propriedade Industrial, aprovado pelo Decreto-Lei n.º 110/2018, de 10 de dezembro;

- Regulamento (CE) n.º 733/2002, do Parlamento Europeu e do Conselho, de 22 de Abril de 2002, relativo à implementação do domínio de topo .eu; sobre os nomes de domínio, no direito interno, Decreto-Lei n.º 55/2013, de 17 de abril, e Regulamento DNS.PT 2014;

- Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União; Lei 46/201, de 13 de agosto, e com interesse igualmente na segurança informática a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime);

- Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, sobre competência judiciária, reconhecimento e execução de decisões em matéria civil e comercial (revogou e substituiu o Regulamento 44/2001 de 22 de dezembro de 2000 – «Bruxelas I»);

- Regulamento (CE) n.º 593/20008 do Parlamento Europeu e do Conselho, de 17 de junho de 2008, sobre a lei aplicável às obrigações contratuais («Roma I»);

- Regulamento (CE) n.º 864/2007 do Parlamento Europeu e do Conselho, de 11 de julho de 2007, relativo à lei aplicável às obrigações extracontratuais («Roma II»);

- Regime da concorrência (artigos 101 e 102 do TFUE e respetivos Regulamentos; Lei 19/2012, de 8 de maio, alterada).

Além dos instrumentos legislativos, cumpre estudar igualmente a jurisprudência, com destaque para a jurisprudência do Tribunal de Justiça da União Europeia, como sejam, nomeadamente os acórdãos de 2 de dezembro de 2010 (proc. C-108/09, Ker-Optika), 13 de outubro de 2011 (proc. C-439/09, Pierre Fabre Dermo-Cosmétique), 6 de dezembro de 2017 (proc. n.º C-230/16, Coty Germany), 12 de julho de 2011 (proc. C-324/09, L'Oreal c. eBay), 8 de setembro de 2009 (proc. C-42/07, Bwin/LPFP c. SCML), 5 de maio de 2011 (proc. C-316/09, MSD Sharp & Dohme GmbH c. Merckle GmbH), 11 de julho de 2013 (proc. C-657/11, Belgian Electronic Sorting Technology), 24 de outubro de 2009 (proc. C-489/07, Pia Messner), 3 de julho de 2012 (proc. C-128/11, UsedSoft v Oracle), 29 de abril de 2004 (proc. C-418/01, IMS Health c. NDS), 17 de setembro de 2007 (proc. T - 201/04, Microsoft Corp. v Commission of the European Communities), 16 de julho de 2009 (proc. C-5/08, Infopaq), 7 de março de 2013 (proc. C-607/1, TVCatchup Ltd), 13 de fevereiro de 2014 (proc. C-466/12, Svensson), 21 de outubro de 2014 (proc. C-348/13, BestWater International), 11 de setembro de 2014 (proc. C-117/13, Technische Universität Darmstadt c. Eugen Ulmer KG), 3 de junho de 2010 (proc. C-569/08, Internetportal GmbH), de 23 de março de 2010 (procs. apensos C-236/08 a C-238/08, Google France, Google c. Louis Vuitton), 24 de novembro de 2011 (proc. C-70/10, Scarlet c. Sabam), 13 de maio de 2014 (proc. C-131/12, Google Spain c. AEPD e Mário Costeja González), 16 de maio de 2014 (procs. C-293 & 594/12, Digital Rights Ireland), 5 de março de 2015 (proc. C-463/12, Copydan Båndkopi c. Nokia Danmark), 7 de dezembro de 2010 (proc. C-144/09 e C-585/08, Alpenhof e Pammer), 25 de outubro de 2011 (proc. apensos C-509/09 e C-161/10, eDate Advertising), ou de 29 de novembro de 2017 (proc. C-265/16, VCAST);

Assumem especial relevo os acórdãos sobre proteção do consumidor, dados pessoais, direitos de autor e direito da concorrência. Ainda recentemente a Comissão Europeia "multou" a Google em € 4,340 M bilhões por violar as regras antitrust da EU, em virtude de ter imposto restrições ilegais a fabricantes de dispositivos Androide e operadoras de redes móveis para consolidar sua posição dominante no mercado das pesquisas na Internet. Pouco antes a gigante norte-americana tinha já sido "multada" em € 2,420 M por abuso de posição dominante no mercado dos motores de busca ao favorecer ilicitamente o seu próprio serviço de comparação de vendas. Sendo o direito da concorrência estruturante para o bom funcionamento do mercado interno, o Direito da Informática, enquanto direito empresarial 4.0, deve igualmente abrangê-lo no seu objeto de estudo.

Por outro lado, ao nível da utilização da inteligência artificial na governação empresarial, o quadro normativo ainda está em praticamente branco, embora comecem a ser desenhar-se alguns traços a que importa estar atento de modo a compreender o sentido da evolução deste fenómeno e sem prejuízo de se reconhecer que talvez essa matéria deva ficar em aberto para maiores estudos e reflexões, tanto mais que a questão não é específica das empresas, antes sendo comum à responsabilidade civil em geral, como indica a Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica. O que não impede que se estude o tema em perspetiva empresarial, dado o relevo por ex. dos mandamentos da IA na EU, como sejam: a) a garantia da supervisão e controlo humano ("os sistemas não devem limitar a autonomia humana"), b) a robustez e segurança ("os algoritmos têm de ser capazes de lidar com erros"), c) a privacidade e controlo de dados ("os utilizadores devem manter o controlo dos seus dados e poder revogar o

acesso"), d) a responsabilização ("capacidade de reconhecer erros e corrigi-los"), e) a transparência, diversidade, não-discriminação e justiça, e f) a promoção do bem-estar ambiental e societal.[1]

De igual modo, o Conselho da OCDE elaborou recomendações sobre a utilização "confiável" da Inteligência Artificial[2], com possível aplicação em sede de responsabilidade social das empresas, como sejam: a) utilização da IA em benefício da humanidade e do crescimento inclusivo, o desenvolvimento sustentável e o bem-estar; b) conceção, por defeito, em termos de garantir o respeito pelo Estado-de-Direito, pelos direitos humanos, a democracia e a justiça social, com salvaguardas adequadas que permitam a intervenção humana quando necessário; c) transparência e divulgação sistemas de IA de modo a poderem ser entendidos e questionados pelas pessoas; d) funcionamento robusto e seguro ao longo dos seus ciclos de vida, com avaliação contínua e gestão dos seus riscos potenciais; e) responsabilidade pelo funcionamento adequado de sistemas de IA das pessoas humanas ou jurídicas que os desenvolvem, implementam ou operam. A propósito da utilização de "agentes inteligentes" (ou "inteligência artificial) na governação empresarial coloca igualmente questões de direito das sociedades comerciais, que urge estudar.

Em termos de bibliografia, para além de obras gerais, incluindo periódicos e bases de dados, apresentam-se alguns títulos mais recentes, a título ilustrativo, com interesse para o desenvolvimento da investigação sobre os temas referidas:

- AA.VV., Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde, Liber Amicorum Yves Poullet, Larcier, 2018
- A. Barreto Menezes Cordeiro, Direito de Proteção de Dados Pessoais - À luz do RGPD e da Lei n.º 58/2019, Almedina, Coimbra, 2020
- Alexandre de Sousa Pinheiro, Privacy e protecção de dados pessoais, AAFDL, Lisboa, 2015
- Catherine Seville, EU intellectual property law and policy, 2nd ed., Elgar, 2016
- Christiane Féral-Schuhl, Cyberdroit 2018/2019: Le droit à l'épreuve de l'internet, 7ª ed., Dalloz, 2018
- Christina Tikkinen-Piri, Anna Rohunen; Jouni Markkula, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies», Computer Law & Security Review 34/1 (2018) 134–153
- Comentário ao Regulamento Geral de Proteção de Dados, coord. Alexandre de Sousa Pinheiro, Almedina, 2018
- Copyright in the Information Society, ed. Brigitte Lindner, Ted Shapiro, Elgar, 2019
- Council Of Europe/European Court Of Human Rights, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, Updated on 31 December 2018
- Dário Moura Vicente, Sofia Casimiro, «A proteção de dados pessoais na Internet à luz do Direito Comparado», Revista de Direito Intelectual, Nº 2, 2018, 45-90
- David Mallo Montoto, La difusión en Internet de contenidos sujetos al derecho de autor, Marcial Pons, 2018
- Emmanuel Poinas, Le tribunal des algorithmes: Juger à l'ère des nouvelles technologies, Berger-Levrault, 2019
- EU Internet Law: Regulation and Enforcement, ed. Synodinou, Jougleux, Markou, Prastitou, Spinger, 2017

[1] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[2] https://www.oecd.org/going-digital/ai/principles/

- EU Regulation of E-Commerce, ed. Arno R. Lodder, Andrew D. Murray, Elgar, 2017
- Fabrice Mattatia, Internet et les réseaux sociaux, 3ª ed. Eyrolles, Paris, 2019
- Giovanni De Greogorio, «From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society», European Journal of Legal Studies, 11/2 (2019) 65-103
- Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, ed. Aurelio Lopez-Tarruella, Springer, 2012
- Gustavo Ghidini, Rethinking Intellectual Property, Elgar, 2018
- Indra Spiecker, «A new framework for information markets: Google Spain», Common Market Law Review 52 (2015) 1033-1058
- Intellectual property and innovation, ed. by Robert P. Merges, Amy L. Landers, Elgar, 2017
- Intellectual Property Perspectives on the Regulation of New Technologies, ed. Tana Pistorius, Elgar, 2018
- J. López Calvo, Comentarios al Reglamento Europeo de Protección de Datos, Madrid, Sepin, 2017
- Jan Rosén, European intellectual property law: an Edward Elgar research review, Elgar, 2016
- Jan Trzaskowski, Andrej Savin, Patrik Lindskoug, Björn Lundqvist, Introduction to EU Internet Law, 2.ª ed., Ex Tuto, 2018
- Justine Pila, Paul Torremans, European Intellectual Property Law, 2nd ed., OUP, 2016
- Kritika: essays on intellectual property, ed. Gustavo Ghidini, Hanns Ullrich, Peter Drahos, Elgar, 2017
- Lorna Brazell, Electronic Signatures and Identities: Law and Regulation, Sweet & Maxwell, 2018
- Luís Manuel Couto Gonçalves, Manual de Direito Industrial, 8.ª ed., Almedina, 2019
- Luís Manuel Teles de Menezes Leitão, Direito de autor, 2ª ed. Almedina, 2018
- M. Weigl, «The EU General Data Protection Regulation's Impact on Website Operators and eCommerce», Computerrecht-international 4 (2016) 102-108.
- Margaret Byrne Sedgewick, «Transborder data privacy as trade», California Law Review 105/5 (2017) 1513-1542
- Morgan and Burden on IT Contracts, Sweet & Maxwell, 2018
- Online Distribution of Content in the EU, ed. Taina Pihlajarinne, Juha Vesala, Olli Honkkila, Elgar, 2019
- P. Danneels, B. Verheye, K. Verslype, Quel impact sur le notaire en tant qu'intermédiaire de confiance ? Larcier, 2019
- Pamela Samuelson, "The EU's Controversial Digital Single Market Directive", Communications of the ACM (Association for Computing Machinery) 61/11 (2018) 20-23
- Patricia Llopis Nadal, La protección de la propiedad intelectual vulnerada en Internet - determinación del órgano competente según el sistema español, Marcial Pons, 2018
- Philippe Le Tourneau, Contrats du numérique, informatique et électronique, 10 ed. Dalloz, 2018
- Privacy digitale: Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, ed. Emilio Tosi, Giuffrè, 2019
- Research handbook on copyright law, ed. Paul Torremans, 2nd ed. Elgar, 2017
- Research handbook on intellectual property in media and entertainment, ed. Megan Richardson, Sam Ricketson, Elgar, 2017

- Research Handbook on the Law of Artificial Intelligence, ed. Woodrow Barfield, Ugo Pagallo, Elgar, 2018
- Silvia Martinelli, Diritto all'oblio e motori di ricerca, Giuffrè, 2019
- User generated law: re-constructing intellectual property law in a knowledge society, ed. Thomas Riis, Elgar, 2016
- Vijay Bishnoi, "Data protection law: An inhibition in enforcement and promotion of competition law", European Competition Law Review vol. 40, no. 1 (2019) 34-40

A Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, intitulada "Estratégia para o Mercado Único Digital na Europa", de 6 de maio de 2015 [COM(2015) 192 final], anunciou um pacote de medidas legislativas nos domínios da proteção de dados, das comunicações eletrónicas, da modernização dos direitos de autor face aos desafios das tecnologias digitais, da proteção dos consumidores no comércio eletrónico, e da segurança das redes e dos sistemas de informação. O comércio em linha transfronteiriço no mercado único seria ainda bastante limitado por causa de diversos obstáculos, a eliminação dos quais poderia aumentar o PIB europeu em 415 mil milhões de euros, melhorar a oferta para consumidores e trabalhadores, e facilitar a criação de empresas inovadoras (start-ups). Já antes a Comissão considerara que "O mercado único digital está longe de ter atingido o seu pleno potencial. Estima-se que o custo deste atraso seja no mínimo de 4,1% do PIB daqui até 2020, isto é, 500 mil milhões de euros".[1]

Passados 4 anos sobre a referida Comunicação, é tempo de fazer um estudo aprofundado e um balanço crítico das medidas legislativas adotadas e propor soluções sobre os caminhos a seguir para a correta transposição dessas medidas para a ordem jurídica interna. O processo de adaptação do direito aos desafios das tecnologias digitais não teve início em 2015, antes remontando, pelo menos, a 1989, com "Livro Verde sobre os direitos de autor e o desafio da tecnologia"[2], a que se seguiria o Livro Verde O direito de autor e os direitos conexos na sociedade de informação[3] e, depois, a aprovação de diretivas sobre dados pessoais, comércio eletrónico, direitos de autor na sociedade da informação, direitos do consumidor na contratação à distância, etc, temática que, aliás, acompanhamos há cerca de duas décadas e meia.[4]

Coimbra, abril de 2020

[1] *Um enquadramento coerente para reforçar a confiança no mercado único digital do comércio eletrónico e dos serviços em linha*, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, COM(2011) 942 final, p. 2.

[2] Aspectos dos direitos de autor que requerem uma acção imediata, COM (88) 172 final, de 16 de Março de 1989.

[3] COM(95) 382 final, de 19 de julho de 1995.

[4] Desde os primeiros trabalhos no Instituto Jurídico da Comunicação, o ensaio *Comércio eletrónico na sociedade da informação: da segurança técnica à confiança jurídica* (Almedina, 1999) e a dissertação de mestrado *Informática, direito de autor e propriedade tecno-digital* (Coimbra Editora, 2001), até aos *Estudos* de *Direito da propriedade intelectual & novas tecnologias*, em publicação pela Gestlegal, (vol. I, 2019), sem esquecer o doutoramento *Direitos de autor e liberdade de informação* (Almedina 2008).

UM NOVO FÔLEGO HUMANISTA: UMA CIVILIZAÇÃO CIBERNÉTICA NO TERCEIRO MILÉNIO?*

1. Vivemos, actualmente, na chamada *Era da Comunicação*. O progresso científico-tecnológico transformou este nosso Mundo numa pequena Aldeia Global, dotando o Homem não apenas da possibilidade de dar a Lua de presente aos seus filhos, mas também do poder de autodestruição enquanto espécie (pense-se nas «adormecidas» ogivas nucleares e nas armas bioquímicas), e ainda na possibilidade de criar o Frankenstein perfeito através de manipulações genéticas e de duplicar formas de vida humana (pense-se na clonagem de embriões humanos).

Além disso, o progresso científico-tecnológico tornou possível a comunicação em tempo real à escala mundial e, quase, uma virtual viagem no tempo. À panóplia de meios de comunicação já existentes, como a televisão, a rádio, a imprensa, o vídeo, para não falar já no telégrafo e no telefone, vieram juntar-se outras tantas invenções como os satélites, os computadores e sistemas informáticos, os faxes, o correio electrónico, a Internet, etc., naquilo a que se designam as auto-estradas da informação e da comunicação.

É a Revolução das tecnologias da informação uma autêntica marca do nosso tempo, atirando para segundo plano os problemas do tráfico de armas nucleares, dos desastres ecológicos, do terrorismo, da engenharia genética, etc. A "Terceira Vaga" de que somos protagonistas, e na qual somos surpreendidos, conduz-nos, no limiar do terceiro milénio, a uma *Telecomunidade*, i.e. uma Civilização Cibernética, a qual poderá carregar no seu ventre o gérmen da robotização do Homem.

2. É um lugar comum a afirmação de que o Homem só se compreende e reconhece enquanto ente comunicante (*homo communicans* ou, também, *loquens*), que vive com os outros, i.e. na comunidade. Ora, na teia de relações comunicativas que tece e em que é surpreendido, o Homem orienta-se por um código de signos que o precede: a linguagem. A linguagem que interioriza modela o seu pensamento e o seu agir, traduza-se ele num juízo valorativo, num raciocínio lógico-matemático, num devaneio do sonho ou numa obra de engenho.

Numa palavra, é em linguagem que comunicamos, herdando e instituindo sentidos sobre nós próprios e sobre o meio que nos rodeia. Pelo que a nossa vida com os outros é modelada pela linguagem, i.e. pelo código de signos que gravita no universo que nos entretece. Nesta ordem de ideias, pode dizer-se, com propriedade, que quem domina a nossa linguagem controla o modo como comunicamos, como vivemos uns com os outros, enfim, como agimos. Por isso dizem os cientistas da linguagem que o poder se inscreve e se exerce na linguagem em que comunicamos.

Ora, se esta linguagem for reduzida a um conjunto de signos técnicos, ou seja, a signos cujos sentidos susceptíveis de lhes poderem ser imputados se encontrem

---

* Rua Larga 22, 2008, 20-22 (Revista da Reitoria da Universidade de Coimbra).

exaustivamente predefinidos em termos inequívocos, então encontrar-se-á a nossa liberdade de pensar e de agir encarcerada em tais comandos pré-ditados. Não seremos então mais do que meros robots executantes das instruções e das funções contidas no *software* que nos programa. Pense-se na Novilíngua de Ingsoc *ficcionada* por Orwell na sua obra Mil Novecentos e Oitenta e Quatro.

3. Se nos predispusermos a reflectir um pouco sobre o ambiente que nos rodeia, facilmente nos aperceberemos que nunca como neste nosso tempo a tentação de robotizar o homem foi tão grande e encontrou condições tão propícias à sua consumação. Com efeito, esta nova escravidão não é apenas mero tema dos devaneios da ficção literária, mas antes algo cuja iminência deve despertar a nossa meditação.

O melindre e a delicadeza que o problema encerra exigem que se encontre resposta para duas ordens de perguntas, a saber: 1ª quem edita a linguagem que hoje nos comanda e por que meios é processada? 2ª que tipo de linguagem nos é ditada?

3.1. Relativamente à primeira pergunta, impõe-se responder que a linguagem que nos comanda é editada, em primeira linha, pelos que detêm o poder dos *media*, sendo processada por sistemas informáticos e telemáticos. Na verdade, o universo de signos que nos absorve desde a fecundação até ao sono de *Morpheu* é um universo mediatizado e informatizado, prejudicando os lugares mais recônditos da nossa convivência.

Por um lado, tornamo-nos, gradualmente, em sujeitos transparentes em virtude da cristalização operada pelos arquivos informáticos de dados pessoais. Pense-se na importância para uma instituição financeira, que tem na mira a maximização do lucro pela diminuição do risco, do acesso às informações sobre as convicções políticas e religiosas, a conta bancária, a saúde, o código genético, e mesmo os hábitos sexuais de um candidato a uma apólice de seguros ou a um empréstimo bancário. Não é por acaso que o mercado dos serviços de informação se apresenta como um dos mais prósperos, assistindo-se, paralelamente, a uma inflação de leis, quer a nível nacional quer internacional, tendentes a proteger o direito fundamental de privacidade contra a devassa informática.

Por outro lado, o consumidor/eleitor apenas acede à informação de que carece para a escolha de um automóvel ou de um líder político nos termos em que essa informação se lhe apresenta mediatizada pelos seus emissores. As suas fronteiras são, *a priori*, delimitadas pelos senhores da informação e da publicidade. Nestes termos, é também um lugar-comum dizer-se que o que não está na televisão não está no mundo.

A televisão, mais do que os restantes meios de comunicação como a rádio e a imprensa, assume-se ainda como o filtro selectivo e o referente primeiro da convivência das massas, resistindo à "guerrilha" dos novos *média* interactivos e integrando-os. De braços caídos no fim da jorna, o «televisionário» entrega-se indefeso à magia persuasiva da publicidade das marcas, à inesgotável perspicácia dos comentadores de ocasião, à criteriosa escolha dos eventos dignos de registo, absorvendo, sem se aperceber, as palavras que vai repetir, as modas que vai seguir, a opinião que vai perfilhar. Sofrendo de um incurável complexo do botão, pois que quando muito muda de canal, o «televisionário» rende-se perante este quarto poder.

É a televisão o Grande Irmão que vela por nós, sentando-se à cabeceira da mesa, cuidando do que cada um precisa de saber sobre o mundo e sobre si próprio e fornecendo as actualizações automáticas.

3.2. Quanto à segunda pergunta, o tipo de linguagem que nos é ditada pelos media é uma linguagem do mercado. O nosso tempo não é já o das sociedades disciplinares da modernidade, assentes institucionalmente no «panóptico», e comandadas pela linguagem da fábrica.

Atenta a globalização dos mercados que a Revolução das Comunicações tornou possível, o primado da planificação calculadora e da disciplina da produção cedeu, via de regra, à lógica do controlo do mercado, à lei da oferta e da procura regida pelos comandos da *ratio* do *marketing*. São os comandos da normalização, da performance, da eficácia, que, em última análise, reduzem o Homem ao estatuto funcional de produtor/consumidor, em obediência ao *Diktat* economicista e tecnocrático.

Por outro lado, tendo a Revolução das Tecnologias da Informação transformado este Mundo numa pequena Aldeia Global, pela primeira vez desde o episódio bíblico da Torre de Babel, podem todos os homens da Terra falar uma mesma linguagem: a linguagem do mercado das sociedades de consumo.

4. Nesta ordem de ideias, a Civilização Cibernética emergente carrega no seu ventre o gérmen do «Homem autómato», robotizando o ser humano por via da sua programação pelos media segundo o *software* da linguagem do mercado. Neste quadro, a dignidade de cada Homem seria aferida pela sua utilidade enquanto produtor/consumidor e pelas suas possibilidades de re-programação e de reciclagem, ficando os seres humanos sujeitos à escravidão do consumismo ditado pela tirania do *marketing* exercida pelos media à escala mundial.

Ora, sob pena de esta Civilização Cibernética que desponta no Terceiro Milénio pouco ter de humanamente civilizada - no sentido de ser composta por Homens, i.e. seres humanos livres, iguais e fraternos -, urge um novo fôlego para o Humanismo solidário, que resista ao *Diktat* economicista e tecnocrático. Impõe-se, por conseguinte, ver o Homem para além da Máquina!

A PROTEÇÃO DOS DADOS PESSOAIS E O DIREITO À SEGURANÇA INFORMÁTICA NO COMÉRCIO ELETRÓNICO*

Introdução

A proteção dos dados pessoais no comércio eletrónico é um tema de grande atualidade e interesse face ao Regulamento Geral de Proteção de Dados (RGPD)[1] plenamente aplicável a partir de 25 de maio de 2018. No setor segurador têm especial importância os dados relativos à saúde, que o RGPD define 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). É uma noção muito ampla, especialmente se tivermos em conta que 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 qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde, 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 quaisquer 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."

"Principiologia" da proteção de dados pessoais

A proteção de dados pessoais, em especial de saúde, é uma componente fundamental do comércio eletrónico. As empresas, incluindo as seguradoras, têm que adaptar a sua

---

* Revista Banca, Bolsa e Seguros - BBS, n.º 3 (2018) 303-329.

[1] 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. Sobre a proteção de dados pessoais na bibliografia portuguesa ver, designadamente, Garcia MARQUES & Lourenço MARTINS, *Direito da Informática*, 2.ª ed., Almedina, Coimbra, 2006, p. 129-313, 422-442, 330-391; Paulo Mota PINTO, «O direito à reserva sobre a intimidade da vida privada», *Boletim da Faculdade de Direito de Coimbra* 64 (1993) p. 479-586; Helena MONIZ, «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; Eduarda GONÇALVES, *Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2.ª ed., Almedina, Coimbra, 2003, p. 82-111, 173-183; Catarina CASTRO, *Direito da informática, privacidade e dados pessoais*, Almedina, Coimbra, 2005; A. Sousa PINHEIRO, *Privacy e protecção de dados pessoais*, AAFDL, Lisboa, 2015. Em castelhano vide, por ex., J.P. APARÍCIO VAQUERO e A. BATUECAS CALETRÍO (coord,), *En torno a la privacidad y la protección de datos en la sociedad de la información*, Granada. Comares, 2015; LÓPEZ CALVO, J., *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin, 2017.

política de privacidade e de dados pessoais às novas exigências do RGPD[1], que é já a 3.ª geração de leis de dados pessoais na União Europeia.

O RGPD prevê diversos princípios relativos ao tratamento de dados pessoais, designadamente 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, diagnóstico médico, 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. O tratamento de dados de saúde é ainda permitido e 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.

O preâmbulo do RGPD 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

[1] Para uma análise do impacto do RGPD nos sítios dos operadores de comércio eletrónico, *vide* M. WEIGL, «The EU General Data Protection Regulation's Impact on Website Operators and eCommerce», *Computerrecht-international* 4 (2016), p. 102-108.

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, 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." Todavia ressalva este considerando, *in fine*: "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*).[1]

[1] A exceção para fins de investigação científica justifica tratamentos derivados ou secundários (consentimento amplo), tratamentos de categorias sensíveis de dados pessoais sem consentimento do respetivo titular, bem como derrogações ao direito de apagamento e do direito de oposição ao tratamento, mediante salvaguardas adequadas. Os fins da investigação científica abrangem pro ex. o desenvolvimento tecnológico, a investigação aplicada e a investigação financiada pelo setor privado, a realização de um espaço europeu de investigação, ou estudos de interesse público realizados no domínio da saúde pública (considerando 159 do RGPD).

A exceção ao princípio da limitação do tratamento atende à natureza dinâmica da investigação e pretende justificar a aplicação de inteligência artificial (IA) às minas de dados pessoais. Os tratamentos posteriores para fins de investigação científica são considerados compatíveis com o consentimento inicial (art. 5/1-b), lendo-se no considerando 33 que "os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica."

Por outro lado, os fins de investigação científica justificam a possibilidade de tratamento de categorias especiais de dados pessoais, com os dados de saúde (art. 9/2-j). Parte-se do princípio de que, nos termos do considerando 157: "Combinando informações provenientes dos registos, os investigadores podem obter novos conhecimentos de grande valor relativamente a problemas médicos generalizados, como as doenças cardiovasculares, o cancro e a depressão." Ressalva-se, todavia, que os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde, ou seja, os Estados-Membro podem adotar regras mais restritivas a nível nacional relativamente a estas categorias de dados. Por ex., em Portugal a Lei 12/2005, de 26 de janeiro, prevê limites à utilização de informação genética em sede de investigação sobre o genoma humano (Artigo 16/4: "A investigação sobre o genoma humano em pessoas não pode ser realizada sem o *consentimento informado* dessas pessoas*, expresso por escrito,* após a explicação dos seus direitos, da natureza e finalidades da investigação, dos procedimentos utilizados e dos riscos potenciais envolvidos para si próprios e para terceiros."), e estabelece inter alia o princípio da *proibição da discriminação* em função do património genético (art. 11) e uma *proibição geral* de testes genéticos ou informação genética para a celebração de contratos de seguro de vida ou acidente, trabalho, ou na adoção (arts. 12 a 14). Ainda ao nível da legislação interna, o referido Código Deontológico da Ordem dos Médicos permite o acesso a informação de saúde para fins de investigação, mas desde que *anonimizada*. Note-se, a este respeito, que os *dados anónimos* não são regulados pelo RGPD nos termos do considerando 26: "Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação."

Direitos do titular e deveres do responsável pelo tratamento dos dados pessoais

Ao titular de dados é reconhecido um leque de direitos, incluindo o direito de informação na recolha de dados (artigos 13 e 14), o direito de acesso (artigo 15)[1], o direito de retificação (artigo 16), o direito ao apagamento dos dados (artigo 17 - «direito a ser esquecido»)[2], o direito à limitação do tratamento (artigo 18), o direito de portabilidade dos dados (artigo 20), e o direito de oposição a definição de perfis e decisões automatizadas (artigo 21).

A Lei n.º 26/2016, de 22 de agosto, sobre o acesso aos documentos da administração e à sua reutilização, estabelece que "O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico se o titular da informação o solicitar, com respeito pelo disposto na Lei n.º 12/2005" (artigo 7/1). Além disso, esta lei possibilita o acesso a dados de saúde a terceiros sem consentimento do titular dos dados embora por intermédio do médico e limitado à "informação estritamente necessária à realização do interesse direto, pessoal, legítimo e constitucionalmente protegido que fundamenta o acesso" (artigo 7/4). A este propósito, o RGPD ressalva que os organismos públicos podem tratar dados pessoais sem o consentimento dos titulares para execução de tarefa no *interesse público* (art. 6-e). De todo o modo, os dados licitamente tratados para fins de investigação científica não podem ser livremente tratados por terceiros, nomeadamente por seguradoras, conforme se lê no considerando 54 do RGOD: "O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. (…) 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."

A exceção de investigação científica está sujeita a certas condições (art. 89). Por um lado, são exigidas medidas técnicas e organizativas adequadas para cumprir o princípio da minimização do tratamento. Remete-se, a este propósito, para os *padrões éticos* da investigação científica, sem prejuízo de se estabelecer que a a *pseudonimização* e *a cifragem* dos dados pessoais são medidas adequadas (art. 32/1-a; a pseudonimização surge definida no art. 4/3-b). Todavia, a pseudonimização só é obrigatória "desde que os fins visados possam ser atingidos desse modo" (art. 89/2). Quando ao dever de informação, decorrente do princípio da transparência dos dados, a investigação científica afasta-o se os dados forem obtidos por terceiros ou a partir de fontes públicas acessíveis ou se o cumprimento desse dever impossibilitar ou dificultar seriamente a prossecução dos objetivos visados, na medida em que sejam adotadas medidas adequadas.

Para terminar, referir ainda que os fins de investigação científica justificam outras exceções aos direitos dos titulares de dados pessoais, como o direito ao apagamento, em caso de necessidade superveniente (art. 17/3-), ou o direito de oposição, havendo interesse público na investigação em causa (art. 21/6). Além disso, a lei interna dos Estados-Membros pode estabelecer exceções adicionais aos direitos de acesso, retificação, limitação ou oposição, ressalvando-se, todavia, que o tratamento de dados para fins científicos deverá igualmente respeitar outra legislação aplicável, tal como a relativa aos ensaios clínicos. (art. 89). Em Portugal, o projeto de lei de "regulamentação" do RGPD prevê que os fins de investigação científica prevalecem sobre os direitos de acesso, retificação, limitação do tratamento e de oposição (art. 31/2). Por seu turno, a investigação clínica é regulada pela Lei n.º 21/2014, de 16 de abril.

[1] O direito de acesso significa, em matéria de dados de saúde, que os seus titulares têm direito de lhes aceder, como refere o considerando (63), "por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados."

[2] Este "direito a ser esquecido" foi afirmado pelo Tribunal de Justiça da União Europeia no 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. Sobre este acórdão ver por ex. Indra SPIECKER, «A new framework for information markets: Google Spain», *Common Market Law Review,* 52 (2015), p. 1033-1058; Sofia CASIMIRO, «O direito a ser esquecido pelos motores de busca: o Acórdão Costeja», *Revista de Direito Intelectual*, 2014/2, p. 307-353; Filipa CALVÃO, «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual,* 2015/2, p. 67-84 (preferindo falar em "direito à desassociação").

Por seu turno, o responsável pelo tratamento e o seu subcontratante têm vários deveres a seu cargo, designadamente 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). Em certas condições, o responsável pelo tratamento poderá ser obrigado a ter um Encarregado de Proteção de Dados (EPD/DPO, instituído pelo Regulamento (artigo 37 e seguintes), para além da previsão de códigos de conduta e de artigo 40 e seguintes) com o Selo Europeu de Proteção de Dados, e organismos de certificação (artigo 40 e seguintes). 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.[1]

Prevê-se ainda 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.[2]

A obrigação de segurança e confidencialidade dos dados pessoais

O responsável pelo tratamento de dados tem uma obrigação de segurança e confidencialidade do tratamento, "incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas", conforme se lê no considerando (39).[3] A segurança da rede e da informação, em sede de tratamento de dados pessoais, consiste nos termos do considerando (49) do RGPD na "capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas,

[1] O protocolo *Safe Harbor* de transferência de dados da União Europeia para os EUA foi declarado inválido pelo TJUE no acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*. Posteriormente, 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.

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

[3] Já a Lei 67/98, de 26 de outubro (que transpôs 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) obrigava o responsável pelo tratamento de dados a adotar medidas especiais de segurança adequada ao controlo da entrada nas instalações, dos suportes de dados, inserção, da utilização, de acesso, da transmissão, da introdução (o quê, quando e por quem), do transporte, a separação lógica dos dados de saúde e da vida sexual, incluindo os genéticos, dos restantes dados pessoais. Por seu turno, a Lei 12/2005, de 26 de janeiro, sobre informação pessoal genética e de saúde estabelece deveres do responsável pelo tratamento da informação de saúde, como sejam a confidencialidade e segurança das instalações e dos equipamentos, o controlo do acesso à informação, sigilo e educação deontológica dos profissionais, a proibição de acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, níveis de segurança contra destruição, acidental ou ilícita, alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação, a realização regular e frequente de cópias de segurança (back-up regulares).

pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança". Entende-se que a segurança informática, assim caraterizada, constitui um interesse legítimo do responsável pelo tratamento, justificando, por exemplo, "impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas" (*ibidem*).

A violação de dados pessoais é definida como "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (artigo 4/12).

Um dos princípios que regem o tratamento é o da integridade e confidencialidade. Significa que o tratamento dos dados deve garantir "a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)" (artigo 5/1-f).[1]

Por outro lado, a segurança dos dados pessoais é regulada no artigo 32 do RGPD: o responsável pelo tratamento e o subcontratante devem ter em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, e aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

1 - A pseudonimização e a cifragem dos dados pessoais[2];

2 - A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

3 - Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. A segurança informática é também um requisito da subcontratação do tratamento, podendo ser demonstrada através do cumprimento de um código de conduta aprovado ou um procedimento de certificação aprovado - artigo 32/ 3 e considerando (81).

---

[1] A confidencialidade dos dados de saúde é uma das condições da telemedicina, nos termos do Código Deontológico da Ordem dos Médicos, aprovado pelo Regulamento n.º 707/2016, de 21 de julho. Sobre o tema, Alexandre L. Dias PEREIRA, «Telemedicina e farmácia online: aspetos jurídicos da eHealth», *Revista da Ordem dos Advogados* 75 I/II (2015), p. 55-78.

[2] A cifragem é apontada como uma medida de controlo dos riscos de segurança no tratamento de dados pessoais, "tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais" (considerando 83 do RGPD).

Por outro lado, o responsável pelo tratamento tem o *dever de notificar* uma violação de dados pessoais à autoridade de controlo, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, devendo nesse caso ser acompanhada dos motivos do atraso (artigo 33/1). Quanto ao seu *conteúdo* a notificação deve descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa. Além disso, a notificação deve comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações, e descrever as consequências prováveis da violação de dados pessoais e as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos (artigo 33/3).

Para além da notificação à autoridade competente, com os referidos elementos, o responsável pelo tratamento deve comunicar ao titular dos dados, sem demora injustificada, a violação de dados pessoais quando essa violação puder implicar um *elevado risco* para os direitos e liberdades das pessoas singulares, salvo se o responsável: a) tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem, ou b) tiver tomado medidas subsequentes que assegurem que o referido elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar; ou c) implicar um esforço desproporcionado. Não comunicando justificadamente a violação ao titular dos dados, deverá ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz (artigo 34/3).

Obrigação de avaliação de impacto

A obrigação de *avaliação de impacto* sobre a proteção de dados das operações de tratamento significa que o responsável pelo tratamento deve solicitar o parecer do *encarregado da proteção de dados*, nos casos em que este tenha sido designado, e a avaliação incluirá, pelo menos, *inter alia*, as medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o RGPD, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa (artigo 35).

Direito do consumidor à segurança informática?

A Constituição da República (CRP) consagra o direito fundamental à liberdade e à segurança (artigo 27/1), e atribui aos trabalhadores e aos consumidores o direito à segurança (artigos 59/1-c e 60/1). O regime da utilização da informática previsto no artigo 35 da CRP não contempla a segurança informática *qua tale*. Trata dos dados

pessoais, máxime informatizados, remetendo a sua proteção para diploma legal, e estabelece a garantia de acesso universal e livre às redes informáticas de uso público.[1]

[1] Embora sem consagração na letra da lei constitucional, a jurisprudência tem encontrado no espírito do artigo 35 um "direito à autodeterminação informativa" – cf. por ex. o acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1, Cons. Helena Moniz, <www.dgsi.pt>. O Tribunal Federal Constitucional Alemão (BFGH) utilizou a expressão 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). 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»'" JJ. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa Anotada*, vol. 1, 4.ª ed., Coimbra Editora, 2007, p. 55; cf. o referido acórdão do STJ de 16 de outubro de 2014). Segundo J. Sousa RIBEIRO («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. 85), 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)».

«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», considerou o Tribunal Constitucional no seu acórdão n° 442/2007, de 14 agosto de 2007. Num 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 outros acórdãos. Alguns tratam da existência de «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 Regime Geral de Instituições de Crédito (RGIC): vide acórdão do TC nº 278/95, de 31 de maio de 1995; 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). Outros acórdãos tratam do 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 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 STJ de 16 de outubro de 2014). 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 do 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,

Por seu turno, a Lei de Defesa do Consumidor (LDC)[1] protege a segurança do consumidor (artigos 3/b e 5). O artigo 8/3 estabelece que "Os riscos para a saúde e segurança dos consumidores que possam resultar da normal utilização de bens ou serviços perigosos devem ser comunicados, de modo claro, completo e adequado, pelo fornecedor ou prestador de serviços ao potencial consumidor." Além disso, o artigo 21/2 da LDC atribui à Direção-Geral do Consumidor poderes para "d) Ordenar medidas cautelares de cessação, suspensão ou interdição de fornecimentos de bens ou prestações de serviços que, independentemente de prova de uma perda ou um prejuízo real, pelo seu objeto, forma ou fim, acarretem ou possam acarretar riscos para a saúde, a segurança e os interesses económicos dos consumidores."

A segurança informática não é aqui expressamente prevista, mas deve considerar-se uma dimensão do direito do consumidor à segurança.[2] Por isso, no comércio eletrónico, a segurança informática do consumidor (diferente da segurança pública) poderá justificar a adoção de medidas restritivas, incluindo providências concretas contra um prestador de serviços, à circulação de um determinado serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente os consumidores, nos termos do artigo 7/1 do DL 7/2004, de 7 de janeiro.[3]

O regime da segurança das redes e da informação

Os deveres de segurança informática a cargo de operadores de serviços essenciais e de prestadores de serviços digitais protegem igualmente os consumidores. A Diretiva 2016/1148[4] estabelece obrigações de segurança face ao "papel vital" das redes e da

---

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 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 de 10 de julho de 2013, proc. 1728/12.8JAPRT.P1, Des. Joaquim Gomes).

[1] Lei 24/96, de 31 de julho, com alterações posteriores.

[2] Seguimos de perto a comunicação sobre o direito do consumidor à segurança informática (*cibersecurity*) que apresentámos no I Congresso Internacional de Direito do Consumidor: Os Desafios do Mercado Digital para os Contratos de Consumo, organizado pelo Instituto Jurídico da Universidade Portucalense Infante D. Henrique Porto nos dias 19 e 20 de janeiro de 2018.

[3] Transpõe para o direito interno a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno.

[4] Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Entretanto transposta Lei n.º 46/2018, de 13 de agosto (regime jurídico da segurança do ciberespaço).

Podemos também afirmar a segurança informática como um bem jurídico-penal. O Código Penal prevê tipos legais de crime relacionados com a segurança informática, como a devassa da vida privada, em especial por meio de informática (artigos 192 e 193), e a burla informática e nas comunicações (artigo 221). Além disso, a Lei do Cibercrime (aprovada pela Lei 109/2009, de 15 de setembro, que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa) erige a segurança informática à dignidade de bem jurídico-penal, prevendo os seguintes tipos legais de crime (cibercrimes): a falsidade informática, o dano relativo a programa ou outros dados informáticos, a sabotagem informática, o acesso ilegítimo, e a interceção ilegítima. É a ainda

informação na sociedade e na economia e ao potencial lesivo dos incidentes de segurança. Cria uma Rede de equipas de resposta a incidentes de segurança informática («Rede CSIRT») e um Grupo de Cooperação, incluindo os Estados-Membros, a agência europeia ENISA e a Comissão Europeia. Nos incidentes de segurança estão em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, e dos serviços utilizados.

Os deveres de segurança recaem sobre os operadores de serviços essenciais, categoria que abrange as empresas de energia, transportes, banca e bolsas, hospitais e clínicas privadas, fornecedores de água potável, e infraestruturas digitais (anexo II). Os deveres de segurança valem igualmente para os prestadores de serviços digitais, incluindo mercados em linha, motores de pesquisa em linha, e serviços de computação em nuvem (anexo III). De fora ficam as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE, e os prestadores de serviços de confiança na aceção do Regulamento 910/2014[1], uma vez que tanto estes como aquelas ficam sujeitos aos requisitos de segurança estabelecidos nos respetivos diplomas.[2]

O preâmbulo da Dir. 2016/1148 esclarece no considerando 22 que a prestação de serviços essenciais pode não corresponder a toda a atividade da empresa, ficando esta sujeita aos deveres de segurança apenas no que respeita aos serviços essenciais:

"Por exemplo, no setor do transporte aéreo, os aeroportos prestam serviços que podem ser considerados essenciais por um Estado-Membro, tais como a gestão das pistas, mas também uma série de serviços que podem ser considerados não essenciais, como a disponibilização de áreas comerciais. / Os operadores de serviços essenciais deverão estar sujeitos aos requisitos de segurança específicos apenas no que respeita aos serviços considerados essenciais."

Os Estados-Membros devem identificar os *operadores de serviços essenciais* nos setores da *energia* (eletricidade, petróleo, gás, incluindo empresas de comercialização,

---

previsto o crime de reprodução ilegítima de programa protegido, o qual, todavia, transcende a lógica estrita da cibersegurança.

[1] Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (eIDAS) (e no direito interno o Decreto-Lei n.º 290-D/99, de 2 de agosto, com alterações posteriores).

[2] Por exemplo, o Regulamento eIDAS estabelece como requisitos de segurança aplicáveis aos prestadores de serviços de confiança (1) a adoção de medidas para impedir ou reduzir ao mínimo o impacto dos incidentes de segurança e informar as partes interessadas dos efeitos adversos dos eventuais incidentes, e (2) o dever de notificação da autoridade nacional de segurança e da autoridade de proteção de dados de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados. Em caso de violação de segurança dos sistemas de ID, que prejudique a fiabilidade da autenticação transfronteiriça do sistema, o Estado-Membro notifica os outros Estados-Membros e a Comissão. Ao fim de 3 meses sem ter sido corrigida a falha o meio de ID é suprimido.

As medidas de controlo de segurança e gestão dos riscos de segurança na moeda eletrónica, em especial a notificação de incidentes, estão previstas na Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno (altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) 1093/2010, e revoga a Diretiva 2007/64/CE).

de distribuição, de transporte, operadores de rede, operadores de instalações de refinamento, tratamento ou armazenamento), *dos transportes* (aéreo, ferroviário, marítimo e fluvial, rodoviário - por ex., entidades gestoras aeroportuárias, aeroportos, operadores de controlo da gestão do tráfego aéreo, gestores de infraestruturas e empresas rodoviárias, empresas de transporte e entidades gestores dos portos, operadores de serviços de tráfego marítimo, autoridades rodoviárias e operadores de sistemas de transporte inteligentes), no *setor bancário* (instituições de crédito e infraestruturas do mercado financeiro, incluindo operadores de plataformas de negociação (bolsas) e contrapartes centrais), no *setor da saúde* (incluindo instalações de prestação de saúde, nomeadamente hospitais e clínicas privadas), no *setor do fornecimento e distribuição de água potável para consumo humano*, e *no setor das infraestruturas digitais* (incluindo pontos de troca de tráfego, prestadores de serviços e registos de DNS).

Nos termos do artigo 6 da Dir. 2016/1148, a identificação dos operadores de serviços essenciais faz-se segundo determinados critérios, tais como, por exemplo, saber se a entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais, se a prestação desse serviço depende de redes e sistemas de informação, e se um incidente pode ter efeitos perturbadores importantes na prestação desse serviço, tendo em conta: a) O número de utilizadores que dependem dos serviços prestados pela entidade em causa; b) A dependência de outros setores essenciais em relação ao serviço prestado por essa entidade; c) O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais ou a segurança pública; d) A quota de mercado dessa entidade; e) A distribuição geográfica, no que se refere à zona que pode ser afetada por um incidente; f) A importância da entidade para a manutenção de um nível suficiente do serviço, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço.

São ainda previstos fatores específicos por setor tais como a quantidade ou a percentagem de energia nacional gerada, para os fornecedores de energia, o volume diário, para os fornecedores de petróleo, e a sua importância sistémica com base nos ativos totais ou no rácio ativos totais/PIB, para os serviços bancários ou as infraestruturas do mercado financeiro.

Os operadores de serviços essenciais devem adotar *medidas técnicas e organizativas* adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.[1]

As políticas de segurança dos operadores de serviços essenciais estão sujeitas a avaliação devendo para o efeito apresentar a respetiva documentação e provas da sua aplicação efetiva, tais como os resultados de uma *auditoria de segurança* efetuada pela autoridade competente ou por um auditor qualificado e que, no último caso, facultem os resultados dessa auditoria, incluindo os elementos de prova subjacentes, à autoridade competente. Se detetarem deficiências nas políticas de segurança ou na sua implementação, as autoridades competentes podem emitir instruções vinculativas

[1] Uma norma técnica de segurança é, atualmente, a ISO 27001 <https://www.27001.pt/>

dirigidas aos operadores de serviços essenciais, para que estes corrijam as deficiências detetadas (artigo 15 da Dir. 2016/1148).

Por seu turno, os *prestadores de serviços digitais* são obrigados a garantir um nível de segurança proporcional ao grau de risco para a segurança dos serviços digitais que fornecem, dada a importância dos seus serviços para as operações de outras empresas na União.

Os serviços digitais abrangem os mercados em linha, os motores de pesquisa em linha e os serviços de computação em nuvem (art. 4/5, anexo III). Nos termos do artigo 4/17-19 da Dir. 2016/1148: a) o *mercado em linha* permite a consumidores e/ou a comerciantes a celebração de contratos de venda ou de prestação serviços, quer no sítio do mercado em linha quer no sítio web do comerciante que utiliza os serviços de computação do mercado em linha (por ex. Amazon); b) o *motor de pesquisa em linha* disponibiliza aos seus utilizadores a consulta de todos os sítios web disponíveis "numa determinada língua com base numa pesquisa sobre qualquer assunto, sob a forma de uma palavra-chave, de uma frase ou de outros dados, e que responde fornecendo ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado" (por ex., Google); c) o serviço de computação em nuvem faculta o "acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis".

Entende-se que os requisitos de segurança aplicáveis aos prestadores de serviços digitais podem ser menos exigentes já que, na prática, o seu grau de risco é inferior ao grau de risco a que estão sujeitos os operadores de serviços essenciais. Assim, por exemplo, a autoridade competente não tem uma obrigação geral de supervisionar os prestadores de serviços digitais (considerandos 49 e 60 da Dir. 2016/1148).[1]

Dever de notificação dos incidentes de segurança

As entidades sujeitas a deveres de segurança têm um dever de notificar incidentes, i.e., eventos com um efeito adverso real na segurança das redes e da informação (artigo 14/3 da Dir. 2016/1148). As notificações de incidentes devem ser recebidas pelas autoridades competentes ou pelas equipas de resposta a incidentes de segurança informática (CSIRT).

Para determinar a importância do impacto de um incidente são estabelecidos alguns parâmetros como (1) o número de utilizadores afetados pela perturbação do serviço essencial, (2) a duração do incidente, e (3) a distribuição geográfica, no que se refere à zona afetada pelo incidente (artigo 14/4 da Dir. 2016/1148).

Os prestadores de serviços digitais não estabelecidos na União que ofereçam serviços na União devem designar obrigatoriamente um representante. Segundo o considerando 65 da Dir. 2016/1148: "A fim de determinar se esses prestadores oferecem ou não serviços na União, haverá que apurar se é evidente a sua intenção de oferecer serviços a pessoas num ou mais Estados-Membros. O mero facto de estar acessível na União um sítio web do fornecedor de serviços digitais ou de um intermediário ou um endereço

[1] O artigo 16/11 da Dir. 2016/1148 isenta dos referidos deveres de segurança as microempresas e as pequenas empresas, tal como definidas na Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, de modo a não a ficarem sujeitas a encargos financeiros e administrativos desproporcionados (considerando 53).

eletrónico ou outro tipo de contactos ou de ser utilizada uma língua de uso corrente no país terceiro em que o fornecedor de serviços digitais se encontra estabelecido não é suficiente para determinar essa intenção. Contudo, há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar serviços nessa outra língua, ou a referência a clientes ou utilizadores na União, que podem ser reveladores de que o fornecedor de serviços digitais tenciona oferecer serviços na União."[1]

Conclusão

A promoção do comércio eletrónico depende em larga medida da proteção dos dados pessoais e da segurança das redes e da informação, aí se alicerçando a confiança dos consumidores. O consumidor, enquanto pessoa singular, é titular de dados pessoais protegidos pelo Regulamento Geral de Proteção de Dados. Por outro lado, enquanto utilizador de serviços essenciais e de serviços digitais beneficia do regime da segurança das redes e da informação.

O consumidor tem direito nomeadamente à confidencialidade e à segurança do tratamento dos seus dados pessoais, ficando as empresas que tratam os dados pessoais dos consumidores sujeitas às sanções especialmente gravosas previstas no RGPD. As empresas que pratiquem comércio eletrónico, sem cumprir as exigências de dados pessoais dos consumidores e de segurança informática das redes e da informação, ficam igualmente sujeitas a medidas cautelares de cessação, suspensão ou interdição de fornecimentos, nos termos do artigo. 21/2-d) da LDC.

Relativamente a empresas não estabelecidas em Portugal, mas que dirigem as suas atividades para o mercado português, a segurança informática do consumidor justificará a adoção de medidas restritivas, incluindo providências concretas contra um prestador de serviços, à circulação de um determinado serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente os consumidores, nos termos do diploma do comércio eletrónico.

[1] Para efeitos de determinação do foro competente nos termos do Regulamento Bruxelas I (Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (revogou e substituiu o Regulamento 44/2001)], o Tribunal de Justiça clarificou a noção de atividades dirigidas no contexto da Internet nos acórdãos *Alpenhof* e *Pammer*, de 7 de dezembro de 2010 (procs. C-144/09 e C-585/08, Colet., p. I-12527). Para determinar se um sítio profissional dirige a sua atividade ao EM do domicílio do consumidor deve ter-se em conta se, antes da celebração de qualquer contrato, resultava desse sítio e da sua atividade em geral que procurava oportunidades de negócio nesse EM. A mera acessibilidade do profissional no EM de domicílio do consumidor é insuficiente para estabelecer a conexão. O Tribunal de Justiça apresenta uma lista não exaustiva de tópicos, tais como: a) a natureza internacional da atividade, b) a referência a itinerários a partir de outros EM para ir ao local de estabelecimento do profissional, c) a utilização de línguas ou de moedas para além das que são geralmente aceites no seu EM de estabelecimento, d) a menção a números de telefone com código internacional, e) recurso a serviços pagos de indexação de resultados de pesquisa para facilitar acesso ao seu sítio por parte de consumidores domiciliados em outros EM, etc.

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

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.

1. 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 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

* *Lex Medicinae* 15/29 (2018) 51-70.

[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, pp. 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, pp. 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* 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>), obra 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.*

Europeia.[1] 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).2 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 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 internacional3 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)4, 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[5], proibindo a sua utilização para o "tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e

---

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/>).

[1] 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).

[2] 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.

[3] 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).

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

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

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 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"1. Todavia, o regime dos dados

[1] 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

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.

2. Panorama da lei portuguesa dos dados pessoais

2.1. 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 da origem e do destino dos dados. Quanto aos destinatários, abrange tanto empresas

---

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 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 12/2005, 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).

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"1, 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 singular2, 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 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

---

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

[2] 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.

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.[1]

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).[2]

No acórdão *Google Spain*3, 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".

---

[1] 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."

[2] 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. 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).

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

2.2.**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 tratamento (artigo 5) e a legitimidade do seu tratamento, que depende de consentimento do seu titular1 ou de autorização legal (artigo 6).

2.3.**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)[2], 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

[1] 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).

[2] 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.

sigilo) dos dados, e um dever de colaboração (prestando informações, permitindo a realização de inspeções, facultando documentos).

2.4. Transferência de dados para outros países e a liberdade de circulação de dados na EU

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[1], a situação depende de apreciação caso a caso. Se a Comissão considerar que o país terceiro oferece um nível de proteção adequado, a transferência é permitida.2 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

[1] 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

[2] 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.

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.

2.5.**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).

3. Os dados de saúde

3.1.**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.[1]

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.2

3.2.**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).3 O tratamento de dados

---

[1] *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).

[2] 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.

[3] 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 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 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 profissional1

c) notificado à CNPD, nos termos do artigo 27º2, 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 interconexão3, que deve ser solicitada pelo responsável pelo tratamento, exceto quando legalmente prevista (artigo 9).

3.3.**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).4 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 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,

---

de autorização de tratamento de outras categorias de dados sensíveis devem indicar obrigatoriamente os elementos previstos no artigo 30.

[1] 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.

[2] 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>

[3] 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).

[4] 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).

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[1] 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.

3.4.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 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).

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

3.5.**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[1], 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 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).[2]

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

---

[1] 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.

[2] 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.

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 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).

4. O "direito ao esquecimento" e o regulamento geral de proteção de dados

4.1. O acórdão *Google Spain*

No acórdão *Google Spain*[1], o Tribunal de Justiça pronunciou-se sobre o chamado "direito ao esquecimento" nos termos da Dir. 95/46. Esta diretiva garante às pessoas em

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

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 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 arts. 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."1

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., aos seus algoritmos e resultados de pesquisa, não abrangendo terceiros. Por outro lado, os motores de pesquisa não seriam protegidos pelos "media privileges".2

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').3 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.4

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

---

[1] 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*, 2/2014, 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, pp. 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, pp. 53-72.

[2] 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).

[3] 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.").

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

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.[1]

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 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[2]. 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[3], 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 Europeia4.

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[5]. 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"6

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"7. Além disso, entende-se que a decisão

---

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

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

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

[4] 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.").

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

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

[7] 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.

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

O RGPD[1] aplica-se diretamente a partir de 25 de maio de 2018. Terá um impacto significativo no setor da saúde[2], e procura responder a desafios lançados pela Nuvem.[3]

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 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

---

[1] 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).

[2] 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.

[3] 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>

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.[1]

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)[2], o direito de

[1] 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, 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*)

[2] 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

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.[1]

5. 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,

---

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."

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

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"[1]

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

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

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

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

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

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, pp. 624-638

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

DIAS PEREIRA, A.G., *Direitos dos pacientes e responsabilidade médica*, Coimbra Editora, Coimbra, 2015

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

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

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

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, M.E., *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, 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

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

SARMENTO E CASTRO, C., *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, pp. 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, p. 853.

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

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

TJUE, Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*

TJUE - 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 - Acórdão de 13 de maio de 2014, proc. C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

TJUE - Acórdão de 19 de outubro de 2016, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779

TJUE - 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)

O RESPONSÁVEL PELO TRATAMENTO DE DADOS SEGUNDO O RGDP*

RESUMO: O responsável pelo tratamento de dados (data controller) é o destinatário principal dos deveres impostos pelo RGPD em matéria de tratamento de dados e das sanções previstas para o seu não cumprimento. É uma noção ampla que abrange pessoas singulares ou coletivas, públicas ou privadas, estabelecidas dentro ou, sendo caso disso, fora da UE. Cabe ao "responsável" respeitar os princípios relativos ao tratamento de dados pessoais e respeitar os direitos dos titulares, para além de cumprir um conjunto de obrigações previstas no RGPD, como sejam, por ex., designar representante quando não estiver estabelecido na UE, aplicar medidas técnicas e organizativas adequadas, registar os tratamentos, avaliar o impacto dos tratamentos ou, consoante os casos, designar um encarregado de proteção de dados (EPD). Este estudo passa em revista as principais obrigações do responsável pelo tratamento de dados face ao RGPD (e, bem ainda, outros mecanismos ao seu dispor como a adoção de códigos de conduta ou procedimentos de certificação junto de organismos acreditados), bem como as sanções civis e administrativas a que ficam sujeitos no caso de não cumprimento desses deveres.

1. Introdução

1.1. O responsável pelo tratamento de dados como destinatário principal dos deveres impostos pelo Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD)[1] regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, garantindo a liberdade de circulação de dados pessoais no interior da União Europeia (art. 1/1 e 3). Por dados pessoais entende-se, para efeitos do RGPD, "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)", sendo "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (art. 4/1).[2]

Se o titular dos dados pessoais é o sujeito principal de direitos no RGPD, o *Responsável pelo Tratamento de Dados* (RTD) é o principal sujeito de deveres e

---

* *RDTec - Revista de Direito & Tecnologia* n.º 1/2 (2019) 143-173.

[1] 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. Doravante, salvo outra indicação, os artigos e considerandos citados são do RGPD.

A Diretiva 95/46/CE foi transposta para a ordem jurídica interna pela Lei 67/98, de 26 de outubro, agora revogada pela Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.

[2] Para efeitos do RGPD, são ainda definidas certas categorias de dados, nomeadamente os dados genéticos, os dados biométricos e os dados relativos à saúde – *vide infra*. O considerando (26) esclarece que "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica."

obrigações aí estabelecidos, e responsável pelas coimas e outras sanções previstas no RGDP para o não cumprimento das suas disposições e que são sensivelmente gravosas (artigos 83-84): o não cumprimento de uma ordem emitida pela autoridade de controlo (por ex. em Portugal, a CNPD) fica sujeito a coimas até € 20 000 000 ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado (artigo 83/6).[1] Para além da responsabilidade pelo cumprimento dos princípios do tratamento de dados e do respeito pelos direitos dos seus titulares, o RGPD dedica especificamente um capítulo, o IV, ao responsável pelo tratamento e subcontratante.

1.2. Noção de responsável pelo tratamento de dados

O RGPD estabelece uma noção ampla de RTD, definindo-o como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as *finalidades* e os *meios* de tratamento de dados pessoais" (art. 4/7, itálico nosso).[2] Assim, o RTD pode ser uma pessoa de direito privado, singular ou coletiva (por ex. associação, fundação, sociedade civil ou comercial, cooperativa), ou uma autoridade pública, agência ou outro organismo (por ex. uma câmara municipal, uma universidade pública, uma agência de regulação, uma entidade pública empresarial). A natureza pública ou privada da entidade é irrelevante. O que conta é saber se a entidade em causa, isolada ou conjuntamente com outras, determina as *finalidades* e os *meios* de tratamento de dados, i.e., o *para quê* e o *como*.

Ao RTD junta-se o subcontratante, entendido como qualquer pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do RTD (art. 4/8). Ambos realizam, por conseguinte, tratamento de dados, igualmente definido em termos amplos como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4/2).

1.3. Proteção de dados pessoais: do direito à vida privada ao direito à autodeterminação informativa

A proteção jurídica dos dados pessoais funda-se no direito ao respeito pela vida privada proclamado na Declaração Universal dos Direitos Humanos de 1948 (artigo 12) e consagrado com força normativa na Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950 (artigo 8), e no Pacto Internacional dos Direitos Civis e Políticos de 1966 (artigo 17). Portugal aderiu à Convenção Europeia dos

[1] Para consultar os números das chamadas empresas GAFA (Google, Apple, Facebook, Amazon) ver por ex. <https://www.statista.com/topics/4213/google-apple-facebook-and-amazon-gafa/>

[2] Para efeitos de determinação do RTD, acrescenta o referido preceito que, "sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

Direitos Humanos em 1978, se bem que na lei interna o Código Civil já consagrava, como direito de personalidade, a reserva sobre a intimidade da vida privada (artigo 80), tal como sucederia com a Constituição da República Portuguesa de 1976 (artigo 33 – posteriormente inserido no artigo sobre direitos pessoais – artigo 26), a qual dedicou um artigo à inviolabilidade do domicílio e da correspondência (artigo 34), limitando quaisquer restrições a casos e procedimentos previstos na lei e sujeitas a ordem judicial (nº 3), assim como proibindo "a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal" (nº 4; vide atualmente os artigos 187 a 190 do Código de Processo Penal). Além disso, a CRP proibiu genericamente a utilização da informática para tratar dados da vida privada das pessoas (art. 35), matéria cujo principal regime se encontra atualmente no RGPD.

Embora gerada no seio do "direito à privacidade", como é conhecido nos EUA o direito à reserva da vida privada, a proteção dos dados pessoais desenvolveu-se e adquiriu uma "vida própria", com fundamento no direito fundamental à "autodeterminação informativa", segundo a designação dada pelo tribunal constitucional federal alemão no seu acórdão de 15 dezembro de 1983, no âmbito de um processo relativo a informações pessoais coletadas durante o censo de 1983, em que o BFGH considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados dos seus dados pessoais é abrangida pelo direito fundamental de cada pessoa determinar, em princípio, a divulgação e o uso dos seus dados pessoais, sujeitando esta autodeterminação informacional apenas a limitações justificadas por razões de interesse público primordial.[1]

Esse "produto da doutrina alemã tão exportado, quanto mal conhecido na sua origem"[2] seria recebido pela doutrina constitucional portuguesa, ao abrigo do artigo 35 da CRP, no sentido de o "direito à autodeterminação informativa" atribuir "a cada pessoa o direito de controlar a informação disponível a seu respeito" e se impedir a

[1] Cf. Antoinette Rouvroy, Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in *Reinventing Data Protection?*, ed. Gutwirth (et al.), Springer, Dordrecht, 2009, p. 45-76. Para desenvolvimentos, v. Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", *Boletim da Faculdade de Direito de Coimbra* 64 (1993) 479-586; Catarina Sarmento e Castro, *Direito da informática, privacidade e dados pessoais*, Coimbra, Almedina, 2005; Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, *passim.* Sobre a proteção de dados antes do RGPD Garcia Marques, Lourenço Martins, *Direito da Informática*, 2.ª ed., Coimbra, Almedina, 2006, p. 129-313, 422-442, 330-391; Helena Moniz, "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) 231-298; Maria Eduarda Gonçalves, *Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2.ª ed., Coimbra, Almedina, 2003, p. 82-111, 173-183; Juan Pablo Aparício Vaquero, Alfredo Batuecas Caletrío (coord.), *En torno a la privacidad y la protección de datos en la sociedad de la información*, Granada. Comares, 2015; Alexandre Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in Algunos desafios en la proteccion de datos personales, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Madrid, Comares, 2018. Para comentários ao RGPD, J. López Calvo, *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin, 2017; Alexandre Sousa Pinheiro (coord)., *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, Coimbra, 2018.

[2] Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais*, cit., p. 825 (propondo em alternativa à proteção de dados pessoais a designação direito à "identidade informacional").

redução da pessoa a mero "objeto de informação"[1]. Assim, a autodeterminação informativa confere à pessoa, por um lado, um *"direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes)" e, por outro, "um *direito à reserva* (proibição de revelação)".[2] Na jurisprudência, o direito à autodeterminação informativa foi consagrado em diversos acórdãos do Tribunal Constitucional[3]. O Supremo Tribunal de Justiça consagrou igualmente este direito à "autodeterminação informativa" em diversos casos[4], encontrando-se a figura também em acórdãos dos Tribunais de Relação[5].

De igual modo, o Tribunal Europeu dos Direitos do Homem acolheu o direito à autodeterminação informacional. No acórdão *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia*, o TEDH considerou que o artigo 8.º da Convenção estabelece "o direito a uma forma de autodeterminação informacional" contra ingerência no exercício do seu direito à vida privada resultantes de recolha, processamento e disseminação coletiva dos seus dados pessoais.[6]

A afirmação do direito à "autodeterminação informativa" contra a redução da pessoa a mero objeto de informação não impede, todavia, o reconhecimento do valor económico dos dados pessoais, considerados bens transacionáveis, por ex. como forma de pagamento de serviços digitais[7], defendendo-se, por isso, que deveriam ser objeto de um acordo internacional entre os EUA e a UE com vista a promover o seu fluxo transatlântico[8], e ainda que os dados pessoais, enquanto valores de exploração, não podem ser excluídos do direito da concorrência, designadamente do abuso de posição dominante, na medida em que podem constituir recursos essenciais da economia digital[9].

---

[1] J.J. Gomes Canotilho & Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. 1, 4.ª ed., Coimbra, Coimbra Editora, 2007, p. 551

[2] Joaquim de Sousa Ribeiro, "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. 853-859.

[3] Cf. acórdão n° 442/2007, de 14 agosto de 2007, proc. n.º 815/2007 (considerando que o sigilo bancário não integra a esfera íntima da vida privada) e acórdão n.º 403/2015, proc. 773/15, de 17 de setembro de 2015 (considerando o direito à autodeterminação informativa como manifestação, juntamente com o direito à solidão e o direito ao anonimato, do direito ao livre desenvolvimento da personalidade previsto no artigo 26 da CRP).

[4] Acórdão de uniformização de jurisprudência n.º 2/08, de 13 de fevereiro de 2008, proc. n.º 894/07-3, e acórdão de 16 de outubro de 2014, proc. no. 679/05.7TAEVR.E2.S1 (Helena Moniz)

[5] Cf. também os acórdãos do Tribunal da Relação do Porto, de 31 de maio de 2006, proc. 0111584, do Tribunal da Relação de Coimbra, de 6 de abril de 2010, proc. 120-C/2000.C1, e do Tribunal da Relação de Évora, de 14 de setembro de 2017, proc. 2829/16.9T8PTM-B.E1, in www.dgsi.pt.

[6] *Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlândia* [GC], § 137, 27 de junho de 2017.

[7] Cf. B. Sloot, F.Z. Borgesius, "Google and Personal Data Protection", in *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, ed. A. Lopez-Tarruela, Hague, Asser/Springer, 2012, 75-111; A. Franceschi, A. Lehmann, "Data as tradeable commodity and new measures for their protection", *The The Italian Law Journal* 1/1 (2015) 51-72.

[8] Margaret Byrne Sedgewick, "Transborder data privacy as trade", *California Law Review* 105/5 (2017) 1513-1542.

[9] Vijay Bishnoi, "Data protection law: An inhibition in enforcement and promotion of competition law", *European Competition Law Review* 40/1 (2019) 34-40, alertando para o facto de que excluir o controlo sobre dados pessoais do direito da concorrência significa reforçar a posição das empresas dominantes na economia digital (as "GAFA"), para além do potencial de alavancagem que representam para atividades tradicionais.

1.4. Âmbito territorial de aplicação do RGPD para efeitos de determinação do RTD

O RGPD delimita o seu âmbito de aplicação territorial (art. 3) no sentido de abranger o tratamento de dados pessoais:

1. efetuado no contexto das atividades de um estabelecimento[1] de um RTD ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União;

2. 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[2]; ou b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União[1];

---

[1] O RTD com estabelecimentos em vários Estados-Membros tem estabelecimento principal no local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal (art. 4/16).

[2] O considerando (23) esclarece que "A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União."

Em sede de competência judiciária, para saber se um vendedor pela Internet «dirige» a sua atividade ao Estado-Membro do domicílio do consumidor, na aceção do artigo 15/1-c) do Regulamento 44/2001, de 22 de dezembro de 2000, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (entretanto revogado e substituído pelo Regulamento 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012), o Tribunal de Justiça da União Europeia decidiu, no acórdão *Pammer e Hotel Alpenhof*, de 7 de dezembro de 2010 (proc. apensos C-585/08 e C-144/09, ECLI:EU:C:2010:740), ser "necessário apurar se, antes da eventual celebração de um contrato com o consumidor, resulta desses sítios na Internet e da atividade global do comerciante que este pretendia estabelecer relações comerciais com consumidores domiciliados num ou vários Estados-Membros, incluindo o do domicílio do consumidor, no sentido de que estava disposto a com eles contratar./ Os elementos seguintes, cuja enumeração não é exaustiva, podem constituir indícios que permitem considerar que o comerciante dirige a sua atividade ao Estado-Membro do domicílio do consumidor: a natureza internacional da atividade, a menção de itinerários a partir de outros Estados-Membros para chegar ao local onde o comerciante está estabelecido, a utilização de uma língua ou moeda diferentes das habitualmente utilizadas no Estado-Membro em que o comerciante está estabelecido, com a possibilidade de reservar e confirmar a reserva nessa língua, a menção de números de telefone com a indicação de um indicativo internacional, a realização de despesas num serviço de referenciação na Internet para facilitar aos consumidores domiciliados noutros Estados-Membros o acesso ao sítio do comerciante ou a um sítio do seu intermediário, a utilização de um nome de domínio de primeiro nível diferente do do Estado-Membro em que o comerciante está estabelecido e a menção de uma clientela internacional constituída por clientes domiciliados em diferentes Estados-Membros. Cabe ao juiz nacional apurar se existem esses indícios. / Pelo contrário, é insuficiente a simples acessibilidade do sítio na Internet do comerciante ou do intermediário no Estado-Membro do domicílio do consumidor.

3. 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, por ex. no âmbito de uma missão diplomática ou num posto consular de um Estado-Membro, como refere o considerando (25).[2]

1.5. Exclusão de atividades pessoais ou domésticas

As atividades pessoais ou domésticas não são abrangidas pelo RGPD. O considerando (18) esclarece que o RGPD "não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas."

Assim, por exemplo, os utilizadores de redes sociais como o *Facebook* ou o *Instagram*, não estão sujeitos ao RGPD, mas a empresa "Facebook Inc." já é considerada RTD para efeitos do RGPD. Ora, como o RGPD não prejudica a aplicação da Diretiva 2000/31/CE sobre, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12 a 15 (art. 2/4), os operadores de redes sociais ou de plataformas de partilha de conteúdos em linha não são considerados prestadores intermediários de serviços para efeitos do respetivo regime de responsabilidade estabelecido na diretiva sobre comércio eletrónico[3].

2. Deveres do responsável pelo tratamento de dados (*data controller*)

2.1. O dever de respeitar os princípios de tratamento de dados pessoais

No leque de deveres a cargo do RTD surge à cabeça o de respeitar os princípios relativos ao tratamento de dados pessoais estabelecidos no RGPD, a saber: a licitude, lealdade e transparência, a limitação das finalidades, a minimização dos dados, a

---

O mesmo se aplica à menção de um endereço eletrónico e de outros elementos ou à utilização de uma língua ou moeda que sejam habitualmente utilizadas no Estado-Membro em que o comerciante está estabelecido."

[1] Segundo o considerando (24), "A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes."

[2] O recurso à computação em nuvem para o tratamento de dados não prejudica o âmbito de aplicação do RGPD. Sobre a questão do tratamento de dados pessoais em ambiente de computação em nuvem, *vide* P. Blume, "Data Protection in the Cloud", *Computer Law Review International* 2011/3, 76-80; W.K. Hon, J. Hörnle, C. Millard, "Data protection jurisdiction and Cloud Computing – when are cloud users and providers subject to EU Data protection law? The Cloud of Unknowing", *International Review of Law, Computers & Technology* 26/2-3 (2012) 129-164.

[3] Sobreo tema, Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista Bolsa, Banca e Seguros* 3 (2018) 215-6, em nota.

exatidão, a limitação da conservação, e a integridade e confidencialidade (art. 5/1). Aliás, a responsabilidade do RTD pelo cumprimento dos princípios do tratamento de dados pessoais é, também, um desses princípios, o da responsabilidade, fazendo recair sobre o RTD o ónus da prova do cumprimento dos referidos princípios (art. 5/2).[1]

A licitude do tratamento pode resultar de consentimento do titular de dados ou da sua necessidade em sede contratual, cumprimento de obrigação jurídica do responsável, defesa de interesses vitais do titular ou de terceiro, exercício de funções públicas ou autoridade pública do responsável[2], ou interesses legítimos do responsável ou de terceiro (art. 6).[3]

2.2. O consentimento para o tratamento de dados pessoais

O consentimento deve ser demonstrável, específico, livre e livremente revogável (art. 7). Para ser livre, o consentimento não deve ser condição *sine qua non* de prestação de um serviço, se o tratamento de dados pessoais não for necessário para o efeito[4].

---

[1] Em sede de responsabilidade por danos é o RTD quem terá que "provar que de modo algum é responsável pelo evento que deu causa aos danos" (art. 82/3), ao contrário da regra geral da responsabilidade extracontratual.

[2] O fundamento jurídico previsto no direito da EU ou interno pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX

[3] Nos termos do considerando (46), "Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana." Além disso, o considerando (48) informa que "O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta." Sobre o tema, A. Barreto Menezes Cordeiro, "O tratamento de dados pessoais fundado em interesses legítimos", *Revista de Direito e Tecnologia* 1/1 (2019) 1-31.

A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), estabelece no artigo 13/1, relativamente a comunicações não solicitadas que a utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio eletrónico para fins de comercialização direta apenas poderá ser autorizada em relação a assinantes que tenham dado o seu *consentimento prévio* (no direito interno, vide o artigo 13-A da Lei 41/2004, de 18 de agosto).

[4] Nos termos do considerando (42), "Em conformidade com a Diretiva 93/13/CEE do Conselho (1), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado." Por seu turno, segundo o considerando (43), "Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução."

Por outro lado, na oferta direta de serviços da sociedade da informação a crianças, o tratamento de dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos, embora os EM possam reduzir até 13 anos a idade para consentir (art. 8). Cabe ao RTD implementar medidas técnicas de controlo da idade do menor, operação que envolverá, só por si, o tratamento de dados pessoais do menor.[1]

O tratamento de categorias especiais de dados – "dados sensíveis"[2] – está sujeito a uma proibição geral, pelo que apenas é admitido excecionalmente verificados determinados requisitos específicos. Por ex. a proteção de interesses vitais só justifica o tratamento de dados se o titular estiver incapaz de consentir. Por outro lado, é reservada aos Estados-Membros a possibilidade de manterem ou imporem novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde (art. 9/4).[3] A importância destes dados retira alcance à unificação visada pelo RGPD, e compromete a almejada liberdade de circulação de dados no interior da União Europeia.

2.3. O dever de respeitar os direitos do titular dos dados

O RTD deve respeitar os direitos do titular de dados. Desde logo o direito à *transparência* das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. Para o efeito deve prestar informações por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos, de forma concisa, transparente, inteligível e de fácil acesso, gratuita, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. O RGPD especifica as informações a facultar consoante os dados pessoais sejam ou não recolhidos junto do titular (art. 13 e 14).

Depois, no exercício do direito de acesso, o titular dos dados deve poder saber que dados, para que fins, durante quanto tempo, de que modo, é feito o tratamento e a quem se destinam os dados (art. 15). O RTD fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o RTD pode

---

[1] Segundo o considerando (51): "O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular."

[2] Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

[3] Os primeiros (*genéticos*) são definidos como "os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa" (art. 4/13). Os segundos (biométricos) consistem em "dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (art. 4/15). Por último, os dados relativos à saúde são "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" (art. 4/15). Sobre o tema, Filipe Miguel Cruz de Albuquerque Matos, "O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde", *Revista Bolsa, Banca e Seguros* 3 (2018) 51-122.

exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente (art. 15/3).[1]

São ainda direitos do titular de dados o direito de retificação e de apagamento (ou direito a ser esquecido)[2] (art. 16), o direito à limitação do tratamento (art. 17 e 18), o direito de portabilidade dos dados (art. 20)[3] e o direito de oposição ao tratamento e a decisões individuais automatizadas (art. 21).

O exercício destes direitos pelo titular gera obrigações para o RTD, nomeadamente, no que respeita à retificação ou ao apagamento, o dever de comunicar "a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais […], salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado" (art. 19).[4]

---

[1] Segundo o considerando (63), "Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. (…) Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido."

[2] Este "direito a ser esquecido" foi afirmado pelo Tribunal de Justiça da União Europeia no 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* (ECLI:EU:C:2014:317). No sentido de que se trata antes de um "direito à desassociação" nos motores de pesquisa na internet, Filipa Calvão, "A protecção de dados pessoais na internet: desenvolvimentos recentes", *Revista de Direito Intelectual,* 2015/2, 67-84. Sobre o acórdão *Google Spain,* ver também por ex. Indra Spiecker, "A new framework for information markets: Google Spain", *Common Market Law Review,* 52 (2015) 1033-1058; Sofia de Vasconcelos Casimiro, "O direito a ser esquecido pelos motores de busca: o Acórdão Costeja", *Revista de Direito Intelectual*, 2014/2, 307-353. No sentido de que o direito ao esquecimento, enquanto "direito geral de eliminação de dados pessoais", em especial na Internet, não tem equivalente na lei nem na jurisprudência dos Estados Unidos da América, Dário Moura Vicente, Sofia de Vasconcelos Casimiro, "A proteção de dados pessoais na Internet à luz do Direito Comparado", *Revista de Direito Intelectual*, 2018/2, 45-90, 67. A propósito do direito comparado registe-se no direito britânico a elaboração jurisprudencial de um novo ilícito, o chamado "tort of misuse of personal information", por ex. no caso *Naomi Campbell* c. *The Mirror*, e o critério da "expetativa razoável de privacidade": *v.* Ian Cram, *The right to respect for private life: digital challenges, a comparative-law perspective – The United Kingdom*, European Parliamentary Research Service, Bruxelas, October 2018, 14-20.

Mais recentemente, no acórdão de 24 de Setembro, proc. C-507/17, *Google c. CNIL* (EU:C:2019:772), o Tribunal de Justiça da União Europeia concluiu que "o operador de um motor de busca não tem de efetuar [a] supressão de referências em todas as versões do seu motor, devendo fazê-lo nas versões deste que correspondem a todos os Estados-Membros, e isto, se necessário, em conjugação com medidas que, embora satisfaçam as exigências legais, permitam efetivamente impedir ou, pelo menos, desencorajar seriamente os internautas que efetuam uma pesquisa a partir do nome da pessoa em causa dentro de um dos Estados-Membros de, através da lista de resultados exibida após essa pesquisa, aceder às hiperligações que são objeto desse pedido."

[3] O direito à portabilidade está também previsto na Lei das Comunicações Eletrónicas (Lei 5/2004, de 10 de fevereiro, com alterações posteriores) e no Regulamento 58/2005, de 18 de agosto, da ANACOM (alterado várias vezes), que estabelece os princípios e regras aplicáveis à portabilidade nas redes de comunicações públicas (Regulamento da Portabilidade), e no Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho de 14 de junho de 2017 relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno. Sobre o direito à portabilidade ver por ex. Vítor Palmela Fidalgo, "O direito à portabilidade de dados pessoais", *Revista de Direito e Tecnologia* 1/1 (2019) 89-135.

[4] Todavia, os direitos do titular são limitados, nomeadamente por *razões de interesse público*. Segundo o considerando (71), "a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros

2.4. Dever de aplicar medidas técnicas e organizativas adequadas

O RTD deve aplicar *medidas técnicas e organizativas adequadas* (consoante a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares) para assegurar e comprovar a conformidade do tratamento com o RGPD, devendo rever e atualizá-las consoante as necessidades (art. 24). Para demonstrar o cumprimento das suas obrigações o RTD pode utilizar o cumprimento de códigos de conduta ou de procedimentos de certificação aprovados nos termos do RGPD (arts. 41 e 42).

Depois, o RTD deve adotar medidas técnicas e organizativas adequadas, como a *pseudonimização*, no sentido da proteção de dados *desde a conceção e por defeito*. Por exemplo, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25/1-2). O cumprimento desta obrigação pode fazer-se através de um procedimento de certificação aprovado nos termos do RGPD (art. 42).

No caso de as finalidades e os meios de tratamento serem determinados conjuntamente por dois ou mais responsáveis, dá-se uma situação de *responsáveis conjuntos* pelo tratamento, respondendo todos solidariamente sem prejuízo do acordo de divisão interna de responsabilidades (art. 26).

2.5. Dever de designação de representante na União

Os responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União devem *designar por escrito um representante*[1] na União, salvo se forem atividades ocasionais e que não envolvam o tratamento em larga escala de dados sensíveis, ou realizadas por autoridades ou organismos públicos (art. 27).[2] O RTD só pode recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e

---

aplicável ao responsável pelo tratamento, incluindo para efeitos de *controlo e prevenção de fraudes e da evasão fiscal*, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular."

[1] Por *representante* entende-se "uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do" RGPD (art. 4/17).

[2] Segundo o considerando (80), "Sempre que um responsável pelo tratamento ou um subcontratante não estabelecidos na União efetuarem o tratamento de dados pessoais de titulares de dados que se encontrem na União, e as suas atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente de a estes ser exigido um pagamento, ou com o controlo do seu comportamento na medida que o seu comportamento tenha lugar na União, o responsável pelo tratamento ou o subcontratante deverão designar um representante, a não ser que o tratamento seja ocasional, não inclua o tratamento, em larga escala, de categorias especiais de dados pessoais, nem o tratamento de dados pessoais relativos a condenações penais e infrações, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento ou se o responsável pelo tratamento for uma autoridade ou organismo público. (…) *O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento ou subcontratante, emitido por escrito*, que permita ao representante agir em seu nome no que diz respeito às obrigações que lhes são impostas pelo presente regulamento" (*itálico nosso*).

organizativas adequadas a cumprir o RGPD e respeite os direitos do titular dos dados (art. 28).

2.6. Dever de manter um registo dos tratamentos

O RTD tem o dever de manter um registo por escrito de todas as atividades de tratamentos efetuados, especificando as informações como o seu nome e contactos, e do seu representante e EPD, as finalidades do tratamento, as categorias de titulares de dados, dados pessoais, e destinatários, as transferências, prazos de apagamento dos dados, e descrição das medidas técnicas e organizativas de segurança (art. 30). Ficam isentos os RTD com menos de 250 trabalhadores, a menos que tratem "dados sensíveis" ou relativos a condenações penais (art. 30/5).

2.7. Dever de assegurar um nível de segurança adequado ao risco

O RTD tem o dever de aplicar medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco, incluindo a pseudonomização e a cifragem de dados, a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e um processo para testar, apreciar e avaliar regularmente a eficácia dessas medidas (art. 32). A prova do cumprimento desta obrigação pode ser feita pelo cumprimento de um código de conduta ou de um procedimento de certificação aprovados conforme o RGPD (art. 40 e 42).[1]

2.8. Dever de cooperar com a autoridade de controlo, incluindo o dever de notificação

O RTD tem o dever de cooperação com a autoridade de controlo (art. 31). Desde logo, o RTD deve notificar, em princípio no máximo de 72 horas, uma violação de dados pessoais à autoridade de controlo (art. 33). Se a violação de dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, o RTD deve comunicar esse facto ao titular dos dados, a menos que tenha usado técnicas como a cifragem (art. 34). Como informa o considerando (85), "Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares."

[1] O regime jurídico da cibersegurança foi aprovado pela Lei 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Sobre o tema, Alexandre L. Dias Pereira, "Proteção do consumidor e segurança informática no comércio eletrónico", *Revista Bolsa, Banca e Seguros* 3 (2018) 303-329.

2.9. Dever de avaliação de impacto

O RTD deve avaliar o impacto sobre a proteção de dados por ex. em caso de tratamento sistemático de dados sensíveis em larga escala (art. 35). [1] Se concluir que o tratamento envolve um elevado risco para os direitos e liberdades das pessoas singulares, o RTD tem o dever de proceder a consulta prévia à autoridade de controlo (art. 36).

O RGPD ressalva ainda que a lei interna de cada Estado-Membro pode inclusivamente sujeitar a autorização prévia da autoridade de controlo o tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública (art. 36/6).[2]

2.10. Dever de designar um Encarregado de Proteção de dados (EPD/DPO)

O RTD deve designar um *Encarregado de Proteção de Dados* (EPD) se for autoridade ou organismo público (podendo ser comum a vários organismos ou autoridades, tendo em conta a respetiva estrutura organizacional e dimensão), ou exercer atividade que exija o controlo de titulares de dados ou o tratamento de dados em grande escala (art. 37). Segundo as Orientações do Grupo de Trabalho do Artigo 29[3], consideram-se de grande escala: "o tratamento de dados de doentes no exercício normal das atividades de um hospital; tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem); o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços; o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco; o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca; o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet". Pela negativa, não são de grande escala os tratamentos de dados de doentes pacientes por um médico e os de dados pessoais relacionados com condenações penais e infrações por um advogado.

---

[1] Nos termos do considerando (91), "O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória." A referência ao hospital juntamente com os profissionais de saúde isentos do dever de avaliação de impacto resulta manifestamente de um lapso de redação da versão portuguesa do RGPD, como se constata comparando-a com as versões inglesa, francesa ou castelhana.

[2] Sobre a avaliação de impacto, ver o documento do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Adotadas em 4 de abril de 2017, Revistas e adotadas pela última vez em 4 de outubro de 2017, WP 248 rev.01.

[3] Sobre o EPD, ver o documento do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações sobre os encarregados da proteção de dados (EPD). Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, WP 243 rev.01, p. 10.

Sendo um grupo empresarial[1], o RTD pode designar um único EPD se houver um EPD facilmente acessível a partir de cada estabelecimento (art. 37/2). O RTD deve publicar os contactos do EPD e comunica-los à autoridade de controlo. O RTD deve apoiar o EPD e respeitar a sua autonomia no desempenho das suas funções de zelar pelo cumprimento do RGPD; funções essas que pode cumular com outras funções e atribuições que não resultem num conflito de interesses, o que cabe ao RTD assegurar (art. 38/8).[2]

2.11. Adoção de código de conduta e obtenção de certificação de proteção de dados (facultativo)

As associações de RTD elaboram códigos de conduta (art. 40). A supervisão destes códigos pode ser efetuada por um organismo que tenha um nível adequado de competência relativamente ao objeto do código e esteja acreditado para o efeito pela

[1] Por "empresa", entende-se "uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica". Segundo o considerando (22), "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." Por grupo empresarial entende-se um grupo composto pela empresa que exerce o controlo e pelas empresas controladas (art. 4/18-19). O considerando (36) informa que "A existência e utilização de meios técnicos e de tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituem, em si mesmas, um estabelecimento principal nem são, portanto, um critério definidor de estabelecimento principal. […]Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa."

[2] O Conselho Geral da Ordem dos Advogados emitiu Parecer no sentido de os advogados estarem "impedidos de exercer o mandato forense ou a consulta jurídica, para entidades para quem exerçam, ou tenham exercido as funções de encarregado de Proteção de dados" (proc. n.º 14/PP/2018-G). No essencial, cabendo ao EPD fiscalizar o RTD, não teria condições deontológicas para, ao mesmo tempo, lhe prestar o mandato forense ou a consulta jurídica. O Parecer mereceu a crítica acertada de A. Barreto Menezes Cordeiro, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *Revista da Ordem dos Advogados* 78/I-II (2018) 17-38. Tendo em conta que as *Orientações do Grupo de Trabalho do Art. 29.º sobre o Encarregado de Proteção de Dados*, p. 19, dão como exemplo de possível conflito de interesses se "um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados", defende o referido Autor que "Fora do universo da proteção de dados importa verificar, casuisticamente, a existência ou não de conflitos de interesses concretos" (*ibidem,* 38). Com efeito, o referido Parecer estabelece um impedimento geral que nos parece manifestamente excessivo. Tal como o Estatuto Deontológico dos Advogados pretende assegurar a autonomia e independência do advogado, o mesmo sucede com o RGPD relativamente ao EPD, estabelecendo que o RTD assegura que o EPD "não recebe instruções relativamente ao exercício das suas funções" e que "não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções" (art. 38/3). O Parecer reconhece a autonomia do EPD, mas o entendimento sobre natureza das funções de fiscalização do EPD não têm, a nosso ver, base no RGPD. Dá a entender que nesse papel, e no desempenho da função de cooperação com a autoridade de controlo, o EPD seria obrigado a denunciar eventuais infrações cometidas pelo RTD à autoridade de controlo, o que não é manifestamente o caso, tanto mais que está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, sem prejuízo de poder de contatar e solicitar o parecer da autoridade de controlo (cf. *Orientações do Grupo de Trabalho do Art. 29.º sobre o Encarregado de Proteção de Dados*, cit., p. 21)

autoridade de controlo competente (art. 41).[1] O organismo de *supervisão acreditado* pode suspender ou excluir um RTD que não cumpra o código de conduta.

Os RTD podem cumprir *procedimentos de certificação* em matéria de proteção de dados, bem como adotar selos e marcas de proteção de dados, para efeitos de comprovação da conformidade dos tratamentos com o RGPD (art. 42). A certificação, válida em princípio por três anos, é efetuada por organismo de certificação acreditado pela autoridade de controlo ou diretamente por esta (art. 43).

2.12. Transferências de dados para fora da União Europeia

O RTD pode transferir dados pessoais para países terceiros ou organizações internacionais, se atuar em conformidade com o RGPD (art. 44). Para o efeito, o RTD pode fazer transferências com base numa decisão da Comissão de adequação do nível de proteção do país terceiro (art. 45).[2]

Na falta de uma tal decisão de adequação, a transferência pode ocorrer se o RTD apresentar garantias adequadas e os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (art. 46). Essas garantias adequadas podem resultar, por exemplo, de *regras vinculativas aplicáveis às empresas* (art. 47), de cláusulas-tipo de proteção de dados adotadas ou aprovadas pela Comissão, de código de conduta ou procedimento de certificação, acompanhados de compromissos vinculativos e com força executiva – cf. considerando (108).

Além disso, mesmo na ausência de uma decisão de adequação ou de garantias adequadas (por ex. regras vinculativas aplicáveis às empresas), as transferências para países terceiros podem ser efetuadas para situações específicas, nomeadamente se houver consentimento explícito e informado do titular dos dados, se a transferência for necessária em sede contratual ou por razões de interesse público ou para proteger interesses vitais de pessoa incapaz de consentir, para além de outras derrogações para situações específicas previstas no art. 49.

2.13. Derrogações (liberdade de expressão e informação, acesso aos documentos da Administração Pública, em contexto laboral)

A liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária, justifica derrogações específicas ao regime geral de tratamento de dados (art. 85), tal como sucede com o tratamento e acesso do público aos documentos oficiais (art. 86), o tratamento do número de identificação nacional (art. 87) e o tratamento no contexto laboral (art. 88). Além disso, são previstas garantias e derrogações relativas ao

[1] Segundo o considerando (77) "As orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações fornecidas pelo Comité ou às indicações fornecidas por um encarregado da proteção de dados."

[2] Ver o "US-EU Privacy Shield" e 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.

tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos (art. 89). Por exemplo a pseudonimização só é obrigatória se os referidos fins puderem ser alcançados desse modo.

De igual modo, podem ser estabelecidas derrogações aos direitos de acesso, retificação, limitação e oposição na medida em que esses direitos possam tornar impossível ou prejudicar gravemente a realização dos fins específicos de investigação científica ou histórica ou fins estatísticos e que tais derrogações sejam necessárias para a prossecução desses fins (art. 89/2).

2.14. Obrigação de sigilo

O RGPD não prejudica a obrigação de sigilo a que o RTD esteja sujeito, por lei interna do Estado-membro, relativamente aos dados pessoais que tenha recebido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma (art. 90). Por ex., o Regulamento de Deontologia Médica[1] encarrega os responsáveis pelo tratamento da informação de saúde de tomarem 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" (art. 37). O dever de confidencialidade da informação de saúde é reiterado no capítulo VII do Regulamento sobre a telemedicina (arts. 46 a 49).[2]

3. Aplicação privada dos direitos relativos aos dados pessoais

Os titulares de dados pessoais têm o direito de reclamar junto de uma autoridade de controlo (art. 77), bem como o direito de agir judicialmente contra uma autoridade de controlo (art. 78) e/ou contra um responsável pelo tratamento ou um subcontratante (art. 79). Para o efeito, podem ser representados por organismo sem fins lucrativos, incluindo uma associação de defesa dos consumidores.

O RGPD garante expressamente o direito a obter uma indemnização por danos causados pela violação de dados pessoais (art. 82). Os titulares dos dados deverão ser *integral e efetivamente* indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados (responsabilidade solidária). Porém, se os processos forem apensos num único processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode

[1] Regulamento n.º 707/2016, de 21 de julho.

[2] Cf. Alexandre L. Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in *Algunos desafios en la proteccion de datos personales*, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Comares, Madrid, 2018.

posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento (art. 82/4-5).

O titular de dados pode intentar uma ação judicial contra o RTD perante os tribunais do seu Estado-Membro de residência ou os tribunais do Estado-Membro de estabelecimento do RTD, indica o considerando (145), ressalvando, todavia, a competência exclusiva destes últimos se o RTD "for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos".

Para ser exonerado de responsabilidade, o RTD ou o subcontratante terá que provar o facto que causou o dano não lhe é de modo algum imputável [considerando (146) e art. 82/3].

4. Conclusão

O RGPD impõe um conjunto de deveres sobre o RTD, entendido como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" (art. 4/7).[1]

O RGPD aplica-se a tratamentos de dados feitos por RTD estabelecido na União Europeia, tratamentos "ativos" (mediante oferta de bens ou serviços ou controlo de comportamento) de dados de pessoas residentes na UE, independentemente do lugar de estabelecimento do RTD, e tratamentos efetuados em lugar no qual se aplica o direito da UE por força do direito internacional público. São excluídas do âmbito de aplicação do RGPD as atividades exclusivamente pessoais ou domésticas (grosso modo, consumidores, incluindo usuários de redes sociais, mas não as dos provedores dessas plataformas).

O RTD deve respeitar os princípios relativos ao tratamento de dados pessoais, como sejam (1) a licitude, lealdade e transparência; (2) a limitação das finalidades; (3) a minimização de dados; (4) a exatidão; (5) a limitação da conservação; (6) integridade e confidencialidade; (7) a responsabilidade do RTD pelo "data compliance". Nos requisitos de licitude, surge à cabeça a exigência de consentimento demonstrável, específico, livremente dado e revogável. Sendo que, relativamente a tratamento de

[1] Por ex. o operador de um sítio de comércio eletrónico é considerado um RTD para efeitos do RGPD, como já antes apontado, ao abrigo da Diretiva 95/46/CE. Cf. Grupo de trabalho do artigo 29 sobre proteção de dados, Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante, WP 169, fevereiro de 2010. Para uma exposição sucinta sobre o impacto do RGPD nos sítios dos operadores de comércio eletrónico, v. Michaela Weigl, "The EU General Data Protection Regulation's Impact on Website Operators and eCommerce", *Computerrecht-international* 4 (2016), 102-108; e em especial nas empresas que fazem tratamento intensivo de dados, Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", *Computer Law & Security Review* 34 (2018) 134–153. Por outro lado, antes da aprovação do RGPD, o Tribunal de Justiça da União Europeia considerou o operador de motor de busca na Internet como RTD: "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", devendo o operador desse motor de busca ser considerado "responsável" pelo dito tratamento: 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.*

dados no contexto de serviços da sociedade da informação, o RGPD estabelece a idade mínima para consentir em 16 anos, embora permita que os Estados-Membros baixem até aos 13 anos. Além disso, o próprio RGOD confere autorização legal para certos tratamentos, por razões, nomeadamente, de proteção de interesses vitais do titular, interesse público, formação e execução de contratos, interesses legítimos, ou cumprimento de obrigação legal.

O RTD deve respeitar os direitos dos titulares, a saber: transparência do tratamento, acesso (e cópia), retificação e apagamento ("direito a ser esquecido"), limitação do tratamento, portabilidade, oposição à definição de perfis e de sujeição a decisões individuais automatizadas.[1] Por outro lado, o RTD deve: (1) designar representante quando não estiver estabelecido na EU, salvo para atividades ocasionais e sem tratamento em larga escala de dados sensíveis; (2) aplicar medidas técnicas e organizativas adequadas para cumprir o RGPD e proteger os dados desde a conceção e por defeito (por ex. pseudonimização); (3) abster-se de disponibilizar, sem intervenção humana, dados a um número indeterminado de pessoas singulares; (4) registar os tratamentos, especificando determinados elementos (podendo estar isentas deste dever as PME); (5) cooperar com a autoridade de controlo; (6) aplicar medidas de segurança informática adequadas ao risco; (6) notificar a autoridade de controlo e, havendo perigo elevado para direitos do titular, comunicar-lhe uma violação de dados; (7) avaliar o impacto e, em certos casos, consultar previamente a autoridade de controlo (estando isentos do dever de avaliação de impacto certos profissionais como advogados e médicos); (8) designar encarregado de proteção de dados (EPD), quando efetue tratamentos em "grande escala", designadamente quando o tratamento de dados faz parte das atividades principais do responsável, como sucede com os hospitais[2].

O RTD pode comprovar o cumprimento do RGPD pela adoção de códigos de conduta ou mediante procedimento de certificação junto de organismos acreditados, incluindo obtenção de selos e marcas de proteção de dados, aprovados pela Comissão Europeia ou pelo Autoridade de controlo, consoante os casos.

As transferências para países terceiros ou organizações internacionais podem ser feitas com base: a) numa decisão de adequação da Comissão ou, na falta disso, b) em regras vinculativas aplicáveis às empresas, c) cláusulas-tipo de proteção de dados adotadas pela Comissão, d) código de conduta ou procedimento de certificação aprovados em conformidade com o regulamento, i.e., acompanhados de compromissos vinculativos e com força executiva. O RGPD prevê ainda derrogações para tratamentos de dados para fins jornalísticos, expressão literária, artística ou científica, arquivo de interesse público, investigação científica ou histórica, ou estatísticos.

Finalmente, o RGPD consagra a possibilidade de aplicação privada dos direitos sobre dados pessoais, no sentido de que o RTD deve indemnizar integral e efetivamente os titulares de dados pelos danos sofridos, sendo solidária a responsabilidade no caso de

[1] Sobre a transparência ao nível da configuração dos algoritmos de definição de perfis e da automatização de decisões com base nesses algoritmos, Giovanni de Gregorio, "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society", *European Journal of Legal Studies* 11/2 (2019) 65-103.

[2] Cf. Orientações do Grupo de Trabalho do Art. 29 sobre o Encarregado de Proteção de Dados, p. 8.

tratamento conjunto por vários responsáveis ou subcontratante, sem prejuízo de ação de regresso. Além disso, o RTD fica sujeito ao pagamento de avultadas coimas, que podem a 4% do seu volume de negócios, e de um modo geral deve cumprir as determinações das autoridades competentes.

Bibliografia

A. Barreto Menezes Cordeiro, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", Revista da Ordem dos Advogados 78/I-II (2018) 17-38 - A. Barreto Menezes Cordeiro, "O tratamento de dados pessoais fundado em interesses legítimos", Revista de Direito e Tecnologia 1/1 (2019) 1-31

A. Franceschi, A. Lehmann, "Data as tradeable commodity and new measures for their protection", The The Italian Law Journal 1/1 (2015) 51-72

Alexandre L. Dias Pereira, "A proteção dos dados pessoais no direito português, em especial no setor da saúde", in Algunos desafios en la proteccion de datos personales, org. Alfredo Batuecas Caletrio, Juan Pablo Aparicio Vaquero, Madrid, Comares, 2018 - "Proteção do consumidor e segurança informática no comércio eletrónico", *Revista Bolsa, Banca e Seguros* 3 (2018) 303-329

Alexandre Sousa Pinheiro, Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional, Lisboa, AAFDL, 2015.

Antoinette Rouvroy, Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in Reinventing Data Protection?, ed. Gutwirth (et al.), Springer, Dordrecht, 2009, 45-76

B. Sloot, F.Z. Borgesius, "Google and Personal Data Protection", in Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, ed. In A. Lopez-Tarruela, Hague: Asser/Springer, 2012, 75-111.

Catarina Sarmento e Castro, Direito da informática, privacidade e dados pessoais, Coimbra, Almedina, 2005

Christina Tikkinen-Piri, Anna Rohunen, Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", Computer Law & Security Review 34 (2018) 134–153

Dário Moura Vicente, Sofia de Vasconcelos Casimiro, "A proteção de dados pessoais na Internet à luz do Direito Comparado", Revista de Direito Intelectual, 2018/2, 45-90

Filipa Urbano Calvão, "A protecção de dados pessoais na internet: desenvolvimentos recentes", Revista de Direito Intelectual, 2015/2, 67-84

Filipe Miguel Cruz de Albuquerque Matos, "O Regulamento de Protecção de Dados Pessoais (2016/679) no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde", *Revista Bolsa, Banca e Seguros* 3 (2018) 51-122

Garcia Marques, Lourenço Martins, Direito da Informática, 2.ª ed., Coimbra, Almedina, 2006

Giovanni de Gregorio, "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society", European Journal of Legal Studies 11/2 (2019) 65-103

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Adotadas em 4 de abril de 2017, Revistas e adotadas pela última vez em 4 de outubro de 2017, WP 248 rev.01 - Orientações sobre os encarregados da proteção de dados (EPD). Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, WP 243 rev.01

Helena Moniz, "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) 231-298

Ian Cram, *The right to respect for private life: digital challenges, a comparative-law perspective – The United Kingdom*, European Parliamentary Research Service, Brussels, October 2018

Indra Spiecker, "A new framework for information markets: Google Spain", Common Market Law Review, 52 (2015) 1033-1058

J. López Calvo, Comentarios al Reglamento Europeo de Protección de Datos, Madrid, Sepin, 2017

J. Seabra LOPES, "A proteção da privacidade e dos dados pessoais na sociedade de informação", Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa, UCP, Lisboa, 2002, 779

J.J. Gomes Canotilho & Vital Moreira, Constituição da República Portuguesa Anotada, vol. 1, 4.ª ed., Coimbra, Coimbra Editora, 2007, p. 551

Joaquim de Sousa Ribeiro, "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, 853-859

J.P. Aparício Vaquero, A. Batuecas Caletrío (coord.), En torno a la privacidad y la protección de datos en la sociedad de la información, Granada. Comares, 2015

Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", Revista Bolsa, Banca e Seguros 3 (2018) 147-216

Margaret Byrne Sedgewick, "Transborder data privacy as trade", California Law Review 105/5 (2017) 1513-1542 - Maria Eduarda Gonçalves, Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação, 2.ª ed., Coimbra, Almedina, 2003

Michaela Weigl, "The EU General Data Protection Regulation's Impact on Website Operators and eCommerce", Computerrecht-international 2016/4, 102-108.

P. Blume, "Data Protection in the Cloud", Computer Law Review International 2011/3, 76-80.

Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", Boletim da Faculdade de Direito de Coimbra 64 (1993) 479-586

Sloot, F.Z. Borgesius, "Google and Personal Data Protection", in Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, ed. A. Lopez-Tarruela, Hague, Asser/Springer, 2012, 75-111

Sofia de Vasconcelos Casimiro, "O direito a ser esquecido pelos motores de busca: o Acórdão Costeja", Revista de Direito Intelectual, 2014/2, 307-353

Vijay Bishnoi, "Data protection law: An inhibition in enforcement and promotion of competition law", European Competition Law Review 40/1 (2019) 34-40

Vítor Palmela Fidalgo, "O direito à portabilidade de dados pessoais", Revista de Direito e Tecnologia 1/1 (2019) 89-135.

W.K. Hon, J. Hörnle, C. Millard, "Data protection jurisdiction and Cloud Computing – when are cloud users and providers subject to EU Data protection law? The Cloud of Unknowing", International Review of Law, Computers & Technology, 26/2-3 (2012) 129-164

OS DIREITOS DE AUTOR NO MERCADO ÚNICO DIGITAL SEGUNDO A DIRETIVA 2019/790*

Resumo: O bom funcionamento do mercado único digital exigiu alterações às leis dos direitos de autor para esclarecer a responsabilidade das plataformas de partilha pelos conteúdos carregados pelos seus utilizadores, assegurando ao mesmo tempo que esta responsabilidade não se traduz num sistema de censura na internet nem na instituição do poderio económico-tecnológico de alguns gigantes da Internet. De igual modo, a nova diretiva alarga exceções já existentes, com vista à realização de atividades sem fins comerciais, como conservação do património cultural e ensino à distância, e estabelece novas, como a mineração de dados e textos para fins de investigação científica. Este trabalho passa em revista as novidades trazidas pela Diretiva 2019/790 e procura alertar para alguns possíveis efeitos económicos e tecnológicas das novas regras.

1. Introdução

Em ordem a responder a desafios colocados pela evolução das tecnologias digitais o Parlamento Europeu e o Conselho aprovaram, no dia 17 de abril de 2019, a Diretiva sobre direitos de autor e direitos conexos no mercado único digital (doravante Dir. 2019/790)[1]. Esta diretiva faz parte das prioridades de modernização das regras do

* *Revista de Direito Intelectual* 2019/2. Texto de apoio à comunicação apresentada no IV Congresso de Propriedade Intelectual (APDI/Almedina) e no XIII CODAPI (GEDAI-UFPR/Unicuritiba/PUCPR).

[1] Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital (JO L 130, de 17 de maio de 2019, pp. 92-125) e que altera a Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de Março de 1996,

mercado único constantes da "Agenda Digital" da Comissão Juncker, e integra uma já longa lista de diretivas sobre direitos de autor e direitos conexos que começou em 1991 com a diretiva sobre proteção jurídica dos programas de computador, e que têm sido objeto de muitos acórdãos do Tribunal de Justiça da União Europeia em resposta a pedidos prejudiciais[1].

A criação do mercado único digital exigiu a configuração do sistema jurídico pela União Europeia em diversos aspetos, incluindo os direitos de autor, juntamente com proteção dos dados pessoais, direito das sociedades, bloqueio geográfico ou transparência das plataformas[2]. No domínio dos direitos de autor, a intervenção da União Europeia já tinha um histórico bastante significativo, pelo que a Dir. 2019/790 sobre direitos de autor no mercado único digital surge como mais uma de uma já longa série de diretivas. De resto, esta diretiva poderia ser denominada "Diretiva Infosoc 2", isto é, a segunda diretiva de adaptação dos direitos de autor aos desafios da sociedade da informação.

O acervo de direitos da UE deixava em aberto algumas questões para as quais uma resposta harmonizada foi considerada fundamental para o bom funcionamento do mercado único digital. Para começar, na sequência dos Tratados da OMPI de 1996, a Dir. 2001/29 harmonizou os direitos de reprodução, de distribuição e de comunicação ao público, incluindo a disponibilização ao público para acesso individual, mas não harmonizou as exceções ou limitações aos direitos exclusivos, salvo a exclusão do direito de reprodução de atos de reprodução temporária tecnicamente sem valor económico e necessários a uma utilização legítima. No que respeita às exceções ou limitações propriamente ditas, a Dir. 2001/29 estabeleceu uma lista de adoção opcional e facultativa, deixando aos Estados-Membros a sua escolha "a la carte", em qualquer caso subordinadas à sua conformidade com a regra dos três passos. O regime agora aprovado implica alterações à Dir. 2001/29 e à Dir. 96/9 sobre bases de dados, terminado o prazo de transposição no dia 7 de junho de 2021.

2. Visão geral da Diretiva 2019/790

A Dir. 2019/790 sobre direitos de autor e direitos conexos no mercado único digital divide-se em cinco títulos. O primeiro contém disposições gerais sobre o objeto, âmbito de aplicação e definições. O segundo estabelece exceções e limitações, obrigatórias e imperativas, no contexto digital e transfronteiriço[3], como sejam a prospeção de textos e

---

relativa à protecção jurídica das bases de dados (JO L 77, de 27 de março de 1996, pp. 20-28) e a Directiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação (JOL 167, de 22 de junho de 2001, pp. 10.19).

[1] http://copyrightblog.kluweriplaw.com/category/cjeu/.

[2] https://www.consilium.europa.eu/pt/policies/digital-single-market/.

[3] Outras exceções obrigatórias tinham já sido estabelecidas pela União Europeia, designadamente no que respeita a utilizações permitidas de obras em benefício de pessoas cegas, nos termos da Diretiva 2017/1564, do Parlamento Europeu e do Conselho, de 13 de Setembro (*JO L* 242, de 20 de setembro de 2017, pp. 6-13), transposta para o direito interno pela Lei 92/2019, de 4 de setembro, que além disso descriminaliza a execução pública não autorizada de fonogramas e videogramas editados comercialmente, alterando o Código do Direito de Autor e dos Direitos Conexos, aprovado pelo DL 63/85, de 14 de março (com várias alterações posteriores), o DL 252/94, de 20 de outubro (programas de computador), o DL 332/97, de 27 de novembro (aluguer e comodato), e ao DL n.º 122/2000, de 4 de julho (bases de dados).

dados para fins de investigação científica, a utilização em atividades pedagógicas digitais e transfronteiriças (ilustração pedagógica no ensino à distância sem fins comerciais), a conservação do património cultural (coleções das instituições responsáveis); este título prevê ainda uma exceção de prospeção de textos e dados para outros fins, ressalvando a possibilidade de essa utilização ser expressamente reservada pelos titulares de direitos.

Depois, o terceiro título regula as práticas de concessão de licenças e assegura acesso mais alargado aos conteúdos. Por um lado, é permitido o licenciamento por entidade de gestão coletiva da utilização de obras fora do circuito comercial por instituições responsáveis pelo património cultural, podendo essa utilização ser transfronteiriça e os titulares de direitos terem ou não conferido mandato para o efeito à entidade de gestão; para determinar o estatuto de "obra fora do comércio" e regular o seu licenciamento são estabelecidas medidas de publicidade e de diálogo entre as partes interessadas. Por outro lado, para facilitar o licenciamento são estabelecidas as "licenças coletivas com efeitos alargados" a titulares de direitos da mesma categoria que não tenham mandatado a entidade de gestão coletiva. Além disso, é previsto um mecanismo de negociação (organismo imparcial ou de mediadores) para facilitar o acesso a obras audiovisuais através de plataformas de vídeo a pedido e a disponibilidade das mesmas. Ainda a fim de assegurar acesso mais alargado aos conteúdos, é estabelecido que as reproduções de obras de arte visual no domínio público não são sujeitas a direitos de autor ou a direitos conexos, a menos que a reprodução seja original enquanto criação intelectual do próprio autor.

O título quarto estabelece um conjunto de medidas com vista ao "funcionamento correto do mercado dos direitos de autor". Para começar, é estabelecido um direito conexo sobre publicações de imprensa relativamente a utilizações em linha por prestadores de serviços da sociedade da informação, com a duração de 2 anos a contar da sua primeira publicação na imprensa. A utilização privada e não comercial por utilizadores individuais, as hiperligações e os termos isolados ou excertos muito curtos são excluídos deste novo direito. Além disso, ao editor (titular de direitos por transmissão ou licença) é atribuído o direito de receber uma parte da compensação equitativa, devida ao abrigo de exceções ou limitações, como a cópia privada, ou seja, o editor pode ser igualmente titular do direito à compensação equitativa pela cópia privada, como já sucede no direito português.

Relativamente às utilizações de conteúdos protegidos por serviços em linha (p.e., "Youtube"), a diretiva estabelece que a partilha de conteúdos em linha pelos utilizadores desses serviços implica atos de reprodução e de comunicação ao público e nessa medida depende de autorização do titular de direitos de autor[1]. Os serviços de partilha de conteúdos em linha não são considerados serviços de armazenamento em servidor para efeitos da limitação de responsabilidade prevista no art. 14.º/1 da diretiva

[1] Entendimento recentemente adotado pelo Tribunal de Roma, conforme notícia veiculada: http://ipkitten.blogspot.com/2019/07/rome-court-finds-videosharing-platform.html.

sobre comércio eletrónico (Dir. 2000/31)[1]. De todo o modo, ficam excluídos os utilizadores que não atuem com caráter comercial ou cuja atividade não gere receitas significativas. Além disso, os prestadores de serviços de partilha de conteúdos em linha podem afastar a sua responsabilidade por infração aos direitos de autor se provarem que envidaram todos os esforços para obter autorização e assegurar, segundo elevados padrões de diligência profissional no setor, a indisponibilidade de obras cuja identificação lhe foi fornecida pelos titulares de direitos, bem como para bloquear ou remover as obras objeto de notificação e impedir o seu futuro carregamento. Os prestadores destes serviços não ficam sujeitos a nenhuma obrigação geral de monitorização e a adoção de medidas deve ser feita em conformidade com o princípio da proporcionalidade, tendo em conta nomeadamente o tipo, público-alvo e dimensão do serviço, bem como a disponibilidade de meios adequados e eficazes e respetivo custo para os prestadores de serviços.

Todavia, para promover a concorrência com as grandes plataformas, é estabelecido um regime especial para as *start-up* PME: as plataformas surgidas na União nos últimos três anos e com volume de negócios anual inferior a 10 milhões de euros ficam isentas do dever de assegurar a indisponibilidade das obras cuja identificação lhes foi fornecida pelos titulares de direitos; mas, se tiverem em média mais de 5 milhões de visitante por mês, já são obrigadas a impedir novos carregamentos das obras identificadas e notificadas.

Além da concorrência no mercado único digital, o regime das plataformas de partilha de conteúdos pretende assegurar igualmente a liberdade de expressão, de modo que o controlo dos servidores das plataformas não torne indisponíveis obras que não violem direitos de autor, designadamente pela utilização ser autorizada ao abrigo de uma exceção ou limitação, sendo expressamente obrigatórias certas exceções no contexto destes serviços bem como a disponibilização de conteúdos gerados pelos utilizadores desses serviços, para fins de citações, crítica, análise, caricatura, paródia ou pastiche. Ou seja, o controlo das plataformas não pode traduzir-se numa "censura" de obras do domínio público (p.e., um controlo do "Index Librorum Prohibitorum"). Aliás, a Dir. 2019/790 confere um papel pedagógico às plataformas de partilha de conteúdos, obrigando-as a informar os utilizadores nas condições gerais de serviço sobre as utilizações permitidas ao abrigo de exceções ou limitações aos direitos de autor e direitos conexos[2]. O que vai exigir um esforço adicional de adaptação nacional, uma vez que não havendo harmonização completa das exceções e limitações, será necessário configurar as condições de serviço face à legislação de direitos de autor de cada Estado-Membro. Um outro dever que impende sobre as plataformas é disponibilizarem aos utilizadores das plataformas um mecanismo de reclamação e de recurso eficaz e rápido, no caso de bloqueio ou de remoção de conteúdos por si carregados[3].

---

[1] Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno (*JO L* 178, de 17 de julho de 2000, pp. 1-16).

[2] Ver, a propósito, a orientações de direitos autorais da Youtube – Creating with common sense" https://creatoracademy.youtube.com/page/lesson/copyright-guidelines.

[3] No direito interno, a Lei 36/2017, de 2 de junho, alterou o CDADC de modo a garantir o exercício dos direitos dos beneficiários das utilizações livres de obras.

A diretiva parece estabelece um mecanismo de "notice and take-down" semelhante ao da lei norte-americana "Digital Millenium Copyright Act" de 1998, mas "a duas velocidades", consoante a idade e a dimensão das plataformas. Os titulares de direitos devem justificar os seus pedidos de bloqueio ou de remoção, e as decisões dos prestadores de serviços ficam sujeitas a controlo humano, ao invés de serem tomadas automaticamente por tecnologias de reconhecimento de conteúdos[1]. Este mecanismo não prejudica outros mecanismos imparciais de resolução extrajudicial de litígios, nem o direito dos utilizadores a recursos judiciais eficazes.

Ainda para assegurar o correto funcionamento do mercado dos direitos de autor é estabelecido o direito a remuneração justa de autores e artistas intérpretes ou executantes nos contratos de exploração. Considerando os autores e os artistas intérpretes ou executantes como parte contratual mais fraca, a Dir. 2019/790 estabelece (1) o princípio da remuneração adequada e proporcionada pela licença ou transferência de direitos, (2) a obrigação de transparência a cargo dos licenciados ou transmissários (prestação anual de contas sobre os modos de exploração, receitas geradas e remuneração devida), e (3) garante aos autores e aos artistas um mecanismo de modificação contratual (um direito a remuneração adicional, adequada e justa quando a inicial se revele desproporcionadamente baixa por referência a todas as receitas geradas pela exploração da obra), suscetível de sujeição a procedimento alternativo de resolução de litígios. Para situações de não exploração da obra, é estabelecido um direito de revogação ou, em alternativa, de por termo à exclusividade, a exercer num prazo razoável após a licença ou a cessão de direitos. Do princípio da remuneração justa são excluídos os autores de programas de computador e do seu regime ficam também excluídos os artistas intérpretes ou executantes, à semelhança do que prevê a lei portuguesa quando estes atuam como trabalhadores dependentes.

3. Desenvolvimentos

Um dos objetivos principais da Diretiva 2019/790 é prevenir a distorção da concorrência no mercado interno (Considerando 1) atentos os novos "modelos empresariais" e numa perspetiva "orientada para o futuro" Considerando 3). São visados, em particular, os «prestadores de serviços de partilha de conteúdos em linha», definidos como o prestador de serviços da sociedade da informação "que tem como principal objetivo ou um dos seus principais objetivos armazenar e facilitar o acesso do público a uma quantidade significativa de obras… carregados pelos seus utilizadores, que organiza e promove com fins lucrativos". São igualmente visadas novas atividades como as dos agregadores de notícias e do tratamento de *Big Data* típica dos chamados G.A.F.A. ("Google", "Apple", "Facebook" e "Amazon"). Ao contrário de "acabar com a Internet tal como a conhecemos", a Dir. 2019/790 afirma a subsistência dos direitos de autor face a novos modelos de negócio que utilizam conteúdos digitais protegidos por direitos de autor distinguindo consoante a utilização tenha ou não fins comerciais.

[1] Resta saber como será possível assegurar o controlo sem recurso a tecnologias de reconhecimento de conteúdos, tendo em conta o volume só de vídeo carregado diariamente só no "Youtube" segundo as estatísticas oficiais divulgadas pela "Google" - https://www.youtube.com/intl/pt-PT/about/press/.

Relativamente a utilizações sem fins comerciais são introduzidas novas exceções e é prescrita a obrigatoriedade de outras já existentes. Por exemplo, nos termos do Considerando 70: "Os utilizadores deverão ter a possibilidade de carregar e disponibilizar conteúdos gerados pelos utilizadores para fins específicos de citação, crítica, caricatura, paródia ou pastiche. (…) Essas exceções ou limitações deverão, por conseguinte, ser obrigatórias".

3.1. Exceções novas ou alargadas: liberdade imperativa de prospeção de textos e dados por organismos de investigação científica (incluindo universidades e as suas bibliotecas) e instituições responsáveis pelo património cultural (arquivos, bibliotecas e centros de documentação)

A Dir. 2001/29 estabeleceu uma lista fechada e opcional de exceções ou limites aos direitos de autor. A adaptação ao digital justificou a introdução de novas exceções e o alargamento de outras já existentes. São consagradas exceções obrigatórias e imperativas, no sentido de que não podem ser afastadas por contrato nem por medidas tecnológicas de proteção (art. 7.º), nos termos da Dir. 2001/29.

São introduzidas "exceções ou limitações obrigatórias para a utilização de tecnologias de prospeção de textos e dados no domínio da investigação científica, para a ilustração didática no contexto digital e para a conservação do património cultural" (Considerando 5). Considera-se, em especial, que a "prospeção de textos e dados torna possível o tratamento de grandes quantidades de informação para obter novos conhecimentos e descobrir novas tendências", e que a normalização de dados no processo de prospeção de textos e dados implica a reprodução de obras (Considerando 8). A utilidade desta nova exceção para o desenvolvimento da inteligência artificial é apontada pela Comissão[1].

Depois, os organismos de investigação e as instituições responsáveis pelo património cultural passam a beneficiar de uma exceção aos direitos de reprodução ou de extração para realizar prospeção de textos e dados para fins de investigação científica (art. 3.º/1). Para o efeito, devem armazenar as cópias com um nível de segurança adequado, podendo conservá-las para fins de investigação científica, incluindo para a verificação dos resultados da investigação (art. 3.º/2), e podendo os titulares de direitos aplicar medidas para assegurar a segurança e a integridade das redes e bases de dados em que as obras são integradas (art. 3.º/3), p.e., através da validação de endereços de IP ou autenticação do utilizador. Segundo o preâmbulo, "não deverão ser considerados organismos de investigação para efeitos da presente diretiva, os organismos sobre as quais as empresas comerciais têm uma influência decisiva, permitindo às referidas empresas exercer controlo devido a condições estruturais, nomeadamente através da sua qualidade de acionistas ou sócios, o que poderá conduzir a um acesso preferencial aos resultados da investigação" (Considerando 12).

[1] *Inteligência artificial para a Europa*, COM (2018) 237 final, p. 11.

3.2. Exceções novas ou alargadas: liberdade (dispositiva) de prospeção de textos e dados para outros fins

A exceção geral aos direitos de reprodução e de extração para fins de prospeção de textos e dados inclui a faculdade de conservar as cópias enquanto for necessário para fins de prospeção de textos e dados (art. 4.º/1-2). A criação de uma exceção para prospeção de textos e dados parece significar que esta atividade não é uma reprodução meramente técnica de obras excluída do direito de reprodução nos termos do artigo 5.º/1 da Dir. 2001/29, exclusão que abrange, p.e., o *browsing*.

Todavia, os titulares de direitos podem reservar expressamente essa utilização, de forma adequada, nomeadamente por meio de leitura ótica tratando-se de conteúdos disponibilizados ao público em linha (art. 4.º/3). Sendo que as exceções de prospeção de textos e dados causam apenas prejuízo mínimo, por isso não dão direito a compensação (Considerando 17).

3.3. Exceções novas ou alargadas: atividades pedagógicas digitais e transfronteiriças

Em derrogação dos direitos de reprodução e de comunicação ao público, é permitida a utilização de obras em atividades pedagógicas digitais e transfronteiriças, para fins exclusivos de ilustração didática sem objetivos comerciais e desde que ocorra sob a responsabilidade de um estabelecimento de ensino, nas suas instalações ou noutros locais, ou através de um meio eletrónico seguro acessível apenas pelos alunos, estudantes e pessoal docente do estabelecimento de ensino (mediante validação de IP ou autenticação do utilizador), e seja acompanhada da indicação da fonte, incluindo o nome do autor, exceto quando tal se revele impossível. Anteriormente a jurisprudência reconhecia a estas instituições o direito de digitalizarem "as obras que fazem parte das suas coleções, se esse ato de reprodução for necessário para efeitos da colocação à disposição dos utilizadores dessas obras, através de terminais destinados a esse efeito, nas instalações desses estabelecimentos"[1].

São abrangidos todos os estabelecimentos de ensino reconhecidos nos Estados-Membros (primário, secundário, profissional e superior): "A estrutura organizativa e os meios de financiamento de um estabelecimento de ensino não deverão ser fatores decisivos para determinar o caráter não comercial da atividade" (Considerando 20). Considera-se ainda que: "Na maior parte dos casos, o conceito de ilustração implicará, por conseguinte, a utilização apenas de parte ou de excertos de obras, o que não deverá substituir a compra de materiais essencialmente destinados aos mercados do ensino" (Considerando 21). Ou seja, a exceção permitirá apenas, em princípio, a utilização de partes ou de excertos de obras (p.e., capítulos de livros ou artigos de revista), mas não obras completas[2].

[1] Acórdão TJUE, de 11 de setembro de 2014, proc. C-117/13 (*Eugen Ulmer*). Os acórdãos do TJUE citados neste texto estão disponíveis para consulta em http://curia.europa.eu/juris/recherche.jsf

[2] No direito interno, o regime de utilização de dispositivos digitais de uso pessoal nas bibliotecas e arquivos públicos, aprovado pela Lei n.º 31/2019, de 3 de maio, que permite a fotografia digital dos documentos, embora sujeite os dispositivos a registo obrigatório e estabeleça que "as imagens e reproduções digitais que resultam da recolha e investigação do leitor são exclusivamente utilizadas para uso privado, excluindo-se qualquer outra forma de utilização de obras, nomeadamente a sua

Esta exceção fica sujeita ao princípio do país de origem, no sentido de que a utilização de obras para fins exclusivos de ilustração didática através de meios eletrónicos seguros ocorre exclusivamente no Estado-Membro onde o estabelecimento de ensino se encontra estabelecido (artigo 5.º/3) [1]. Por exemplo, um estudante Erasmus de Coimbra poderá aceder no seu país de residência habitual aos materiais de apoio disponibilizados pelo docente na plataforma Inforestudante, considerando-se que a utilização é feita no país de origem do estabelecimento, ou seja, em Portugal.

Além disso, os Estados-Membros podem prever uma compensação equitativa para os titulares de direitos por esta utilização das suas obras (art. 5.º/4). Ou seja, o sistema da compensação equitativa pela reprodução para uso privado e outros fins permitidos por lei pode ser alargado para abranger esta nova forma de utilização permitida.

Determinados tipos ou utilizações de obras, como o material que se destina principalmente ao mercado do ensino ou partituras musicais, na medida em que as licenças adequadas estejam facilmente disponíveis no mercado, podem ser excluídos desta exceção para fins de ensino à distância (art. 5.º/1-2).

3.4. Exceções novas ou alargadas: conservação do património cultural

As instituições responsáveis pelo património cultural beneficiam de uma exceção ao direito de reprodução destinada a permitir, quando necessária, a conservação do património cultural, isto é, as obras e outros materiais que façam permanentemente parte das suas coleções, em qualquer formato ou suporte (art. 6.º). A previsão desta exceção permite às instituições de conservação do património cultural reproduzir as obras em novos formatos tendo em conta as mudanças permanentes nas tecnologias.

3.5. Obras fora do circuito comercial: gestão coletiva com efeitos alargados ou licença legal

Além da reprodução para conservação, as instituições responsáveis pelo património cultural podem utilizar, para fins não comerciais, "obras fora do circuito comercial", obtendo licença não exclusiva junto de entidade de gestão coletiva, "independentemente do facto de todos os titulares de direitos abrangidos pela licença terem ou não conferido um mandato à entidade de gestão coletiva", a qual deverá todavia ser suficientemente representativa, com base em mandatos, dos titulares de direitos no tipo de obras que são objeto da licença, e tratar de igual modo todos os titulares de direitos em relação às condições da licença (gestão coletiva com efeitos alargados – art. 7.º/1).

Não havendo entidade de gestão coletiva que satisfaça esses requisitos, as instituições responsáveis pelo património cultural podem ainda assim disponibilizar

---

disponibilização pública ou comercialização", sem prejuízo das utilizações livres previstas no CDADC (art. 6.º).

[1] O princípio do país de origem é também consagrado pela Diretiva (UE) 2019/789 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, sobre o exercício dos direitos de autor e direitos conexos aplicáveis a determinadas transmissões em linha dos organismos de radiodifusão ("serviços acessórios em linha") e à retransmissão de programas de televisão e de rádio (*JO L* 130, de 17 de maio de 2019, pp. 82-91) e que altera a Directiva 93/83/CEE do Conselho, de 27 de Setembro de 1993, relativa à coordenação de determinadas disposições em matéria de direito de autor e direitos conexos aplicáveis à radiodifusão por satélite e à retransmissão por cabo (*JO L* 248, de 6 de outubro de 1993, pp. 15-21).

essas "obras fora do comércio" em sítios Internet não comerciais, devendo indicar o nome do autor ou de qualquer outro titular de direito que possa ser identificado, a não ser que essa indicação seja impossível (art. 7.º/2-3). Aos titulares de direitos é reconhecido um direito de retirada, que lhes permita, "a qualquer momento e de forma fácil e eficaz, excluir as suas obras ou outro material" das licenças alargadas ou da exceção referida (art. 7.º/4)[1].

Existe obra fora do circuito comercial "quando se possa presumir de boa-fé que a obra ou outro material protegido na sua totalidade não estão acessíveis ao público através dos canais habituais de comércio depois de se efetuar um esforço razoável para determinar a sua disponibilidade ao público", podendo para o efeito os Estados-Membros fixar requisitos específicos, como uma data-limite, que não excedam o necessário e razoável nem excluam a possibilidade de determinar que um conjunto de obras ou outro material protegido na sua globalidade está fora do circuito comercial, quando for razoável presumir que todas as obras ou outro material protegido estão fora do circuito comercial (art. 7.º/5-6). Considera-se que: "A disponibilidade limitada de uma obra (…), como a sua disponibilidade em lojas de segunda mão, (…) não deverá ser considerada como estando disponível ao público nos canais habituais do comércio" (Considerando 38)[2].

As licenças atrás referidas abrangem utilizações transfronteiriças (art. 9.º/1), as quais ocorrem exclusivamente no Estado-Membro onde está estabelecida a instituição responsável pelo património cultural que procede a essa utilização (art. 9.º/2). As informações sobre as partes incluídas na licença, os territórios abrangidos e as utilizações devem ser disponibilizados de forma permanente, fácil e eficaz num portal público em linha único a partir de, pelo menos, seis meses antes de as obras ou outro material protegido serem utilizados, sendo o referido portal criado e gerido pelo Instituto da Propriedade Intelectual da União Europeia, nos termos do Regulamento (UE) 386/2012[3] (art. 10.º/1). Cabe aos Estados-Membros adotar medidas de diálogo entre as partes interessadas (titulares de direitos, entidades de gestão coletiva e instituições responsáveis pelo património cultural) em cada setor antes de estabelecerem requisitos específicos, e encorajar um diálogo periódico entre organizações representativas de utilizadores e de titulares de direitos, incluindo entidades de gestão coletiva, bem como quaisquer outras organizações interessadas, para promover, numa

[1] O regime das obras fora do comércio acresce ao das chamadas obras órfãs estabelecido pela Diretiva 2012/28/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativa a determinadas utilizações permitidas de obras órfãs (*JO L* 299, de 27 de outubro de 2002, pp. 5-12).

[2] Os conjuntos de obras fora do circuito comercial são excluídos se consistirem predominantemente em (a) obras, exceto obras cinematográficas ou audiovisuais, publicadas pela primeira vez ou, na falta de publicação, difundidas pela primeira vez num país terceiro; (b) obras cinematográficas ou audiovisuais cujos produtores tenham a sua sede ou residência habitual num país terceiro; ou (c) obras de nacionais de países terceiros, caso, após um esforço razoável, não tenha sido possível determinar o Estado-Membro ou país terceiro.

[3] Regulamento (UE) n.º 386/2012 do Parlamento Europeu e do Conselho, de 19 de abril de 2012, que atribui ao Instituto de Harmonização no Mercado Interno (Marcas, Desenhos e Modelos) funções relacionadas com a defesa dos direitos de propriedade intelectual, nomeadamente a de reunir representantes dos setores público e privado num Observatório Europeu das Infrações aos Direitos de Propriedade Intelectual (*JO L* 129, de 16 de maio de 2012, pp. 1-6).

base setorial, a pertinência e a possibilidade de utilização das licenças com efeitos alargados e para assegurar a eficácia das garantias dos titulares de direitos (art. 11.º/1).

3.6. Gestão coletiva com efeitos alargados (mandato legal ou presunção de autorização de gestão de negócios)

Em ordem a facilitar a concessão de licenças coletivas são ainda estabelecidas outras medidas, como sejam permitir que a entidade de gestão coletiva alargue o acordo de licença aos titulares de direitos que não tenham autorizado essa entidade de gestão coletiva a representá-los por transmissão, licença ou qualquer outra disposição contratual, ou que disponha de um mandato legal ou se presuma que representa titulares de direitos que não lhe tenham dado autorização nesse sentido (art. 12.º/1). Todavia, estas licenças coletivas com efeitos alargados só devem ser aplicadas em "zonas de utilização bem definidas", onde a obtenção de autorizações de titulares de direitos numa base individual seja de um modo geral onerosa e impraticável a ponto de tornar improvável a operação necessária para obter uma licença, devido à natureza da utilização ou dos tipos de obras em causa, e devem salvaguardar os interesses legítimos dos titulares de direitos (art. 12.º/2). Além disso, as entidades de gestão coletiva devem ter suficiente representatividade (número de mandatos), assegurar igualdade de tratamento e adotar medidas de publicidade adequadas e eficazes, e os titulares de direitos têm direito de retirada.

3.7. Organismo imparcial ou mediadores para as plataformas de vídeo a pedido

Para promover o acesso a obras audiovisuais através de plataformas de vídeo a pedido e a disponibilidade das mesmas é obrigatório (à semelhança da retransmissão por cabo) existir um mecanismo de negociação através de um organismo imparcial ou de mediadores, os quais devem também prestar assistência às partes nas suas negociações e ajudá-las a chegar a acordo, nomeadamente apresentando-lhes propostas (art. 13.º).

3.8. Utilização livre de imagens de obras de arte visual no domínio público

A reprodução de obras de arte visual no domínio público não está sujeita a direitos de autor ou direitos conexos, a menos que seja original, enquanto criação intelectual do próprio autor (art. 14.º). Assim, as fotografias de pinturas, esculturas ou monumentos no domínio público não são protegidas por direis de autor. Face a esta norma, pode falar-se num princípio de liberdade de utilização e de partilha dessas fotografias na Internet, cabendo ao eventual autor provar que satisfazem os requisitos de proteção. Segundo o Considerando 16 e o art. 6.º da Dir. 2006/116[1]: "Uma obra fotográfica, na aceção da Convenção de Berna, deve ser considerada original sempre que for criação intelectual própria do respetivo autor, refletindo a sua personalidade, sem que outros critérios, tais como o mérito ou a finalidade, sejam tomados em consideração".

[1] Directiva 2006/116/CE do Parlamento Europeu e do Conselho, de 12 de Dezembro de 2006, relativa ao prazo de protecção do direito de autor e de certos direitos conexos (versão codificada) – *JO L* 372, de 27 de dezembro de 2006, pp.12-18.

3.9. Funcionamento correto do mercado dos direitos de autor

Apesar de a Diretiva se intitular "direitos de autor no mercado único digital", só no título III surgem medidas para "criar um mercado dos direitos de autor que funcione corretamente": direitos dos editores, plataformas de partilha de conteúdos e contratos autorais.

3.9.1. Direito conexo do editor de imprensa e direito do editor a compensação equitativa pela utilização livre. As publicações de imprensa são protegidas relativamente a utilizações em linha por parte de serviços da sociedade da informação como agregadores de notícias e recortes de imprensa ou *media clipping* (art. 15.º). Este novo direito responde ao facto de que "A vasta disponibilidade de publicações de imprensa em linha deu origem à emergência de novos serviços em linha, como os agregadores de notícias ou os serviços de monitorização dos meios de comunicação social, para os quais a reutilização de publicações de imprensa constitui uma parte significativa dos seus modelos de negócios e uma fonte de receitas" (Considerando 54).

Este direito dos editores não se aplica à utilização privada e não comercial por utilizadores individuais, às hiperligações, a termos isolados ou de excertos muito curtos de publicações de imprensa e, de modo geral, às publicações científicas. Além disso, este direito não prejudica a utilização de obras no domínio público nem os direitos dos autores de obras incluídas nessas publicações e a respetiva exploração independente, tendo aliás direito a uma parte adequada das receitas dos editores de imprensa relativas à utilização das suas publicações pelos prestadores de serviços da sociedade da informação. Tem a duração de dois anos contados a partir de 1 de janeiro do ano seguinte à data das publicações de imprensa efetuadas a partir de 6 de junho de 2019.

Em consequência desta norma, os agregadores de notícias praticamente limitam-se a colocar uma hiperligação para a fonte da notícia juntamente com breves excertos. Saber quão breve deve ser o excerto é matéria que cumpre ainda clarificar, sendo que as revistas de imprensa não são protegidas pelos direitos de autor nos termos do CDADC.

Por outro lado, os editores podem ser por lei titulares do direito a uma parte da compensação equitativa por utilização ao abrigo de uma exceção (p.e., cópia privada), como efeito de transferência ou licença de direitos (art. 16.º). Esta norma tem por base um entendimento da jurisprudência que recusava essa possibilidade[1].

3.9.2. Responsabilidade das plataformas de partilha de conteúdos que exploram comercialmente os conteúdos carregados pelos seus utilizadores. A oferta ao público de acesso a obras e outros materiais carregados pelos utilizadores de serviços de partilha de conteúdos em linha é expressamente considerada uma utilização (comunicação ao público ou colocação à disponibilização do público) sujeita a autorização dos respetivos titulares de direitos (art. 17.º/1). A autorização abrange não apenas a oferta, mas também os atos praticados pelos utilizadores dos serviços se não agirem com caráter comercial ou se a sua atividade não gerar receitas significativas (art. 17.º/2). Sendo que,

[1] Acórdão TJUE, de 12 de novembro de 2015, proc. C-572/13 (*Hewlett-Packard*).

o princípio é o de que "os titulares de direitos não deverão ser obrigados a conceder uma autorização ou a celebrar acordos de concessão de licenças" (Considerando 61). Ou seja, os titulares de direitos são soberanos para autorizar ou não a utilização das suas obras nas novas plataformas de partilha de conteúdos. Sendo que, enquanto atividade sujeita a autorização, exclui-se da limitação da responsabilidade prevista para os prestadores de serviços da sociedade da informação nos termos do art. 14.º/1 da Dir. 2000/31/CE (art. 17.º/3)[1].

Na ausência de autorização, os prestadores de serviços de partilha de conteúdos em linha respondem por infração aos direitos de autor, a menos que provem que se esforçaram seriamente ou diligentemente para obter autorização, para não disponibilizar obras identificadas pelos titulares de direitos ou para bloquear ou remover obras objeto de notificação pelos titulares de direitos e para impedir o seu futuro carregamento (art. 17.º/4). O cumprimento destas obrigações é aferido à luz do princípio da proporcionalidade (consagrado em vários acórdãos pelo TJUE), tendo em conta, designadamente, o tipo, o público-alvo e a dimensão do serviço e o tipo de conteúdos carregados pelos utilizadores do serviço, e a disponibilidade de meios adequados e eficazes, bem como o respetivo custo para os prestadores de serviços (art. 17.º/5). Com efeito, as tecnologias de controlo de conteúdos (filtragem e apagamento) podem ser pouco eficazes e/ou muito dispendiosas, sendo necessário caso a caso apreciar a sua onerosidade de modo a salvaguardar a liberdade de empresa[2].

Por esta razão e de modo a prevenir a eliminação das *start-up* concorrentes, as pequenas e médias empresas novas setor (que atuam há menos de três anos e com volume de negócios anual inferior a 10 milhões de euros), têm que provar apenas que se esforçaram seriamente ou diligentemente para obter autorização e, após recebimento de uma notificação, para bloquear o acesso ao ou remover o conteúdo protegido dos seus sítios Internet; mas, se ultrapassarem os 5 milhões de visitantes individuais, já têm que provar que se esforçaram seriamente para prevenir futuros carregamentos de obras objeto de notificação adequada por parte dos titulares de direitos (art. 17.º/6). A nosso ver, se o objetivo era dar uma oportunidade às novas PME digitais, a verdade é que o limite de 5 milhões de visitantes por mês é facilmente superado e, por isso, na prática esta diretiva tem o efeito de criar um mercado para as tecnologias de reconhecimento de conteúdos (software "ID content") que já é dominado pelas empresas que supostamente seriam as principais visadas pelo novo regime. Além de terem que obter autorizações e pagar direitos de autor, as PME terão ainda que pagar estas tecnologias, cujo mercado já é dominado pelos gigantes da internet.

O controlo dos conteúdos carregados pelos utilizadores não deve impedir utilizações de obras já caídas no domínio público ou utilizações de conteúdos gerados por utilizadores em serviços de partilha de conteúdos em linha para fins de citações, crítica, análise, ou para efeitos de caricatura, paródia ou pastiche (os famosos memes)[3].

---

[1] Na jurisprudência, a propósito de marcas, acórdão TJUE, de 12 de julho de 2011, proc. C-324/09 (*L'Oreal c eBay*), parag. 124.

[2] Ver o acórdão TJUE, de 24 de novembro de 2011, proc. C-70/10 (*Scarlet Extended*).

[3] Sobre a liberdade de paródia ver o acórdão TJUE, de 3 de setembro de 2014, proc. C-201/13 (*Deckmyn e Vrijheidsfonds*). Invertendo uma jurisprudência favorável a interpretação das exceções às luz

Além disso, os prestadores de serviços de partilha de conteúdos em linha devem criar um mecanismo de reclamação e de recurso eficaz e rápido para os utilizadores dos seus serviços em caso de litígio sobre o bloqueio do acesso a obras que carreguem ou que sejam removidas (*notice and take-down*). Os titulares de direitos devem justificar devidamente os seus pedidos de bloqueio ou de remoção de conteúdos e as queixas formuladas ao abrigo do mecanismo de aviso e retirada devem ser processadas sem "demora injustificada" e as decisões de bloqueio ou de remoção "são sujeitas a controlo humano".

Este mecanismo de autorregulação não prejudica a disponibilidade de mecanismos de resolução extrajudicial de litígios, os quais por seu turno também não prejudicam o direito dos utilizadores a recursos judiciais eficazes, nomeadamente mediante acesso a um tribunal ou a outro órgão jurisdicional pertinente para reivindicar a utilização de uma exceção ou limitação, cabendo aliás aos prestadores de serviços de partilha de conteúdos em linha informar os seus utilizadores, nas suas condições gerais, da possibilidade de utilizarem obras ao abrigo de exceções ou limitações aos direitos de autor e direitos conexos previstas no direito da União. A Comissão promoverá o diálogo entre as partes interessadas e emitirá orientações sobre as melhores práticas, tendo em conta igualmente os direitos fundamentais e a utilização de exceções e limitações (art. 17.º/9).

3.9.3. A proteção dos autores como "parte contratual mais fraca" nas relações com os editores, produtores, radiodifusores e outros intermediários. A fim de garantir a *remuneração justa* de autores e artistas intérpretes ou executantes nos contratos de exploração, é estabelecido o princípio da remuneração adequada e proporcionada (art. 18/1), cabendo a cada Estado-Membro a definição do mecanismo remuneratório, que deve respeitar o princípio da liberdade contratual e do equilíbrio justo de direitos e interesses (art. 18.º/2). Esta medida destina-se a proteger a "posição contratual mais fraca" (Considerando 72) e regula a relação entre os autores e artistas nas relações com os editores, produtores, radiodifusores e outros intermediários. O Código do Direito de Autor e dos Direitos Conexos prevê já o direito a remuneração a favor dos autores no caso, p.e., de serem extraídas "vantagens não incluídas nem previstas na fixação da remuneração ajustada" nas obras criadas no âmbito de contrato de trabalho ou de contrato de encomenda (art. 14.º/4-b), o direito a compensação suplementar no caso de

---

do balanço dos direitos fundamentais segundo o princípio da proporcionalidade, o TJUE adotou recentemente dois acórdãos que apontam no sentido da interpretação restritiva das exceções, não admitindo sequer a criação de novas exceções para além das previstas na Dir. 2001/29 e em outras, mesmo que justificadas à luz dos direitos fundamentais constitucionalmente protegidos: acórdãos TJUE, de 29/7/2019, procs. C-469/17 (*Funke Medien*), C-476/17 (*Pelham*), e C-516/17 (*Spiegel Online*), (a liberdade de informação e a liberdade de imprensa não justificam derrogações aos direitos exclusivos harmonizados pela Dir. 2001/29 além das previstas aí; *numerus clausus* das exceções aos direitos do produtor fonográfico; o conceito de «citações» exige a possibilidade de identificação da obra em questão através da citação em causa e "abrange o reenvio, através de uma hiperligação, para um ficheiro consultável de forma autónoma"). De todo o modo, o TJUE ressalva expressamente que a interpretação das exceções, embora deva respeitar a sua redação e preservar o seu efeito útil, deverá também ser "plenamente conforme com os direitos fundamentais garantidos pela Carta dos Direitos Fundamentais da União Europeia".

o criador intelectual ou os seus sucessores ter transmitido onerosamente o seu direito de exploração e de sofrer uma "grave lesão patrimonial por manifesta desproporção entre os seus proventos e os lucros auferidos pelo" transmissário (art. 49.º/1). De igual modo, sendo obrigação do editor produzir e vender exemplares da obra (arts. 83.º e 90.º), o não cumprimento justificará a resolução do contrato (art. 106). Sendo que o regime da edição se aplica, supletivamente, a outros contratos de direitos de autor (arts. 147.º, 156.º, 172.º).

Por outro lado, é consagrada uma *obrigação de transparência*, proporcionada e eficaz, nos termos da qual "os autores e artistas intérpretes ou executantes recebem, regularmente — pelo menos, uma vez por ano — e tendo em conta as especificidades de cada setor, informações atualizadas, pertinentes e exaustivas sobre a exploração das suas obras e prestações por parte daqueles a quem foram concedidas licenças ou transferidos os seus direitos, bem como dos seus sucessores legais, nomeadamente no que diz respeito aos modos de exploração, a todas as receitas geradas e à remuneração devida" (art. 19.º/1). A obrigação de transparência exigirá, igualmente, um investimento considerável em software de gestão de direitos, reforçando a importância das empresas de *software* no mercado digital.

A obrigação de transparência confere ainda o direito de pedir "informação adicional dos subtitulares da licença se a sua primeira contraparte contratual não dispuser de todas as informações que seriam necessárias", devendo a primeira contraparte contratual identificar os subtitulares da licença (art. 19.º/2). A obrigação de transparência pode ser limitada se os encargos administrativos decorrentes da obrigação de transparência forem desproporcionados face às receitas provenientes da exploração (art. 19.º/3) e até excluída relativamente a contribuições insignificantes, tendo em conta o conjunto das obras ou prestações (art. 19.º/4, ressalvando a necessidade dessas informações para o exercício do direito a remuneração adicional). Sem prejuízo dos acordos de negociação coletiva, as referidas regras de transparência não podem ser derrogadas por esses acordos (art. 19.º/5). As entidades de gestão coletiva sem fins lucrativos devem prestar aos titulares de direitos as informações previstas no artigo 18.º da Dir. 2014/26/UE sobre gestão coletiva[1].

É ainda estabelecido um mecanismo de modificação contratual nos termos do qual, na falta de acordos de negociação coletiva com efeito semelhante, "os autores e artistas intérpretes ou executantes ou respetivos representantes têm o direito de reclamar uma remuneração adicional, adequada e justa à parte com quem celebraram um contrato de exploração dos seus direitos, ou aos sucessores legais dessa parte, sempre que a remuneração inicialmente acordada se revele desproporcionadamente baixa relativamente a todas as receitas pertinentes subsequentes decorrentes da exploração das obras ou prestações" (art.20/1). Este direito a remuneração adicional não se aplica aos acordos celebrados por entidades de gestão coletiva abrangidas pela Diretiva 2014/26/UE (art. 20.º/2).

[1] Diretiva 2014/26/EU do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à gestão coletiva dos direitos de autor e direitos conexos e à concessão de licenças multiterritoriais de direitos sobre obras musicais (*JO L* 84, de 20 de março de 2014, pp. 72-98).

Para efetivar a obrigação de transparência e o direito a remuneração adicional é obrigatória a existência de um procedimento alternativo e voluntário de resolução de litígios, que deverá poder ser iniciado por organizações representativas "a pedido expresso de um ou mais autores ou artistas intérpretes ou executantes" (art. 21.º). Esta norma reforça o papel dos mecanismos alternativos de resolução de litígios.

Igualmente importante é o direito de revogação consagrado no art. 22.º/1, nos termos do qual o autor ou artista intérprete ou executante pode revogar, total ou parcialmente, a licença ou a transferência de direitos, em caso de falta de exploração da obra ou prestação. O direito de revogação pode ser regulado especificamente por setor ou tipo de obra, e tendo em conta a "importância relativa das contribuições individuais e os interesses legítimos de todos os autores ou artistas intérpretes ou executantes afetados pela aplicação do mecanismo de revogação por parte de um único autor ou artista intérprete ou executante" (art. 22.º/2). O direito de revogação pode, aliás, ser excluído relativamente a obras que contenham "normalmente contribuições de vários autores ou artistas intérpretes ou executantes", valer apenas num prazo específico e até pode ser substituído, a nível nacional, pelo direito de terminar a exclusividade do contrato (art. 22.º/1-2). Aliás, o direito de terminar a exclusividade parece ser garantido no caso de a licença ou a transferência não ser revogada num período de tempo razoável após a celebração do contrato (art. 22.º/3). O direito de revogação não pode ser objecto de renúncia salvo por acordo de negociação coletiva (art. 22.º/5).

São ineficazes, relativamente aos autores e aos artistas intérpretes ou executantes, as cláusulas contratuais contrárias à obrigação de transparência, ao direito a remuneração adicional e ao direito de revogação (ou cessação da exclusividade). Este reforço da proteção dos autores nos contratos autorais não se aplica aos autores de programas de computador, que igualmente não beneficiam do princípio da remuneração adequada e proporcionada (art. 23.º).

4. Conclusão

A criação e o bom funcionamento de um mercado único digital justificaram a adoção de um pacote de diretivas, incluindo a Dir. 2019/790 sobre direitos de autor e direitos conexos, que procura modernizar o acervo da União Europeia neste domínio alterando nomeadamente a Dir. 2001/29 sobre direitos autorais na sociedade da informação e a Dir. 96/9 sobre bases de dados.

Por um lado, é revisto o regime das exceções e limitações estabelecendo a obrigatoriedade e imperatividade de exceções já existentes, como as relativas às bibliotecas, ao ensino à distância e à conservação do património cultural, cujo âmbito é alargado, e é introduzida uma exceção nova de prospeção de textos e dados para fins de investigação científica ou, sujeita a reserva expressa pelo titular de direitos, para outros fins (uma espécie de direito a ficar fora do Google ou de não ser "googlado"). No campo da utilização livre destaca-se ainda a exclusão dos direitos de autor nas fotografias de obras do domínio público, bem como a exceção de crítica, análise ou paródia relativamente à disponibilização as plataformas de partilha de conteúdos gerados pelos utilizadores.

Por outro lado, é reforçado o papel da gestão coletiva no que respeita à gestão dos direitos de autor de obras fora do comércio, que podem até ser utilizadas para fins de conservação do património pelas entidades responsáveis mesmo se não for possível obter licença junto da gestão coletiva. De igual modo, torna-se obrigatória a existência de organismos de mediação relativamente ao licenciamento de conteúdos para os serviços de vídeo em linha.

Um dos pontos mais críticos nos trabalhos preparatórios foi a criação de um direito conexo a favor dos editores de imprensa relativamente a utilizações feitas por novos serviços como os agregadores de notícias e os recortes de imprensa ("media clipping"), o qual todavia conhece exceções, como as hiperligações, e tem a duração de 2 anos. Os operadores têm procurado evitar o pagamento deste "link tax" reduzindo a utilização dos conteúdos a hiperligações e excertos muito curtos, o que de resto é o objetivo visado de modo a não privar a publicação fonte dos acessos por parte dos interessados (sendo que a receita publicitária dos editores de imprensa varia em função dos acessos às suas páginas).

Quanto ao famoso «value gap», a Dir. 2019/790 esclarece que as plataformas de partilha com fins comerciais devem obter autorização dos autores dos conteúdos carregados pelos utilizadores dos seus serviços, sendo os autores livres de não disponibilizar as suas obras nessas plataformas, sejam de acesso livre ou de acesso condicional. Assim, os provedores destes novos serviços, que monetizam os conteúdos (p.e., associando-lhes publicidade e desse modo obtendo receitas, registando-se uma migração em massa do investimento publicitário dos media tradicionais para estas novas plataformas), são excluídos do "porto seguro" estabelecido no art. 14.º da diretiva do comércio eletrónico no que respeita à responsabilidade dos provedores de serviços de alojamento de conteúdos.

Todavia, os fornecedores de plataformas podem excluir a sua responsabilidade provando que atuaram diligentemente no sentido de obter autorizações e impedir o carregamento ilícito de conteúdos bem como para bloquear ou remover conteúdos ilícitos e prevenir o seu novo carregamento, cabendo aos titulares de direitos identificar as suas obras junto das plataformas. Na prática, as plataformas terão que controlar os conteúdos que disponibilizam. Ressalva-se que as medidas de controlo não podem ser excessivamente onerosas e devem ser feitas segundo o princípio da proporcionalidade. Sendo à partida exoneradas do dever de controlo prévio as novas PME, embora alcançando os 5 milhões de visitantes mensais já deverão prevenir o carregamento ilícito de conteúdos. Por outro lado, a responsabilidade das plataformas não se aplica a vários prestadores de serviços sem fins comerciais, como enciclopédias em linha (wikipédia), mercados em linha, plataformas de software de fonte aberta, serviços de computação em nuvem para uso privado. Sendo que, de igual modo, o controlo não deve impedir utilizações de obras já caídas no domínio público ou utilizações de conteúdos gerados por utilizadores em serviços de partilha de conteúdos em linha para fins de citações, crítica, análise, ou para efeitos de caricatura, paródia ou pastiche (os famosos memes). Resta saber, na prática, como funcionarão as exceções, uma vez que não é certo que os algoritmos tenham sentido de humor nem sejam tão inteligentes

como seria desejável[1]. Um outro aspeto inovador da Dir. 2019/790 é, a nível da União Europeia, a consagração do princípio do direito à remuneração justa e adequada dos autores e a consagração do direito à revisão contratual para obter remuneração suplementar no caso de a exploração da sua obra gerar receitas extraordinárias ou para cancelar contratos (ou a exclusividade) no caso de não exploração da obra. Consagra-se, assim, a proteção do autor como "parte contratual mais fraca" nas relações com os editores, produtores, radiodifusores e outros intermediários.

O balanço geral da diretiva parece-nos positivo, restando saber como funcionará na prática o complexo sistema de controlo dos conteúdos nas plataformas de partilha, sobretudo ao nível das utilizações livres que se pretendem salvaguardar. A este respeito, seria interessante ponderar a introdução de uma cláusula geral de «fair use» ao estilo norte-americano, de modo a permitir o controlo judicial do exercício concreto das exceções ou até a consagração de novas utilizações livres, tanto mais que a recente jurisprudência do TJUE tende a enclausurar a utilização livre nas exceções e limitações já legalmente tipificadas. Ou, ao invés de uma cláusula de «fair use», seria interessante, tal como sugerido por RETO HILTY subordinar o exercício das exceções ao teste do balanço económico, à semelhança do direito da concorrência, perguntando o que é mais eficiente para o sistema a médio e longo prazo, se conteúdos novos que geram consumo e estimulam a inovação tecnológica ou conteúdos que surgem como uma espécie de dos direitos autorais "walking dead". De igual modo, não é inteiramente claro porque razão são apenas obrigatórias as exceções previstas na Dir. 2019/790, ao passo que as restantes previstas na Dir. 2001/29 continuam facultativas e opcionais, mantendo-se a fragmentação nacional das exceções e com isso a complexidade das regras de direitos de autor.

Finalmente, um ponto que a diretiva não tratou diz respeito ao esgotamento digital. Pese embora o modelo de negócio das plataformas de vídeos a pedido e de partilha de conteúdos funcionar sobretudo em termos de *streaming* (com sujeição ao princípio do país de origem), isso não prejudica o modelo alternativo da compra de exemplares digitais para livre utilização, independente de ligação à rede e de um serviço associado, e o interesse na possibilidade de revenda desses exemplares, permitida pelo esgotamento do direito de distribuição, à semelhança do regime dos programas de computador[2]. Recentemente, o advogado-geral manifestou-se pelo não esgotamento *de iure condito* face à Dir. 2001/29[3], mas deixando a questão em aberto *de lege ferenda*. Matéria, certamente, para mais uma diretiva ou até, quem sabe, para um regulamento geral de direitos de autor e direitos conexos na União Europeia, à semelhança do sucedido em matéria de dados pessoais.

---

[1] Recorde-se o famoso bloqueio da estatueta da Vénus pelo Facebook enquanto conteúdo impróprio (*nude*).

[2] Acórdão TJUE, de 3 de julho de 2012, proc. C-128/11 (*UsedSoft*).

[3] Nas conclusões apresentadas, em 10 de setembro de 2019, no proc. C-263/18 (*Nederlands Uitgeversverbond*), apesar de "concluir que existem argumentos jurídicos e teleológicos a favor do reconhecimento da regra do esgotamento do direito de distribuição no que diz respeito às obras fornecidas por transferência (*download*) para uma utilização permanente", o Advogado-Geral Maciej Szpunar entende que, "no estado atual do direito da União […] o fornecimento de livros eletrónicos por transferência (*download*) para utilização permanente não se enquadra no direito de distribuição […] mas do direito de comunicação ao público".

COMUNICAÇÃO AO PÚBLICO: UM "GRANDE DIREITO" NA JURISPRUDÊNCIA DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA?*

A comunicação ao público como tipo aberto de modos de exploração económica de obras literárias ou artísticas

Sucedendo historicamente aos privilégios de impressão, os direitos de autor formaram-se em torno do conceito de cópia ou reprodução, radicando ainda hoje nessa matriz a designação do sistema anglo-americano de *Copyright*. Todavia, já no século XVIII se afirmou o direito de representação pública de obras literárias ou artísticas, independentemente de reprodução. À representação das obras em salões e salas de espetáculos, típica dos concertos musicais, do teatro, da ópera ou do bailado, juntaram-se posteriormente outras formas de comunicação pública tornadas possíveis pelas novas tecnologias da comunicação, como a rádio, o cinema ou a televisão, culminando mais recentemente com a disponibilização pública em redes informáticas.

O Tratado da OMPI sobre Direito de Autor de dezembro de 1996 (TODA) integrou o direito de disponibilização em linha no direito de comunicação ao público (art. 8º). Idêntica abordagem foi adotada pela Diretiva 2001/29/CE, definindo o direito exclusivo de comunicação ao público em sentido amplo, de modo a abranger "Qualquer comunicação ao público das suas obras, por fio ou sem fio, incluindo a sua colocação à disposição do público por forma a torná-las acessíveis a qualquer pessoa a partir do local e no momento por ela escolhido" (art. 3º/1).

Por seu turno, o Tratado da OMPI sobre Execuções e Fonogramas (TOEF) autonomizou um direito de colocação à disposição do público a favor dos artistas intérpretes ou executantes (art. 10º) e dos produtores de fonogramas (art. 14º), ao invés de o integrar num grande direito de comunicação ao público. Ao passo que a Diretiva 2001/29 consagrou também esse novo direito a favor de artistas intérpretes ou executantes, produtores audiovisuais, organismos de radiodifusão, no art. 3º/2 sob epígrafe "Direito de comunicação de obras ao público, incluindo o direito de colocar à sua disposição outro material", definindo-o como "a colocação à disposição do público, por fio ou sem fio, por forma a ser acessível a qualquer pessoa a partir do local e no momento por ela escolhido".

Em Portugal, o Código do Direito de Autor e dos Direitos Conexos (CDADC), aprovado em 1985 e alterado várias vezes, não consagra expressamente um direito geral de comunicação ao público, embora estabeleça a comunicação ao público como uma das grandes modalidades de utilização que integram o direito exclusivo do autor.[1] O Código prevê diversas formas de comunicação ao público como modos de utilização das obras (artigo 68º/2), para as quais estabelece regimes especiais, como sejam a representação cénica (art. 107º), a recitação e execução (artigo 121º), a radiodifusão sonora ou visual da obra, direta ou por retransmissão (artigo 149º), a comunicação da

---

* *Revista Julgar* 38 (2019) 193-202. Conferência proferida nas Primeiras Jornadas do Tribunal de Propriedade Intelectual realizadas em Lisboa no dia 27 de abril de 2018, com o apoio do Instituto Nacional da Propriedade Industrial (INPI).

[1] *Vide* Ferrer Correia, Almeno de Sá, «Direito de autor e comunicação pública de emissões de rádio e televisão», BFD 70 (1994), p. 1-96.

obra em qualquer lugar público, por qualquer meio que sirva para difundir sinais, sons ou imagens (artigo 149º), a comunicação pública de obra radiodifundida (artigo 155º), e o espetáculo baseado em comunicação ao público de obra radiodifundida (artigo 156º).

A disponibilização pública em rede não foi inicialmente prevista no catálogo de exemplos de modos de utilização de obras que ilustram o direito exclusivo, embora pudesse ser aí abrangida face à abertura do direito de utilização a modos que de futuro viessem a ser conhecidos (art. 68/1). Só mais tarde, em 2004, na sequência do TODA e da Diretiva 2001/29, o CDADC passou a prever expressamente a disponibilização em rede na internet como modo de utilização abrangido pelo direito exclusivo, definindo-o como: "A colocação à disposição do público, por fio ou sem fio, da obra por forma a torná-la acessível a qualquer pessoa a partir do local e no momento por ela escolhido" (art. 68º/2-j). O CDADC não incluiu expressamente este novo modo de utilização no direito de comunicação ao público porque, desde logo, ao contrário de outros ordenamentos jurídicos, não tipifica como "grandes direitos" de utilização a reprodução, a distribuição, a comunicação pública e a adaptação. Pelo contrário, o CDADC prevê uma lista "quase empírica"[1] de modos de utilização.

Não obstante, a disponibilização pública em rede releva sobretudo, em termos de enquadramento sistemático, como uma nova forma de comunicação ao público[2], segundo a jurisprudência do Tribunal de Justiça da União Europeia (TJUE) relativa ao direito de comunicação ao público consagrado no art. 3°/1 da Diretiva 2001/29/CE, tendo em conta o respetivo preâmbulo.

O direito de comunicação ao público na jurisprudência do TJUE

Para o TJUE, a comunicação ao público é um conceito amplo, tendencialmente uniforme, e marcado pela neutralidade tecnológica, no sentido de abranger tanto os media tradicionais como os novos media. Pressupõe um ato deliberado por parte do utilizador, diferente do mero intermediário técnico que apenas assegura ou melhora a radiodifusão ou a receção das obras pelo público já visado pela comunicação original. Além disso, esse ato deve dirigir-se a um "público novo", enquanto número indeterminado, mas significativo de destinatários potenciais não visados pela utilização inicialmente autorizada. O ato deve ainda, em princípio, ser praticado com "intuito lucrativo", direto ou indireto, isto é, a comunicação deve conferir uma vantagem competitiva ou valor acrescentado à atividade principal do sujeito que a pratica.

Segundo o TJUE, cumprem estes requisitos a disponibilização de televisores em quartos de hotel (*Rafael Hoteles*)[3], pubs (*Football Association Premier League*)[1],

[1] J. Oliveira ASCENSÃO, *Direito de autor e direitos conexos,* Coimbra Editora, 1992, p. 225.

[2] Sobre o enquadramento sistemático desta nova forma de utilização, com mais indicações, ver os nossos *Informática, Direito de Autor e Propriedade Tecnodigital* (Coimbra Editora, 2001) e *Direitos de Autor e Liberdade de Informação* (Almedina, 2008). Para uma resenha da evolução da tutela dos direitos autorais face aos desafios digitais, ver também J.P. Remédio MARQUES, "A tutela dos direitos de autor à luz da Era digital no ordenamento jurídico português – com um olhar para o direito da União Europeia", *BFD* 93/2 (2017) 651-691.

[3] Acórdão de 7 de dezembro de 2006, proc. C-306/05, ECLI:EU:C:2006:764. Antes da Dir. 2001/29, o TJUE considerou, no acórdão *Egeda*, que a Diretiva 93/83/CEE não regulava a captação num estabelecimento hoteleiro de sinais de televisão por satélite ou por via terrestre e a sua distribuição por

estabelecimento de SPA estética e relax (OSA)[2], e centros de reabilitação (*Reha Training*)[3].

A este respeito, cumpre assinalar que o Supremo Tribunal de Justiça (STJ) divergiu parcialmente do TJUE ao decidir que "A aplicação, a um televisor, de aparelhos de ampliação do som, difundido por canal de televisão, em estabelecimento comercial, não configura uma nova utilização da obra transmitida, pelo que o seu uso não carece de autorização do autor da mesma, não integrando consequentemente essa prática o crime de usurpação, p. e p. pelos arts. 149.º, 195.º e 197.º do Código do Direito de Autor e dos Direitos Conexos".[4]

Para o STJ, a aplicação de amplificadores de som num televisor disponível num bar ou restaurante não constitui, só por si, uma nova utilização da obra radiodifundida e por isso não integra o conceito de comunicação ao público constante do CDADC. Sendo a aplicação de amplificadores irrelevante, parece que, por maioria de razão, a mera disponibilização dos televisores em cafés, snack-bares ou restaurantes também seria excluída da noção de comunicação pública, segundo o STJ.

Impõe-se, todavia, uma interpretação restritiva do sumário do acórdão no sentido de se referir apenas a restaurantes ou snack-bares, já que na fundamentação o STJ concorda com o TJUE no sentido de que o direito de comunicação ao público de obra radiodifundida é aplicável à instalação de aparelhos de televisão em quartos de hotel.[5] Por outro lado, o acórdão do STJ não terá logrado o objetivo de uniformizar a jurisprudência interna, já que o Tribunal da Relação de Lisboa tem seguido antes a jurisprudência do TJUE.[6]

A noção de comunicação ao público releva igualmente em sede radiodifusão por satélite e retransmissão por cabo. A Diretiva 93/83/CEE regulou aspetos de direito de autor e direitos conexos neste domínio, prevendo no art. 2º o direito de comunicação ao público por satélite, que o TJUE interpretou no sentido de abranger a radiodifusão e a comunicação a um novo público por satélite em pacotes televisivos com acesso livre ou condicionado (*Airfield and Canal Digitaal*).[7] Por outro lado, num acórdão em que afirmou que o direito de comunicação ao público abrange a retransmissão de obras radiodifundidas por *live streaming*, o TJUE considerou irrelevante a prossecução de um escopo lucrativo (*ITV Broadcasting*).[8] Essencial parece ser apenas aqui a utilização da

---

cabo aos seus diferentes quartos, devendo por isso a questão ser apreciada de acordo com o direito nacional - acórdão de 3 de fevereiro de 2000, proc. C-293/98, ECLI:EU:C:2000:66.

[1] Acórdão de 4 de outubro de 2011, proc. C-403/08, ECLI:EU:C:2011:631

[2] Acórdão de 27 de fevereiro de 2014, proc. C-351/12, ECLI:EU:C:2014:110.

[3] Acórdão de 31 de maio de 2016, proc. C-117/15, ECLI:EU:C:2016:379.

[4] Acórdão n.º 15/2013 de uniformização de jurisprudência, D.R. n.º 243, Série I de 2013-12-16.

[5] O acórdão merece-nos outras reservas, nomeadamente por desconsiderar a autonomia normativa da comunicação ao público de obra radiodifundida nos termos do art. 155º CDADC, pese embora ter o mérito de excluir o ato do crime de usurpação. Alexandre L Dias PEREIRA, «Direitos de autor e comunicação pública de obra radiodifundida em estabelecimento comercial (Anotação ao Acórdão de Uniformização de Jurisprudência do S.T.J. n.º 15/2013. De 13 de novembro)», *Revista de Legislação e de Jurisprudência*, Ano 144º, Nº 3990 (jan./fev. 2015), p. 215-244.

[6] Ver, por ex., o acórdão de 16 de maio de 2017, proc. no. 197/14.2YHLSB.L1-7 <www.dgsi.pt>

[7] Acórdão de 13 de outubro de 2011, proc. apensos C-431/09 e C-432/09, ECLI:EU:C:2011:648.

[8] Acórdão de 7 de março de 2013, proc. C-607/11, ECLI:EU:C:2013:147 : o direito de comunicação ao público abrange (i) uma retransmissão das obras incluídas numa radiodifusão televisiva terrestre que

obra através de um novo modo de comunicação, em termos de constituir um público novo. Neste sentido, o TJUE decidiu que "um organismo de radiodifusão não procede a um ato de comunicação ao público[…] quando transmite os seus sinais portadores de programas exclusivamente aos distribuidores de sinais, sem que esses sinais estejam acessíveis ao público durante ou por causa dessa transmissão, sendo os distribuidores que em seguida enviam os referidos sinais aos seus assinantes para que estes possam visualizar esses programas, exceto se a intervenção dos distribuidores em causa constituir apenas um simples meio técnico" (*SBS Belgium*).[1]

Os direitos conexos dos produtores de fonogramas e dos organismos de radiodifusão

O conceito de comunicação ao público deveria, em princípio, ter idêntico significado em sede de direitos de autor e de direitos conexos. Todavia, o regime legal dos direitos de autor não corresponde integralmente ao dos direitos conexos e, por isso, a noção de comunicação ao público não tem um significado uniforme nos direitos de autor e nos direitos conexos.

Assim, para efeitos do direito a remuneração equitativa e única estabelecido a favor dos artistas intérpretes e executantes no art. 8°/2 da Diretiva 92/100 pela utilização de fonogramas publicados com fins comerciais "em qualquer tipo de comunicações ao público", o TJUE decidiu que este conceito "não cobre a difusão gratuita de fonogramas num consultório de dentista […] no âmbito do exercício de uma profissão liberal, em benefício da clientela, que dela frui independentemente da sua vontade" (SCF).[2]

Por outro lado, relativamente aos direitos conexos dos organismos de radiodifusão, a Diretiva 2006/115 (que substitui a Dir. 92/100), prevê o direito exclusivo de permitir ou proibir a comunicação ao público das suas emissões, "se essa comunicação for realizada em locais abertos ao público com entrada paga." Por força deste condicionalismo e para efeitos dessa norma - a que corresponde internamente o art. 187º/1-e) do CDADC -, o TJUE concluiu que a transmissão de emissões de televisão e de rádio através de aparelhos de televisão instalados nos quartos de um hotel não constitui uma comunicação realizada num local aberto ao público com entrada paga (*Verwertungsgesellschaft).*[3] Ou seja, o que em sede de direitos de autor constitui uma comunicação ao público já nos direitos conexos dos artistas intérpretes e executantes e dos organismos de radiodifusão não é um ato abrangido por essa noção.

De todo o modo, articulando a noção de comunicação ao público do art. 8º/3 da Diretiva 2016/115 com o art. 3º/2 da Diretiva 2001/29, o TJUE concluiu no acórdão *C More Entertainment* que esta última disposição "não se opõe a uma legislação nacional

(ii) é efetuada por uma entidade que não seja o radiodifusor de origem, (iii) através de um fluxo Internet colocado à disposição dos subscritores dessa entidade que podem receber essa transmissão acedendo ao seu servidor; (iv) ainda que esses subscritores se encontrem na zona de receção da referida radiodifusão televisiva terrestre e a possam receber legalmente num recetor de televisão; independentemente de a retransmissão ser financiada pela publicidade e revestir assim um caráter lucrativo, (v) e de ser efetuada por uma entidade que se encontra em concorrência direta com o radiodifusor de origem.

[1] Acórdão de 19 de novembro de 2015, proc. C-325/14, ECLI:EU:C:2015:764

[2] Acórdão de 15 de março de 2012, proc. C-135/10, ECLI:EU:C:2012:140 (*Marco del Corso*)

[3] Acórdão de 16 de fevereiro de 2017, proc. C-641/15, ECLI:EU:C:2017:131.

que alarga o direito exclusivo dos organismos de radiodifusão […] a atos de comunicação ao público que possam constituir transmissões de encontros desportivos realizadas em direto através da Internet, […] desde que tal alargamento não afete a proteção do direito de autor."[1] Ou seja, o art. 8º/3 da Diretiva 2016/115 não harmonizou completamente o direito de comunicação ao público dos organismos de radiodifusão, não prejudicando, por isso, a atribuição, a nível nacional, de um direito mais amplo, abrangendo a prática, "nomeadamente, de emissões a que qualquer pessoa pode ter acesso a partir do local por ela escolhido" (*C More Entertainment*, para. 35).

Hiperligações, *peer-to-peer* e computação em nuvem

As novas tecnologias da Internet tornaram possíveis novos modos de utilização de obras literárias ou artísticas. Todavia, as leis não preveem expressamente realidades como as hiperligações, as plataformas de partilha peer-to-peer e a computação em nuvem como novos modos de utilização de obras ou prestações protegidas por direitos de autor ou direitos conexos.

A problemática das hiperligações chegou ao TJUE para saber se constituem comunicação ao público da obra hiperligada. Inicialmente o TJUE respondeu negativamente, tratando-se do "fornecimento, num sítio Internet, de hiperligações para obras livremente disponíveis noutro sítio Internet" (*Svensson*)[2], sendo que o art. 3º/1 da Diretiva 2001/29 fixara harmonização máxima do conceito de comunicação ao público no sentido de não poder incluir "mais operações do que as abrangidas por essa disposição" (*ibidem*). Este entendimento foi reiterado no despacho *BestWater International*[3], a propósito de hiperligação segundo a técnica do "framing" (vídeo no "YouTube"), na medida em que a obra em questão não seria transmitida para um novo público nem comunicada através de um modo técnico específico diferente do da comunicação original.

Além disso, uma hiperligação para obra disponibilizada ilicitamente num sítio Internet não seria uma comunicação ao público se não tivesse fins lucrativos por uma pessoa que não conhecia ou não podia razoavelmente conhecer a ilicitude da disponibilização da obra. Todavia, sendo a hiperligação feita com fins lucrativos, já existiria comunicação ao público, devendo nesse caso presumir-se o conhecimento da ilicitude por parte do autor da hiperligação (*GS Media*).[4] A semelhante entendimento chegou o TJUE relativamente:

- "à venda de um leitor multimédia[…] no qual foram pré-instaladas aplicações complementares, disponíveis na Internet, contendo hiperligações que remetem para sítios Internet, livremente acessíveis ao público, nos quais foram colocadas à disposição do público obras protegidas por direitos de autor sem autorização dos titulares desses direitos" (*Stichting Brein*)[5];

[1] Acórdão de 26 de março de 2015, proc. C-279/13, ECLI:EU:C:2015:199.
[2] Acórdão de 13 de fevereiro de 2014, proc. C-466/12, ECLI:EU:C:2014:76.
[3] Acórdão de 21 de outubro de 2014, proc. C-348/13, ECLI:EU:C:2014:2315.
[4] Acórdão de 8 de dezembro de 2016, proc. C-160/15, ECLI:EU:C:2016:644 ("Playboy").
[5] Acórdão de 26 de abril de 2017, proc. C-527/15, ECLI:EU:C:2017:300.

- à "colocação à disposição e a gestão, na Internet, de uma plataforma de partilha que, através da indexação de metainformação relativa a obras protegidas e da disponibilização de um motor de busca, permite aos utilizadores dessa plataforma localizar essas obras e partilhá-las no âmbito de uma rede descentralizada (peer-to-peer)" (*Stichting Brein II*)[1];

- ao fornecimento a particulares por uma empresa comercial de um serviço de gravação à distância, na nuvem, de cópias privadas de obras protegidas pelo direito de autor, através de um sistema informático, intervindo a empresa ativamente no ato de gravação dessas cópias, sem o consentimento do titular dos direitos (*VCAST*).[2]

Mais recentemente, contra um alegado princípio de que a partilha de obra na Internet faz presumir o consentimento para a sua republicação, o Tribunal de Justiça no acórdão *Renckhoff*, concluiu que a noção de comunicação ao público do artigo 3º/1 da Dir. 2001/29 "abrange a publicação numa página da Internet de uma fotografia previamente publicada, sem restrições que impeçam que seja descarregada e com a autorização do titular do direito de autor, noutra página da Internet".[3]

Atos não abrangidos pela noção de comunicação ao público

A noção de comunicação ao público tem revelado assinalável elasticidade hermenêutica, em especial para incluir modos de disponibilização pública em rede para acesso a partir do local e do momento individualmente escolhidos. Todavia, nem tudo será abrangido por este "grande direito".

Desde logo, no direito interno, é ressalvada a liberdade de comunicação privada, isto é, a comunicação "sem fim lucrativo e em privado, em meio familiar" (art. 108º/2 do CDADC). Por outro lado, segundo o TJEU, o direito de comunicação ao público não abrange as "cópias no ecrã de um computador do utilizador e as cópias na memória de armazenamento temporária (memória «cache») do disco rígido desse computador, efetuadas por um utilizador final durante a consulta de um sítio Internet, por serem cópias temporárias, transitórias ou episódicas e constituírem parte integrante e essencial de um processo tecnológico" (*Public Relations Consultants Association).*[4] Nas referidas condições, acrescenta o TJUE, as cópias em ecrã e em memória cache do computador do utilizador podem sem realizadas sem autorização dos titulares de direitos de autor.

Não obstante – *et pour cause* -, não é certo que estas reproduções em cache possam ser licitamente realizadas independentemente da licitude da fonte. Com efeito, o TJUE decidiu que, para efeitos da compensação equitativa, a reprodução para uso privado, ao abrigo do art. 5º/2-b) da Diretiva 2001/29, em conjugação com o teste dos três passos consagrado no seu número 5, não é licita *per se*, antes depende da licitude ou ilicitude da fonte a partir da qual é efetuada (*ACI Adam*).[5] Fonte ilícita essa que pode resultar, como decidido no acórdão "The Pirate Bay", da colocação à disposição e da gestão, na Internet, de uma plataforma de partilha que, através da indexação de metainformação

[1] Acórdão de 14 de junho de 2017, proc. C-610/15, ECLI:EU:C:2017:456 ("The Pirate Bay").
[2] Acórdão de 29 de novembro de 2017, proc. C-265/16, ECLI:EU:C:2017:913.
[3] Acórdão de 7 de agosto de 2018, proc. C-161/17, ECLI:EU:C:2018:634
[4] Acórdão de 5 de junho de 2014, proc. C-360/13, ECLI:EU:C:2014:1195.
[5] Acórdão de 10 de abril de 2014, proc. C-435/12, ECLI:EU:C:2014:254.

relativa a obras protegidas e da disponibilização de um motor de busca, permite aos utilizadores dessa plataforma localizar essas obras e partilha-las obras no âmbito de uma rede descentralizada (peer-to-peer) (*Stichting Brein II*).[1] Com efeito, a partilha de obras no âmbito de uma rede descentralizada (*peer-to-peer*) cai fora da liberdade de uso privado mesmo que não tenha fins lucrativos, uma vez que não é efetuada "em meio familiar", recordando a fórmula do art. 108º/2 do CDADC.

Além disso, o TJUE decidiu também que "os atos de reprodução temporária, através de um leitor multimédia […], de uma obra protegida por direitos de autor, obtida através de *streaming* num sítio Internet pertencente a um terceiro que disponibiliza essa obra sem autorização do titular dos direitos de autor, não preenchem os requisitos previstos" nas referidas disposições do art. 5°/1-5 da Diretiva 2001/29, que excluem da noção de reprodução as cópias temporárias, transitórias ou episódicas que constituam apenas parte integrante e essencial de um processo tecnológico (*Stichting Brein I*).[2]

Por outro lado, o TJUE excluiu da noção de comunicação ao público a revenda de uma licença de utilização que envolva a revenda de uma cópia de um programa de computador descarregado a partir do sítio Internet do titular do direito de autor; licença inicialmente concedida ao primeiro adquirente pelo referido titular do direito sem limite de duração e através do pagamento de um preço destinado a permitir a este último obter uma remuneração correspondente ao valor económico da referida cópia da sua obra (*UsedSoft)*.[3] Neste caso tratava-se da qualificação da comercialização de licenças de programas de computador em segunda mão descarregados a partir da Internet para efeitos da Diretiva 2009/24/CE sobre proteção jurídica de programas de computador. O direito aplicável não seria aqui o direito de comunicação ao público, mas antes o direito de distribuição, sendo o adquirente considerado adquirente legítimo para efeitos do esgotamento desse direito.

Conclusão

O direito de comunicação ao público tem revelado elasticidade hermenêutica suficiente para abranger novos modos de utilização de obras em rede. É questionável se o TJUE não estará a interpretar *praeter legem* a noção de comunicação ao público segundo ditames marcadamente funcionais, de modo a salvaguardar os interesses dos titulares de direitos de autor face a novas formas de exploração das obras em rede (e.g. *live streaming*, hiperligações, *peer-to-peer*). Afirma-se a prática de comunicação ao público nas hiperligações quando visam fins lucrativos, presumindo-se até nesse caso o conhecimento, por parte do autor, da ilicitude da disponibilização em rede da obra hiperligada. Já em matéria de *live streaming* não se exige a prossecução de fins lucrativos, e considera-se que a comunicação simultânea através de um canal diferente (*streaming*) é igualmente comunicação ao público apesar de tornar a obra acessível ao mesmo público. Além disso, a interpretação da noção de comunicação ao público não é uniforme nos direitos de autor e nos direitos conexos, face à diferença de regimes legais.

[1] Acórdão de 14 de junho de 2017, proc. C-610/15, ECLI:EU:C:2017:456 ("The Pirate Bay").
[2] Acórdão de 26 de abril de 2017, proc. C-527/15, ECLI:EU:C:2017:300 ("Filmspeler).
[3] Acórdão de 3 de julho de 2012, proc. C-128/11, ECLI:EU:C:2012:407.

Pese embora a abrangência do grande direito de comunicação ao público, o TJUE salvaguarda a liberdade de uso privado, embora não nos pareça irrelevante – até por razões de coerência sistemática – a licitude da fonte para aferir a licitude da cópia privada. Daí que o uso privado não justifique, só por si, a licitude de redes descentralizadas de partilhas de ficheiros (*peer-to-peer*), como mostra o acórdão "The Pirate Bay", nem a venda de dispositivos multimédia com hiperligações instaladas pelo vendedor para obras ilicitamente disponibilizadas, como decidido no acórdão "Filmspeler". Aliás, a ilicitude da fonte é critério de preenchimento do conceito de comunicação ao público relativamente a hiperligações com fins lucrativos para fotografias ilicitamente disponibilizadas num sítio Internet, justificando o seu intuito lucrativo a presunção de conhecimento da ilicitude da fonte ("Playboy").

Todas estas questões colocadas por novos modelos de negócio surgidos com a Internet somam-se às questões já clássicas dos media tradicionais, como a da comunicação ao público de obras radiodifundidas. Assinala-se, neste particular, uma divergência na jurisprudência, no sentido de o TJUE integrar no conceito de comunicação ao público atos que o STJ considera estarem isentos de direitos de autor. É o caso da comunicação ao público em cafés e restaurantes de obras radiodifundidas. Se o entendimento do STJ deve ser louvado por excluir esses atos da relevância penal em direitos de autor, também nos parece, todavia, estarem em causa direitos de remuneração a favor dos autores; e que idêntico entendimento deve valer tanto para cafés e restaurantes como para quartos de hotel e seus semelhantes.

Tendo em conta a jurisprudência do TJUE, a proposta de diretiva sobre direitos de autor no mercado único digital afirma que "os prestadores de serviços da sociedade da informação conservam e facultam ao público acesso a obras ou outro material protegido por direitos de autor carregados pelos utilizadores, excedendo assim a mera disponibilização de instalações físicas e executando um ato de comunicação ao público", pelo que nesses casos devem "ser obrigados a celebrar acordos de licenciamento com os titulares de direitos, a menos que sejam elegíveis para a isenção de responsabilidade prevista no artigo 14.º da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho", consoante desempenhem ou não "um papel ativo, incluindo através da otimização da apresentação das obras ou materiais carregados ou da sua promoção, independentemente da natureza dos meios utilizados para esse efeito" (considerando 38 e art. 13 sobre o chamado "Value Gap"). Sendo que, mesmo que se conclua estarem isentos de responsabilidade e nessa medida não serem obrigados a celebrarem acordos de licenciamento, devem ainda assim aplicar "tecnologias eficazes" de proteção de obras ou outro material protegido (*ibidem*). Isto apesar de o TJUE ter decidido que os prestadores de serviços da sociedade da informação não podem, em princípio, ser obrigados a instalar "filtros" de direitos de autor.[1] O que, se para uns

[1] Acórdãos do Tribunal de Justiça de 24 de novembro de 2011, proc. C-70/10 - Scarlet Extended, ECLI:EU:C:2011:771, de 16 de fevereiro de 2012, proc. C-360/10, ECLI:EU:C:2012:85 (*Netlog*), de 27 de março de 2014, proc. C-314/12 - UPC Telekabel Wien, ECLI:EU:C:2014:192, e de 15 de setembro de 2016, C-484/14 - Mc Fadden, ECLI:EU:C:2016:689.

apenas vem clarificar o acervo comunitário[1], para outros será uma porta aberta à legalização da censura privada através de tecnologias de reconhecimento e bloqueio de conteúdos.[2] Seria, no fundo, a instauração da anunciada "propriedade tecno-digital" em gestação há pelo menos duas décadas.[3]

Jurisprudência citada

Acórdão de 7 de dezembro de 2006, proc. C-306/05, ECLI:EU:C:2006

Acórdão de 3 de fevereiro de 2000, proc. C-293/98, ECLI:EU:C:2000:66

Acórdão de 4 de outubro de 2011, proc. C-403/08, ECLI:EU:C:2011:631

Acórdão de 27 de fevereiro de 2014, proc. C-351/12, ECLI:EU:C:2014:110

Acórdão de 31 de maio de 2016, proc. C-117/15, ECLI:EU:C:2016:379

Acórdão do STJ n.º 15/2013 de uniformização de jurisprudência, DR 243-I 2013-12-16.

Acórdão do Tribunal da Relação de Lisboa de 16 de maio de 2017, proc. no. 197/14.2YHLSB.L1-7

Acórdão de 13 de outubro de 2011, proc. apensos C-431/09 e C-432/09, ECLI:EU:C:2011:648

Acórdão de 7 de março de 2013, proc. C-607/11, ECLI:EU:C:2013:147

Acórdão de 19 de novembro de 2015, proc. C-325/14, ECLI:EU:C:2015:764

Acórdão de 15 de março de 2012, proc. C-135/10, ECLI:EU:C:2012:140 (*Marco del Corso*)

Acórdão de 16 de fevereiro de 2017, proc. C-641/15, ECLI:EU:C:2017:131

Acórdão de 26 de março de 2015, proc. C-279/13, ECLI:EU:C:2015:199

Acórdão de 13 de fevereiro de 2014, proc. C-466/12, ECLI:EU:C:2014:76

Acórdão de 21 de outubro de 2014, proc. C-348/13, ECLI:EU:C:2014:2315

Acórdão de 8 de dezembro de 2016, proc. C-160/15, ECLI:EU:C:2016:644 ("Playboy")

Acórdão de 26 de abril de 2017, proc. C-527/15, ECLI:EU:C:2017:300

Acórdão de 14 de junho de 2017, proc. C-610/15, ECLI:EU:C:2017:456 ("The Pirate Bay").

Acórdão de 29 de novembro de 2017, proc. C-265/16, ECLI:EU:C:2017:913

Acórdão de 7 de agosto de 2018, proc. C-161/17, ECLI:EU:C:2018:63

Acórdão de 5 de junho de 2014, proc. C-360/13, ECLI:EU:C:2014:1195

Acórdão de 10 de abril de 2014, proc. C-435/12, ECLI:EU:C:2014:254

Acórdão de 26 de abril de 2017, proc. C-527/15, ECLI:EU:C:2017:300 ("Filmspeler).

Acórdão de 3 de julho de 2012, proc. C-128/11, ECLI:EU:C:2012:407.

Acórdão de 24 de novembro de 2011, proc. C-70/10, ECLI:EU:C:2011:771 (*Scarlet Extended*)

Acórdão de 16 de fevereiro de 2012, proc. C-360/10, ECLI:EU:C:2012:85 (*Netlog*)

Acórdão de 27 de março de 2014, proc. C-314/12, ECLI:EU:C:2014:192 (Telekabel Wien)

Acórdão de 15 de setembro de 2016, C-484/14, ECLI:EU:C:2016:689 (Mc Fadden).

---

[1] Silke von LEWINSKI, *Comments on the 'value gap' provisions in the European Commission's Proposal for a Directive on Copyright in the Digital Single Market (Article 13 and Recital 38)*, http://copyrightblog.kluweriplaw.com/2017/04/10 ("the proposed Recital 38 merely clarifies the acquis communautaire").

[2] Ver por ex. <https://edri.org/eu-copyright-directive-privatised-censorship-and-filtering-of-free-speech/>, <https://juliareda.eu/eu-copyright-reform/>

[3] Ver o nosso *Informática, direito de autor e propriedade tecnodigital* (Coimbra Editora, 2001).

A PROTEÇÃO JURÍDICA DO SOFTWARE EXECUTADO POR ROBOTS (E OBRAS GERADAS POR I.A.) *

Introdução

O robot é, basicamente, um autómato ou dispositivo automático, cujas funcionalidade, mobilidade e capacidade de comunicação e aprendizagem variam consoante os modelos. O significado da palavra abrange desde o brinquedo *cão-robot* ao robot *Sofia* apresentado na Cimeira Web de Lisboa, passando ainda pelos autómatos da produção industrial, em especial nos setores automóvel, eletrónico ou têxtil.

Os robots executam instruções programadas na forma de software, i.e., o programa de computador ou programa informático. Significa o conjunto de instruções que compõem uma tarefa a ser executada por um dispositivo informático, nomeadamente um PC ou um *smartphone*. O programa desenvolve algoritmos através de um código-fonte, escrito em linguagem de programação (Fortran, Basic, Cobol, Pascal, C++, Java, Python, etc.) e depois convertido em código-objeto ou arquivo executável (em linguagem binária de máquina). Existem vários tipos de software, desde o *firmware*, que é o software embutido na máquina (por ex. ROM, BIOS), aos sistemas operativos (iOS, Android, Windows, Linux) e as aplicações (Office, antivírus, navegadores, jogos). Em sentido amplo, o software abrange ainda os algoritmos e a documentação do suporte lógico (descrição do programa e manual de instruções), bem como as bases de dados ou informação lato senso que processa (*dataware*).

No campo da robótica, o software é, portanto, o centro de operações ou comandos do robot, e o grau de "inteligência" do robot depende do software que executa. O robot é, muitas vezes, feito à imagem e semelhança do seu criador humano, tanto na aparência física como no comportamento e na comunicação. Todavia, nem todos os robots têm *rosto humano*. Compare-se, por exemplo, o androide astro-mecânico *R2-D2* com o *C-3PO*, este último um androide de protocolo, com formas mais próximas dos humanos, e que se apresenta nos seguintes termos: "Eu sou C-3PO, ciborgue de relações humanas e fluente em 6 milhões de línguas e falas de comunicações diferentes."

Estes personagens do épico filme de ficção científica *Star Wars - Guerra das Estrelas*, de George Lucas, são seres mecânicos (por oposição a biológicos) dotados de inteligência. Inteligência esta que evoluirá não apenas em termos comunicacionais e comportamentais, mas também em termos fisionómicos, com os *Transformers* da *Hasbro*, robots alienígenas que são capazes de transformar os seus corpos em outros objetos tais como veículos automóveis. Seres prediletos do reino da ficção, muitos deles não são sequer criação humana, antes provêm de mundos ainda por descobrir e ameaçam até a sobrevivência da espécie humana…

Detenhamo-nos nos robots gerados por humanos e cada vez mais providos de inteligência artificial (IA), ainda que não necessariamente com forma humana.[1] A IA é

* Comunicação apresentada no Congresso "Robótica e Direito", organizado pelo grupo Contrato e Desenvolvimento Social do Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra no dia 17 de novembro de 2017.

um ramo da ciência informática que procura métodos ou dispositivos computacionais capazes de emular a capacidade racional do ser humano de resolver problemas, pensar ou, de um modo geral, atuar de modo inteligente. É o que sucede com o *Watson* da IBM, com aplicações relevantes no setor de saúde e no setor jurídico, bem como nos sistemas de gestão de água, energia ou trânsito. Fala-se até na substituição do *Dr. Google* pelo *Dr. Watson*: não apenas localiza a informação como a processa em termos semelhantes ao pensamento humano nos mais variados setores, nomeadamente na saúde, podendo ser instalado num *smartphone* e ficar à distância de um clique, à semelhança do que já hoje sucede em tantos outros domínios e que ainda num passado não muito distante dificilmente passariam de algo mais do que ficção científica do tipo *Guerra das Estrelas*.

Os desafios jurídicos colocados pelos avanços tecnológicos fazem-se sentir em vários domínios, do civil ao laboral, passando pelo administrativo e fiscal, nomeadamente com o desenvolvimento do chamado "governo eletrónico". O Parlamento Europeu aprovou uma Resolução, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica. Define princípios gerais, nomeadamente um sobre propriedade intelectual sustentando que "não existem disposições legais especificamente aplicáveis à robótica, mas que os regimes e as doutrinas jurídicas existentes podem ser rapidamente aplicados à robótica, embora alguns aspetos pareçam requerer uma ponderação específica;" por isso, "insta a Comissão a apoiar uma abordagem horizontal e neutra do ponto de vista tecnológico da propriedade intelectual aplicável aos diversos setores onde a robótica poderá ser aplicada".[2]

Proteção jurídica do software executado pelo robot

Neste contexto, uma primeira questão que se coloca é a da proteção jurídica do software executado pelo robot, i.e., saber se o software do robot pode e deve ser protegido, e, em caso afirmativo, em que termos.

O software do robot, enquanto programa de computador, não apenas pode como é protegido ao abrigo da propriedade intelectual. A questão foi suscitada há mais de meio

[1] Segundo a Comunicação da Comissão Europeia sobre *Inteligência artificial para a Europa* [Bruxelas, 25.4.2018 COM(2018) 237 final, p. 1]: "*O conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos.* / *Os sistemas baseados em inteligência artificial podem ser puramente confinados ao* software*, atuando no mundo virtual (por exemplo, assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso), ou podem ser integrados em dispositivos físicos (por exemplo, robôs avançados, automóveis autónomos, veículos aéreos não tripulados ou aplicações da Internet das coisas).*"

[2] Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de *Direito Civil sobre Robótica*, para. 18.

século, tendo sido objeto de animada discussão e de inúmeros estudos[1], ao ponto de um autor exclamar: "Not another one!"[2]

Confrontaram-se várias teses. Uns defenderam que o software, pela sua natureza, deveria ser protegido como invenção técnica pelo direito das patentes, ao passo que outros pugnaram pela tutela do programa de computador ao abrigo dos direitos de autor. Uma terceira via consistiria em atribuir uma proteção dita *sui generis*, um misto de patente e de direitos de autor, sendo certo que, em qualquer caso, poder-se-ia sempre recorrer à proteção dos segredos comerciais ou saber-fazer tecnológico.

Todavia, em 1973 a Convenção de Munique sobre a Patente Europeia excluiu os programas de computador, enquanto tais, do objeto de patente. Depois, em 1980, os EUA adotaram o "Software Copyright Act"[3] e, em 1985, praticamente todos os países do G7 aprovaram legislação no mesmo sentido. A então CEE consagrou igualmente a solução direitos de autor, e o mesmo sucedeu posteriormente nos instrumentos internacionais da propriedade intelectual, como sejam o Acordo ADPIC de 1994 (OMC) e os Tratados de dezembro de 1996 da OMPI.[4]

Os direitos de autor no software

Na UE, a então CEE aprovou a Dir. 91/250 do Conselho, de 14 de maio de 1991, relativa à proteção jurídica dos programas de computador, posteriormente substituída pela Dir. 2009/24/CE. A diretiva foi transposta para o nosso direito interno pelo Decreto-Lei n.º 252/94, de 20 de outubro, consagrando a doutrina dos direitos de autor "anómalos". Ao invés de alterar o CDADC, o legislador nacional optou pela elaboração de um diploma próprio, cuja interpretação nem sempre é simples.

Em síntese, são protegidos os programas de computador que, na sua forma de expressão – incluindo o respetivo material preliminar de conceção (por ex. diagramas) - tenham caráter criativo (art. 1º/2), i.e., quando constituam criações intelectuais. Todavia, os direitos de autor não protegem os princípios nem os algoritmos implementados no programa, nem a respetiva funcionalidade (art. 1/2 CDADC), mas apenas a forma pela qual são apresentados, nomeadamente em código-fonte.

Os direitos de autor pertencem em princípio ao respetivo criador intelectual. Todavia, podem ser cedidos a terceiro por contrato e a lei atribui-os ao comitente, ao empregador ou à empresa quando são criados, respetivamente, por encomenda, por trabalhador no âmbito do contrato de trabalho, ou no âmbito de uma empresa (presumindo-os neste caso obra coletiva - art. 3º DL 252/94 e art. 19º CDADC).

Os direitos morais do criador de programas de computador parecem reduzidos ao direito de paternidade, assistindo-lhe apenas reivindicar a autoria do programa e a sua

[1] Dedicámos ao tema boa parte da nossa dissertação de mestrado *Informática, direito de autor e propriedade tecnodigital*, Coimbra Editora, 2001.

[2] G. Dworkin "Copyrights, Patents and/or 'Sui Generis': What Regime Best Suits Computer Programs", in H. Hansen (ed.), *International Intellectual Property Law and Policy*, I, London, 1996, p. 165.

[3] Cf. Arthur Miller, Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU? *Harvard Law Review* 106/5 (1993), p. 985 ss.

[4] *Vide* José Alberto Vieira, *A proteção jurídica do programa de computador pelo direito de autor*, Lisboa, 2005.

identificação na obra (art. 9º). O direito à integridade e genuinidade da obra é afastado dos direitos morais, ao excluir-se expressamente a aplicação do nº 2 do artigo 15º do CDADC (art. 3º/5), nos termos do qual "A faculdade de introduzir modificações na obra depende do acordo expresso do seu criador e só pode exercer-se nos termos convencionados." Todavia, a jurisprudência ressalva o direito moral à integridade, não permitindo à luz desse direito que o empregador ou dono do programa o modifique livremente.

Quanto aos direitos económicos, partem de uma noção ampla de atos de reprodução, que é confirmada pela jurisprudência, e são ainda enumerados os direitos de transformação e de colocação em circulação ou distribuição de exemplares (sujeito este último ao esgotamento comunitário). A duração dos direitos de autor obedece à regra geral dos 70 anos *post mortem auctoris* ou, pertencendo os direitos à empresa, a partir da sua divulgação (art. 36º CDADC).

Em sede de utilização livre, comparando com os direitos de autor em geral, não é prevista a liberdade de reprodução para uso privado de programas de computador. De todo o modo, um aspeto inovador para os direitos de autor introduzido pela diretiva do software diz respeito aos direitos do utente legítimo (ou titular de licença). Assistem-lhe os direitos de reproduzir e estudar o programa no âmbito da sua utilização, realizar cópia de apoio, reproduzir e alterar o programa para efeitos de correção de erros, incluindo a nosso ver a descompilação estritamente necessária para fins de interoperabilidade com programa independente e a utilização, para esses fins, das informações assim obtidas. Os direitos do utente têm natureza imperativa e não afastam outras vias de proteção do software, nomeadamente o direito de patente e a tutela dos segredos comerciais (arts. 6º e 7º).

A proteção do software pelos direitos de autor não prejudica outras vias de tutela, nomeadamente as patentes de invenção e os segredos comerciais.

Patentes de invenções relacionadas com programas de computador

A atribuição de patentes depende de o pedido preencher certos requisitos. As patentes dizem respeito a invenções técnicas, isto é, obras do espírito sobre problemas técnicos e que não são apenas fórmulas matemáticas ou lógicas. As invenções técnicas devem ter novidade, face ao estado da arte, e resultar de atividade inventiva, no sentido de não resultarem evidente ou obviamente do estado da arte. Finalmente, a invenção deve ser suscetível de aplicação industrial, i.e., poder ser usada na indústria ou na agricultura.

O objeto de patente não cobre todas as obras do espírito. Nos termos do artigo 52º/1 CPI, não podem ser objeto do direito de patente (1) as descobertas, as teorias científicas e os métodos matemáticos, (2) os materiais ou as substâncias já existentes na natureza e as matérias nucleares, (3) as criações estéticas, (4) os projetos, os princípios e os métodos do exercício de atividades intelectuais em matéria de jogo ou no domínio das atividades económicas, assim como os *programas de computadores, como tais, sem qualquer contributo*, e (5) as apresentações de informação. Todavia, em qualquer caso, só é excluída a patenteabilidade se o objeto para que é solicitada a patente se limitar aos elementos nele mencionados (art. 52º/3 CPI).

A norma da Convenção de Munique sobre a Patente Europeia que subjaz ao referido regime interno não tem impedido o Instituto Europeu de Patentes de emitir patentes para invenções relacionadas com programas de computador, em especial no setor dos dispositivos médicos. Em matéria de robots, refira-se a patente EP 1169092 B1[1] sobre um robot de combate ao fogo (*robot bombeiro*), controlado manual ou remotamente, e ligado automaticamente ao sistema de canalização de água e pendurado num monotrilho em túneis. Segundo o resumo da descrição da invenção, o robô de combate ao fogo serve para apagar incêndios em túneis. Está pendurado numa carruagem que funciona em um monotrilho até a abóbada do túnel. Um pistão telescópico óleo-dinâmico permite que o transporte seja reduzido à superfície da estrada. Tal característica permite ao robô superar qualquer obstáculo, proteger pessoas e transportar pessoas sem os obstáculos do trânsito e combater o incêndio. Para conseguir apagar continuamente o incêndio, o robô está conectado à canalização de água por um tubo flexível com 30 metros com um braço automático.

Nos EUA a atribuição de patentes não conhece norma semelhante à da CPE. São atribuídas patentes de software, incluindo software de robots. É o caso, por exemplo, da patente US 8996429 B1: método de desenvolvimento da personalidade de robot. Segundo o resumo da patente[2], a tecnologia patenteada consiste em métodos e sistemas de interação do robot com o utilizador a fim de gerar uma personalidade do robô. O robot pode aceder ao dispositivo de um usuário para determinar ou identificar informações sobre a identidade de um usuário e o robot pode ser configurado à medida do usuário com as informações identificáveis. O robot pode encontrar dados associados à identidade do usuário através de reconhecimento de voz ou facial. O robot pode fornecer uma interação ou resposta personalizada ao usuário com base nas informações especificadas do usuário. A personalidade robótica tem portabilidade, i.e., pode ser transferida de um robot para outro robot (máquina), e as informações armazenadas em um robot podem ser partilhadas com outro robot através da nuvem.[3]

Cumpre referir, todavia, que o desenvolvimento de software executado por robots baseia-se frequentemente em soluções de software livre. Trata-se de uma via que previne a formação de patentes sobre a componente lógica do robot. A *Free Software Foundation* lançou as licenças de software livre GNU GPL (*General Public License)* assegurando a liberdade de reprodução, modificação e distribuição de software. A utilização do software desenvolvido por esta comunidade é sujeita apenas ao dever de fornecer a licença juntamente com o software, e de dar a terceiros a mesma liberdade de que se beneficia. O objetivo é impedir que os direitos de autor e as patentes impeçam o

[1] <http://www.freepatentsonline.com/EP1169092.html>

[2] <https://patents.google.com/patent/US8996429B1/en>

[3] Outra questão é saber se podem ser patenteadas partes do robot que repliquem partes do corpo humano, em especial próteses robóticas. O artigo 54.º/c do CPI dispõe que pode ser patenteada uma invenção nova, que implique atividade inventiva e seja suscetível de aplicação industrial, que incida sobre qualquer elemento isolado do corpo humano ou produzido de outra forma por um processo técnico, incluindo a sequência ou a sequência parcial de um gene, ainda que a estrutura desse elemento seja idêntica à de um elemento natural, desde que seja observada expressamente e exposta concretamente no pedido de patente, a aplicação industrial de uma sequência ou de uma sequência parcial de um gene.

livre desenvolvimento do software, que se considera uma linguagem sujeita aos imperativos constitucionais da liberdade de expressão (*free speech*).[1]

Segredos comerciais

Além dos direitos de autor e das patentes, cumpre ainda referir a possível proteção do software enquanto segredos comerciais ou saber-fazer. Os segredos comerciais estão atualmente protegidos ao abrigo do artigo 318º do Código da Propriedade Industrial (CPI) enquanto informações não divulgadas, à semelhança da norma do Acordo ADPIC/TRIPS. Trata-se de uma forma especial de concorrência desleal. Considera-se ato de concorrência contrário às normas e usos honestos de qualquer ramo de atividade económica a divulgação, a aquisição ou a utilização de segredos de negócios de um concorrente, sem o consentimento do mesmo, se essas informações (1) forem secretas, no sentido de não serem geralmente conhecidas ou facilmente acessíveis, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, para pessoas dos círculos que lidam normalmente com o tipo de informações em questão; (2) tiverem valor comercial pelo facto de serem secretas; (3) tiverem sido objeto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas.

Na União Europeia foi adotada a Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de *know-how* e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais. Consideram-se informações comerciais confidenciais as informações (1) *secretas*, no sentido de, na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos, não são geralmente conhecidas pelas pessoas dos círculos que lidam normalmente com o tipo de informações em questão, ou não são facilmente acessíveis a essas pessoas; (2) com *valor comercial* pelo facto de serem secretas; (3) e que foram objeto de *diligências razoáveis*, atendendo às circunstâncias, para serem mantidas secretas pela pessoa que exerce legalmente o seu controlo.[2]

A proteção jurídica das obras geradas por robots ou inteligência artificial (IA)

A capacidade de os robots gerarem obras literárias ou artísticas suscita igualmente a questão da proteção jurídica destas criações robóticas (IA). Os direitos de autor protegem obras literárias ou artísticas originadas por pessoas humanas no exercício da sua liberdade de criação cultural. Do dogma da autoria humana decorre que, em princípio, as pessoas jurídicas só podem adquirir direitos de autor a título derivado, seja por atribuição legal ou transmissão contratual.

---

[1] Na UE foi desenvolvida uma versão europeia da GPL, a *European Union Public License.* Ver por ex. o nosso "Empresa, comércio eletrónico e propriedade intelectual", in *Nos 20 Anos do Código das Sociedades Comerciais* - Homenagem aos Professores Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier, vol. I, Coord. A. Pinto Monteiro, Coimbra, 2007, p. 439-478.

[2] Sobre o tema, desenvolvidamente, Dário Moura Vicente, "Proteção do know-how, segredo de negócio e Direito Intelectual", in *Propriedade Intelectual – Estudos Vários*, Lisboa, 2018, p. 281-309. *[PS – A Diretiva 2016/943 foi transposta pelo DL 110/2018, de 10 de dezembro, que aprovou o novo Código da Propriedade Industrial]*

Esta caraterística separa os países de *droit d'auteur* dos países de *copyright*, nomeadamente o Reino Unido e os Estados Unidos da América, que preveem a atribuição originária do *copyright* a pessoa diferente do criador intelectual, incluindo pessoas jurídicas como sociedades comerciais, nomeadamente nas criações por encomenda ou em contexto laboral. Mesmo no direito de autor português, à semelhança de outros países latinos, é atribuído o direito de autor sobre obra coletiva à pessoa singular ou coletiva que tiver organizado a criação da obra e em nome de quem a obra tiver sido publicada (artigo. 19 CDADC).[1] Parece-nos, todavia, que esta solução se destina a atribuir o direito sobre títulos de publicações periódicas e de obras inéditas, como dicionários ou enciclopédias, cuja proteção depende de registo. Sendo que a proteção do título, pelos seus requisitos específicos, está mais próxima dos direitos conexos do que dos direitos de autor propriamente ditos, como alerta Oliveira Ascensão.[2] Além disso, mesmo no copyright estadunidense, afirma-se a autoria humana como requisito essencial, pelo que o Copyright Office só regista obras originais criadas por seres humanos, rejeitando o registo nomeadamente de obras produzidas por máquina ou por mero processo mecânico que funcione aleatória ou automaticamente sem qualquer contributo criativo ou intervenção de um autor humano.[3]

Resulta então da vinculação a uma criação intelectual humana a inexistência de direitos de autor sobre criações literárias ou artísticas de robots ou de inteligência artificial? No Reino Unido a lei estabeleceu uma regra especial de autoria para as obras literárias, dramáticas ou artísticas geradas por computador, determinando que o autor é a pessoa que realiza os arranjos necessários à criação da obra.[4] É uma solução tão pioneira quanto ímpar, uma vez que não foi seguida por outros países, nem sequer da família do copyright. E, não obstante, é uma solução que nos remete para a figura dos direitos conexos, em especial para o direito do editor previsto no Reino Unido a favor da pessoa que fizer os arranjos tipográficos (sec. 15 CPDA). Trata-se, em todo o caso, de atribuir os direitos de autor a pessoas físicas ou jurídicas, e não de reconhecer direitos de autor ao robot ou à inteligência artificial.

Por outro lado, o facto de não se reconhecer autoria aos robots não significa que a robótica e a inteligência artificial beneficiem de uma espécie de liberdade de utilização de obras e prestações protegidas por direitos de autor e conexos. A Comissão Europeia considera "necessária uma reflexão sobre as interações entre a IA e os direitos de propriedade intelectual, da perspetiva dos institutos de propriedade intelectual e dos utilizadores, que vise promover a inovação e a segurança jurídica de forma equilibrada".[5] Não se trata, todavia, de criar uma zona franca ou livre de direitos de

[1] Para desenvolvimentos, *vide* o nosso *Direitos de Autor e Liberdade de Informação*, Coimbra, 2008, § 6.

[2] J. Oliveira Ascensão, *Direito Civil – Direito de Autor e Direitos Conexos*, Coimbra, 1992, p. 590.

[3] US Copyright Office, *Compendium of U.S. Copyright Office Practices*, 3rd ed., 2017, para. 306, 313.2 (<https://www.copyright.gov/comp3/docs/compendium.pdf>)

[4] Cf. § 9(3) do UK CPDA 1988 ("the author shall be the person by whom the arrangements necessary for the creation of the work are undertaken"). *Vide* por ex. Chris Holder, Vikram Khurana, Faye Harrison, Louisa Jacobs, Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age (Part I of II), *Computer Law & Security Review* 32 (2016), p. 383-402 (referindo, a propósito, o acórdão *Nova Productions v Mazooma Games* de 2006 - 401).

[5] COM(2018) 237 final, p. 17.

autor que facilite o livre desenvolvimento dos robots e da inteligência artificial, sem prejuízo naturalmente da aplicação das exceções aos direitos de autor, em matéria de utilizações livres, também neste domínio, nomeadamente para fins de informação, ensino ou investigação. De resto, a Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos direitos de autor no mercado único digital[1] estabelece uma exceção obrigatória em termos de utilizações permitidas para prospeção de textos e dados (art. 3) que servirá, sem dúvida, para facilitar o desenvolvimento da inteligência artificial.[2]

Conclusão

O software robótico é uma dimensão essencial dos sistemas de IA. Este trabalho abordou várias vias possíveis para se proteger o software robótico por direitos de propriedade intelectual. A primeira via é a lei de direitos autorais, já que os programas de computador são listados como objeto de direitos autorais elegíveis, ainda que com regras especiais. No entanto, os direitos autorais têm alcance limitado e não esgotam a proteção legal do software robótico. Em particular, o sistema de patentes de invenção pode ser uma solução relevante ao nível da proteção da funcionalidade imbuída nos programas. Finalmente, independentemente das leis de direitos autorais e de patentes, a proteção dos segredos comerciais também será, certamente, uma via importante de proteção legal do software robótico. Em qualquer caso, é importante preservar a liberdade de inovação para que a IA possa ser desenvolvida para o benefício da Humanidade e da Natureza.

Por outro lado, não existe fundamento para atribuir direitos de autor aos robots ou à IA sobre as obras literárias ou artísticas que geram. A isso se opõe o dogma da autoria humana, sem prejuízo da eventual atribuição de um direito conexo sobre tais criações robóticas ou "artificiais", à semelhança do direito do editor existente no Reino Unido e cuja consagração na União Europeia foi recentemente proposta. Por outro lado, a inexistência de uma *autoria robótica* não significa que as obras e prestações protegidas por direitos de autor e conexos possam ser livremente utilizadas por robots ou sistemas de inteligência artificial, sem prejuízo de certas utilizações livres em sede de análise e prospeção de dados e de textos, recentemente propostas, poderem contribuir significativamente para o desenvolvimento da IA.

[1] COM(2016) 593 final. *[PS - Ver agora a Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE]*

[2] No sentido de que a exceção de prospeção e mineração de dados pode ser útil para promover a IA pronunciou-se, recentemente, a Comissão na sua comunicação *Inteligência artificial para a Europa*, COM(2018) 237 final, p. 11.

A MODERNIZAÇÃO DO DIREITO DE AUTOR NA UNIÃO EUROPEIA*

1.O pacote de modernização do Direito de Autor na UE

A modernização do Direito de Autor na União Europeia traduz-se num pacote de medidas anunciado e proposto, a dois tempos, pela Comissão.

Por um lado, a Comunicação "Rumo a um quadro de direitos de autor moderno e mais europeu"[1] e a proposta de Regulamento sobre portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno[2].

Por outro lado, a Comunicação "Promover no Mercado Único Digital uma economia europeia justa, eficiente e competitiva, baseada nos direitos de autor3 e as propostas para adaptar as normas dos direitos de autor e dos direitos conexos ao mercado único digital, e para incorporar o Tratado de Marraquexe no direito da UE4, a saber:

(1) Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos direitos de autor no mercado único digital5;

(2) Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece normas sobre o exercício do direito de autor e direitos conexos aplicáveis a determinadas transmissões em linha dos organismos de radiodifusão e à retransmissão de programas de rádio e televisão6;

(3) Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a determinadas utilizações permitidas de obras e outro material protegidos por direito de autor e direitos conexos em benefício das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos e que altera a Diretiva 2001/29/CE relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação7;

(4) Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao intercâmbio transfronteiras, entre a União e países terceiros, de cópias em formato acessível de certas obras e outro material protegido por direitos de autor e direitos conexos em benefício das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos8.

Deste pacote modernizador do Direito de Autor foram já aprovados o Regulamento da portabilidade[9], a Diretiva sobre utilizações por invisuais[10] e o regulamento conexo[1],

---

* *Revista de Direito Intelectual* 2017/2: 7-22.

[1] COM(2015) 626 final, 9.12.2015.

[2] COM(2015) 627 final, 9.12.2015.

[3] COM(2016) 592 final, Bruxelas, 14.9.2016.

[4] https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules

[5] COM(2016) 593 final, Bruxelas, 14.9.2016

[6] COM(2016) 594 final, Bruxelas, 14.9.2016.

[7] COM(2016) 596 final, Bruxelas, 14.9.2016.

[8] COM(2016) 595 final, Bruxelas, 14.9.2016.

[9] *Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno (JO L 168, 30.6.2017, p. 1-11).*

[10] Diretiva (UE) 2017/1564 do Parlamento Europeu e do Conselho, de 13 de setembro de 2017, relativa a determinadas utilizações permitidas de determinadas obras e outro material protegidos por direito de autor e direitos conexos em benefício das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos e que altera a Diretiva 2001/29/CE relativa à harmonização de

que *sucedem a uma série de instrumentos de harmonização dos direitos de autor e direitos conexos na União Europeia.*[2]

Além disso, merece também referência o papel do Tribunal de Justiça da União Europeia, não apenas pela quantidade de acórdãos proferidos, mas também pelo impacto da sua jurisprudência enquanto cânone hermenêutico do direito de autor da União.[3]

---

certos aspetos do direito de autor e dos direitos conexos na sociedade da informação (JO L 242, 20.9.2017, p. 6-13).

[1] Regulamento (UE) 2017/1563 do Parlamento Europeu e do Conselho, de 13 de setembro de 2017, relativo ao intercâmbio transfronteiras, entre a União e países terceiros, de cópias em formato acessível de certas obras e outro material protegido por direitos de autor e direitos conexos em benefício das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos (JO L 242, 20.9.2017, p. 1-5).

[2] A saber, Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados (JO L 77 de 27.3.1996, p. 20-28); Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de maio de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação (JO L 167 de 22.6.2001, p. 10-19); Diretiva 2006/115/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa ao direito de aluguer, ao direito de comodato e a certos direitos conexos ao direito de autor em matéria de propriedade intelectual (JO L 376 de 27.12.2006, p. 28-35); Diretiva 2009/24/CE do Parlamento Europeu e do Conselho, de 23 de abril de 2009, relativa à proteção jurídica dos programas de computador (JO L 111 de 5.5.2009, p. 16-22); Diretiva 2012/28/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativa a determinadas utilizações permitidas de obras órfãs (JO L 299 de 27.10.2012, p. 5-12); Diretiva 2014/26/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à gestão coletiva dos direitos de autor e direitos conexos e à concessão de licenças multiterritoriais de direitos sobre obras musicais para utilização em linha no mercado interno (JO L 84 de 20.3.2014, p.72-98); Diretiva 2001/84/CE do Parlamento Europeu e do Conselho, de 27 de setembro de 2001, relativa ao direito de sequência em benefício do autor de uma obra de arte original que seja objeto de alienações sucessivas (JO L 272 de 13.10.2001, p. 32-36) (Diretiva «Direito de sequência»); Diretiva 93/83/CEE do Conselho, de 27 de setembro de 1993, relativa à coordenação de determinadas disposições em matéria de direito de autor e direitos conexos aplicáveis à radiodifusão por satélite e à retransmissão por cabo (JO L 248 de 6.10.1993, p. 15-21) (Diretiva «Satélite e cabo»); Diretiva 2006/116/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa ao prazo de proteção do direito de autor e de certos direitos conexos (JO L 372 de 27.12.2006, p. 12-18) (Diretiva «Prazo»).

A estas Diretivas junta-se uma outra sobre os remédios da propriedade intelectual (*enforcement*), a Diretiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade intelectual (JO L 195 de 2.6.2004, p. 16-25) (IPRED), e o Regulamento (UE) n.º 386/2012 do Parlamento Europeu e do Conselho, de 19 de abril de 2012, que atribui ao Instituto de Harmonização no Mercado Interno (Marcas, Desenhos e Modelos) funções relacionadas com a defesa dos direitos de propriedade intelectual, nomeadamente a de reunir representantes dos setores público e privado num Observatório Europeu das Infrações aos Direitos de Propriedade Intelectual (JO L 129 de 16.5.2012, p. 1-6). Outras medidas com impacto nos direitos de auto no mercado único digital são a Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (JO L 178 de 17.7.2000, p. 1-16), 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 de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31-50), que será revogada a partir de 25 de maio de 2018 e substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1-88), e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37-47), designada «Diretiva Privacidade e Comunicações Eletrónicas», na redação que lhe foi dada pelas Diretivas 2006/24/CE e 2009/136/CE.

[3] Temos acompanhado a jurisprudência do TJUE em estudos sobre o direito de reprodução e a compensação para uso privado, o direito de comunicação ao público, as obras radiodifundidas, as hiperligações e as plataformas de partilha P2P, ou as licenças de software, o direito de distribuição e

2. Traços gerais do pacote de modernização do Direito de Autor e sua apreciação crítica

2.1 O pacote de modernização visa aumentar a disponibilidade de obras na Europa, criando condições favoráveis para a distribuição transfronteiriça de programas de televisão e rádio em linha, aumentando a disponibilidade de obras audiovisuais em plataformas de VoD[1], e facilitando a digitalização e divulgação de obras fora do comércio.

Depois, procura melhorar as regras de direitos de autor sobre investigação, educação e património cultural. Ao contrário da atual natureza facultativa da maior parte das exceções ao direito de autor da UE (e por isso do seu âmbito não transfronteiriço), é proposto um conjunto de exceções obrigatórias relacionadas com atividades de ensino, prospeção de texto e dados (*data & text mining*), e a preservação do património cultural por entidades como os museus e as cinematecas.

A fim de melhorar o funcionamento do mercado dos direitos de autor é proposto um direito conexo para os editores (*publisher's right*), reforça-se a posição dos titulares de direitos em sede de negociação e remuneração da exploração em linha do seu conteúdo em plataformas de partilha de vídeo, e estabelecem-se novas regras de transparência para a remuneração dos autores e dos artistas intérpretes ou executantes.

Quanto às medidas para incorporação do Tratado de Marraquexe no direito da UE2, pretende-se facilitar o acesso, em formato adequado, a obras publicadas às pessoas cegas, com deficiência visual ou com outras dificuldades para aceder ao texto impresso. Neste sentido, institui-se uma exceção obrigatória e possibilita-se o intercâmbio transfronteiriço de exemplares dessas obras entre a UE e países terceiros que são partes no Tratado.

2.2 O pacote de modernização do direito de autor da União Europeia constitui objeto de análise crítica por parte de diversas organizações. Em especial, no que respeita às propostas de dezembro de 2016, o Instituto Max-Planck para a Inovação e

---

esgotamento online. *Vide*, por ex., Alexandre Dias PEREIRA: "Levies in EU copyright law: an overview of the CJEU's judgments on the fair compensation of private copying and reprography", *Journal of Intellectual Property Law & Practice*, vol. 12:7/1 (2017) 591–600; "Tutela efetiva da propriedade intelectual (enforcement), em especial a proteção dos direitos de autor e conexos contra a pirataria", *RLJ – Revista de Legislação e Jurisprudência*, 146:4003 (2017) 241-266; "Portugal: broadcast works in bars and restaurants: «resistant» case-law to the CJEU's rulings", *Queen Mary Journal of Intellectual Property*, col. 6/4 (2016) 525–535; "O novo regime das obras órfãs", Revista de Direito Intelectual 2016/1, 21-49; "O «Marco Civil da Internet» e seus Reflexos no Direito da União Europeia", Revista da ABPI 142 (2016) 2-21; "Direitos de remuneração equitativa pela comunicação pública de obras e prestações", in *Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão – 50 Anos de Vida Universitária*, Coord. Dário Moura Vicente et. al., Almedina, Coimbra, 2015, 57-75.

[1] Entende-se que os operadores de serviços baseados em tecnologias equivalentes à retransmissão por cabo (por ex., os provedores de IPTV) não podem beneficiar da gestão coletiva obrigatória da retransmissão por cabo.

[2] Tratado de Marraquexe para facilitar o acesso a obras publicadas às pessoas cegas, com deficiência visual ou com outras dificuldades para aceder ao texto impresso, assinado em Marraquexe, Marrocos, em 28 de junho de 2013.

Concorrência, de Munique, emitiu uma declaração de posição[1], nos termos da qual, em síntese:

Primeiro, o pacote não se apoiaria numa "reavaliação sistemática" do direito de autor da União Europeia e, ao invés de simplificar o já complicado quadro jurídico existente, adicionaria novos "estratos de regulação largamente desnecessários", potenciando "inconsistências significativas". Por exemplo, não se descortinaria a razão para que as exceções propostas para educação à distância, a mineração de dados e textos e a preservação do património cultural fossem obrigatórias, ao passo que certas exceções como a liberdade de citação, crítica, paródia e uso privado continuariam facultativas.

Segundo, o pacote teria um impacto de "fragmentação" do quadro normativo[2], uma vez que certas matérias, como a educação à distância, seriam simultaneamente objeto de diretivas e de regulamentos, para além de, segundo os autores, não apresentar uma concetualização coerente (por ex. a noção de titular de direitos, as distinções entre exceções e limites, remuneração equitativa e compensação equitativa, comunicação ao público e colocação à disposição do público e ausência de clarificação dos atos de hiperligação que constituem comunicação ao público).

Terceiro, pese embora a criação de um sistema unitário de direitos de autor na União Europeia ter sido abordada pela Comissão em diversas Comunicações e de o artigo 118 do TFUE fornecer a base legal para tal ensejo – considerando-se o regulamento como o instrumento não apenas adequado, mas também necessário para promover o bom funcionamento do mercado interno -, atualmente a criação de um sistema unitário poderia não ser realista nem viável.

Em suma, pelas razões sumariamente expostas, entendem os subscritores da tomada de posição do MPI, que o pacote de modernização deveria simplificar o direito de autor da EU ao invés de o tornar ainda mais complicado e inconsistente e, além disso, embora sejam favoráveis a um sistema unitário de direitos de autor a médio prazo, atualmente esse objetivo poderia ser "irrealista", pelo que as medidas propostas deveriam ser contidas numa única diretiva, que estabeleceria todas as exceções obrigatórias, incluindo as relativas às utilizações em benefício de pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos, implementando desse modo o Tratado de Marraquexe.

---

[1] Reto M. HILTY & Valentina MOSCON, *Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules*, February 2017.

[2] Neste sentido, ver também a Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market' (COM(2016) 593 final — 2016/0280 (COD)), on the 'Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes' (COM(2016) 594 final — 2016/0284 (COD)) and on the 'Proposal for a Directive of the European Parliament and of the Council on certain permitted uses of works and other subject-matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired or otherwise print disabled and amending Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society' (COM(2016) 596 final — 2016/0278 (COD)): "The EU lacks an integrated copyright system. To establish such a system, the main objective is to eliminate fragmentation while, at the same time, enhancing protection for creators who are sometimes pitted against technological giants that dominate the markets."

2.3. De um modo geral, saudamos as propostas da Comissão e o seu esforço no sentido da atualização das normas de direitos de autor da União Europeia aos desafios do mundo digital. Não obstante, importa realçar alguns pontos.

Para começar, o processo de modernização do direito de autor não é novo, remontando pelo menos ao Livro Verde de 1988 sobre os direitos de autor e o desafio da tecnologia digital, cujo programa de ação então traçado levou à adoção de diversas diretivas de harmonização.[1] Por isso, tal como salientado pela declaração do MPI, a modernização deve harmonizar-se com o quadro jurídico já existente, buscando maior coerência sistemática e conceitual, ao invés de fragmentar noções legais cujo sentido vai sendo clarificado pela jurisprudência do TJUE, que já conta mais de meia centena de acórdãos neste domínio.[2]

Por outro lado, o pacote de modernização representa um passo qualitativo, uma vez que acarreta a unificação de regimes através da adoção de regulamentos. Ao contrário do que já sucede em outros domínios da propriedade intelectual, como as marcas e os modelos e desenhos, não existe um título jus-autoral unitário na União Europeia, conservando o direito de autor no essencial a sua base territorial nacional.[3] Adotar um regulamento no domínio dos direitos de autor poderá ser um primeiro passo no sentido de um sistema unitário de direitos de autor na União Europeia. Talvez seja essa uma via possível a médio prazo e até permitida pelo princípio da proporcionalidade. Todavia, é duvidoso que passe no crivo do princípio da subsidiariedade, já que não está demonstrado que o atual sistema prejudique injustificadamente o bom funcionamento do mercado interno, nem que um sistema unitário seria um meio mais eficaz para alcançar esse fim.

De todo o modo, o regulamento terá sido a via necessária para a relação da União Europeia com países terceiros, para possibilitar o intercâmbio transfronteiriço de exemplares de obras em formato adequado para invisuais entre a UE e países terceiros que são partes no Tratado de Marraquexe. O regulamento foi também o instrumento utilizado para assegurar a portabilidade de serviços de conteúdos em linha no mercado interno, como melhor veremos seguidamente.

3. O Regulamento 2017/1128 sobre portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno

O Regulamento da Portabilidade visa "assegurar que os assinantes de serviços de conteúdos em linha portáteis que são licitamente prestados nos respetivos Estados-Membros de residência possam ter acesso a esses serviços e utilizá-los quando se encontrem temporariamente presentes num Estado-Membro que não seja o seu Estado-Membro de residência" (art. 1/1).

---

[1] Sobre a harmonização do direito de autor na União Europeia, com uma análise comparada da dicotomia *droit d'auteur* / *copyright*, pode ver-se Alexandre L. Dias PEREIRA, *Direitos de Autor e Liberdade de Informação*, Almedina, Coimbra, 2008, § 3.

[2] *Vide* http://copyrightblog.kluweriplaw.com/category/cjeu/

[3] Sobre esta matéria *vide* Dário Moura VICENTE, *A tutela internacional da propriedade intelectual*, Almedina, Coimbra, 2008.

Em causa está o chamado "geo-blocking", isto é, o bloqueio geográfico de acesso a e utilização de serviços de conteúdos em linha decorrente da territorialidade dos direitos de autor (*pay per country*). Fazendo a analogia com o esgotamento do direito de distribuição, dir-se-ia que o Regulamento da portabilidade consagra uma espécie de esgotamento temporário dos direitos. São visados os serviços de conteúdos em linha, abrangendo os serviços de comunicação social audiovisual (definidos pela Diretiva 2010/13) ou os serviços de acesso a, e utilização de obras ou outro material protegido, ou transmissões (lineares ou a pedido) de organismos de radiodifusão. Pense-se, por exemplo, em serviços como o "Spotify", o "Netflix, ou o "iTunes".

Ao utilizador legítimo é atribuído um direito de acesso a, e de utilização de serviços de conteúdos em linha quando se encontre temporariamente presente num Estado-Membro que não seja o seu Estado-Membro de residência. Sobre o prestador recai uma obrigação de permitir a portabilidade transfronteiriça de serviços de conteúdos em linha relativamente a assinantes pagantes dos serviços (art. 3/1), ficando vedado de impor-lhes quaisquer encargos adicionais para o acesso a serviços de conteúdos em linha e a sua utilização quando se encontra temporariamente em outro Estado-Membro (art. 3/2). A portabilidade diz respeito aos mesmos conteúdos, tipo e número de dispositivos, para o mesmo número de utilizadores e com a mesma gama de funcionalidades, sem prejuízo de os requisitos de qualidade do serviço não serem idênticos aos do país de origem (art. 3/3).

Consagra-se o princípio do país de origem, no sentido de que o Estado-Membro de residência do assinante é considerado o local da prestação dos serviços, do acesso aos mesmos e da sua utilização. Nos termos do artigo 4º, a prestação dos serviços de conteúdos em linha, o acesso aos mesmos e a sua utilização localizam-se no Estado-Membro de residência do assinante. Cabe ao prestador do serviço verificar o Estado-Membro de residência do assinante, com base nomeadamente em meios de identificação eletrónica, em particular os abrangidos pelos sistemas de identificação eletrónica notificados nos termos do Regulamento eIDAS[1], os dados de pagamento (número de conta bancária ou do cartão de débito ou de crédito), o endereço do protocolo Internet (art. 5).

Relativamente aos serviços de conteúdos em linha não remunerados, o prestador pode autorizar a portabilidade transfronteiriça na condição de identificar devidamente o Estado-Membro de residência do assinante e de informar os titulares de direitos de autor ou outros sobre essa política (art. 6).[2]

[1] Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

[2] O Regulamento da portabilidade estabelece ainda algumas regras sobre tratamento dos dados pessoais dos assinantes, o princípio da limitação pelo fim, e a regra segundo a qual "esses dados não podem ser comunicados, transferidos, partilhados, ser objeto de licenças ou de outra forma transmitidos ou divulgados aos titulares de direitos de autor ou direitos conexos, ou aos titulares de quaisquer outros direitos sobre o conteúdo de serviços de conteúdos em linha ou a outros terceiros" (art. 8/2). Depois de concluída uma verificação do Estado-Membro de residência do assinante, os dados devem ser, imediata e irreversivelmente, destruídos (art. 8/3).

4. As utilizações permitidas para pessoas invisuais: Diretiva 2017/1564, Regulamento 2017/156 e a exceção Braille no CDADC

4.1 A Diretiva (EU) 2017/1564, do Parlamento Europeu e do Conselho, de 13 de setembro de 2017 estabelece utilizações permitidas de determinadas obras e outro material, protegidos por direito de autor e direitos conexos, em benefício de pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos. Altera a Diretiva 2001/29/CE relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação.

Considera-se que a proteção das pessoas com deficiência, nos termos da Carta de Direitos Fundamentais da União e da Convenção das Nações Unidas dos Direitos da Pessoas com Deficiência (CNUDPD), justifica medidas para aumentar a disponibilidade de livros e outras obras em formatos acessíveis e melhorar a sua circulação no mercado interno. Por outro lado, em 30 de abril de 2014, a União assinou o Tratado de Marraquexe, que visa facilitar o acesso a obras publicadas por parte das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos, estabelecendo exceções ou limitações aos direitos de autor e direitos conexos.

Assim, a Diretiva 2017/1564 introduz uma exceção obrigatória em benefício de pessoas invisuais lato senso. Os materiais protegidos abrangidos pela exceção incluem obras sob a forma de livro, publicações periódicas (jornal, revista) ou outro tipo de escritos (por ex. partituras), incluindo ilustrações, independentemente do respetivo suporte, incluindo sob formato sonoro, como áudio-livros, e sob a forma digital (art. 2/1). Quanto aos beneficiários, são visados diretamente os invisuais, lato senso (art. 2/2) e, indiretamente, entidades autorizadas ou reconhecidas por um Estado-Membro para prestar aos beneficiários serviços sem fins lucrativos em matéria de educação, formação pedagógica, leitura adaptada ou acesso à informação, e também bibliotecas, estabelecimentos de ensino e outros organismos sem fins lucrativos que prestem esses serviços no quadro das suas atividades principais, obrigações institucionais ou missões de interesse público (art. 2/4).

As utilizações permitidas incluem a reprodução, a distribuição, a comunicação ao público e a disponibilização em comodato, sem fins lucrativos (art. 3/1). O exercício das utilizações permitidas deve respeitar a integridade da obra (art. 3/2) e a chamada regra dos três passos (art. 3/3). As utilizações permitidas são imperativas (art. 3/5) e os Estados-Membros podem cobrar uma compensação equitativa relativamente a atos praticados por entidades autorizadas estabelecidas no seu território (art. 3/6). Estas entidades podem prestar livremente os seus serviços a pessoas beneficiárias ou entidades autorizadas de outros Estados-Membros, e as cópias em formato acessível a invisuais licitamente realizadas podem circular livremente no mercado interno (art. 4).

As entidades autorizadas ficam sujeitas a um conjunto de obrigações, nomeadamente controlar os beneficiários efetivos das utilizações permitidas, adotar boas práticas de registo e manipulação das obras e das respetivas cópias em formato acessível e disponibilizar a lista das obras (cópias) e respetivos formatos disponíveis (art. 5).

Finalmente, a Diretiva 2017/1564 altera a Diretiva 2001/29, que harmonizou as exceções e limitações aos direitos de autor e direitos conexos, passando a alínea b) do seu artigo 5/3 a ter a seguinte redação: "Utilização a favor de pessoas portadoras de

deficiências que esteja diretamente relacionada com essas deficiências e apresente caráter não comercial, na medida exigida por cada deficiência específica, sem prejuízo das obrigações dos Estados-Membros decorrentes da Diretiva (UE) 2017/1564 do Parlamento Europeu e do Conselho".

4.2. O Regulamento (UE) 2017/1563 (sobre intercâmbio transfronteiras, entre a União e países terceiros, de cópias em formato acessível de certas obras em benefício das pessoas cegas, com deficiência visual ou com outras dificuldades de acesso a textos impressos) regula a exportação e importação entre a União e países terceiros, que são partes no Tratado de Marraquexe, de cópias em formato acessível com fins não comerciais a favor das pessoas beneficiárias.

As cópias realizadas em qualquer Estado-Membro em conformidade com a Diretiva 2017/1564 podem ser distribuídas, comunicadas ou disponibilizadas a uma pessoa beneficiária ou a uma entidade autorizada em países terceiros que são partes nesse mesmo tratado, mas apenas sem fins lucrativos e por entidades estabelecidas num Estado-Membro (art. 3). De igual modo, podem ser importadas de um país terceiro com fins não comerciais em benefício de pessoas cegas, com deficiência visual ou outras dificuldades de leitura de textos impressos (art. 4). Segundo o considerando 6, os formatos acessíveis incluem braille, letras grandes, livros digitais adaptados, audiolivros e radiodifusão.

Tal como previsto na Diretiva 2017/1564, também o Regulamento 2017/1563 sujeita as entidades autorizadas a um conjunto de obrigações, nomeadamente adotar boas práticas para controlar a fraude e publicar e atualizar uma lista de obras ou outro material disponível em formato acessível e os formatos disponíveis.

4.3. Possivelmente a utilização permitida pela Diretiva e pelo Regulamento em benefício de pessoas invisuais é menos ampla do que a que o Código do Direito de Autor e dos Direitos Conexos atualmente prevê. Nos termos do artigo 80º do CDADC, que consagra a exceção Braille,

"Será sempre permitida a reprodução ou qualquer espécie de utilização, pelo processo Braille ou outro destinado a invisuais, de obras licitamente publicadas, contanto que essa reprodução ou utilização não obedeça a intuito lucrativo."

A Diretiva 2017/1564 parece estabelecer um regime mais restritivo no que respeita ao exercício das utilizações livres para pessoas invisuais, e que de resto alarga a todas as utilizações permitidas para pessoas portadoras de deficiência, visual ou outra. Entre nós, não é conhecido nenhum projeto de transposição da Diretiva, em todo o caso seria desejável evitar repetição de normas que estabelecem utilizações livres, como sucedeu no domínio da reprodução para uso privado.[1]

5. As medidas sobre direitos de autor no mercado único digital e transmissão em linha de emissões de radiodifusão

[1] Com mais indicações, Alexandre Dias PEREIRA, "A compensação equitativa pela cópia privada no direito de autor português e da União Europeia", *Revista de Direito Intelectual*, 2016/2, 7-57.

5.1. A proposta de diretiva sobre direitos de autor e direitos conexos no mercado único digital estabelece um conjunto de exceções obrigatórias**.** Ao contrário da atual natureza facultativa da maior parte das exceções ao direito de autor da UE (e por isso do seu âmbito não transfronteiriço), a diretiva proposta consagra um conjunto de utilizações obrigatoriamente permitidas para atividades de prospeção de textos e dados (art. 3), atividades pedagógicas transnacionais e digitais (art. 4), preservação do património cultural por entidades como os museus e as cinematecas (art. 5), e utilização de obras fora do comércio (art. 7).

Com vista aumentar a disponibilidade de obras audiovisuais em plataformas de VoD, é previsto um mecanismo de negociação para facilitar a disponibilização de obras audiovisuais em plataformas de vídeo a pedido face a dificuldades relacionadas com o licenciamento de direitos (art. 10).

A proposta pretende igualmente conferir aos editores de publicações de imprensa os direitos de reprodução e de comunicação ao público relativos à utilização digital das suas publicações de imprensa (art. 11), vincular os prestadores de serviços da sociedade da informação que armazenam e permitem o acesso a grandes quantidades de obras e outro material protegido carregados pelos seus utilizadores a tomar medidas, nomeadamente através de tecnologias efetivas de reconhecimento de conteúdos, para cumprir os acordos com os titulares de direitos com vista ao controlo da disponibilização ilícita de conteúdos protegidos (art. 13), estabelecer uma obrigação de transparência de modo a garantir a remuneração justa de autores e artistas intérpretes ou executantes nos contratos (art. 14), bem como um mecanismo de ajustamento contratual que permita aos autores obter uma compensação adicional (art. 15).

5.2. De modo a facilitar a distribuição transfronteiriça de programas de televisão e rádio em linha e considerando que os operadores de serviços baseados em tecnologias equivalentes à retransmissão por cabo (por ex., os provedores de IPTV) não beneficiam da gestão coletiva obrigatória prevista para a retransmissão por cabo, a proposta de Regulamento sobre o exercício dos direitos de autor nas transmissões em linha dos organismos de radiodifusão e a retransmissão de programas de rádio e televisão sujeita os chamados "serviços acessórios em linha" ao *princípio do país de origem*, no sentido de que os atos juridicamente relevantes em termos de direitos de autor e direitos conexos ocorrem exclusivamente no Estado-Membro do estabelecimento principal do organismo de radiodifusão (art. 2). O serviço acessório em linha consiste no fornecimento ao público, por ou sob o controlo e responsabilidade do organismo de radiodifusão, de programas de rádio ou televisão em simultâneo com ou num determinado período de tempo após a sua transmissão pelo organismo de radiodifusão, bem como de quaisquer materiais produzidos pelo ou para o organismo de radiodifusão, que seja acessório em relação a difusão (art. 1/a).

O exercício dos direitos de transmissão por titulares de direitos que não sejam organismos de radiodifusão só pode ser feito através de entidades de gestão coletiva (art. 3/1), as quais ficam mandatadas para gerir os direitos em nome mesmo dos titulares que não lhes atribuíram esses poderes (art. 3/2). A gestão coletiva obrigatória não se aplica "aos direitos exercidos por um organismo de radiodifusão em relação às suas

próprias transmissões, independentemente de lhes pertencerem ou de lhes terem sido transferidos por outros titulares do direito de autor ou titulares de direitos conexos" (art. 4).

5.3. Estas propostas suscitaram críticas, nomeadamente na referida tomada de posição do MPI. Desde logo, não se compreenderia a razão para continuarem facultativas as exceções de citação, crítica, paródia e uso privado, quando se introduz a obrigatoriedade para outras exceções, com o consequente risco de *fragmentação* do regime dos direitos de autor. Por outro lado, os direitos de autor parecem ser reduzidos a direitos de remuneração, com o alargamento da gestão coletiva obrigatória à transmissão em linha de programas televisivos e de rádio, e não seria suficientemente justificada a necessidade de atribuir um direito conexo aos editores.

6. Conclusão

O pacote de modernização dos direitos de autor e dos direitos conexos na União Europeia pretende atualizar o regime destes direitos face aos desafios do mercado digital, acentuando a desindividualização do direito de autor. Os objetivos são louváveis, como sejam promover a distribuição transfronteiriça de programas de televisão e rádio em linha e aumentar a disponibilidade de obras audiovisuais em plataformas de VoD. Todavia, alargar a gestão coletiva obrigatória prevista para a retransmissão por cabo significa, na prática, retirar poder aos titulares de direitos, reduzindo os direitos de autor a meros direitos de remuneração, como sucederá igualmente no domínio da digitalização e divulgação de obras fora do comércio (pese embora a possibilidade de *opt-out*), ou com a exploração on-line de conteúdos em plataformas de partilha de vídeo. É verdade que as regras propostas de transparência para a remuneração dos autores e dos artistas intérpretes ou executantes contribuirão para uma maior clareza do sistema, mas nem por isso a desindividualização, em termos de desnecessidade de autorização individual, deixará de ocorrer.

A tendência para a "socialização" dos direitos de autor nota-se igualmente nas propostas que, visando melhorar as regras de direitos de autor sobre investigação, educação e património cultural, consagram um conjunto de exceções obrigatórias relacionadas com atividades de ensino, prospeção de textos e dados, e a preservação do património cultural por entidades como os museus e as cinematecas. Ao mesmo tempo estas propostas têm o efeito algo contraditório de significar, a contrario, que não estando já expressamente previstas as utilizações aí referidas, não são autorizadas por lei, já que pelo menos, em caso de dúvida, não passariam no teste dos três passos. Além disso, pode questionar-se se não terão por efeito dispor mais contenção na interpretação das utilizações permitidas, haja em vista por exemplo o acórdão *Ulmer* do TJUE.[1]

O objetivo principal parece ser tornar essas exceções obrigatórias de modo a impedir a fragmentação de regimes nacionais que perturbem ou prejudiquem o bom funcionamento do mercado único digital, por exemplo no contexto do ensino à

[1] Cf. Alexandre Dias PEREIRA, "A digitalização de obras e sua colocação à disposição do público em terminais de bibliotecas universitárias: o acórdão *Eugen Ulmer* do Tribunal de Justiça da União Europeia", *Revista de Direito Intelectual*, 2015/2, 153-173.

distância. De resto, na doutrina vários Autores já defenderam a obrigatoriedade das exceções, de modo a evitar o atual mosaico de regimes nacionais.[1] De entre estas exceções deverá contar-se, naturalmente, a destinada a permitir o acesso, em formato adequado, a obras publicadas às pessoas invisuais. Já não se compreende, todavia, que outras tantas exceções permaneçam meramente facultativas, haja em vista desde logo as utilizações livres no domínio da imprensa e de outos meios de comunicação social.

Se a consagração da obrigatoriedade de exceções aprofunda a função social dos direitos de autor, já a proposta de criação um direito conexo para os editores - existente em alguns Estados Membros - aponta em sentido contrário. Um dos princípios que norteiam a harmonização dos direitos de autor na União Europeia é o princípio do elevado nível de proteção. Na prática isso significa harmonizar por cima, isto é, tornar padrão comum o nível de proteção mais elevado praticado por um Estado-Membro (veja-se, por exemplo, o que sucedeu no domínio da duração de proteção, o mesmo valendo, em certo sentido, para o direito especial do fabricante de base de dados).

Todavia, não está demonstrado que a atribuição de um direito conexo a mais uma categoria de titular de direitos – no caso, os editores de publicações impressas – promova o bom funcionamento do mercado interno. Basta pensar que o direito especial do fabricante de bases de dados não foi replicado por outros países e nem por isso as grandes empresas da Internet procuraram a Europa como principal centro de negócios. Além de que, na prática, os editores já são titulares, por cessão legal ou contratual, de direitos de autor, como sucede por exemplo na figura da obra coletiva ou da obra anónima. Esse novo direito reforçará provavelmente a posição dos editores em sede de negociação com os operadores de novos modelos de negócios. Resta saber, todavia, se esse reforço de proteção não terá um efeito contraproducente em termos de estímulo à criação cultural.

Para terminar, há questões não abrangidas pelo pacote e que sem dúvida contribuiriam para a modernização dos direitos de autor no mundo digital. Pense-se, por exemplo, na distribuição de conteúdos digitais, incluindo programas de computador, e a questão do esgotamento online, tendo presente o acórdão *UsedSoft*.[2] O mercado único digital assentará fundamentalmente no alargamento do princípio do país de origem aos direitos de autor e da gestão coletiva obrigatória para utilizações semelhantes à retransmissão por cabo, seguindo o modelo do "balcão único". Atualmente os direitos de autor e direitos conexos estão excluídos do princípio do país de origem nos termos da Diretiva sobre comércio eletrónico. O pacote de modernização terá um impacto significativo neste domínio, colocando os direitos de autor no mercado único digital na órbita do princípio do país de origem.

Há o risco da "corrida para baixo", no sentido de os Estados-Membros competirem entre si na criação de ambientes jurídicos mais favoráveis ao estabelecimento das empresas da nova economia, à semelhança da concorrência em sede fiscal. Os direitos

[1] No sentido do reforço da proteção jurídica da liberdade de utilização, veja-se a nova redação do art. 221/2 do CDADC, introduzida pela Lei 36/2017, de 2 de junho.

[2] Acórdão do Tribunal de Justiça (Grande Secção) de 3 de julho de 2012, *UsedSoft GmbH c. Oracle International Corp*., proc. C-128/11 (adquirente legítimo e esgotamento do direito de distribuição na comercialização de licenças de programas de computador em segunda mão descarregados a partir da Internet), ECLI:EU:C:2012:407.

de autor serão então um mero custo de transação, cujo valor assentará apenas num juízo de eficiência económica. Todavia, no atual enquadramento jurídico-constitucional, os direitos de autor são, em primeira linha, um instrumento da liberdade de criação cultural – e da dignidade da pessoa humana que a encarna - e não apenas uma ferramenta das indústrias culturais e da eficiência económico-financeira dos mercados digitais ou outros. Pelo que preservar e dignificar o papel do autor enquanto criador intelectual é – e deverá ser – o cerne da modernização do direito de autor na União Europeia, e a marca de contraste relativamente a modelos como o *Copyright* mais voltados para os interesses da indústria e do mercado.

CONTRATOS DE FORNECIMENTO DE CONTEÚDOS E SERVIÇOS DIGITAIS*

Resumo: A Diretiva 2019/770 disciplina os contratos de fornecimento de conteúdos e serviços digitais estabelecendo diversos direitos do consumidor no caso de não fornecimento e de não conformidade dos conteúdos ou dos serviços com o contrato. O presente trabalho analisa os remédios consagrados pela diretiva para a quebra do contrato e identifica aspetos importantes que não foram abrangidos pela diretiva.

Introdução

Na economia digital, o fornecimento de conteúdos e serviços digitais é objeto de novos contratos, que têm sido celebrados e regulados ao abrigo da liberdade contratual[1]. Todavia, a proteção jurídica do consumidor a nível europeu foi considerada insuficiente e, por isso, um obstáculo ao bom funcionamento do mercado único digital. Segundo dados da Comissão Europeia, por falta de confiança jurídica, só 10% das transações envolveriam operadores europeus com consumidores de outros Estados-Membros, tendo um em cada três consumidores problemas com a aquisição de conteúdos digitais como música, jogos ou computação em nuvem, sem encontrar respostas adequadas para esses problemas.[2]

Na União Europeia, a proteção do consumidor no comércio eletrónico foi objeto de diversas medidas, como sejam desde logo a Dir. 2000/31 sobre comércio eletrónico[3] e a

* *Estudos de Direito do Consumidor* n.º 15 (2019) 9-36. Texto elaborado para o Congresso «Direito do Consumidor: Ruturas e Continuidades após as Recentes Alterações Legislativas», organizado pelo Centro de Direito do Consumo em parceria com o Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, no dia 22 de novembro de 2019.

[1] Ver, por ex., os «Termos de Serviço do Google» <https://policies.google.com/terms?hl=pt-BR>, do Facebook <https://www.facebook.com/legal/terms>, do Youtube < https://www.youtube.com/t/terms> ou dos Recursos Netflix <https://media.netflix.com/pt_pt/terms-and-conditions>

[2] European Commission, «Digital contract rules» <https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en>

[3] Diretiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno, transposta pelo DL 7/2004 de 7 de janeiro, alterado pelo DL 62/2009 de 10 de março e pela Lei 46/2012 de 29 de agosto. Sobre a proteção do consumidor no comércio eletrónico pode ver-se o nosso

Dir. 2011/83/UE sobre direitos dos consumidores[1]. Mais recentemente, em ordem a promover a confiança jurídica do consumidor - enquanto fator-chave do comércio eletrónico - e com isso o bom funcionamento do mercado interno digital foi adotada a Dir. 2019/770 sobre contratos de fornecimento de conteúdos e serviços digitais[2], a qual faz parte do pacote de modernização legislativa para a realização do mercado único digital da Comissão JUNCKER[3], juntamente com outras medidas, em especial a Dir. 2019/771 sobre os contratos de compra e venda[4], que revogou e substituiu a Dir. 1999/44 sobre as garantias na venda de bens de consumo[5]. Sendo a noção de bem de consumo para efeitos desta diretiva limitada aos bens móveis corpóreos (art. 1/2-b)[6], os consumidores de conteúdos e serviços digitais privados não tinham os remédios e as garantias contratuais contra o respetivo fornecedor. Entretanto, alguns Estados-Membros anteciparam-se na produção legislativa, regulando especificamente o fornecimento de conteúdos e serviços digitais, como sucedeu no Reino Unido com as "Consumer Protection (Amendment) Regulations" de 2014.[7]

---

ensaio *Comércio electrónico na sociedade da informação: da segurança técnica à confiança jurídica* (Coimbra, Almedina, 1999) e diversos textos publicados nos *Estudos de Direito do Consumidor*, tais como «A protecção jurídica do consumidor no quadro da directiva sobre o comércio electrónico», «Os pactos atributivos de jurisdição nos contratos electrónicos de consumo», «Comércio electrónico e consumidor», «A via electrónica da negociação (alguns aspectos)», e «Consumer Protection Online (in special the expected changes to e-commerce from S-commerce, VR-Commerce and AR-Commerce)», respetivamente n.º 2 (2000: 43-140), 3 (2001: 281-300), 6 (2004: 341-400), 8 (2007: 275-290), e 14 (2018: 9-19).

[1] Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho (JO L 304 de 22.11.2011, p. 64).

[2] Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019 sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais.

[3] *A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

[4] Em especial a Diretiva (UE) 2019/771 do Parlamento Europeu e do Conselho de 20 de maio de 2019 relativa a certos aspetos dos contratos de compra e venda de bens que altera o Regulamento (UE) 2017/2394 e a Diretiva 2009/22/CE e que revoga a Diretiva 1999/44/CE

[5] Diretiva 1999/44/CE do Parlamento Europeu e do Conselho, de 25 de maio de 1999, relativa a certos aspetos da venda de bens de consumo e das garantias a ela relativas (JO L 171 de 7.7.1999, p. 12).

[6] O diploma interno (DL 67/2003, de 8 de abril, alterado pelo DL 84/2008, de 21 de maio) apesar de alargar a noção de bem consumo aos bens imóveis, limitou os bens móveis aos bens corpóreos (art. 1-b/b e 3). Sobre este regime ver por ex. Paulo Mota Pinto, «Conformidade e garantias na venda de bens de consumo. A Directiva 1999/44/CE e o direito português», *Estudos de Direito do Consumidor*, 2 (2000) 199-331.

[7] Cf. «The new UK consumer agenda and digital content» : <https://www.freshfields.com/492380/globalassets/our-thinking/campaigns/digital/mediainternet/pdf/uk-consumer-agenda-and-digital-content-briefing_aw_not.pdf>. Sobre a problemática da proteção do consumidor nos contratos de fornecimento de conteúdos digitais, ver Natalie Helberger, M.B. Loos, Lucie Guibault, Chantal Mak, Lodewijk Pessers, «Digital Content Contracts for Consumers», *Journal of Consumer Policy* 36/1 (2013) 37-57; Lucie Guibault, Natalie Helberger, *Digital Consumers and the Law: Towards a Cohesive European Framework*, Wolters Kluwer, 2012. Entre nós, com mais referências, Jorge Morais de Carvalho, «Venda de Bens de Consumo e Fornecimento de Conteúdos e Serviços Digitais – As Diretivas 2019/771 e 2019/770 e o seu Impacto no Direito Português», *RED – Revista Eletrónica de Direito* 20/3 (2019) 63-87; sobre a proposta de diretiva, podem ver-se também os nossos «Comércio eletrónico de conteúdos digitais: proteção do consumidor a duas velocidades?» e «Novos direitos do consumidor no mercado único digital», ambos publicados nos *Estudos de Direito do Consumidor*, nº 9 (2015) 177-207 e 10 (2016) 155-174.

1. Não interferência com o direito civil clássico

No direito português não existe ainda um corpo de regras específicas dos contratos de fornecimento de conteúdos e serviços digitais. O Código Comercial de 1888 e o Código Civil de 1966, ambos anteriores à "revolução digital", são omissos nesta matéria e mesmo na legislação do consumidor não abundam referência a estes contratos. E não obstante é ainda o direito nacional que se aplica nas questões não reguladas pela Dir. 2019/770, como a formação, a validade, a nulidade e os efeitos dos contratos ou a legalidade do conteúdo ou serviço digital, como se lê no considerando 12 da diretiva, acrescentando que "A presente diretiva também não deverá determinar a natureza jurídica dos contratos para o fornecimento de conteúdos ou serviços digitais, cabendo ao direito nacional determinar a natureza de um contrato, ou seja, se se trata, por exemplo, de um contrato de venda, de um contrato de serviços, de um contrato de aluguer ou de um contrato sui generis."

Esta é, aliás, uma questão discutida há mais de duas décadas, em especial no que respeita às licenças de software[1] e que não foi objeto de harmonização, ficando antes para o direito interno de cada Estado-Membro, sem prejuízo do regime instituído pela diretiva em ordem à proteção do consumidor e do bom funcionamento do mercado interno. Mas, no fundo, a Dir. 2019/770 pretende interferir o menos possível com o direito civil de cada Estado-Membro, preocupando-se antes em assegurar um elevado nível de defesa do consumidor e a promoção da concorrência no mercado único digital. Dirige-se a problemas concretos experimentados pelos consumidores relativamente à qualidade e ao acesso, pelos consumidores, aos conteúdos e/ou serviços digitais, que podem ser errados ou defeituosos, ou simplesmente inacessíveis. Juntamente com a sua "diretiva gémea" - Dir. 2019/771 -, a Dir. 2019/770 estabelece remédios a favor do consumidor no caso de não cumprimento ou de não conformidade com o contrato (grosso modo, "vícios redibitórios"), acautelando todavia o princípio *favor negotii*, no sentido de a "destruição" destes contratos não ser o primeiro remédio de que o consumidor dispõe.

2. Direitos do consumidor de conteúdos ou serviços digitais contratados à distância previstos no DL 24/2014

A Dir. 2019/770 regula o fornecimento de conteúdos e serviços digitais como contratos de consumo. Por isso, o regime agora aprovado acresce ao já previsto por ex. no DL 24/2014 (alterado por último pelo DL 78/2018, de 15/10) que transpõe a Dir. 2011/83/UE sobre direitos dos consumidores.

Informação pré-contratual sobre funcionalidade e interoperabilidade. Em sede de informação pré-contratual nos contratos celebrados à distância, cabe ao fornecedor indicar a funcionalidade dos conteúdos digitais, incluindo as medidas de proteção

[1] Sobre a possível recondução das licenças de software aos tipos contratuais da compra e venda, da locação e da empreitada, podem ver-se, por ex., os nossos «Programas de computador, sistemas informáticos e comunicações electrónicas: alguns aspectos jurídico-contratuais», *Revista da Ordem dos Advogados* 59/III (1999) 915-1000, e «Das licenças de software e de bases de dados (software and database licenses)», *Revista Jurídica Portucalense* 14 (2011) 9-25.

técnica, e qualquer interoperabilidade relevante dos conteúdos digitais com equipamentos e programas informáticos de que o profissional tenha ou possa razoavelmente ter conhecimento, quando for o caso (art. 4-x/z).

Direito de livre resolução? No fornecimento de conteúdos digitais sem suporte material o prazo para o exercício do direito de livre resolução conta-se a partir do dia da celebração do contrato (art. 10/1-c). E o consumidor não suporta quaisquer custos relativos ao fornecimento, na totalidade ou em parte, de conteúdos digitais que não sejam fornecidos num suporte material, se o consumidor não tiver dado o seu consentimento prévio para que a execução tenha início antes do fim do prazo de 14 dias referido no artigo 10.º e reconhecido que perde com isso o seu direito de livre resolução, ou o fornecedor de bens não tiver fornecido a confirmação do consentimento prévio e expresso do consumidor (art. 15/b).

De qualquer modo, o direito de livre resolução é excluído relativamente aos conteúdos digitais não fornecidos em suporte material se a sua execução tiver início com o consentimento prévio e expresso do consumidor e este reconhecer que o seu consentimento implica a perda do direito de livre resolução (art. 17).

Proibição de cobrança de conteúdos digitais não solicitados. De referir ainda, na lei dos contratos à distância, a proibição de cobrança de pagamento por fornecimento de conteúdos digitais não solicitados (art. 28).

3. Fornecimento de conteúdos ou serviços digitais

Em acréscimo ao regime dos contratos à distância, a Dir. 2019/770 regula, em termos de harmonização completa ou plena (art. 4), os contratos de fornecimento de conteúdos ou serviços digitais em questões como a conformidade com o contrato, os remédios por desconformidade (meios de ressarcimento), e o fornecimento de conteúdos ou serviços digitais. Os direitos estabelecidos têm natureza imperativa a favor do consumidor de conteúdos e serviços digitais (art. 22).

Partes. Quanto às partes, trata-se de contratos entre profissionais e consumidores (contratos de consumo). Por consumidor entende-se a "pessoa singular que[…] atue com fins que não se incluam no âmbito da atividade comercial, empresarial, artesanal ou profissional" (art. 2/6).

Todavia, o preâmbulo da diretiva considera que os Estados-Membros são "livres de alargar a proteção concedida aos consumidores ao abrigo da presente diretiva por forma a abranger pessoas singulares ou coletivas que não sejam consumidores na aceção da presente diretiva, como, por exemplo, as organizações não-governamentais, as empresas em fase de arranque (start-ups) ou PME" (considerando 16). A Dir. 2019/770 mostra-se favorável ao alargamento dos remédios especiais de proteção do consumidor a outras entidades que ficam fora da noção de consumidor, mas que ainda assim podem ter uma necessidade de proteção semelhante à dos consumidores enquanto parte mais vulnerável (ou "hiposuficiente", como se diz no Brasil).

Objeto. O objeto é composto por conteúdos e serviços digitais, incluindo o carregamento e partilha de conteúdos gerados pelo consumidor. O preâmbulo da diretiva (considerando 19) ilustra exemplificativamente a noção de conteúdos e serviços digitais com os programas informáticos, as aplicações, os ficheiros de vídeo, de áudio e de música, os jogos digitais, os livros eletrónicos e outras publicações eletrónicas, por um lado (por ex. "Netflix", "Spotify"), e os serviços digitais que permitem a criação, o tratamento ou o armazenamento de dados em formato digital ou o acesso aos mesmos (e.g. o software enquanto serviço - SaS) tais como a partilha de ficheiros de vídeo e áudio e outro tipo de alojamento de ficheiros (por ex. "YouTube"), o processamento de texto ou jogos disponibilizados no ambiente de computação em nuvem (por ex. "Dropbox", "Google Drive"), e as redes sociais (e.g. "Facebook", "Instagram", "Twitter"). Quanto aos modos de fornecimento dos conteúdos ou serviços digitais, distinguem-se o suporte material (e.g. DVD, CD, chaves USB e cartões de memória), o descarregamento feito pelos consumidores para os seus dispositivos (*download*), a difusão em linha (*streaming*), o acesso e a utilização de redes sociais e de "armazéns" de conteúdos digitais[1].

Não abrange os conteúdos ou serviços digitais incorporados em ou interligados com bens e que sejam fornecidos com os bens nos termos de um contrato de compra e venda desses bens, independentemente de os conteúdos ou serviços digitais serem fornecidos pelo profissional ou por um terceiro, *presumindo-se, em caso de dúvida, que estão abrangidos pelo contrato de compra e venda* (art. 3/4). A venda de equipamentos, como telemóveis, televisões ou relógios inteligentes com aplicações normalizadas pré-instaladas e fornecidas nos termos do contrato de compra e venda (e.g. aplicações de alarme ou de câmara), é regulada pela Dir. 2019/771. Esta diretiva sobre garantias na venda de bens de consumo aplica-se não apenas aos tradicionais bens corpóreos, mas igualmente aos «bens com elementos digitais», isto é, "todos os conteúdos ou serviços digitais incorporados ou interligados com esses bens, de tal forma que a ausência desse conteúdo ou serviço digitais impediria os bens de desempenhar as suas funções. Os conteúdos digitais incorporados ou interligados com os bens podem ser quaisquer dados produzidos ou fornecidos em formato digital, tais como sistemas operativos, aplicações e qualquer outro software. O conteúdo digital pode estar pré-instalado no momento da celebração do contrato de venda ou, nos termos desse contrato, ser instalado posteriormente. Os serviços digitais interligados com um bem podem incluir serviços que permitem criar, tratar, aceder ou armazenar dados em formato digital, tais como o software enquanto serviço disponibilizado no ambiente de computação em nuvem, o fornecimento contínuo de dados de tráfego num sistema de navegação [GPS], ou o fornecimento contínuo de programas de treino personalizado no caso dos relógios inteligentes"[2]. O preâmbulo esclarece ainda que "Se, por exemplo, uma televisão inteligente tiver sido anunciada como incluindo uma determinada aplicação de vídeo, considerar-se-á que tal aplicação faz parte do contrato de compra e venda. Esta solução

[1] Sobre os acordos de nível de serviço na computação em nuvem (*Cloud Computing Service Level Agreements* – SLA) pode ver-se o nosso «Cloud Computing», *Boletim da Faculdade de Direito* 92/1 (2017) 367-401.

[2] Considerando 14 da Dir. 2019/771.

deverá aplicar-se independentemente de os conteúdos ou serviços digitais estarem pré-instalados nos próprios bens ou terem de ser descarregados posteriormente noutros dispositivos e estarem apenas interligados aos bens. […] Tal deverá aplicar-se também se os conteúdos ou serviços digitais incorporados ou interligados não forem fornecidos pelo próprio vendedor, mas sim, nos termos do contrato de compra e venda, por terceiros. A fim de evitar incertezas para os operadores e para os consumidores relativamente à questão de saber se o fornecimento dos conteúdos ou serviços digitais faz parte do contrato de compra e venda, deverão aplicar-se as regras da presente diretiva. […]Em contrapartida, se a falta de conteúdos ou serviços digitais incorporados ou interligados não impedir os bens de desempenharem as suas funções ou se o consumidor celebrar um contrato de fornecimento de conteúdos ou serviços digitais que não faça parte de um contrato de compra e de bens com elementos digitais, esse contrato deverá considerar-se distinto do contrato de compra e venda dos bens, mesmo que o vendedor atue como intermediário nesse segundo contrato com o operador terceiro, e poderá estar abrangido pelo âmbito de aplicação da Diretiva (UE) 2019/770 se estiverem preenchidas as condições nela previstas. Por exemplo, se o consumidor descarregar uma aplicação de jogo de uma loja de aplicações para um telemóvel inteligente, o contrato de fornecimento da aplicação de jogo é distinto do contrato de compra e venda do próprio telemóvel inteligente. […] Outro exemplo é o caso em que é expressamente acordado que o consumidor compra um telemóvel inteligente sem um sistema operativo específico e posteriormente celebra com um terceiro um contrato para o fornecimento de um sistema operativo."[1]

Assim, uma coisa é o contrato de compra e venda do próprio telemóvel inteligente, incluindo o respetivo suporte lógico, outra é o fornecimento por terceiro de sistema operativo, aplicações ou jogos que não sejam indispensáveis para o bom funcionamento do bem vendido (e.g. computador, telemóvel, televisor ou relógio "smart").

Por outro lado, a Dir. 2019/770 não se aplica aos serviços de comunicações eletrónicas[2], saúde, jogos a dinheiro (lotarias, apostas, casino, póquer), serviços financeiros, software livre, e transmissões cinematográficas digitais. Relativamente à saúde importa referir que, nos termos do preâmbulo, a exclusão dos «cuidados de saúde» abrange quaisquer conteúdos ou serviços digitais que constituam um dispositivo médico sempre que esse dispositivo médico seja prescrito ou fornecido por um profissional de saúde, mas já não a todo e qualquer conteúdo ou serviço digital que constitua um dispositivo médico, como, por exemplo, aplicações de saúde, que possa ser obtido pelo consumidor sem prescrição ou fornecimento por um profissional de saúde[3].

[1] Considerandos 15 e 16 da Dir. 2019/771.

[2] Nessa medida, os contratos de fornecimento de serviços e conteúdos digitais não são abrangidos pela Lei 23/96, de 26 de julho (alterada), que regula o fornecimento de serviços públicos essenciais, incluindo os serviços de comunicações eletrónicas, prevendo normas como o dever de os prestadores destes serviços informarem regularmente, de forma atempada e eficaz, os utentes sobre as tarifas aplicáveis aos serviços prestados, designadamente as respeitantes às redes fixa e móvel, ao acesso à Internet e à televisão por cabo (art. 4/3) e a proibição de suspensão da prestação do serviço sem pré-aviso adequado, salvo caso fortuito ou de força maior (art. 5/1 – norma que, de resto, não se aplica aos serviços de comunicações eletrónicas – art. 5/5).

[3] Considerando 29 da Dir. 2019/771.

4. Onerosidade: os dados pessoais como possível moeda

O fornecimento dos conteúdos ou serviços é normalmente oneroso, isto é, prestado em troca pelo pagamento de um preço, incluindo o dinheiro ou uma representação digital do valor que é devido pelos conteúdos ou serviços digitais fornecidos (incluindo dados pessoais). Os conteúdos e serviços digitais são fornecidos muitas vezes de forma gratuita ou em troca por representações digitais de valor, como os vales ou cupões eletrónicos. Tais representações digitais de valor, incluindo moedas virtuais (bitcoins), são consideradas um meio de pagamento, embora o reconhecimento das bitcoins dependa do direito nacional.[1] Os dados pessoais surgem como moeda de pagamento quando o consumidor permite que o fornecedor dos serviços digitais retire proveitos desses dados, i.e., como se escreve no preâmbulo quando "o consumidor abre uma conta nas redes sociais e indica um nome e um endereço de correio eletrónico que são utilizados para outros fins que não apenas o fornecimento de conteúdos ou serviços digitais ou o cumprimento dos requisitos legais"[2], o mesmo valendo para o consentimento do consumidor relativamente a todo o tipo de material que constitua dados pessoais, como fotografias ou mensagens que irá carregar, posteriormente processado pelo profissional para fins de comercialização.

Enquanto responsável pelo tratamento de dados, o fornecedor deve cumprir os deveres previstos no Regulamento Geral sobre a Proteção de Dados (RGPD)[3] e na lei interna de execução do RGPD[4]. Já as atividades pessoais ou domésticas não são abrangidas: o RGPD "não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas."[5]

---

[1] Segundo o Banco de Portugal, a aceitação de moeda virtual pelo seu valor nominal não é obrigatória, os direitos de reembolso ao consumidor não estão legalmente protegidos no caso de pagamento com moedas virtuais, não existe fundo que cubra sua desvalorização, para além de poderem ser utilizadas indevidamente em atividades criminosas, incluindo de branqueamento de capitais e de financiamento do terrorismo. o Banco de Portugal esclarece que "as entidades que emitem e comercializam moedas virtuais não estão sujeitas a qualquer obrigação de autorização ou de registo junto do Banco de Portugal, pelo que a sua atividade não é sujeita a qualquer tipo de supervisão prudencial ou comportamental" e, por isso, na sua Carta Circular nº 11/2015/DPG, recomenda às instituições de crédito, às instituições de pagamento e às instituições de moeda eletrónica sujeitas à sua supervisão que se abstenham de comprar, deter ou vender moedas virtuais – ver <https://www.bportugal.pt/page/moedas-virtuais>

[2] Considerando 24 da Dir. 2019/770.

[3] 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. Sobre isto pode ver-se o nosso «O Responsável pelo Tratamento de Dados segundo o RGPD (Data Controller According to the GDPR)», *Revista de Direito e Tecnologia* 1/2 (2019) 143-173.

[4] Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.

[5] **C**onsiderando (18) do RGPD.

Assim, por ex., os utilizadores de redes sociais como o "Facebook" ou o "Twitter", não estão sujeitos ao RGPD, mas a empresa "Facebook Inc." já é considerada responsável pelo tratamento de dados para efeitos do RGPD. Ora, como o regulamento não prejudica a aplicação da Dir. 2000/31/CE sobre, nomeadamente, responsabilidade dos prestadores intermediários de serviço previstas nos seus artigos 12 a 15 (art. 2/4), os operadores de redes sociais ou de plataformas de partilha de conteúdos em linha não são considerados prestadores intermediários de serviços para efeitos desses artigos[1].

5. Princípio da pontualidade e princípio da conformidade com o contrato

Regem os princípios gerais do fornecimento *sem demora indevida* (art. 5/1) e *em conformidade com o contrato*, e sobre o profissional recai o ónus da prova do fornecimento dos conteúdos ou serviços digitais (art. 12/1).

A conformidade afere-se subjetivamente por diversos fatores (art. 7), quais sejam: a) correspondência à descrição, quantidade, qualidade, funcionalidade, compatibilidade, interoperabilidade e demais características exigidas pelo contrato; b) adequação à finalidade específica pretendida pelo consumidor; c) fornecimento juntamente com os acessórios e instruções de instalação e apoio ao cliente; d) atualização dos conteúdos.

Quanto a requisitos de conformidade objetiva, destacam-se: a) a adequação às utilizações a que os conteúdos ou serviços digitais do mesmo tipo normalmente se destinam; b) quantidade, qualidades, características de desempenho, inclusive no que respeita à funcionalidade, compatibilidade, acessibilidade, continuidade e segurança, correspondentes às habituais em conteúdos ou serviços digitais do mesmo tipo e que o consumidor possa razoavelmente esperar, dada a natureza do conteúdo ou serviço digital e tendo em conta qualquer declaração pública feita pelo profissional ou em nome deste, ou por outras pessoas em estádios anteriores da cadeia contratual, particularmente através de publicidade ou rotulagem[2] (valor negocial da publicidade); c) fornecimento juntamente com os acessórios e as instruções que o consumidor possa razoavelmente esperar receber; e d) conformidade com quaisquer versões de teste ou pré-visualizações dos conteúdos ou serviços digitais disponibilizadas pelo profissional antes da celebração do contrato.

6. Direito às atualizações e direito à integração correta dos conteúdos e serviços digitais

O consumidor tem o direito a ser informado sobre as atualizações e ao fornecimento das mesmas, incluindo atualizações de segurança[3] (art. 8/2), e o direito à conformidade

[1] Sobre tema, Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista Bolsa, Banca e Seguros* 3 (2018) 215-6, em nota.

[2] Ver, a propósito do possível valor da publicidade, o disposto no artigo 7/5 da Lei do Consumidor, aprovada pela Lei 24/96, de 31 de julho (várias vezes alterada, a última pela Lei 63/2019, de 16 de agosto), nos termos do qual: " As informações concretas e objetivas contidas nas mensagens publicitárias de determinado bem, serviço ou direito consideram-se integradas no conteúdo dos contratos que se venham a celebrar após a sua emissão, tendo-se por não escritas as cláusulas contratuais em contrário."

[3] A segurança informática ("cibersecurity") tem um "papel vital" para as redes e a informação, sendo objeto de um regime específico, que também aproveita aos consumidores, estabelecido pela Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, transposta para o direito interno pela Lei 46/2018,

com a versão mais recente dos conteúdos ou serviços digitais disponíveis no momento da celebração do contrato (art. 8/6).[1]

Além disso, o consumidor tem direito à integração incorreta dos conteúdos ou serviços digitais (art. 9). Nos termos do preâmbulo (considerando 40): "O conceito de funcionalidade deverá entender-se por referência ao modo como os conteúdos ou serviços digitais podem ser usados. Por exemplo, a ausência ou presença de restrições técnicas, como a proteção através da gestão dos direitos digitais ou de codificação regional podem ter um impacto sobre a capacidade dos conteúdos ou serviços digitais para desempenhar a totalidade das suas funções, tendo em conta a respetiva finalidade. O conceito de interoperabilidade respeita a se, e em que medida, os conteúdos ou serviços digitais são capazes de funcionar com hardware ou software diferente dos que normalmente são usados com conteúdos ou serviços digitais do mesmo tipo. O bom funcionamento incluirá, por exemplo, a capacidade dos conteúdos ou serviços digitais para trocarem informações com outro software ou hardware e para utilizarem as informações trocadas."

7. "Remédios para a quebra do contrato" por não fornecimento ou por falta de conformidade

A Dir. 2019/770 prevê ainda como direitos do consumidor os chamados remédios para a quebra do contrato (*breach of contract remedies*). Em caso de *não fornecimento* (art. 13), o consumidor pode solicitar ao profissional o fornecimento dos conteúdos ou serviços digitais sem demora indevida, ou num prazo adicional convencionado entre as partes; no caso de o fornecedor não cumprir novamente, o consumidor pode rescindir o contrato; mas o direito à rescisão é imediato se o profissional tiver declarado, ou resultar claramente das circunstâncias, que não irá fornecer os conteúdos ou serviços digitais, ou que o momento específico do fornecimento é essencial para o consumidor, e o profissional não fornecer os conteúdos ou serviços digitais até esse momento ou nesse momento.[2]

Em caso de *falta de conformidade*, o consumidor tem direito a que os conteúdos ou serviços digitais sejam repostos em conformidade (a título gratuito e sem inconvenientes importantes para si), a beneficiar de uma redução proporcional do preço ou a rescindir o contrato (art. 14). Se a reposição dos conteúdos ou serviços digitais em

---

de 13 de agosto (regime jurídico da segurança do ciberespaço). Sobre o tema pode ver-se o nosso «A proteção dos dados pessoais e o direito à segurança informática no comércio eletrónico», *Revista Banca, Bolsa e Seguros* 3 (2018) 303-329.

[1] Nos termos do preâmbulo, "(44) Uma vez que os conteúdos digitais e serviços digitais estão em constante evolução, os profissionais podem acordar com os consumidores o fornecimento de atualizações e características à medida que estas ficarem disponíveis. Por conseguinte, a conformidade dos conteúdos ou serviços digitais deverá também ser avaliada em relação à atualização dos mesmos de acordo com o estipulado no contrato. A não disponibilização de atualizações que tenham sido acordadas no contrato deverá ser considerada uma falta de conformidade dos conteúdos ou serviços digitais. Além disso, as atualizações defeituosas ou incompletas deverão também ser consideradas uma falta de conformidade dos conteúdos ou serviços digitais, visto que tal significaria que essas atualizações não são executadas de acordo com o estipulado no contrato."

[2] A essencialidade do prazo de fornecimento pode ser o caso, por ex., de o consumidor contratar o serviço por ocasião do Campeonato Europeu de Futebol.

conformidade for impossível ou impuser ao profissional custos desproporcionados, o consumidor terá apenas direito à redução proporcional do preço ou à rescisão do contrato, podendo todavia exercer estes direitos se a gravidade da falta de conformidade o justificar ou se o profissional tiver declarado, expressa ou tacitamente, que não irá repor os conteúdos ou serviços digitais em conformidade num prazo razoável ou sem inconvenientes importantes para o consumidor. Sendo fornecimento oneroso, o consumidor só tem direito a rescindir o contrato se a falta de conformidade não for menor, presumindo-se todavia que não é menor (art. 14/6).

O consumidor pode ainda lançar mão dos remédios por falta de conformidade se a não conformidade dos conteúdos ou serviços digitais resultar de infrações a direitos de terceiros, em especial direitos de propriedade intelectual, a menos que o direito nacional determine a nulidade ou a rescisão do contrato de fornecimento de conteúdos ou serviços digitais nesses casos (art. 10). Por ex. se os serviços forem bloqueados por razões de direitos de autor o consumidor pode ver a sua tarifa reduzida ou então rescindir o contrato, se o serviço não lhe interessar sem os conteúdos bloqueados. A este propósito interessa referir que a Diretiva sobre direitos de autor e direitos conexos no mercado único digital (doravante Dir. 2019/790)[1] entre outros aspetos estabelece um conjunto de medidas com vista ao "funcionamento correto do mercado dos direitos de autor", como sejam um direito conexo sobre publicações de imprensa relativamente a utilizações em linha por prestadores de serviços da sociedade da informação, e esclarece que a partilha de conteúdos em linha pelos utilizadores desses serviços implica atos de reprodução e de comunicação ao público e nessa medida depende de autorização do titular de direitos de autor". Os serviços de partilha de conteúdos em linha não são considerados serviços de armazenamento em servidor para efeitos da limitação de responsabilidade prevista no art. 14 /1 da Dir. 2000/31 sobre comércio eletrónico[2]. De todo o modo, ficam excluídos os utilizadores que não atuem com caráter comercial ou cuja atividade não gere receitas significativas; para promover a concorrência com as grandes plataformas prevê-se um regime especial para as *start-up* PME, além de se salvaguardar a liberdade de expressão.[3]

De notar que a Dir. 2019/770 "não prejudica o direito de distribuição aplicável a tais bens nos termos da legislação em matéria de direitos de autor", "incluindo a portabilidade dos serviços de conteúdos em linha" (considerando 20 e 36, *in fine*, e art. 3/9). A portabilidade é consagrada num regulamento específico[4]. Relativamente ao direito de distribuição, discute-se o seu esgotamento no caso de fornecimento por

[1] Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera a Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à proteção jurídica das bases de dados e a Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de maio de 2001, relativa à harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação.

[2] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno.

[3] Sobre esta diretiva pode ver-se o nosso «Os direitos de autor no mercado único digital segundo a diretiva 2019/790», Revista de Direito Intelectual, 2019/2.

[4] Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho de 14 de junho de 2017 relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno.

transmissão digital. A diretiva dos direitos de autor mercado único digital não respondeu a esta questão. Pese embora o modelo de negócio das plataformas de vídeo a pedido e de partilha de conteúdos funcionar sobretudo em termos de *streaming*, isso não impede que continue o modelo alternativo da compra de exemplares digitais para livre utilização, independente de ligação à rede e de um serviço associado, e o interesse na possibilidade de revenda desses exemplares, em virtude do esgotamento do direito de distribuição, à semelhança do que é permitido, segundo o Tribunal de Justiça da União Europeia, ao abrigo do regime dos programas de computador[1]. Recentemente, o Advogado-Geral manifestou-se, *de iure condito,* pelo não esgotamento do direito de esgotamento face à Dir. 2001/29, mas deixando a questão em aberto *de lege ferenda.*[2] A ser assim, o regime dos conteúdos e serviços digitais será dualista, consoante se trate de programas de computador ou de outros bens digitais, embora nos pareça que o esgotamento é sustentável desde já relativamente aos bens digitais incorporados nos chamados "bens com elementos digitais" (telemóveis, relógios ou televisores "smart").

8. Exercício do direito de rescisão e seus efeitos

A rescisão exerce-se mediante declaração pelo consumidor ao profissional (art. 15), o qual deve reembolsar o consumidor de todos os montantes pagos no âmbito do contrato, relativos ao período durante o qual teve lugar a não conformidade, salvo no fornecimento oneroso e duradouro em que o reembolso é limitado ao proporcional do preço pago correspondente ao período de não conformidade e a eventual antecipação (art. 16/1). O prazo de reembolso é de 14 dias após a redução do preço ou cessação do contrato e deve ser livre de encargos (art. 18).

Além do reembolso, o profissional deve ainda abster-se de utilizar quaisquer conteúdos, que não sejam dados pessoais, que tenham sido facultados ou criados pelo consumidor aquando da utilização dos conteúdos ou serviços digitais fornecidos pelo profissional (art. 16/3), assistindo ao consumidor o direito de recuperar esses conteúdos digitais, a título gratuito e sem entraves por parte do profissional, num prazo razoável e num formato de dados de uso corrente e de leitura automática (art. 16/4). De igual modo, após a rescisão do contrato, o consumidor deve abster-se de utilizar os conteúdos ou serviços digitais e de colocá-los à disposição de terceiros (art. 17/1), podendo o profissional impedir qualquer utilização posterior, em especial tornando-os inacessíveis ao consumidor ou desativando a sua conta de utilizador (art. 16/5).

9. Direito de alteração dos conteúdos ou serviços digitais

[1] Acórdão TJUE, de 3 de julho de 2012, proc. C-128/11 (*UsedSoft*).

[2] Nas conclusões apresentadas, em 10 de setembro de 2019, no proc. C-263/18 (*Nederlands Uitgeversverbond*), apesar de "concluir que existem argumentos jurídicos e teleológicos a favor do reconhecimento da regra do esgotamento do direito de distribuição no que diz respeito às obras fornecidas por transferência (*download*) para uma utilização permanente", o Advogado-Geral Maciej Szpunar entende que, "no estado atual do direito da União […] o fornecimento de livros eletrónicos por transferência (*download*) para utilização permanente não se enquadra no direito de distribuição […] mas do direito de comunicação ao público". Ver sobre o tema, por ex., o nosso *Informática, direito de autor e propriedade tecnodigital*, Coimbra, Coimbra Editora, 2001.

No caso de fornecimento duradouro, o profissional pode alterar os conteúdos ou serviços digitais para além do necessário para manter os conteúdos ou serviços digitais em conformidade, se o contrato estipular razão válida para a alteração, se esta for feita sem custos adicionais para o consumidor e notificada de forma clara e compreensível ao consumidor, com antecedência razoável, num suporte duradouro, das características e do momento das alterações, informando-o também do seu direito de rescisão no caso de impacto substancial ou da possibilidade de manter os conteúdos ou serviços digitais inalterados, em conformidade, sem custos adicionais (art. 19/1). Sendo que o consumidor tem direito a rescindir o contrato gratuitamente se a alteração tiver um impacto negativo no acesso ou na utilização, por si, dos conteúdos ou serviços digitais, a menos que tal impacto seja apenas menor. O prazo para rescindir o contrato é de 30 dias a contar da data de receção da notificação ou do momento em que os conteúdos ou serviços digitais foram alterados pelo profissional, consoante a data que for posterior (art. 19/2).

A diretiva fala em alteração dos conteúdos ou serviços, mas pode o prestador de serviços e/ou fornecedor de conteúdos reservar o direito de descontinuar o serviço a qualquer momento e mesmo sem justificação? Lê-se, por ex. nos termos de serviço do Google, que "O Google também poderá deixar de prestar os Serviços a você ou, incluir ou criar novos limites a nossos Serviços a qualquer momento." Sendo objetivo da diretiva proteger o consumidor, seria desejável acautelar a sua posição face a ruturas bruscas e injustificadas do serviço. Imagine-se o dano em massa à escala global se o Google descontinuasse os seus serviços sem aviso prévio!

10. Responsabilidade objetiva do fornecedor de conteúdos e serviços digitais?

Será aplicável ao fornecedor de conteúdos e serviços digitais o regime da responsabilidade do produtor por danos causados aos consumidores por produtos defeituosos?

A questão está de novo na ordem do dia.[1] A Comissão Europeia elaborou um documento[2] nos termos do qual não existem dados suficientes para concluir com segurança sobre a necessidade de alargar a diretiva da "Product Liability" aos desenvolvimentos tecnológicos trazidos pelas aplicações informática (software), objetos

[1] Ver, por ex., Geraint Howells, Christian Twigg-Flesner, Chris Willett, «Product Liability and Digital Products», *EU Internet Law*, ed. T. Synodinou *et al.*, Springer, Cham, 2017, 183-195, sustentando que os produtos não tangíveis, tais como aplicativos e outro software não fornecidos em um meio tangível, seriam produtos para efeitos da diretiva sobre responsabilidade do produtor. O artigo faz uma distinção crucial entre informações (de forma tangível ou não tangível) que não devem gerar responsabilidade e produtos tangíveis ou não tangíveis que não se limitam à mera prestação de informações e cujos defeitos podem causar danos materiais, devendo estes últimos ser abrangidos pela Diretiva 85/374/CEE em matéria de responsabilidade decorrente de produtos defeituosos, transposta pelo DL 383/89, de 6 de novembro (com alterações). Entre nós, Henrique Sousa Antunes, «Responsabilidade civil do produtor: os danos ressarcíveis na era digital», *Revista de Direito da Responsabilidade* 1 (2019) 1476-1485.

[2] Commission Staff Working Document, Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products - Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) - SWD(2018)157 final.

interligados em termos de IoT ("Internet of Things") e sistema autónomos[1]. De igual modo, não é claro que a vulnerabilidade do software face a ataques cibernéticos ou falhas na atualização de software de segurança devam ser consideradas defeito nos termos da diretiva. O documento constata a divergência doutrinal sobre a qualificação do software como produto para efeitos da diretiva [2] e indica jurisprudência do TJUE segundo a qual o software pode ser um dispositivo médico se for destinado pelo produtor a ser usado especificamente para um ou mais fins médicos. Nesse sentido, o atual Regulamento dos dispositivos médicos[3] inclui expressamente o software na lista de possíveis "dispositivos médicos" (art. 2), esclarecendo o preâmbulo que "o *software*, por si só, é qualificado como dispositivo médico quando especificamente destinado pelo fabricante a ser utilizado para um ou vários fins médicos indicados na definição de dispositivo médico, ao passo que o *software* de uso geral, mesmo quando utilizado num contexto de saúde, ou o *software* previsto para fins relacionados com o estilo de vida e o bem-estar, não são um dispositivo médico. A qualificação de um *software*, quer como dispositivo quer como acessório, deverá ser independente da localização do *software* ou do tipo de interconexão entre este e um dispositivo" (considerando 19).

Mais acrescenta o referido documento de trabalho da Comissão que o software é um componente de muitos produtos e que o produtor responde pelo produto final como um todo, concluindo que "for products which include software at the moment they were put into circulation by the producer, the Directive could address liability claims for damages caused by defects in this software. The more open nature of new products, where the producer is no longer able to control software or other technical features subsequently installed in or learned by the product may however pose a challenge for establishing claims under the Directive. / In conclusion, while there is little evidence of practical problems, the distinction between products and services may in the future no longer be pertinent. Hence, there is a need to clarify what products and features are covered by the Directive."[4]

11. Conclusão

No âmbito realização do mercado único digital foi identificada uma lacuna de proteção do consumidor de serviços e conteúdos digitais suscetível de prejudicar o bom funcionamento do mercado interno. Nesse sentido, o acervo da União Europeia sobre proteção do consumidor no comércio eletrónico, constituído nomeadamente pelas diretivas 2000/31 e 2011/83, foi reforçado pela Dir. 2019/770 sobre os contratos de fornecimento de conteúdos e serviços digitais, juntamente com outras medidas, em especial sua diretiva gémea, a Dir. 2019/771 sobre os contratos de compra e venda, que

[1] SWD(2018)157 final, p. 123

[2] Ver, entre nós, João Calvão da Silva, *Responsabilidade civil do produtor*, Coimbra: Almedina, 1990, 609-614 (considerando que "A definição de produto, contida no art. 3.º, abrange os suportes materiais em que a obra intelectual se materializa, fixa e comunica, pois são coisas móveis corpóreas, embora inconfundíveis com a obra intelectual em si — bem imaterial" – p. 613); pode ver-se também o nosso *Comércio electrónico na sociedade da informação*, cit., 110 s.

[3] Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho de 5 de abril de 2017 relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) 178/2002 e o Regulamento (CE) 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho.

[4] SWD(2018)157 final, p. 52.

revogou e substituiu a Dir. 1999/44 sobre as garantias na venda de bens de consumo. A diretiva sobre contratos de fornecimento de conteúdos e serviços digitais não pretende harmonizar questões internas do direito civil, desde logo a qualificação destes contratos nos tipos contratuais legais. Não obstante, consagra direitos do consumidor no caso de não fornecimento e de não conformidade dos conteúdos ou dos serviços com o contrato. Os remédios para a "quebra do contrato" integram imperativamente o conteúdo destes contratos, qualquer que seja a sua ordenação na tipologia legal dos contratos, prevalecendo, enquanto lei especialíssima, nas relações de consumo e podendo até ser alargada a outros sujeitos que possam justificar proteção semelhante.

Todavia, alguns aspetos não foram regulados, como sejam o esgotamento do direito de distribuição na propriedade intelectual, ou a aplicação da responsabilidade do produtor ao fornecedor de conteúdos e serviços digitais. É expetável que surjam novos desenvolvimentos sobre estas matérias, que face à harmonização completa estabelecida, surgirão primeiro no direito da União Europeia, reforçando a sua "soberania regulatória" na Internet[1].

Bibliografia

ANTUNES, Henrique Sousa, «Responsabilidade civil do produtor: os danos ressarcíveis na era digital», *Revista de Direito da Responsabilidade* 1 (2019) 1476-1485

BANCO DE PORTUGAL, «Moedas Virtuais» <https://www.bportugal.pt/page/moedas-virtuais>

BARBOSA, Mafalda Miranda, «Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil», *Revista Bolsa, Banca e Seguros,* n.º 3 (2018) 147 - 216

BARBOSA, Mafalda Miranda, «Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil», *Revista Bolsa, Banca e Seguros,* n.º 3 (2018) 215-6

CARVALHO, Jorge Morais de, «Venda de Bens de Consumo e Fornecimento de Conteúdos e Serviços Digitais – As Diretivas 2019/771 e 2019/770 e o seu Impacto no Direito Português», *RED – Revista Eletrónica de Direito* 20/3 (2019) 63-87

EUROPEAN COMMISSION, «Digital contract rules» <https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/digital-contract-rules_en>

EUROPEAN COMMISSION, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

EUROPEAN COMMISSION, Staff Working Document, Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products - Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and

[1] Sobre esta problemática pode ver-se o nosso «Direito ciberespacial: "soft law" ou "hard law"? *Estudos em Homenagem ao Prof. J.J. Gomes Canotilho*, org. Alves Correira, Jónatas Machado, João Loureiro, vol. III, Coimbra Editora, 2012, p. 685-710, com mais referências.

administrative provisions of the Member States concerning liability for defective products (85/374/EEC) - SWD(2018)157 final.

FRESHFIELDS. «The new UK consumer agenda and digital content» https://www.freshfields.com/492380/globalassets/our-thinking/campaigns/digital/mediainternet/pdf/uk-consumer-agenda-and-digital-content-briefing_aw_not.pdf

GUIBAULT, Lucie, HELBERGER, Natalie, *Digital Consumers and the Law: Towards a Cohesive European Framework*, Wolters Kluwer, 2012

HELBERGER, Natalie, LOOS, M.B., GUIBAULT, Lucie, MAK, Chantal, PESSERS, Lodewijk, «Digital Content Contracts for Consumers», *Journal of Consumer Policy* 36/1 (2013) 37-57

HOWELLS, Geraint, TWIGG-FLESNER, Christian, WILLET, Chris, «Product Liability and Digital Products», *EU Internet Law* (ed. T. Synodinou *et al.)*, Springer, Cham, 2017, 183-195

PEREIRA, Alexandre L. Dias Comércio electrónico na sociedade da informação: da segurança técnica à confiança jurídica. Coimbra, Almedina, 1999

- «Programas de computador, sistemas informáticos e comunicações electrónicas: alguns aspectos jurídico-contratuais», *Revista da Ordem dos Advogados* 59/III (1999) 915-1000

- «A protecção jurídica do consumidor no quadro da directiva sobre o comércio electrónico», Estudos de Direito do Consumidor, n.º 2 (2000) 43-140)

- *Informática, direito de autor e propriedade tecnodigital*, Coimbra, Coimbra Editora, 2001

- «Os pactos atributivos de jurisdição nos contratos electrónicos de consumo», n.º 3 (2001) 281-300)

- «Comércio electrónico e consumidor», Estudos de Direito do Consumidor, n.º 6 (2004) 341-400

- «A via electrónica da negociação (alguns aspectos)», Estudos de Direito do Consumidor, n.º 8 (2007) 275-290

- «Das licenças de software e de bases de dados (software and database licenses)», *Revista Jurídica Portucalense* 14 (2011) 9-25.

- «Comércio eletrónico de conteúdos digitais: proteção do consumidor a duas velocidades?» *Estudos de Direito do Consumidor*, n.º 9 (2015) 177-207

- «Novos direitos do consumidor no mercado único digital», Estudos de Direito do Consumidor, n.º 10 (2016) 155-174.

- «Cloud Computing», *Boletim da Faculdade de Direito de Coimbra*, vol. 92/1 (2017) 367-401.

- «A proteção dos dados pessoais e o direito à segurança informática no comércio eletrónico», *Revista Banca, Bolsa e Seguros* n.º 3 (2018) 303-329.

- «Consumer Protection Online (in special the expected changes to e-commerce from S-commerce, VR-Commerce and AR-Commerce)», Estudos de Direito do Consumidor, n.º 14 (2018) 9-19

- «Comunicação ao público: um «grande direito» na jurisprudência do Tribunal de Justiça da União Europeia?», *Boletim da Faculdade de Direito* 94/II (2018) 1399-1411

- «O Responsável pelo Tratamento de Dados segundo o RGPD (Data Controller According to the GDPR)», *Revista de Direito e Tecnologia* 1/2 (2019) 143-173.

- «Os direitos de autor no mercado único digital segundo a diretiva 2019/790», Revista de Direito Intelectual, 2019/2 (no prelo).

PINTO, Paulo Mota, «Conformidade e garantias na venda de bens de consumo. A Directiva 1999/44/CE e o direito português», Estudos de Direito do Consumidor, N.º 2 (2000) 199-331

SILVA, João Calvão da, *Responsabilidade civil do produtor*, Coimbra: Almedina, 1990

SZPUNAR, Maciej, Conclusões apresentadas pelo Advogado-Geral em 10 de setembro de 2019, no proc. C-263/18 (*Nederlands Uitgeversverbond*)

Jurisprudência

Tribunal de Justiça da União Europeia, acórdão de 29.11.2017, proc. C-265/16 (VCAST)

- TJUE, acórdão de 3.7.2012, proc. C-128/11 (*UsedSoft*).
- TJUE, Acórdão de 14.6.2017, proc. C-610/15 (Ziggo- "The Pirate Bay")
- TJUE, acórdão de 26.4.2017, proc. C-527/15 (Filmspeler).
- TJUE, acórdão de 8.9.2016, proc. C-160/15 (GS Media - "Playboy")

INTELIGÊNCIA ARTIFICIAL E DECISÃO JURISPRUDENCIAL*

Sumário: 1. Do mito de Golem ao «Dr Iuris Computer». *2. If, then – unless or else?* 3. «Virtualidades entrópicas» da IA. 4. Novos princípios e decisão *contra legem*. 5. Validação científica, causalidade e arbitrariedade. 6. O código-fonte constitucional na sociedade de risco. 7. Interpretação da lei em conformidade com os princípios. 8. A criação jurisprudencial do Direito. 9. O papel da Inteligência Artificial e os limites da tecnologia. Referências.

1. Do mito de Golem ao «Dr Iuris Computer»

O progresso científico-tecnológico promete continuar o processo revolucionário, nomeadamente através da tecnologia bioinformática, anunciando-se o ciborgue (Dufresne 1999) com o "casamento de computadores e genes" (Rifkin 2000: 210s), prevendo-se que os "os computadores da segunda metade deste século pouco terão a ver com os computadores de hoje" (Costa & Simões 2004: 562).

No domínio da justiça e da realização do direito, a informatização do processo decisório administrativo e judicial é já uma realidade, não apenas no processamento e transmissão de dados, mas também - e sobretudo – na solução de casos. Conseguirá a engenharia informática desenvolver a inteligência artificial emulando o *modus operandi* do *logos* jurídico e realizando, no Direito, o mito de Golem (1580), que "reaparece na «sociedade de informação» de N. Wiener, o pai da Cibernética", matemático, com a sua *Cybernetic or the Control and Communication in the Animal and the Machine* (1948)"? (B. Pereira 1996, 51). Evocando um título de D'Amato, "Can/Should Computers Replace Judges?"

Os autómatos jurídicos já não são apenas ficção (Nagel 1998). A automatização jurídica do direito fiscal e dos seguros de acidentes rodoviários foi há muito defendida (Viehweg 1995, Phillips 1995). Na metodologia do direito ressalva-se que o "juiz computador" que "fosse de uma vez só programado per saecula saeculorum causaria "horror até ao positivista mais impávido" (Kaufmann 1997: 121). Todavia, aceita-se que, "quando se trate de fenómenos massivos, que se apresentam sempre de maneira idêntica […], *o juiz que decide o caso concreto pode ser substituído pelo computador*, previamente instruído para todos os casos" (Larenz 1983: 282; v. Catala 1998), qual "robot da subsunção" (Ogorek 1986).

Entre nós surgiram igualmente vozes favoráveis à automatização jurídica (Hespanha 2000, G. Marques 2000), apontando-se o direito com um campo fértil de aplicação da *algoritmia analógica* (Moles 1990: 49). Outros, porém, manifestaram reservas à sua viabilidade, alegando a incapacidade "semântica" dos computadores (C. Neves 1993: 251-2) ou que o "o «Dr. Iur. Computer» [enquanto] prótese mecânica" não conseguiria "*ajuizar"* os casos(Bronze 1998: 76). Numa palavra, o raciocínio jurídico não seria redutível a um algoritmo omnipotente (Dworkin 1992: 287-9). Ao invés da inteligência artificial, dever-se-ia antes apostar nos "processos naturais da inteligência jurídica" (F. Araújo 1999:71).

2. If, then – unless or else?

O nosso sistema jurídico é constituído, fundamentalmente, por normas legais, as quais têm normalmente uma estrutura lógica semelhante à informática: *if, then – unless or else*. Se *x*, logo *w, a menos que y (ou salvo se), então k*. Isto é, têm uma hipótese, que prevê a situação típica, e uma estatuição, que estabelece a consequência, ambas se fundindo por via de uma "cópula" ou "nexo que as une" (S. Justo 2003: 142).

Todavia, a lei utiliza amiúde conceitos indeterminados ou cláusulas gerais (por ex. bons costumes), cuja determinação e concretização é tarefa do intérprete. A programação informática poderia suprir alguma porosidade linguística da lei, indexando tais conceitos indeterminados e cláusulas gerais a bases de dados jurisprudenciais e doutrinais processadas em termos de encontrar uma posição dominante ou maioritária.

Há casos que o sistema logicamente programado não prevê e para as quais não provê solução. São as chamadas lacunas, no sentido de casos omissos. O modelo «se, logo» não reconhece casos que não se subsumem aos conceitos previstos no programa da lei, mas que não deixam de ser juridicamente relevantes, reclamando disciplina análoga à prevista para situações reguladas pela lei, em virtude de nele procederem as razões justificativas dessa disciplina legal (*eadem ratio*), como prescreve o Código Civil (art. 10.º, 2), tarefa que "exige toda a finura por parte do intérprete" (Ascensão 1997: 446).

Estas situações exigem uma programação mais complexa, alargando a hipótese da norma a situações afins, como, por exemplo, programando o sistema no sentido de abrir o regime de uma norma com base no argumento *a fortiori*, por maioria de razão, ou *ad maius ad minus*.

As possibilidades de alargamento da norma poderiam, todavia, ser comprometidas no campo das normas excecionais. Tomada à letra a proibição da analogia relativamente a estas normas, então o programa informático excluiria à partida a possibilidade de aplicação de tais normas a casos atípicos. O argumento por maioria de razão cederia face ao argumento *a contrario*, excluindo do campo de aplicação todas as situações que "contrariam princípios fundamentais, informadores da ordem jurídica ou dum ramo de direito em particular" (Ascensão 1997: 453). Porém, a proibição da analogia das normas excecionais não tem em conta a "radical matriz analógica do discurso jurídico" (Bronze 1994), nem aceita que a norma se aplica analogicamente mesmo aos casos nela expressamente previstos – expondo-se ao argumento apagógico da *reductio ad absurdum*.

A relevância jurídica dos casos omissos é atribuída à sua ressonância no estrato do sistema que anima o *corpus iuris*, os chamados princípios fundamentais (Alexy 1995). O método tradicional denomina esta operação por analogia *iuris*. O caso omisso resolve-se segundo os princípios jurídicos gerais relativos ao instituto convocado pelo caso. Estes princípios seriam decantados a partir das normas que compunham o regime de tal instituto através das operações lógicas da indução e da dedução: por indução infere-se um princípio geral, do qual deduz uma solução para o caso omisso.

A programação informática já permite a indução lógica, com os chamados agentes reativos, aprendizes e adaptativos (Costa & Simões 2004: 37), apontando-se "a grande

capacidade do sistema para reconhecer padrões e depois emular o raciocínio por analogia" (Marques 2000: 37).

É, todavia, duvidoso que a *machine learning* tenha algo de "espontâneo" (Levinson 1998: 255), em especial que consiga decidir *contra legem*. O computador limita-se a cumprir a rotina dos «se, logo» que implementam informaticamente o programa normativo, pelo que a decisão *contra legem* seria, pela natureza das coisas, impossível.

Mas podemos razoavelmente supor que o computador poderá um dia induzir os princípios jurídicos gerais a partir das normas legais, de modo a afastar a normas legais que contrariem tais princípios. O sistema informático integraria lacunas por via da elaboração indutiva dos princípios jurídicos gerais e controlaria a legalidade das normas contrárias a esses princípios. Teríamos uma decisão *contra legem,* mas *secundum ius ex machina*. À semelhança do controlo da constitucionalidade das normas, sendo a Constituição o código-fonte do programa normativo.

Mas, a ser assim, o sistema informático impediria o legislador de introduzir mudanças e alterações no sistema. A lógica do sistema jurídico seria codificada num certo momento pelo sistema informático, o qual aferiria a conformidade das novas leis com a lógica pré-definida e fechada. Não se afastaria a interpretação *ab-rogante* em casos de contradição lógica das normas (Justo 337), mas por certo importaria o risco de clausura do sistema e de necrose do *corpus iuris*.

Em suma, a substituição do juiz humano pela máquina calculadora, ao estilo de um *ius ex machina,* eliminará o papel criativo do intérprete, em especial do juiz, que "realiza, de facto, uma actividade criadora (…). E não sofre dúvida de que, *de direito*, a realiza também" (Andrade 1978: 88). Ao invés de um «dever-ser» a justiça mecânica e automática reduz-se a um «ter-que-ser», indiferente aos princípios fundamentais que "só através da concreta realização do direito (da decisão dos casos jurídicos concretos) se vão revelando" (C. Neves 161). O sistema informático reproduz silogisticamente, com mais ou menos sofisticações, o programa pré-carregado, "mas estar-lhe-ia vedado *ajuizar* deles" (Bronze, 76-9). O juízo, enquanto capacidade de discernir o bem e o mal, o justo e o injusto, é uma categoria que predica a humanidade, pois "um direito sem justiça constituiria, digamos, uma monstruosidade moral" (Carvalho 1996: 4).

Pode, todavia, perguntar-se se a insistência na humanidade em tempos de cruzamento entre o ser humano, a natureza e a tecnologia, não será uma forma de «especismo» (Linhares 2003), discriminando positivamente a vida humana relativamente a formas de vida.

De todo o modo, está igualmente causa a própria "«luta pela sobrevivência» do direito" (Bronze 2006: 77), Com efeito, a maior falácia da inteligência artificial poderá ser a tentação de colocar nas suas mãos a nova "ciência do bem e do mal", para assim regressar ao jardim do paraíso.

A dimensão de responsabilidade envolvida no ato de julgar (Bourcier 1995, 232) exige, da parte do juiz, compromisso enquanto "*viva vox iuris*" (Bronze 1993: 184). Pese embora a norma constitucional que afasta a responsabilidade dos juízes pelas suas decisões (art. 216.º, 2), parece-nos que substituir o juiz pela máquina seria retirar ao julgamento essa dimensão de responsabilidade.

O modelo ideal do positivismo, preocupado apenas com a segurança e a certeza jurídicas, conduz ao apagamento do papel do intérprete e dos agentes decisores. A criação do direito teria lugar apenas em sede legislativa. Segundo o modelo democrático, a soberania radica na vontade popular, pelo que só os representantes do povo teriam legitimidade e competência para criar direito através das leis, incluindo a lei das leis que é a Constituição. Por seu turno, os tribunais teriam apenas legitimidade para, em nome do povo, administrar a justiça resultante do direito legislativamente criado. Ser apenas "a boca que pronuncia as palavras da lei" (Montesquieu) promete um efeito de "anestesia tranquilizante" (Bronze 1993: 182).

3. «Virtualidades Entrópicas» da IA

A "dimensão entrópica" da ordem jurídica analisa-se na sua função secundária ou organizatória (Bronze 2002: 77-92).

Desde logo, no seu "momento de coerência e unidade sistemática", com questões de *antinomias entre normas*, entre normas e princípios, ou mesmo entre princípios, para a superação das quais se apontam critérios formais, nomeadamente o critério da hierarquia (*lex superior derogat inferiori*), o critério da especialidade (*lex posterior generalis non derogat priori speciali*), e o critério da prioridade cronológica (*lex posterior derogat priori*). Mas também no "momento de realização orgânico-processual", enquanto "condição adjetiva do juízo decisório", nomeadamente nas questões da competência judiciária e, de um modo geral, no direito processual.

Já se afigura menos relevante o papel da IA no "momento de desenvolvimento constitutivo" está em causa a dialética "subsistência/mutação" ou estabilidade/evolução da ordem jurídica suscitada pela historicidade da *praxis* e do direito. Trata-se, por ex., do problema das fontes do direito, em especial nos limites normativos temporais e de validade das normas legais, em que o juiz não encontra correspondência entre os princípios que animam o sistema e as normas legais hipoteticamente aplicáveis, devendo proceder-se à "preterição sincrónica" e à "superação diacrónica" de tais normas legais (C. Neves 1985; Bronze 2002*:* 683-746).

4. Novos princípios e decisão *contra legem*

O jurista intérprete pode trazer novos valores para o direito, que muitas vezes introduzem ruturas no sistema (C Neves 1993: 227). Fala-se até na legitimidade da radical insubmissão contra o próprio sistema (Carvalho 1997), ou pelo menos que por via da interpretação se emendem os erros do legislador e se resista contra "os desmandos e abusos do Poder" (Andrade). Mas, não será essa uma falha crítica de segurança do sistema, expondo-o aos rábulas, que "cavilam as leis"? (Paiva 1883: 44).

Admitir que os novos princípios afastem a norma legal não repugna na medida em que não ofendam o espírito do sistema vigente. Já permitir ao juiz criar princípios ofensivos do espírito do sistema vigente pode arruinar o próprio sistema

A Lei Fundamental incumbe os tribunais de velarem pela conformidade constitucional das normas legais: "Nos feitos submetidos a julgamento não podem os tribunais aplicar normas que infrinjam o disposto na Constituição ou os princípios nela consignados" (art. 204.º). Trata-se do expediente da fiscalização concreta da

constitucionalidade, nos termos do qual o tribunal não pode aplicar normas que infrinjam o disposto na Constituição ou os princípios nela consignados (Canotilho 1998: 874).

À luz do preceito constitucional, mesmo as teorias da constituição aberta e material reconhecem que a fonte dos princípios é ainda a lei constitucional, enquanto expressão da vontade soberana do povo. Neste sentido, o intérprete da lei ordinária não seria o criador de princípios jurídicos, ao menos enquanto fundamento de desconsideração de normas legais. A obediência à lei só poderia ser afastada em nome da obediência à Constituição. Numa palavra, em situações de interpretação ab-rogatória, a medida da razoabilidade do legislador seria ditada pelos princípios do código constitucional, ou seja, o teste da razoabilidade da norma seria aferido pelo espírito do sistema tal como contido na Constituição, qual horizonte hermenêutico balizador da "interpretação conforme a Constituição" (Orlando de Carvalho 1996: 15; Neves 1993: 195; Larenz, *Metodologia*, 418; Canotilho 1998: 1099; Miranda 1996). De todo o modo, segundo o regime da fiscalização concreta da constitucionalidade em vigor (art. 280/1-a CRP), "juízo final" cabe ao Tribunal Constitucional (Correia 2003). Em suma, a abertura constitucional permitiria ao juiz uma criatividade de princípios *positiva* (no sentido de recriação de princípios constitucionais já consagrados) e eventualmente *neutra* (no sentido de criação de princípios que não ofendem a lógica constitucional), mas já não *negativa* (no sentido de criação de princípios contrários ao espírito da Constituição, de acordo com as normas e os princípios nela consignados).

A substituição dos Tribunais e do próprio Tribunal Constitucional por um sistema informático será uma tentação para um poder político totalitário, que se serve do direito como instrumento de execução do seu programa de domínio e dispensa o juízo do decisor, bastando-se com a sua fiel obediência à «cópula» lógica do «se, logo». O problema da porosidade e fluidez da linguagem jurídica resolver-se-ia através de uma nova linguagem, com os sentidos das palavras (e de outros signos relevantes) inequivocamente codificados e uma "gramática pura" construída à imagem e semelhança das linguagens de programação informática, ao estilo de uma orwelliana Novilíngua jurídica.

5. Validação científica, causalidade e arbitrariedade

Segundo a ciência e a técnica desempenhariam atualmente o papel da uma ideologia enquanto instância de validação (Habermas 1973: 42-3). Com efeito, o que a ciência tecnologicamente aplicada torna possível desafia constantemente as convenções sobre o bem e o mal, sobre o que está certo e o que está errado, abanando (e por vezes abalando) os alicerces do edifício do sistema jurídico.

Aceitar o progresso científico não implica subordinar as regras da convivência humana exclusivamente a esse paradigma. É verdade que pertencendo o ser humano ao mundo natural, então as regras da convivência humana não poderão ser estranhas às leis da natureza. Todavia, as regras de convivência humana não seriam não são apenas determinadas pelas leis da natureza. Pode, aliás, perguntar-se se o "pecado original" não será a regra de convivência humana, em especial a proibição (F. Costa 1992).

Em comparação com a lei física da causalidade, a lei jurídica é duplamente "imperfeita". Por um lado, a lei jurídica é violada e, por isso, são previstas sanções. Por outro lado, nem sempre se aplicam as sanções para a violação da lei. Assim, quer ao nível da hipótese quer ao nível da estatuição, a lei jurídica não se assemelha à lei física.

A natureza é mecânica no sentido de que a determinados factos correspondem invariavelmente certos efeitos. A justiça não é bem assim, sendo, por vezes, conotada com uma ideia de arbitrariedade, aqui entendida como abuso, prepotência ou até iniquidade, em que *tot sunt sententiae quod capita*.

Os sistemas informáticos de inteligência artificial prometem uma justiça sem arbítrio. Árbitro seria apenas o programador político do sistema que implementaria tecnicamente no software o programa político de domínio e ordenação social contido no código-fonte constitucional e das leis. Juízos só os provenientes da vontade política do legislador. A máquina limitar-se-ia a reproduzi-los mecanicamente nos casos concretos por via de aplicação silogística.

O mandato popular tem sido tacitamente renovado, em razão de não ter ocorrido ainda nova revolução (Hart 1994: 61). A reconfiguração do código constitucional é monopólio do poder legislativo, constituindo ainda expressão do domínio popular, mas "a legitimidade moral mínima na constituição não garante a legitimidade moral mínima de cada lei aprovada ou ato tomado nos termos da constituição" (Fallon 2005: 1792).

A referência aos princípios consignados na Constituição, enquanto bitola da elasticidade interpretativa do juiz, leva a considerar um aspeto do código constitucional, que se pode designar como o dispositivo de interoperabilidade ou compatibilidade externa do sistema jurídico português (ou interface constitucional). Este aspeto fornece mais elementos para responder ao problema da interpretação da própria Constituição, em conformidade com a qual se devem interpretar as leis e resolver os casos omissos (Häberle 1997).

O art. 8/1 da Constituição, relativo ao direito internacional, estabelece que "as normas e os princípios de direito internacional geral ou comum fazem parte integrante do direito português". Este preceito visa garantir a conformidade do direito português com o direito internacional geral ou comum e a sua receção automática na ordem jurídica interna (Almeida 2003: 70), constitucionalizando-o (G. Pereira/Quadros 2004: 387-9). O *ius gentium* é o direito dos povos, destacando-se a democracia e os direitos humanos como os valores fundamentais da "*nomos* mundial" (F. Costa 2004: 77-88).

6. O código-fonte constitucional na sociedade de risco

Assim, a informatização da justiça através do desenvolvimento de sistemas de inteligência artificial teria que basear-se num código-fonte aberto que incorporasse nas rotinas de programação os princípios do dinâmico direito internacional geral ou comum.

Todavia, num tempo de grandes mudanças na ordem internacional, o direito internacional geral ou comum é suscetível de apresentar um nível de "turbulência" considerável. O único valor que parece afirmar-se consensual na cena internacional é o mercado e o livre, ao ponto de se dizer: "Já não é o Direito que regula o mercado, mas o mercado que regula o Direito" (Maduro, 211). Nesta lógica de mercado, a democracia e os direitos humanos aparecem como meros custos de transação, senão mesmo como

excentricidades do Ocidente, a que somaria a proteção da natureza e, em especial, dos animais.

Os profetas do mercado defendem que o mercado é naturalmente justo, enquanto motor de distribuição da riqueza, estando em gestação, à escala global, uma confucionista "economia socialista de mercado". Todavia, é necessário perguntar pelo papel do Estado, que não deve "só prestar culto a interesses materiais, qual simples sociedade comercial" (C. Moncada 1966: 307).

Historicamente, as civilizações mais desenvolvidas (ou pelo menos as dominantes ou mais poderosas) foram sempre as que tiveram ao seu dispor os meios técnicos e científicos mais avançados - pelo menos enquanto instrumentos de domínio -, ao mesmo tempo que dispunham de eficazes sistemas ordenadores de controlo social. A "crença" no progresso técnico-científico tem sido abalada por certas utilizações que o ser humano tem dado às suas invenções tecnológicas. Numa "sociedade de risco" em estado de irresponsabilidade coletiva (Beck 1998) é urgente apurar o papel do Direito. Mas, será ainda possível identificar o cosmos do Direito no caos da «juridicidade»?

Ubi societas, ibi ius, logo sem direito não sequer sociedade, seja de risco ou não. O que verdadeiramente interroga o direito não é a sociedade de risco, mas antes o próprio risco. É um risco de origem humana, resultante das aplicações tecnológicas da ciência, e que se projetam na energia nuclear, na engenharia genética, na biotecnologia do admirável mundo novo de Huxley ou até no poder normalizador dos media ao nível da instituição de uma *Novilíngua* orwelliana. Tanto mais que "não se pode excluir a possibilidade de a Terra vir a ser atingida por um gigantesco meteoro e, assim, ser arrasada por uma catástrofe das proporções de uma guerra atómica" (Eigen/Winkler, 315).

Mas não será a inteligência artificial justamente a resposta para a complexidade das nossas "sociedades de risco"?

Há muito que o ser humano se rendeu à "prótese" calculadora. Desenvolvem-se poderosíssimos algoritmos de cálculo de probabilidade de ocorrência de certos factos. Por exemplo, implementando o "*software darwínico*" (A.L. Pereira 2001) através de códigos de cálculo de adequação de meios à evolução das espécies, seria possível desenvolver um programa normativo de medidas eficazes de eugenia social, por via, nomeadamente, da eliminação dos "genes degenerativos".

De todo o modo, não se saberia ainda qual é o sentido da evolução. Terá a evolução da espécie sido consciente e intencional? Ou o processo evolutivo foi determinado por fatores aleatórios e alheios à sua vontade? No sentido de que tanto podia ser como é agora, como ter ficado, em família, no "paraíso", ou ter evoluído com uma qualquer outra configuração biológica: "a cartografia do genoma revelou que os padrões de ADN do ser humano e do chimpanzé são em mais de 98% iguais (…). E algures nesse pouco mais de 1% de diferença surgem Shakespeare, naves espaciais que vão à Lua, a engenharia genética e a IA – pelo menos no sentido de auxiliar" (Levinson 1998, 257).

Se a teoria da evolução das espécies não engana, o risco tem sido ao longo dos tempos o "fósforo" da evolução: na vida é a "dimensão de risco que a faz exaltante: a eliminação da inquietude que assim se menciona embaciá-la-ia sem remédio, desumanizá-la-ia em absoluto, numa palavra, … desvitalizá-la-ia" (Bronze 2000: 32).

O domínio do risco seria assim a base da "luta pela vida" e da "vontade de poder", segundo o pensamento político do liberalismo pragmático e utilitarista, adverso a valorações morais que transcendam o biologicamente verosímil. Podemos até questionar se a "intenção regulativa" do direito não se funda nesse propósito evolucionário da descendência com modificações.

7. Interpretação da lei em conformidade com os princípios

Este exercício jurídico-filosófico não é meramente especulativo, antes pode ter projeções metodológicas, ao nível da interpretação das leis (Paiva 1883. 51). O problema da interpretação jurídica remete o intérprete para o cânone da interpretação conforme aos princípios e, em especial, da interpretação conforme à constituição. No sentido de que, mesmo que se reconheça natureza aberta do sistema à criação de novos princípios, sempre teriam estes que ser plasmados na constituição ou, pelo menos, por eles não rejeitados, em especial neste tempo de constitucionalismo em que se afirma que o Código Civil é a Constituição: "*notre Constitution c'est le code civil" (*Zenati).

Ora, em primeiro lugar, o código constitucional não pode estabelecer um programa normativo completo, que preveja todas as situações juridicamente relevantes. Ou seja, há vida jurídica fora da constituição. Trata-se, para começar, do desenvolvimento *praeter legem*, que decorre, desde logo, de uma abertura de primeiro grau, resultante da porosidade da linguagem jurídica, em virtude da sua exposição ao uso comum da linguagem. As cláusulas gerais e os conceitos indeterminados utilizados pela lei, desde logo na Constituição, revelam um segundo grau de abertura. Fala-se aqui, com propriedade, de uma "metódica de concretização" visando "a interpretação-concretização de uma *hard law* e não de uma da *soft law*: as regras e princípios constitucionais são padrões de conduta juridicamente vinculantes e não simples «directivas práticas»" (Canotilho 1998: 1073).

Identificamos ainda uma abertura de terceiro grau da legalidade. O código constitucional ainda fornece princípios de decisão, por via da inferência das especificações básicas do seu programa normativo. Fala-se em lacunas, no sentido de referir casos para os quais a lei não provê solução, tendo o intérprete que lançar mão do espírito do sistema para integrar a lacuna (formal). Não se trata apenas de analogia *legis*, uma vez que não existe sequer um critério legal cujas razões justificativas valham igualmente para o caso omisso. A questão é mais funda e chama para primeiro plano os princípios do sistema tocados pelo caso. São situações de analogia *iuris*, mas ainda *secundum legem*. Ou seja, o intérprete não pode usar a analogia como se fosse "apenas um pretexto legitimador das suas improvisações" (O. Carvalho 1997: 83), e deve estar precavido contra o risco do recurso à analogia. Como advertia Goethe: "Estas parábolas são agradáveis e divertidas. Quem é que não gosta de brincar com analogias?" (*As Afinidades Electivas*).

Mas, estará o espírito do sistema contido no texto constitucional, ainda que aberto aos princípios do direito internacional geral ou comum?

Recusa-se o «pan-constitucionalismo» (Canotilho 1982: 467) e aceita-se a legislação *praeter constitutionem*, ainda que nos limites da neutralidade, ou seja, legislação estranha ao sistema, mas não necessariamente contrária ao código constitucional. O

mesmo vale para a atividade jurisprudencial. Aceita-se a decisão *praeter legem* mas não que viole do espírito do sistema. E assim se identifica uma abertura de quarto grau. Assim como na prática surgem novos problemas, também no direito podem emergir novos princípios jurídicos, na medida em que não ofendam o código constitucional.

Suscitam-se, porém, questões delicadas. Como conciliar a abertura do código normativo com os domínios de reserva de lei, de legalidade taxativa (incluindo a legalidade criminal), de tipicidade fechada ou *numerus clausus*? Não será, desde logo, *contra legem* estender um regime legal fechado a situações nele não previstas, ainda que o aplicando apenas a partir dos seus princípios cardinais? Em domínios em que o código constitucional exige a mediação legislativa concretizadora como requisito de possibilidade de implementação do programa normativo que pode o juiz fazer senão proferir um juízo de *non liquet*? O contrário não será justamente decidir *contra legem*?

8. A criação jurisprudencial do Direito

Esta questão prende-se também com o problema do sentido e dos limites do "desenvolvimento transsistemático do direito". O que é e como opera este desenvolvimento do direito? Não se resolvendo a questão *ex nihilo*, parece ainda apelar-se aos princípios do espírito do sistema vigente tocados pelo caso concreto. Pelo que o "desenvolvimento transsistemático do direito" será ainda, afinal, intra-sistemático, sendo uma "«fuga para os princípios»" ainda *systemfreundlich* (Canotilho 1982: 278).

Com efeito, a liberdade de criação judicial parece ser limitada pela lei, desde logo pela constituição. É admitida a criação *praeter legem* na estrita medida em que não viole a reserva de lei e a tipicidade taxativa. Fora de causa está a criação pelo juiz de princípios ofensivos do espírito do sistema vigente. Juízos contra *legem* só seriam permitidos na estrita medida da exigência de conformidade das leis com a constituição e no quadro do procedimento de fiscalização concreta da constitucionalidade.

Devem admitir-se, todavia, os juízos contra *legem*, mas constitucionalmente neutros. O juiz cria princípios não rejeitados pela constituição, mas que também não brotam dela. Serão juízos constitucionalmente neutros, a afirmar a existência de um *tertium genus*, e que não decorrem de qualquer "misticismo" jurídico (Brewer 1996, 933-4). Este *tertium genus* de neutralidade constitucional vale não apenas como fonte de princípios de decisão para casos omissos, mas também como fundamento de desconsideração de normas ofensivas do espírito emergente.

Ora, a informática não disponibiliza ao direito um arsenal metódico que lhe garantirá mais rigor e certeza? Isto é, a informatização da justiça não significará também a assimilação pelo direito da linguagem e do *modus operandi* da informática? Fala-se, a propósito, na "genuína terapêutica" da aplicação da lógica informática ao raciocínio jurídico (F. Araújo 1999: 22).

Se os computadores são mais eficientes, como justificar a despesa pública em justiça não automatizada? O tema não é novo (Neves 1998). Trata-se da alternativa tecnológica ao direito, que vem associada a promessas de regresso ao "jardim do paraíso". O fim do Estado e do Direito é uma "utopia" de longa data. Mas ninguém dispensa a Justiça. Resta saber que justiça seria essa, sem Estado nem Direito.

Além disso, podemos questionar se afinal os computadores não estão cada vez mais parecidos com os humanos, incluindo ao nível do *logos* jurídico. Numa palavra, devemos compreender o fenómeno em termos de simbiose homem-computador, ao invés de numa relação de oposição excludente (Saito 1998, 58).

9. O papel da Inteligência Artificial e os limites da tecnologia

Em nosso entender, os sistemas de inteligência artificial podem auxiliar a tarefa judicial. Todavia, o juízo do juiz é não apenas desejável, mas também insubstituível. Esse juízo não se reduz a uma lógica «se, logo; salvo se, então», nem a um mero cálculo de probabilidades, incluindo a elaboração de normas de segundo grau mediante inferências normativas. O que está em causa não é o «legislador provável», mas antes o «legislador razoável».

A justiça como obra humana só está ao alcance de humanos (Betti 1987: 107, recordando Goethe). Com isto tomamos partido por algo a que poderíamos chamar o "natural" em detrimento do "artificial". Tomar partido tem uma dimensão lúdica ou fantasiosa. Fantasia no sentido de "imaginação criadora" própria do "carácter poiético – e, *hoc sensu*, criador – das decisões judicativas" (Bronze 1993: 183). Quando se conhecerem os processos elementares de armazenamento de informação e sobre a sua localização e manifestação na rede das células nervosas e sinapses, "mesmo então continuará a ser impossível substituir por uma máquina o poder criativo do nosso cérebro" (Eigen/Winkler 1989).

Não se pretende com isso dizer que o juiz pode ludibriar os propósitos da lei com a sua caprichosa imaginação, estando fora de causa a "liberdade sem limites de *sofismar* as leis por parte dos juízes" (Andrade 1978: 62). Pelo contrário, do que se trata é de responsabilizar o juiz como criador do direito no caso concreto. Ajuizar não implica a renúncia à humanidade do juiz, nem o afivelar da máscara do autómato. A responsabilidade do juiz enquanto elemento ético do juízo protege-o, aliás, contra a "prótese mecânica" (Bronze 1998: 122).

Uma das principais modificações que se apontam ao ser humano no processo evolutivo é o seu livre arbítrio, pelo qual foi levado a provar o fruto da árvore do bem e do mal, sofrendo em consequência a expulsão do paraíso. Por causa do livre arbítrio, o ser humano quebrou o código do Criador e modificou a ordem da descendência.

O relato da Criação dá a ideia, porém, de que o fruto do bem e do mal estava já na árvore à disposição do Homem. Por isso, o jardim do paraíso seria o reino da inconsciência. Uma vez consciente do bem e do mal, o ser humano foi expulso do paraíso. Terá sido este porventura o marco distintivo do ser humano em relação às demais espécies, e que se pode dizer radicado no juízo: mais do que a palavra, o pecado original foi o primeiro juízo do ser humano.

Pelo que, a ideia de um juiz sobre-humano, situado para além do bem e do mal, seria pretender devolver o juiz ao jardim do paraíso, isto é, ao reino da inconsciência. Mas se pensarmos por que razão terá o ser humano ajuizado, talvez possamos supor que o juízo foi a resposta encontrada para solucionar problemas relativos à sobrevivência e à evolução da espécie. E por isso terá quebrado o código genético do Criador, multiplicando a espécie para além das fronteiras do jardim do paraíso.

Contudo, a multiplicação da espécie coloca um dos maiores desafios à sua própria sobrevivência. Pergunta-se se não seria útil um computador que calculasse o número de seres humanos admissíveis. Mas qual seria o critério da admissibilidade?

O último século testemunha o crescimento hiperbólico da população: "Se a população continuar a aumentar à taxa actual, daqui a quinhentos anos ou seiscentos anos cada pessoa só terá um m2 à sua disposição. (…) A história da humanidade mostra que todas as armas disponíveis acabam, mais tarde ou mais cedo, por ser utilizadas. (…) No reino animal, o território é defendido até à morte" (Eigen/Winkler 1989: 280-1).

Com efeito, "a tecnologia não é só aquilo que nos permite fazer artefactos, mas também aquilo que tem vindo a transformar o homem naquilo que neste momento é" (Stableford 1991: 234). A revolução científico-tecnológica muniu o homem do *poder de auto-destruição enquanto espécie*. E é a consciência da "*stillste Stunde* [...] [sua] furchtbaren Herrin", escreve Friedrich Nietzsche em *Also sprach Zarathustra* (1976: 162), que o faz assumir-se, hoje, como *homo dolens* (F. Costa 1992: 358).

A revisibilidade científica não impede a irreversibilidade tecnológica, no sentido de que, embora seja possível «falsificar» a teoria da relatividade, já não é possível «desinventar» a bomba atómica. Esta situação de não retorno tecnológico compromete, por seu turno, uma ética que se destine a garantir a sobrevivência da humanidade através dos grupos mais fortes, exigindo antes uma ética equitativa de comunhão ou de inclusão global: "Equity creates just law, and just law is the touchstone of social evolution" (Snyder 1973: 43).

Para estes problemas o computador não tem resposta. E não obstante são problemas que animam o direito internacional comum, que o juiz deve ter no seu horizonte quando ajuíza os casos que lhe cumpre decidir. Os sistemas de inteligência artificial poderão ser um auxílio útil na boa administração da justiça. Mas não podem substituir o prudente arbítrio do juiz. Ajuizar não é apenas nem sobretudo calcular. Os valores éticos do direito escapam à métrica da calculadora. Quanto vale uma vida? Quanto vale a vida? E a liberdade? E a dignidade da pessoa humana?

Dir-se-á que a correção das respostas será aferida pela observância das regras de procedimento argumentativo-decisório. Essa é a tese da teoria da argumentação jurídica, segundo a qual "com estas formas (de argumentos) pode-se justificar qualquer proposição normativa e qualquer regra" (Alexy 1995: 203).

Todavia, como escreve Kaufmann em *Die Aufgaben heutiger Rechtsphilosophie*: "Die moralische Urteilskraft ist wesentlich auf die Phronesis, die Klugheit, gegründet und nicht so sehr auf formale Rationalität." Por essa razão, o próprio imperativo categórico é posto em causa enquanto mera regra de procedimento.

Segundo Holmes, que "the life of the law has not been logic, it has been experience". Há uma dimensão irredutível de "*justitia mediatrix*" no direito. A máquina pode ser utilizada como auxílio mas não como substituto da tarefa decisória, que deverá ser humana e estar ao serviço da Humanidade e da Natureza.

De resto, a pergunta de Eigen e Winkler (1989: 258) impõe-se: "Será razoável conceber máquinas com tais capacidades, provavelmente muito limitadas, de auto-reflexão? Não seria mais importante organizar a *sociedade* humana (…) como um «ser vivo» que reaja de modo razoável, um ser vivo que pare, enfim, de se autodestruir?"

Referências

Alexy, Robert (1995) *Recht, Vernunft, Diskurs: Studien zur Rechtsphilosophie*, Suhrkamp, Frankfurt am Main.

Almeida, Francisco Ferreira de (2003) *Direito Internacional Público*, 2.ª ed., Coimbra Editora, Coimbra.

Alpa, Guido (1996) "L'applicazzione delle tecnologie informatiche nel campo del diritto", *Il Diritto dell'informazione e dell'informatica*

Andel, Peck van; Bourcier, Danièle (1997) «Peut-on programmer la sérendipité? L'ordinateur et l'interprétation de l'inattendu», in *Interpréter le Droit: le sens, l'interprète, la machine*, dir. Claude Thomasset et Danièle Bourcier, Bruylant, Bruxelles.

Andrade, Manuel A. Domingues de (1978) *Ensaio sobre a teoria da interpretação das leis*, 3.ª ed., Arménio Amado, Coimbra.

Araújo, Fernando (1999) "Lógica jurídica e informática jurídica", in *Direito da Sociedade da Informação*, vol. I, Coimbra Editora, Coimbra.

Ascensão, José de Oliveira (1997) *O Direito: Introdução e Teoria Geral*, 10.ª ed., Coimbra.

Beck, Ulrich (1998) *Risikogesellschaft – Die organisierte Unverantwortlichkeit*, Frankfurt am Main.

Betti, Emilio (1987) *L'ermeneutica come metodica generale delle scienze dello spirito*, saggio introduttivo, scelta antologica e bibliografie a cura di Gaspare Mura, trad. Ornella Nobile Ventura, Giuliano Crifò, Gaspare Mura, Roma, Città Nuova Editrice.

Bourcier, D. (1995) *La décision artificielle*, PUF, Paris.

Brewer, Scott (1996) "Exemplary Reasoning: Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy", Harvard Law Review.

Bronze, Fernando José (1994) *A Metodonomologia entre a Semelhança e a Diferença (Reflexão problematizante dos polos da radical matriz analógica do discurso jurídico)*, Coimbra Editora, Coimbra.

Bronze, Fernando José (1998) "O Jurista: Pessoa ou Androide?", in *AB VNO AD OMNES*, Coimbra Editora, Coimbra.

Bronze, Fernando José (2000) *Argumentação jurídica: o domínio do risco ou o risco dominado?*, Boletim da Faculdade de Direito da Universidade de Coimbra.

Bronze, Fernando José (2002) *Lições de Introdução ao Direito*, Coimbra, Editora, Coimbra.

Bronze, Fernando José (2006) "Quae sunt Caesaris, Caesari: et quae sunt iurisprudentiae, iurisprudentiae", in *Comemorações dos 35 Anos do Código Civil e dos 25 Anos da Reforma de 1977*, vol. II., Coimbra Editora, Coimbra.

Canotilho J.J. Gomes (2004) *Estudos Sobre Direitos Fundamentais*, Coimbra Editora, Coimbra.

Canotilho, J.J. Gomes (1982) *Constituição dirigente e vinculação do legislador (Contributo para a compreensão das normas constitucionais programáticas*), Coimbra Editora, Coimbra.

Canotilho, J.J. Gomes (1998) *Direito Constitucional e Teoria da Constituição*, Almedina, Coimbra.

Carvalho, Orlando de (1996) "IVS – QUOD IVSTVM?", *Boletim da Faculdade de Direito*, vol. 72 (1996), 1-12

Carvalho, Orlando de (1997) "Para um Novo Paradigma Interpretativo: o Projecto Social Global", *Boletim da Faculdade de Direito*, vol. 73 (1997), 1-17.

Castanheira Neves, A. Castanheira (1995) *Digesta - Escritos acerca do Direito, do Pensamento Jurídico, da sua Metodologia e outros*, II, Coimbra Editora, Coimbra.

Castanheira Neves, *Entre o «Legislador», a «Sociedade» e o «Juiz» ou entre «Sistema», «Função» e «Problema» - os Modelos Actualmente Alternativos da Realização Jurisdicional do Direito*, Boletim da Faculdade de Direito, 1998, 1-44.

Coelho, Hélder (2002) "Inteligência Artificial, Sistemas Periciais e Realidade Virtual", in *Direito da Sociedade da Informação*, III, Coimbra Editora, Coimbra, 95-107.

Correia, Fernando Alves (2003) "Os direitos fundamentais e a sua protecção jurisdicional efectiva", *Boletim da Faculdade de Direito*.

Costa, Ernesto; Simões, Anabela (2004) *Inteligência Artificial: Fundamentos e Aplicações*, FCA, Lisboa.

Costa, José de Faria (1992) *O Perigo em Direito Penal*, Coimbra Editora, Coimbra.

Costa, José de Faria (2004) "Em redor do nomos ou a procura de um novo nomos para o nosso tempo", in *Diálogos Constitucionais*, org. A.J. Avelãs Nunes, J.N de Miranda Coutinho, Renovar, Rio de Janeiro.

D'Amato, Anthony (1977) "Can/Should Computers Replace Judges?" Georgia Law Review 11: 1277.

Dufresne, Jacques (1999) *Après l'homme... le cyborg?*, MultiMondes, Sainte-Foy.

Dworkin, Ronald (1992) *El Imperio de la Justicia. De la teoría general del derecho, de las decisiones e interpretaciones de los cueces y la integridad política y legal como clave de la teoría y práctica*, trad. Claúdia Ferrari (do orig. *Law's Empire*, 1986), Gedisa Editorial, Barcelona.

Dworkin, Ronald (2001) *Law's Empire*, Hart Publishing, Oxford.

Eigen, Manfred; Winkler, Ruthild (1989) *O Jogo. As leis naturais que regulam o acaso*, trad. Carlos Fiolhais, Gradiva, Lisboa.

Eskridge Jr., William N. (2001) "All About Words: Early Understandings of the «Judicial Power» in Statutory Interpretation (1776-1806)", Columbia Law Review 101.

Fallon Jr., Richard H. (2005) "Legitimacy and the Constitution", *Harvard Law Review*.

Gadamer, Hans-Georg (1993) *Poema y Dialogo. Ensayos sobre los poetas alemanes más significativos del siglo XX*, Gedisa, Barcelona (trad. do alemão *Gedicht und Gespräch*, Insel, Frankfurt am Main, 1990, por Daniel Najmías e Juan Navarro).

Garcia Marques / Lourenço Martins (2000) *Direito da Informática*, Almedina, Coimbra

Greenawalt, Kent (2002) "Constitutional and Statutory Interpretation", in *The Oxford Handbook of Jurisprudence and Philosophy of Law*, ed. Jules Coleman & Scott Shapiro), Oxford University Press, New York

Häberle, Peter (1997) *Hermenêutica constitucional: a sociedade aberta dos intérpretes da Constituição - Contribuição para a interpretação pluralista e procedimental da Constituição*, trad. Gilmar Ferreira Mendes, São Paulo, Sérgio António Fabris Editor.

Habermas, Jürgen (1973) *La technique et la science comme idéologie – La fin de la métaphysique*, pref. e trad. Jean-René Ladmiral (do original *Technick und Wissenschaft als Ideologie*, 1968), Denoël Gonthier, Paris.

Hart, H.L.A. (1994) *The Concept of Law*, 2nd ed., Oxford University Press.

Hespanha, António Manuel (2000) "Os juristas que se cuidem... dez anos de inteligência artificial e direito", Revista Themis, I, 140

Hespanha, António Manuel; Sernadas, Amílcar (1990) *O impacto da computação no direito*, Revista Jurídica, 179.

Justo, A. Santos (2003) *Introdução ao Estudo do Direito*, 2.ª ed., Coimbra Editora, Coimbra.

Katsch, Ethan (1995) *Law in a Digital World*, Oxford University Press, New York/Oxford.

Kaufmann, Arthur (1994) *Rechtsphilosophie*, 2. Aufl., Beck, München.

Kelsen, Hans (2002) *Teoría General del Estado*, trad. Luis Legaz Lacambra, Comares, Granada.

Langhein, A. W. Heinrich (1992) *Das Prinzip der Analogie als juristische Methode: Ein Beitrag zur Geschichte der methodologischen Grundlagenforschung vom ausgehenden 18. bis 20. Jahrhundert*, Duncker & Humblot, Berlin.

Larenz, Karl (1983) *Metodologia da Ciência do Direito*, trad. de José Lamego com revisão de Ana de Freitas (do original *Methodenlehre der Rechtswissentschaft*, Berlin/Heidelberg, Springer-Verlag, 5.ª ed. rev., 1983), 2.ª edição, Fundação Calouste Gulbenkian, Lisboa.

Levinson, Paul (1998) *A Arma Suave. História Natural e Futuro da Revolução da Informação*, trad. J. Freitas e Silva (do original *The Soft Edge*, 1997), Bizâncio, Lisboa.

Levinson, Paul (1998) *A Arma Suave. História Natural e Futuro da Revolução da Informação*, trad. J. Freitas e Silva (do original *The Soft Edge*, 1997), Bizâncio, Lisboa.

Linhares, J.M. Aroso (2003) "A Ética do Continuum das Espécies e a Resposta Civilizacional do Direito. Breves Reflexões", *Boletim da Faculdade de Direito*.

Maduro, Miguel Poiares, *A Crise Existencial do Constitucionalismo Europeu*, in *Colectânea de Estudos em Memória de Francisco Lucas Pires*, UAL, Lisboa.

Manning, John F. (2001) "Textualism and the Equity of the Statute", Columbia Law Review 101.

Molot, Jonathan T. (2006) "The Rise and Fall of Textualism", Columbia Law Review 106.

Moncada, Luís Cabral de (1966) *Filosofia do Direito e do Estado*, vol. II, Atlântida Editora, Coimbra.

Nagel, *Computer-Aided Law Decisions* / Elmi, *Informatics and Philosophy of Law (1998)* in Giannantonio (ed.), *Law and Computers*, Selected Papers from the 4th International Congress of the Italian Corte Suprema di Cassazione, Rome Spring, I. *Legal Informatics*, 667s, e 701s

Neto Paiva, Vicente Ferrer (1883) *Philosophia de Direito*, Tomo Primeiro: Direito Natural, 6.ª ed. augmentada e aprimorada, Imprensa da Universidade, Coimbra.

Neves, A. Castanheira (1993) *Metodologia Jurídica (Problemas fundamentais)*, Coimbra Editora, Coimbra.

Neves, António Castanheira (1967) *Questão de Facto - Questão de Direito ou o problema metodológico da juridicidade (Ensaio de uma reposição crítica*). I, *A Crise*, Coimbra, 1967,

Neves, António Castanheira (2003) *A crise actual da filosofia do direito no contexto da crise global da filosofia (Tópicos para a possibilidade de uma reflexiva reabilitação)*, Coimbra Editora, Coimbra.

Nietzsche, Friedrich, *Also sprach Zarathustra (1883-1885)*, 1976.

Ogorek, R. (1986) *Richterkönig oder Subsumtionsautomat?*, *Zur Justiztheorie im 19. Jahrhundert*, Klostermann.

Pereira, Ana Leonor (201) *Darwin em Portugal: Filosofia, História, Engenharia Social (1965-1914)*, Almedina, Coimbra.

Pereira, Miguel Baptista (1996) *Filosofia da Comunicação Hoje*, in Comunicação e Defesa do Consumidor, Actas do Congresso Internacional organizado pelo Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra, de 25 a 27 de Novembro de 1993, Coimbra.

Phillips, Lothar (1993) "Artificial Morality and Artificial Law", in Berman/Hafner (eds.), *Artificial Intelligence and Law*, Boston, 51

Phillips, Lothar (1994) "Ein bißchen Fuzzy Logic für Juristen", Tinnefeld/Phillips/Weis (Hrsg.), *Institutionen und Einzelne im Zeitalter der Informationstechnik*, Oldenburg, München, 219

Phillips, Lothar (1995), "Von nervösen und phlegmatischen Rechtsbegriffen — Ein Beitrag zur Rechtstatsachenforschung", in Tinnefeld/Phillips/Heil (Hrsg.), *Informationsgesellschaft und Rechtskultur in Europa*, Nomos, Baden-Baden, 192

Rifkin, Jeremy (2000) *O Século Biotech: A Criação de um Novo Mundo*, trad. Fernanda Oliveira, Publicações Europa-América.

Saito, Hiroshi (1998) "Neue Medien und Geistiges Eigentum – Insbesondere Urheberrechte im nahenden Zaitalter", in *Das Recht vor der Herausforderung eines neuen Jahrhunderts*. org. Zentaro Kitagawa et al., Deutsch-japanisches Symposion in Tübingen vom 25. bis 27. Juli 1996, Mohr Siebeck, Tübingen.

Scalia, Antonin (1998) *A Matter of Interpretation: Federal Courts and the Law* (commentary by Amy Gutmann, Gordon Wood, Laurence Tribe, Mary Ann Glendon, Ronald Dworkin), Princeton University Press, Princeton - New Jersey

Snyder, R. Neil (1973) "Natural Law and Equity", in Ralph Newman (ed.), *Equity in the World's Legal Systems*, Brussels.

Stableford, Brian, *Revolução Genética*.

Teubner, Gunther, *O direito como sistema autopoiético*, trad. e pref. de José Engrácia Antunes (do original alemão *Recht als autopoietisches System*, 1989), Fundação Calouste Gulbenkian, Lisboa.

Theodor Viehweg, *Rechtsphilosophie und Rhetorische Rechtstheorie (Gesammelte kleine Schriften)*, Nomos, Baden-Baden, 1995, 186.

Villar Palasí, José Luis (1986) "Informática y derecho", Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, 211

Warner Jr., David R. (1992) "A Neural Network-Based Law Machine: Initial Steps", Rutgers Computer & Technology Law Journal 51

Zippelius, Reinhold (1994) *Rechtsphilosophie (Ein Studienbuch)*, 3. Auf., Beck, München.

* Versão sumariada do nosso trabalho «Lex informatica, ius ex machina e justiça artificial» publicado no vol. I (Filosofia, Teoria e Metodologia) dos *Estudos em Homenagem ao Prof. Doutor António Castanheira Neves*, organizados por Jorge de Figueiredo Dias, J.J. Gomes Canotilho e José de Faria Costa (Coimbra Editora, 2008, 817-886).

Índice Geral

Vol. I

Vol. II

Vol. III