

O «MARCO CIVIL DA INTERNET» E SEUS REFLEXOS NO DIREITO DA UNIÃO EUROPEIA

Alexandre Libório Dias Pereira*

Resumo: Aborda aspetos da Lei Marco Civil da Internet confrontando-a com o direito da União Europeia, com destaque para a problemática da proteção dos dados pessoais, o chamado ‘direito ao esquecimento’ e o papel dos provedores de Internet, tendo em conta a jurisprudência do Tribunal de Justiça da União Europeia.

Abstract: Discusses aspects of the Brazilian Act “Marco Civil da Internet” comparing it with the law of the European Union, mainly with regard to protection of personal data, the role of Internet service providers, and the ECJ case-law in the field of the Internet.

Palavras-chave: Internet - Marco Civil – Dados Pessoais – Neutralidade da Rede – Responsabilidade dos provedores de Internet – Jurisprudência da EU

Keywords: Internet – Marco Civil – Personal Data – Net Neutrality – ISP Liability – EU Internet Case-law

* Professor Auxiliar da Faculdade de Direito da Universidade de Coimbra (Portugal). Este texto, elaborado a partir das notas de apoio à aula que tivemos a honra de lecionar no *Curso de Direito Eletrónico*, organizado conjuntamente pela Pontfice Universidade Católica do Paraná (PUCPR) e pela Faculdade de Direito da Universidade de Lisboa (FDUL), e que teve lugar entre 19 e 23 de janeiro de 2015 na FDUL, integra-se nas atividades do Grupo de Investigação “Globalização, Economia e Direito” do Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, no âmbito do Projeto “Desafios Sociais, Incerteza e Direito” (UID/DIR/04643/2013), financiado pela Fundação para a Ciência e a Tecnologia (FCT).

Sumário: Introdução. 1. A Lei Marco Civil da Internet. 1.1. princípios e objetivos do Marco Civil da Internet. 1.2. *Magna Carta* de direitos e garantias dos usuários da Internet. 1.3. O princípio da neutralidade ou isonomia da rede. 1.4. Controlo do tráfico de dados pessoais e da privacidade. 1.5. Conservação de dados de tráfego. 1.6. Liberdade de expressão e retirada de conteúdos: a responsabilidade dos provedores de conexão. 1.7. Fornecimento de registros de conexão ou de acesso a aplicações de internet. 1.8. Poder público. 2. O Direito da União Europeia para a Internet. 2.1. A sociedade da informação como domínio da União Europeia. 2.2. Proteção do consumidor na Internet. 2.3. Proteção de dados pessoais e da privacidade nas comunicações eletrônicas. 2.4. “Direito ao esquecimento”? 2.5. Liberdade de expressão e responsabilidade dos provedores de Internet 2.6. A neutralidade tecnológica. Conclusão. Referências bibliográficas.

INTRODUÇÃO



o dia 23 de abril de 2014 o Brasil viu nascer a Lei nº 12.965. Denominada *Marco Civil da Internet*¹, chegou a ser considerada a “Constituição da Internet” durante os trabalhos preparatórios pelo então Ministro da Justiça Luiz Paulo Barreto. Trata-se, com efeito, de um passo em frente no sentido de uma regulação da Internet que observe os princípios constitucionais e a *rule of law* no ciberespaço.²

¹ http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Sobre esta Lei ver, nomeadamente, Ronaldo LEMOS, «Uma nova lei para assegurar direitos na internet no Brasil: o Marco Civil», *Propriedades intelectuais*, nº 2 (junho 2014), p. 30-4; José de Oliveira ASCENSÃO, «O “marco civil da internet”: a lei brasileira n.º 12965, de 23 de abril de 2014”. *Revista de Direito Intelectual*, 2015, N. 2, p. 271-90; Marcos WACHOWICZ, Vitor Augusto Wagner Kist, *Marco Civil da Internet e Direito Autoral: uma breve análise crítica* - <http://www.gedai.com.br/>

² Para uma defesa da subordinação do ciberespaço aos parâmetros constitucionais e à *Rule of Law*, Alexandre L. Dias PEREIRA, «Direito ciberespacial: ‘soft law’ ou

A Lei Marco Civil da Internet (MCI) estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. A disciplina do uso da Internet no Brasil assenta no respeito pela liberdade de expressão e em outros valores como os direitos humanos, a livre concorrência e a defesa do consumidor (art. 2º/II-V MCI).

1. A LEI MARCO CIVIL DA INTERNET

1.1. PRINCÍPIOS E OBJETIVOS DO MARCO CIVIL DA INTERNET

São 5 os principais pilares do Marco Civil da Internet.

Primeiro, a liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

Segundo, a proteção da privacidade e dos dados pessoais;³

Terceiro, a neutralidade da rede juntamente com a sua estabilidade, segurança e bom funcionamento segundo as boas práticas tecnológicas;

Quarto, a responsabilização dos agentes pelos seus comportamentos na rede sem prejuízo da preservação da natureza participativa da rede;

‘hard law’?», in *Estudos em Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho, Volume III - Direitos e Interconstitucionalidade: Entre Dignidade e Cosmopolitismo*, org. Fernando Alves Correia, Jónatas Machado, João Carlos Loureiro, Coimbra Editora: Coimbra, 2012, p. 685-710. Ver também, para uma análise comparada da situação luso-brasileira do Direito da Internet anterior ao Marco Civil, J. Oliveira ASCENSÃO, «O Direito da Internet em Portugal e no Brasil», *Direito da Sociedade da Informação*, vol. X, APDI/Coimbra Editora, 2012, p. 101-126.

³ A Constituição brasileira de 1988 tinha já consagrado o *direito de Habeas Data* assinalado por J.J. Gomes CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7ª ed., Almedina, Coimbra, 2003, p. 515, no âmbito do chamado direito à autodeterminação informativa.

Quinto, a liberdade dos modelos de negócios promovidos na Internet, ou seja, a liberdade de acesso ao mercado digital.

Quanto aos objetivos, nos termos do art. 4º MCI, a disciplina do uso da Internet no Brasil visa promover o direito universal de acesso à internet, à informação, ao conhecimento, à cultura e à participação nos assuntos públicos (1), a inovação e difusão de novas tecnologias e modelos de uso e acesso (2), e a adesão a padrões tecnológicos que permitam a interoperabilidade em sentido amplo (3).

Para além dos princípios e dos objetivos, o Marco Civil da Internet contém algumas disposições de alcance duvidoso, tais como as definições de Internet, terminal, endereço IP, conexão à internet e seu registro, aplicações de internet e registo de acesso às mesmas (art. 5º). Com efeito, sendo este um ambiente sujeito a constantes mutações tecnológicas, é questionável o sentido da consagração das referidas definições numa lei com valor quase-constitucional, como então anunciado.

Além disso, contém uma disposição de natureza interpretativa que poderá suscitar algumas dificuldades ao remeter para a ‘natureza da internet, seus usos e costumes particulares’. Com efeito, estabelece o art. 6º que “Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, económico, social e cultural.”

Parece assim que a boa interpretação do Marco Civil depende da compreensão prévia da natureza da internet, seus usos e costumes, i.e., a chamada *Netiqueta*⁴, que tem expressão nomeadamente nos termos de utilização e nas políticas de privacidade dos sítios web. O ponto é sensível, uma vez que a função da lei é também corrigir usos, ou práticas reiteradas, que não estão em conformidade com os princípios e as normas

⁴ <https://pt.wikipedia.org/wiki/Netiqueta>

constitucionais. Devolver à Internet e aos seus agentes a regulação que justamente se procura estabelecer por via legal pode revelar-se um exercício de utilização puramente simbólica e política da legislação.

Parece-nos, todavia, que esse não é o caso, uma vez que na verdade o Marco Civil da Internet introduz aspetos inovadores. É o que sucede, desde logo, com o capítulo II sobre os direitos e garantias dos usuários.

1.2. MAGNA CARTA DE DIREITOS E GARANTIAS DOS USUÁRIOS DA INTERNET

O capítulo II do Marco Civil da Internet define os direitos e garantias dos usuários. Em razão de o acesso à internet ser considerado essencial ao exercício da cidadania, é previsto no art. 7º um rol de direitos do usuário, como sejam a inviolabilidade da intimidade e da vida privada (1); a inviolabilidade e o sigilo do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas (2); a não suspensão da conexão à internet e a manutenção da qualidade contratada da conexão (3); o direito a informação contratual sobre o regime de tratamento de dados pessoais e de proteção dos registros de conexão e de acesso a aplicações de Internet (4); o não fornecimento a terceiros de dados pessoais, incluindo dados de conexão e de acesso a aplicações, salvo mediante consentimento livre, expresso e informado ou nas hipóteses legalmente previstas (5).

O tratamento de dados pessoais é apenas permitido para finalidades que justifiquem a sua coleta (*princípio da finalidade*), não sejam legalmente proibidas e estejam especificadas nos contratos de prestação de serviços ou nos termos de utilização do serviço (*princípio da especialidade*). O tratamento de dados pessoais exige o consentimento expresso e deverá ocorrer de forma destacada das demais cláusulas contratuais (exi-

gência de *consentimento específico e autónomo*). Além disso, o usuário tem o direito de, a seu pedido, excluir definitivamente os seus dados de determinada aplicação da Internet no fim da relação (ou chamado direito de apagamento ou retirada, também conhecido por direito ao esquecimento).

A Lei Marco Civil exige ainda publicidade e transparência das políticas de privacidade e dos termos de utilização praticados pelos provedores de conexão à Internet e de aplicações (1), garantia de acessibilidade a cidadãos com necessidades especiais (2), e respeito pelas normas de proteção do consumidor nas relações de consumo na Internet⁵ (3).

Os direitos e garantias do usuário têm *natureza imperativa*. O acesso à internet é considerado essencial ao exercício da cidadania e a garantia do direito à privacidade e à liberdade de expressão nas comunicações condição para o pleno exercício do direito de acesso à internet, sendo nulas de pleno direito

⁵ Veja-se a este respeito, em especial, o Decreto n. 7.962, de 15 de março de 2013, que regulamenta a Lei n. 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Sobre o tema, com destaque para a proteção do consumidor no comércio eletrônico pode ver-se os nossos ensaios *Comércio eletrônico na sociedade da informação: da segurança técnica à confiança jurídica*, Coimbra, Almedina, 1999 (com nota atualização no site da editora), e «Notários, certificadores e comércio eletrônico», *Estudos Multidisciplinares sobre Integração*, org. Fábio Luiz Gomes, Editora Lumen Juris, Rio de Janeiro, 2004, p. 5-21, bem como a série de trabalhos publicados nos *Estudos de Direito do Consumidor*, dirigidos por António Pinto MONTEIRO, designadamente: «A protecção jurídica do consumidor no quadro da directiva sobre o comércio electrónico», EDC 2(2000), p. 43-140, «Os pactos atributivos de jurisdição nos contratos electrónicos de consumo», EDC 3(2001), p. 281-300, «Comércio electrónico e consumidor», EDC 6(2004), p. 341-400, «A via electrónica da negociação (alguns aspectos)», EDC 8 (2006/2007), p. 275-290, e «Comércio eletrônico de conteúdos digitais: proteção do consumidor a duas velocidades?», EDC 9 (2015), p. 177-207. Destacando a importância empresarial do comércio eletrônico veja-se também os nossos «A Globalização, a OMC e o Comércio Electrónico», *Revista Sequencia (UFSC)* nº 45 (2002), p. 173-195, Idem, «Empresa, comércio electrónico e propriedade intelectual», *Nos 20 Anos do Código das Sociedades Comerciais, Homenagem aos Professores Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier*, coord. António Pinto Monteiro, Vol. I - Congresso Empresas e Sociedades, Coimbra Editora, 2007, p. 439-478.

as cláusulas contratuais tais como as que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas pela Internet ou, tratando-se de contratos de adesão, não permitam ao contratante recorrer aos tribunais do Brasil para dirimir litígios decorrentes de serviços prestados no Brasil (art. 8.º).

Comparando a referida remissão para a ‘natureza da internet, seus usos e costumes’, com o teor imperativo dos direitos e garantias do usuário, torna-se claro que o *Marco Civil da Internet* afirma a prevalência destes últimos, enquanto condições básicas de exercício da cidadania na Internet, sobre as políticas de privacidade e os termos de utilização praticados (e estabelecidos unilateralmente) pelos provedores de serviços na internet. No ano anterior à comemoração do 800.º aniversário da *Magna Carta Libertatum* (1215), o Marco Civil da Internet surge como uma *Bill of Rights* do usuário da internet, em especial quando atua nas vestes de consumidor.

Para além de consagrar direitos fundamentais do usuário, o Marco Civil intervém no modo de ser da internet ao estabelecer princípios cardiais sobre o seu funcionamento, como o da neutralidade. Ou seja, em vez de remeter para a natureza da internet, como parecia à primeira vez, o Marco Civil procura modelar normativamente a natureza da rede segundo os parâmetros constitucionais vigentes, num contexto de concorrência de direitos fundamentais.⁶

1.3. O PRINCÍPIO DA NEUTRALIDADE OU ISONOMIA DA REDE

O princípio da neutralidade de rede é enunciado na secção I do capítulo III e no essencial consiste no dever que impende sobre os provedores de conexão de internet de tratar de

⁶ Sobre o tema, Alexandre Dias PEREIRA, «Concorrência de Direitos Fundamentais na «Constituição da Informação», *Estudos em Homenagem ao Prof. Doutor Jorge de Figueiredo Dias*, org. Manuel da Costa ANDRADE e Maria João ANTUNES, Vol. IV, Coimbra Editora, 2010, p. 795-831

forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço terminal ou aplicação (art. 9.º). Assim se consagra na forma de lei o *princípio da neutralidade da rede*.⁷

A discriminação ou degradação do tráfego só é permitida nos termos de um regulamento da competência do Presidente da República e apenas poderá ter lugar em virtude de requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações e priorização dos serviços de emergência (art. 9.º, § 1). Em todo o caso, estabelece o § 2 do mesmo preceito, que o responsável pela discriminação deve abster-se de causar danos aos usuários (1), agir com proporcionalidade, transparência e isonomia (2), informar previamente de modo transparente, claro e suficientemente descritivo os seus usuários sobre as práticas de gestão e mitigação de tráfego adotadas, incluindo as relativas a segurança (3), e oferecer serviços em condições comerciais não discriminatórias abstendo-se de praticar condutas anticoncorrenciais (4).

O princípio da neutralidade significa, deste modo, que a rede deve ser igual para todos: ao comprar um plano de internet, o usuário paga somente pela velocidade contratada e não pelo tipo de conteúdo. As empresas não poderão, então, diminuir a velocidade da conexão para serviços de voz por IP para dificultar o uso de serviços de comunicações (e.g. Skype) ou reduzir a banda de um produto de uma empresa concorrente, por exemplo.

Todavia, o Marco Civil dá um significado mais profundo ao princípio da neutralidade da rede, ao vedar aos provedores de conexão bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados (art. 9.º, § 3). Ou seja, os provedores de conexão ficam impedidos de interferir nas comunicações dos usuários, cabendo-lhes, portanto, um papel estritamente

⁷ Vide Rolf WEBER, Romana WEBER, *Internet of Things – Legal Perspectives*, Berlin, Springer, 2010.

neutral, mesmo em caso de conflitos entre terceiros e os usuários por razões, por exemplo, de violação de direitos autorais ou outros. Não podem bloquear, nem monitorar, filtrar ou analisar o conteúdo dos pacotes de dados que circulam na internet para a qual fornecem acesso. Não apenas não têm um dever de vigilância, como lhes é imposto uma obrigação de não interferir com as comunicações dos utilizadores dos seus serviços.⁸

1.4. CONTROLO DO TRÁFICO DE DADOS PESSOAIS E DA PRIVACIDADE

Uma das principais preocupações do Marco Civil da Internet é, como vimos, assegurar a proteção dos dados pessoais e das comunicações privadas. Não era certa a proteção do sigilo das comunicações eletrônicas (e-mail, sms, etc) antes de o Marco Civil entrar em vigor. Aliás, pouco antes da aprovação da Lei, a Presidente Dilma defendeu a necessidade de proteger a privacidade na Internet, na sequência do escândalo das escutas a que estaria a ser sujeita juntamente com a sua congénere alemã, tendo ambos os países apresentado uma proposta de resolução nesse sentido.⁹

Nos termos do Marco Civil, o prestador responsável pela guarda desses dados só pode ser obrigado a disponibilizar os registros de conexão e de acesso a aplicação na internet em termos que permitam a identificação do usuário ou do terminal mediante ordem judicial (art. 10.º § 1), o mesmo valendo para

⁸ Sobre o tema, na perspetiva do direito da União Europeia especialmente no domínio dos direitos autorais, podem ver-se os nossos «Direitos de autor e acesso à Internet: uma relação tensa», *Direito Autoral e Interesse Público, Anais do IV Congresso de Direito de Autor e Interesse Público*, org. Marcos WACHOWICZ e Manoel J. Pereira dos SANTOS, Universidade Federal de Santa Catarina – UFSC, Fundação Boiteux, Florianópolis, 2010, p. 98-105; e «A Partilha de Ficheiros na Internet e Direito Autoral: Desenvolvimentos Legislativos e Jurisprudenciais na Europa», *Revista da ABPI*, No 123 (2013) p. 53-62.

⁹ <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-11-03/proposta-sobre-privacidade-na-internet-deve-ter-prioridade-na-onu-diz-dilma>

o conteúdo das comunicações privadas, devendo o juiz proceder nos termos do princípio da legalidade, sem prejuízo do acesso pelas autoridades administrativas competentes aos dados cadastrais que informem qualificação pessoal, filiação e endereço (art. 10.º § 3).

Quanto ao âmbito de aplicação da lei no espaço, o Marco Civil abrange qualquer operação de recolha, armazenamento, guarda e tratamento de registos de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra no território brasileiro, ainda que só um dos terminais esteja localizado no Brasil (art. 11º). A lei aplica-se a empresas estabelecidas fora do Brasil, mas que prestem os seus serviços ao público brasileiro ou cujo grupo económico tenha estabelecimento no Brasil (art. 11.º, § 3).

Além disso, sobre os provedores de conexão e de aplicações recai um dever de reportar às autoridades brasileiras o modo de cumprimento da legislação do Brasil sobre proteção de dados pessoais e sigilo de comunicações, em termos a regulamentar (art. 11.º § 3). A infração destas obrigações sujeita os responsáveis a diversas sanções, incluindo multa até 10% do facturamento líquido do grupo económico no Brasil no seu último exercício, suspensão ou mesmo proibição de exercício das atividades em causa (art. 12º). Faz recordar as sanções do direito da concorrência da União Europeia, se bem que aqui sejam ainda mais severas já que as multas podem chegar a 10% do volume negócios e não apenas do facturamento líquido.¹⁰

¹⁰ Sobre a relação entre direitos de propriedade intelectual e o direito de concorrência no mercado dinâmico dos programas de computador, caracterizado pelo efeito de rede, veja-se, na jurisprudência, o acórdão do TPI de 17 de setembro de 2007, proc. T - 201/04, *Microsoft Corp. v Commission of the European Communities*. Sobre este importante acórdão, no contexto da jurisprudência do TJUE, com mais referências, pode ver-se o nosso «Software Interoperability, Intellectual Property and Competition Law: Compulsory Licenses for Abuse of Market Dominance», *Computer Law & Security Review*, 27 (2011) p. 175-179.

1.5. CONSERVAÇÃO DE DADOS DE TRÁFEGO

Por outro lado, os provedores de conexão têm o dever de guardar, em sigilo, os dados de conexão pelo prazo de 1 ano (art. 13). Esta responsabilidade não pode ser transferida a terceiros (art. 13 §1), parecendo ficar vedado o recurso a soluções de outsourcing de computação em nuvem (*cloud computing*). Mediante ordem judicial ou administrativa o prazo de conservação pode ser alargado (art. 13 §2). Em qualquer caso, depende de autorização judicial a disponibilização aos requerentes dos registros dos dados de conexão (art. 13 § 5).

De todo o modo, o dever de conservação abrange apenas os dados de conexão, sendo vedado ao provedor de conexão guardar os registros de acesso a aplicações de Internet (art. 14). A conservação destes dados cabe ao provedor de aplicações de Internet (‘pessoa jurídica que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos’), ou seja, o provedor de aplicações tem o dever de manter os registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança pelo prazo de 6 meses. Os outros provedores de aplicações poderão ser obrigados por ordem judicial a conservar esses registros relativos a fatos específicos por período determinado (art. 15º, §1) e a disponibilização ao requerente desses registros depende de autorização judicial (art. 15º, § 3). À semelhança da conservação de dados de conexão, também a disponibilização de dados de aplicações a terceiros fica sujeita a controlo judicial, em virtude de se tratar de uma matéria que colide com a tutela do direito fundamental à vida privada e, como é hoje comumente referido, o direito fundamental à “autodeterminação informacional”¹¹. Direito este que se manifesta também no princípio da especialidade, consagrado pelo Marco Civil no sentido de que o provedor de

¹¹ Acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1, Rel. Helena MONIZ – www.dgsi.pt

aplicações não pode guardar registros de acessos a outras aplicações sem consentimento do titular dos dados, nem registros de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular (art. 16º).

1.6. LIBERDADE DE EXPRESSÃO E RETIRADA DE CONTEÚDOS: A RESPONSABILIDADE DOS PROVEDORES DE CONEXÃO

Como atrás referido, um dos eixos do Marco Civil é a preservação da liberdade de expressão, de comunicação e de manifestação de pensamento, nos termos da Constituição Federal. Para o efeito, o provedor de conexão não é civilmente responsável por danos de conteúdos gerados por terceiros (art. 18º), salvo se, após ordem judicial específica que identifique claramente o conteúdo infrator e permita a sua localização, não tomar as providências para o tornar indisponível por período determinado (art. 19º, § 1).¹²

Por outro lado, as medidas cautelares contra infrações a bens e direitos de personalidade (honra, reputação, imagem) podem ser pedidas ao abrigo do Marco Civil (art. 19 §§ 3 e 4). Já as medidas cautelares contra infrações a direitos de autor ou a direitos conexos ficam dependentes de previsão legal específica¹³ e a sua adopção deverá expressamente respeitar a liberdade de expressão (art. 19 § 2).¹⁴ De todo o modo, tratando-se

¹² Para um estudo aprofundado sobre a situação anterior no Brasil, em especial na jurisprudência, vide Paulo Roberto BINICHESKI, *Responsabilidade civil dos provedores de Internet. Direito comparado e perspectivas de regulamentação no direito brasileiro*, Mestrado em Ciências Jurídicas, Faculdade de Direito da Universidade de Lisboa, 2008.

¹³ O que não parece ser o caso da lei dos direitos autorais: Lei nº 9.610, de 19 de fevereiro de 1998 - http://www.planalto.gov.br/ccivil_03/leis/L9610.htm

¹⁴ Em Portugal, por força da transposição da Diretiva 2004/48/CE do Parlamento Europeu e do Conselho de 29 de abril de 2004 relativa ao respeito dos direitos de propriedade intelectual Portugal, o Código do Direito de Autor e dos Direitos Conexos prevê, para além de uma norma sobre providências cautelares (art. 210º-G), uma outra especificamente dirigida aos intermediários, leia-se provedores de conexão e

de provedor de conexão, é necessária ordem judicial, visto estarem em jogo direitos fundamentais dos utilizadores dos serviços, em especial a liberdade de expressão e de comunicação.

Já no caso de provedor de aplicações fica a dúvida sobre a exigência de ordem judicial. O Marco Civil estabelece que o provedor de aplicações deverá comunicar ao usuário responsável pelo conteúdo, quando tiver os seus contatos, os motivos e informações relativos à indisponibilização de conteúdo, de modo a permitir o contraditório e a ampla defesa em juízo, podendo o usuário solicitar ao provedor que substitua o conteúdo indisponível pela motivação ou pela ordem judicial que fundamentou a indisponibilização (art. 20º). Ou seja, o Marco Civil parece validar as cláusulas habituais nos termos de utilização de serviço de vários provedores de aplicações nos termos das quais o provedor se reserva o direito de proceder à indisponibilização de conteúdos sempre que tenha motivos suficientes para tanto.

Todavia, a liberdade de expressão e a tutela judicial que o Marco Civil consagra em sede de provedores de conexão não é menos intensa, parece-nos, no âmbito dos provedores de aplicações. Pense-se, por exemplo, no *Facebook* ou em outras plataformas de redes sociais: deixar ao provedor de aplicações a indisponibilização de conteúdos colocados pelos seus utilizadores pode revelar-se uma solução excessivamente restritiva do ponto de vista da liberdade de expressão, ainda que dando oportunidade ao visado de se manifestar, à semelhança do procedimento de ‘*notice and take down*’ estabelecidos pela lei norte-americana *Digital Millennium Copyright Act* de 1998¹⁵, e que encontrou na lei portuguesa uma réplica com âmbito de

de aplicações (art. 227º). Sobre a adaptação dos direitos de autor ao ambiente digital e a origem da propriedade técnico-digital, pode ver-se a nossa monografia *Informática, direito de autor e propriedade tecno-digital*, Coimbra Editora: Coimbra, 2001.

¹⁵ Para um estudo desta lei em língua portuguesa pode ver-se o nosso «Direitos de autor, códigos tecnológicos e a Lei Milénio Digital», *Boletim da Faculdade de Direito, Universidade de Coimbra*, vol. 75 (1999), p. 475-521.

aplicação mais geral embora com ressalva expressa da liberdade de informação.¹⁶

Isto não obsta a que se reconheça que, relativamente a determinados conteúdos, se possa justificar um procedimento considerado mais expedito e eficaz. É o que sucede, por exemplo, com a pornografia infantil e que porventura deveria ser alargado a outras situações, nomeadamente quando estejam em causa conteúdos que incitem ou consistam na prática de crimes graves, como o terrorismo.

Neste sentido, o Marco Civil responsabiliza o provedor de aplicações de internet que disponibiliza conteúdo gerado por terceiros, subsidiariamente, pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de carácter privado, depois de ser notificado disso pelo participante ou seu representante legal (art. 21).

Nestes casos, o provedor de aplicações tem a obrigação de tornar esses indisponíveis, sob pena de responder, ainda que subsidiariamente, pelos referidos ilícitos. É uma norma que se dirige especialmente às redes sociais, mais ou menos abertas, onde são colocadas cenas de nudez ou atos sexuais de carácter privado, tanto de maiores como de menores. A utilização de *smartphones*, com todas as funcionalidades que se lhes conhecem, coloca nas mãos de qualquer pessoa uma arma fortemente intrusiva na vida privada, não apenas pela captação de imagens e sons, mas também pela sua divulgação em sítios web, incluindo redes sociais, com um potencial lesivo extremamente forte e que tem afetado em crianças e adolescentes, mas também adultos, particularmente em situações de ruturas de relação.

¹⁶ Decreto-Lei n.º 7/2004 de 7 de janeiro. A lei parece admitir medidas com efeito semelhante, ordenadas por autoridades administrativas, o que, todavia, pode suscitar questões de constitucionalidade por ofensa aos direitos fundamentais dos usuários da internet.

1.7. FORNECIMENTO DE REGISTROS DE CONEXÃO OU DE ACESSO A APLICAÇÕES DE INTERNET

O fornecimento de registros de conexão ou de acesso a aplicações de internet fica sujeito a controle judicial. Apenas pode ser ordenado pelo juiz e unicamente para efeitos probatórios em processo judicial cível ou criminal mediante requerimento do interessado, que deve cumprir certos requisitos específicos (art. 22º): existência de fundados indícios da ocorrência do ilícito, justificação da utilidade dos registros, e período a que respeitam.

1.8. PODER PÚBLICO

O poder público é igualmente destinatário do Marco Civil, que lhe impõe um dever geral de atuação no sentido do desenvolvimento da internet no Brasil em termos de governação plural e deveres mais específicos de racionalização e interoperabilidade tecnológica dos serviços públicos eletrônicos (*e-Government*), de utilização preferencial de normas abertas e livres, de otimização da infraestrutura e implantação de centros de dados, e de desenvolvimento da literacia digital (art. 24º).

Além disso, o dever constitucional de o Estado prestar educação é alargado à capacitação para o uso seguro, consciente e responsável da Internet como ferramenta da cidadania (art. 26), devendo as aplicações de internet do poder público buscar acessibilidade a todos os interessados, incluindo os que têm necessidades especiais, e promover a inclusão digital, reduzir as desigualdades no acesso às tecnologias, e fomentar a produção de conteúdo brasileiro (art. 27).

É questionável o efeito útil destas normas, embora nos pareça que têm um valor sobretudo programático, i.e., estabelecem um conjunto de orientações e regras que devem ser observadas pelo poder público no que respeita à utilização da

internet. Por exemplo, o dever de utilização preferencial de normas abertas e livres não é certamente inócuo e não deverá deixar de ser respeitado pelo poder público, pese embora as sanções para o seu não cumprimento não serem claras¹⁷, à semelhança do que sucede com a garantia de liberdade de escolha de programa de computador para exercício do controlo parental (art. 29). De todo o modo, se outro mérito não tiver, terá pelo menos o de consagrar um conjunto de princípios orientadores que não deixarão de ter impacto ao nível do controlo da validade dos atos do poder público no que respeita à utilização da internet.

2. O DIREITO DA UNIÃO EUROPEIA PARA A INTERNET

Passada em revista, nos seus traços fundamentais, a Lei

¹⁷ A lei portuguesa das normas abertas estabelece a nulidade dos atos administrativos que excluam soluções baseadas em normas abertas (Lei 36/2011, de 21 de junho, e Regulamento 91/2012, de 8 de novembro). Adotada com o intuito de promover a ‘liberdade tecnológica dos cidadãos’ e a interoperabilidade dos sistemas informáticos do Estado, esta lei estabelece a nulidade de todo e qualquer ato contratual da AP que exclua as normas abertas, tal como previsto no regulamento nacional da interoperabilidade digital. Complementa, por isso, o regime da contratação pública estabelecido pelo Código dos Contratos Públicos (Decreto-Lei 18/2009, com alterações posteriores). Sobre o tema veja-se o nosso «Normas abertas nos sistemas informáticos do Estado», Revista do CEDOUA No 29 (2012), 39-43. Sobre as licenças de software, com referências, *vide*, do mesmo Autor, «Contratos de licenças de software e de bases de dados», *Contratos de Direito de Autor e de Direito Industrial*, org. Carlos Ferreira de Almeida, Luís Couto Gonçalves e Cláudia Trabuco. Coimbra: Almedina, 2011, p. 345-368; Idem, «As licenças de software livre e *open source* (FOSS) como ferramenta de equidade tecnológica», *O contrato na gestão do risco e na garantia da equidade*, coord. António Pinto MONTEIRO, Instituto Jurídico, Coimbra, 2015, p. 111-131. A interoperabilidade está consagrada na Lei das comunicações eletrónicas e é um imperativo no direito de autor da União Europeia ao ponto de justificar a chamada exceção de descompilação e estar na base do célebre acórdão *Microsoft* no qual a empresa norte-americana foi condenada por abuso de posição dominante ao não permitir aos seus concorrentes o desenvolvimento de soluções compatíveis com o sistema operativo *Windows*. *Vide* o nosso «Inovação tecnológica, propriedade intelectual e defesa da concorrência no mercado do software», *Boletim da Faculdade de Direito, Universidade de Coimbra*, vol. 85 (2009), p. 237-259.

Marco Civil da Internet, vejamos seguidamente quais são os seus reflexos no direito da União Europeia. Antes, porém, cumpre destacar o papel do direito da EU para a Internet, também conhecida por sociedade da informação.

2.1. A SOCIEDADE DA INFORMAÇÃO COMO DOMÍNIO DA UNIÃO EUROPEIA

A propósito do bom funcionamento do mercado interno e, depois, da criação da sociedade da informação e da economia do conhecimento, a União Europeia tem afirmado competência privilegiada para regular a Internet em vários domínios¹⁸, ao ponto de a legislação nacional se limitar, praticamente, à transposição de Diretivas da UE.¹⁹ É o que se sucede, no-

¹⁸ Que se intensificará em vista da criação do mercado único digital anunciado na Comunicação da Comissão *A Digital Single Market Strategy for Europe*, COM(2015) 192 final. Todavia, frequentemente, a propósito da natureza transfronteiriça da Internet e da sociedade da informação, a União Europeia acaba harmonizando aspetos tradicionais do mundo real, ao ponto de as competências serem postas em cheque. Apontando já a tendência para na internet ser tudo competência da União, esvaziando o poder dos Estados-membros, *vide* José de Oliveira Ascensão, «Direito cibernético: a situação em Portugal», *Direito & Justiça* 2 (2001), p. 9 (apontando ainda outras características características do emergente “Direito Cibernético”).

¹⁹ Ver, por ex., Diretiva n.º 98/48/CE, do Parlamento Europeu e do Conselho, de 20 de Julho, relativa aos procedimentos de informação no domínio das normas e regulamentações técnicas e às regras relativas aos serviços da sociedade da informação (transposta pelo Decreto-Lei n.º 58/2000, de 18 de abril), Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000 (transposta pelo Decreto-Lei n.º 7/2004, de 7 de janeiro, alterado pelo Decreto-Lei n.º 62/2009, de 10 de março, e pela Lei n.º 46/2012, de 29 de agosto), 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 (transposta pela Lei 67/98, de 26 de outubro), 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 (transposta pela Lei n.º 41/2004, de 18 de agosto, alterada pela Lei 46/2012, de 29 de agosto, que transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE); Diretiva n.º 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva

meadamente, nos domínios da proteção dos programas de computador e das bases de dados pelos direitos de autor e pela harmonização destes direitos no âmbito da sociedade da informação (leia-se, informática em rede ou internet), da proteção do consumidor na contratação a distância, em especial por via eletrónica, da proteção dos dados pessoais e da vida privada nas comunicações eletrónicas, da responsabilidade civil dos provedores de internet, ou do princípio do país de origem no domínio do comércio eletrónico.

Além disso, é já significativa a jurisprudência do Tribunal de Justiça da União Europeia sobre questões jurídicas da internet em vários domínios, incluindo a responsabilidade dos prestadores de serviços da sociedade da informação pela violação de direitos exclusivos (por ex., marcas ou direitos de autor).²⁰ O desenvolvimento da computação em nuvem²¹ será

n.º 93/13/CEE do Conselho, e a Diretiva n.º 1999/44/CE, do Parlamento Europeu e do Conselho, e que revoga a Diretiva 85/577/CEE, do Conselho e a Diretiva n.º 97/7/CE, do Parlamento Europeu e do Conselho (transposta pelo Decreto-Lei n.º 24/2014, de 14 de fevereiro, com alterações posteriores); 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 (transposta pelo Decreto-Lei n.º 95/2006, de 29 de maio, com alterações posteriores). No domínio do Direito Penal, que é um reduto da soberania dos Estados-Membros, note-se que a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

²⁰ Para uma resenha de decisões entre 2004 e 2014, *vide* Koen LENAERTS, «The Case Law of the ECJ and the Internet (2004-2014)», *ELTE Law Journal*, 2014/1, p. 9-26.

²¹ Nos termos da Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Explorar plenamente o potencial da computação em nuvem na Europa*, COM(2012) 529 final, Bruxelas, 27.9.2012, “A «computação em nuvem» em termos simples pode ser entendida como o armazenamento, tratamento e utilização de dados em computadores remotos a que se acede através da Internet. Isto significa que os utilizadores podem controlar, mediante pedido, uma capacidade computacional quase ilimitada, que não têm de realizar grandes investimentos de capital para satisfazer as suas necessidades e que podem ter acesso aos seus dados em qualquer local através de ligação à Internet. A computação em nuvem permite reduzir substancialmente as despesas informáticas dos utilizadores e desenvolver uma grande quantidade de novos serviços. Recorrendo à computação em nuvem, as empresas, mesmo as de

acompanhado, seguramente, de outras iniciativas de harmonização.

Vejamos então alguns aspetos do direito da União Europeia para a Internet que encontram reflexo no Marco Civil.

2.2. PROTEÇÃO DO CONSUMIDOR NA INTERNET

A proteção do consumidor na Internet, em especial no comércio eletrónico, tem justificado a intervenção do legislador da União Europeia. Desde logo, a Diretiva 2000/31 consagrou algumas medidas especiais, reforçada pela transposição para o direito interno através do Decreto-Lei 7/2004, e mais tarde pela Diretiva 2011/83 sobre direitos dos consumidores²², transposta pelo DL 24/2014, de 14 de fevereiro²³, que acrescem à legislação existente sobre cláusulas abusivas, práticas comerciais desleais ou garantias nas vendas de bens de consumo. Para completar os direitos do consumidor em contratos de compra e venda em linha ou outras vias a distância, bem como no fornecimento de conteúdos digitais, estão em discussão duas propostas de Diretivas, já anunciadas aliás na Comunicação da Comissão sobre uma Estratégia do Mercado Único Digital para a Europa.²⁴

Para além do DL 24/2014, que corresponde já à 3ª geração de leis de proteção do consumidor nas vendas ao domicílio,

menor dimensão, podem penetrar em mercados cada vez maiores e as administrações públicas podem tornar os seus serviços mais atraentes e eficientes, contendo ao mesmo tempo as despesas.”

²² Diretiva n.º 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva n.º 93/13/CEE do Conselho, e a Diretiva n.º 1999/44/CE, do Parlamento Europeu e do Conselho, e que revoga a Diretiva n.º 85/577/CEE, do Conselho e a Diretiva n.º 97/7/CE, do Parlamento Europeu e do Conselho.

²³ Decreto-Lei n.º 24/2014, de 14 de fevereiro, alterado pela Lei n.º 47/2014, de 28 de julho.

²⁴ A Digital Single Market Strategy for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2015) 192 final.

pode ainda referir-se o Decreto-Lei nº 95/2006, de 29 de maio, no que respeita à resolução dos contratos relativos a serviços financeiros prestados a consumidores celebrados através de meios de comunicação à distância.²⁵

2.3. PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE NAS COMUNICAÇÕES ELETRÓNICAS

O direito da União Europeia assegura um elevado nível de proteção de dados pessoais²⁶ e da privacidade nas comunicações à distância, estando em vias de aprovação um Regulamento que unificará o regime jurídico de todos os Estados-Membros da UE.²⁷

Em Portugal o regime jurídico é estabelecido pela chamada Lei da Proteção de Dados Pessoais²⁸, que desenvolve o comando constitucional de proteger as pessoas contra a utilização da informática (art. 35º CRP).²⁹ A Lei 67/98 delimita o seu

²⁵ Transpõe para a ordem jurídica interna a 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.

²⁶ A Comunidade Europeia adotou a Diretiva 95/46/CE, e mais tarde a proteção dos dados pessoais foi consagrada no Artigo 8º da Carta de Direitos Fundamentais da União.

²⁷ <http://ec.europa.eu/justice/data-protection/>

²⁸ Lei n.º 67/98 de 26 de outubro. Revogou a Lei 10/91, de 29 de abril, e transpôs 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. Sobre a proteção jurídica dos dados pessoais, Garcia Marques & Lourenço Martins, *Direito da Informática*, 2.ª ed., Coimbra, Almedina, 2006, p. 129-313, 330-391, 422-442; 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, p. 173-183; Catarina Sarmento e Castro, *Direito da informática, privacidade e dados pessoais*, Almedina, Coimbra, 2005.

²⁹ No direito internacional ver, designadamente, a Declaração Universal do Direitos do Homem (Art. 12º), o Protocolo Internacional dos Direitos Cívicos e Políticos (Art. 17), a Convenção Europeia dos Direitos Humanos (Art. 8), a Convenção No 108 do Conselho da Europa, adotada em Estrasburgo, a 28 de janeiro de 1981), para além de recomendações várias, incluindo a nº 171 da OIT, e das linhas Directrizes

âmbito de aplicação, não apenas material (noção de dados pessoais), mas também geográfico (prestador estabelecido em Portugal independentemente da origem e do destino dos dados) e subjetivo (i.e. os destinatários do regime jurídico, abrangendo tanto empresas como organismos públicos, e com exclusão de atividades puramente domésticas ou particulares).³⁰ O tratamento de dados pessoais está sujeito a obrigação de notificação à Comissão Nacional de Proteção de Dados³¹ (art. 27º), mero registo ou autorização prévia (e.g. dados sensíveis, dados de crédito e solvabilidade).

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”³², incluindo os dados de IP na medida

da OCDE, da ONU, do Acordo Schengen. Inclusivamente, no âmbito da Organização Mundial do Comércio, o Acordo Geral de Comércio e Serviços de 15 de abril de 1994, prevê a proteção de dados (Art. XIV). No direito comparado aponta-se a lei do Land alemão do Hesse, de 30 de setembro de 1970 como a primeira lei de proteção de dados.

³⁰ 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, art. 6º), que estabelecia o período de conservação de 1 ano foi julgada inválida pelo Tribunal de Justiça no acórdão de 8 de abril de 2014, proc. C-293/12 e C-594/12, *Digital Rights Ireland*. Como vimos atrás, 1 ano é o prazo de conservação de dados a cargo do provedor de conexão previsto na Lei Marco Civil da Internet (art. 13).

³¹ A CNPD é a entidade administrativa independente que tutela esta matéria, tendo competências consultivas, decisórias, de fiscalização, e pedagógicas. As consequências da violação do regime de proteção de dados pessoais incluem sanções administrativas, sanções criminais e outras medidas.

³² Acórdão do Tribunal de Justiça de 6 de novembro de 2003, proc. C-101/01, *Bodil Lindqvist*.

em que tornam identificável a pessoa (Diretiva 67/98, 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 singular³³, o regime dos dados pessoais é limitado às pessoas coletivas.

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 (art. 3º-b).³⁴

Vários 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).

³³ 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” (acórdãos nº 569/98 e 174/00).

³⁴ Vide o acórdão do Tribunal de Justiça de 20 de maio de 2003, procs. C-465/00, 138/01 e 139/01.

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.³⁵ 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.³⁶ 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”.³⁷

A proibição geral de tratamento de dados pessoais está sujeita a certas causas de licitude de tratamento de dados pessoais (art. 6 da Lei 67/98): o consentimento do titular, a execução de contrato ou diligências prévias à sua formação ou declaração de vontade negocial do titular de dados; a obrigação legal do responsável do tratamento; a proteção de interesses vitais do titular dos dados, a incapacidade para consentir do titular dos dados; a execução de missão de interesse público ou exercício de autoridade pública; a 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. Quanto ao tratamento de dados sensíveis

³⁵ Ver, por ex., Decreto-Lei n.º 28/2004, de 4 de fevereiro (com alterações posteriores).

³⁶ De acordo com o Supremo Tribunal de Justiça (acórdão de 20 de junho de 2001), essa hipótese abrangerá os postos de combustíveis.

³⁷ Art. 20º do Código do Trabalho, aprovado pela Lei n.º 7/2009, de 12 de fevereiro, com alterações posteriores.

(art. 7º), a regra geral é também a da proibição, ainda que sujeita, todavia, a causas excepcionais de licitude, como sejam a existência de consentimento do titular ou de autorização legal específica, a cláusula geral prevista no art. 7º/3, e o regime dos dados de saúde.

O tratamento de dados pessoais rege-se por certos princípios fundamentais, a saber: transparência, finalidade, qualidade dos dados (licitude e lealdade; adequação, pertinência e proporcionalidade; exatidão e atualização). Os titulares dos dados têm diversos direitos, como sejam o direito de acesso aos dados, o direito de informação, bem como o chamado “direito ao esquecimento”, seja pela existência de um prazo máximo de conservação, seja por via da retificação, atualização, apagamento ou bloqueio de acesso aos dados. É ainda previsto o direito a não sujeição a decisão individual automatizada, bem como o direito de oposição, em especial no marketing direto, e o direito ao não tratamento de dados sensíveis. A conservação dos dados está sujeita a um prazo, regendo-se pelos princípios da proporcionalidade e da finalidade.

São obrigações do responsável pelo tratamento preservar a segurança do tratamento de dados e a sua confidencialidade (dever de sigilo), e a obrigação de colaboração, prestando informações, permitindo a realização de inspeções, facultando documentos, etc.

Quanto à transferência de dados pessoais para outros países, rege a liberdade de circulação de dados entre países da União Europeia (art. 18º). Relativamente a países terceiros, se a Comissão considerar que o país terceiro oferece um nível adequado de proteção, permite-se a transferência. Era o que sucedia, por exemplo, com o protocolo de *Safe Harbor* de transferência de dados da União Europeia para os EUA, que todavia o Tribunal de Justiça declarou inválido.³⁸ Entretanto, a jurisprudência

³⁸ Acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*: “1) O art. 25.º, n.º 6, da Diretiva 95/46/CE do Parlamento

dência do Tribunal de Justiça tem sido especialmente relevante no domínio dos dados pessoais e da privacidade nas comunicações eletrónicas, como o atesta igualmente o acórdão *Google c Costeja González* a propósito do chamado “direito ao esquecimento”. Vejamos.

2.4. “DIREITO AO ESQUECIMENTO”?

No acórdão *Google c. Costeja Gonzalez*³⁹, o Tribunal de Justiça pronunciou-se sobre o chamado “direito ao esquecimento” nos termos da 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.

O Tribunal decidiu que “o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na

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, conforme alterada pelo Regulamento (CE) n.º 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos art.s 7.º, 8.º e 47.º 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.º 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.” De notar que, 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).

³⁹ 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).

seqüência 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 seqüência 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.º e 8.º 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.”⁴⁰

⁴⁰ Sobre o acórdão *Google c Costeja González*, vide JONES, «Control-alter-delete: the ‘right to be forgotten’», *EIPR* 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, «*Google Spain SI 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, «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; Indra SPIECKER, «A new

A Diretiva 95/46 garante às pessoas em causa o direito de obterem do responsável pelo tratamento, consoante o caso, a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpre o regime estabelecido pela Diretiva, nomeadamente devido ao carácter incompleto ou inexato desses dados (art. 12º/b). No caso em concreto, o nome do cidadão espanhol aparecia numa lista de resultados de pesquisa do Google no âmbito de um processo de dívidas já antigo. 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 *Google Inc.* norte-americana, 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.

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 pes-

quisa da Google de apresentar a página de origem onde a informação está disponível.

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”.⁴¹

Todavia, a maior inovação deste acórdão terá sido a definição do âmbito territorial, falando-se a propósito no princípio da territorialidade alargado (*‘principle of territoriality extended’*).⁴² 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.⁴³

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

⁴¹ Indra SPIECKER, «A new framework for information markets: Google Spain Spiecker», *cit.*, p. 1040-1 (com referência ao caso *Satamedia*, C-73/07, EU:C:2008:727).

⁴² 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.”).

⁴³ Nos termos do art. 4º da Diretiva 95/46, sobre o direito nacional aplicável, “1. Cada Estado-membro aplicará as suas disposições nacionais adotadas por força da presente diretiva ao tratamento de dados pessoais quando: a) O tratamento for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável”.

terra a estratégia das empresas que estabelecem sucursais na União Europeia para tratar dos assuntos comerciais enquanto o tratamento dos dados pessoais é efetuado pelas casas-mãe nos EUA (por ex. *Google, Facebook*).

O tribunal considera, à luz de casos anteriores (*Lindqvist*, C-101/01; *Satamedia*, C-73/07) que há tratamento de dados na atividade de encontrar dados na internet, indexá-los automaticamente, armazena-los ainda que temporariamente e finalmente disponibilizá-los na internet aos utilizadores a seu pedido segundo uma ordem de preferência determinada pelo motor de pesquisa. Acrescenta que o mero escanear (*scanning*) de informação já é tratamento de dados. O operador do motor de pesquisa é considerado o responsável pelo tratamento, isto é, a pessoa que determina os fins e os meios da atividade relevante dos dados mesmo que não seja a entidade fonte dessa informação.

Na opinião do Tribunal, o responsável pelo tratamento tem um dever de controlo ativo, no sentido de lhe caber o apagamento dos dados ilegalmente tratados mesmo que as pessoas afetadas não tomem medidas nesse sentido (para. 70-72).

Quanto a saber se o Tribunal terá ponderado devidamente os interesses relevantes, nos termos do art. 7º (o chamado *rectangle of interests*), 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 (para. 81). 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 art. 8 (para. 68-69),

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 Europeia:

“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.”⁴⁴

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 (para. 83). Em termos económicos, este acórdão levaria ao aumento dos custos de processamento de dados, com possível repercussão se no modelo de negócio dos motores de pesquisa. Em síntese:

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

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

⁴⁴ Indra SPIECKER, «A new framework for information markets: Google Spain Spiecker», *cit.*, p. 1055.

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

dados da pessoa na vida pública, etc., embora não tenha ido ao ponto de desenvolver uma teoria geral dos limites ao direito de imagem.⁴⁶

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 conduzir a ‘entregar os gansos à guarda da raposa’⁴⁷. Além disso, entende-se que a decisão pode colocar as pequenas e médias empresas em maiores dificuldades na concorrência em virtude dos investimentos que serão necessários em pessoal qualificado.

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

2.5. LIBERDADE DE EXPRESSÃO E RESPONSABILIDADE DOS PROVEDORES DE INTERNET

No que respeita à liberdade de expressão, em relação com a responsabilidade dos provedores de Internet, a Diretiva 2000/31/CE sobre comércio eletrónico estabelece um conjunto de regras sobre a matéria. Por um lado, os Estados-membros ficam impedidos de sujeitar os provedores de internet a uma obrigação geral de controlo dos conteúdos dos utilizadores dos seus serviços. Por outro lado, regula as atividade de mero transporte, armazenagem temporária e alojamento de conteúdos, no sentido de o fornecedor de internet não ser, à partida, responsável pela licitude dos conteúdos transmitidos ou colocados pelos utilizadores dos seus servidores.⁴⁸

⁴⁶ Considerando ter havido da parte do Tribunal ‘wise self-restraint’, Indra SPIECKER, «A new framework for information markets: Google Spain Spiecker», *cit.*, p. 1050.

⁴⁷ Indra SPIECKER, «A new framework for information markets: Google Spain Spiecker», *cit.*, p. 1053 (“This concept thus sets the fox to keep the geese.”).

⁴⁸ Para melhor estudo ficaram os procedimentos de aviso e retirada (*notice and take-*

Uma questão que tem sido debatida na Europa diz respeito à obrigação de instalação de filtros por parte das provedoras de Internet, de modo a controlarem os conteúdos que circulam na rede, em especial por razões de direitos de autor.⁴⁹

No caso *Scarlet c. Sabam* (proc. C-70/10), o Tribunal de Justiça da União Europeia (TJUE) foi chamado a esclarecer se as Diretivas 2001/29 (direitos de autor na internet) e 2004/48/CE (medidas processuais), conjugadas com as Diretivas 95/46 (dados pessoais), 2000/31 (comércio eletrónico) e 2002/58 (privacidade nas comunicações eletrónicas), interpretadas à luz dos arts. 8.º e 10.º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, permitem que os Estados-Membros confirmem competência a um juiz nacional, requerido no âmbito de um processo principal e com base numa única disposição legal que prevê que: «[o juiz] pode igualmente dirigir uma injunção de cessação aos intermediários cujos serviços sejam utilizados por um terceiro para violar os direitos de autor ou um direito conexo», para ordenar a um fornecedor de acesso à Internet (abreviadamente «FAI») o estabelecimento, em relação a toda a sua clientela, em abstrato e a título preventivo, a expensas exclusivas desse FAI e sem limitação no tempo, de um sistema de filtragem de todas as comunicações eletrónicas, tanto as que entram, como as que saem, transitando pelos seus serviços, nomeadamente através da utilização de software *peer-to-peer*, com vista a identificar na sua rede a circulação de ficheiros eletrónicos contendo uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega possuir direitos, e bloquear de seguida a transferência desses ficheiros, seja no momento do pedido, seja no momento do envio.

down) consagrados pela norte-americana *Digital Millennium Copyright Act* (DMCA).

⁴⁹ Seguimos de perto o nosso «A Partilha de Ficheiros na Internet e Direito Autoral: Desenvolvimentos Legislativos e Jurisprudenciais na Europa». *Revista da Associação Brasileira da Propriedade Intelectual*, nº 123 (2013) p. 53-62.

Em caso de resposta afirmativa à primeira questão, estava em causa saber se essas Diretivas exigem que o juiz nacional, chamado a decidir sobre um pedido de injunção em relação a um intermediário cujos serviços são utilizados por um terceiro para violar os direitos de autor, aplique o *princípio da proporcionalidade* quando tiver de se pronunciar sobre a eficácia e o efeito dissuasor da medida requerida?

A Sociedade Belga de autores, compositores e editores (*Société belge des auteurs compositeurs et éditeurs - Sabam*) requereu uma medida provisória contra um fornecedor de acesso à Internet, a *Scarlet Extended SA*. De acordo com o pedido, a *Sabam* pretendia que fosse declarado que a troca não autorizada, pelo intermediário dos serviços fornecidos pela *Scarlet*, de ficheiros musicais efetuada nomeadamente através de *software peer-to-peer* representava violação dos direitos de autor sobre as obras musicais pertencentes ao seu repertório. Em consequência, a *Sabam* solicitava que a *Scarlet* fosse condenada a fazer cessar essas violações, impossibilitando ou paralisando qualquer forma de envio ou de receção pelos seus clientes, sob pena de aplicação de uma sanção pecuniária compulsória.⁵⁰

O tribunal de primeira instância, na decisão de 26 de novembro de 2004, declarou a existência destas violações dos direitos de autor, e mais tarde, na decisão de 29 de junho de 2007, condenou a *Scarlet*, na sequência de peritagem técnica, a cessar essas violações dos direitos de autor, tornando impossível, no prazo de seis meses e sob pena de aplicação de uma sanção pecuniária compulsória de 2,500 euros por cada dia de incumprimento, qualquer forma de envio ou receção pelos seus

⁵⁰ Por força da legislação nacional, os tribunais competentes belgas podem ordenar por via de injunção a cessação de qualquer violação de um direito de propriedade intelectual. Está previsto, em especial, que quando um terceiro utiliza os serviços de um intermediário para cometer uma violação deste tipo, os tribunais podem adotar injunções de cessação dirigidas a esse intermediário, tal como previsto nas Diretivas 2001/29 (art. 8º/3) e 2004/48 (art. 11º, 3º período).

clientes, através de software peer-to-peer, nomeadamente, de ficheiros contendo obra musical do reportório da *Sabam*. Inconformada com esta medida, a *Scarlet* interpôs recurso para o Tribunal de recurso de Bruxelas, o qual apresentou ao Tribunal de Justiça da União Europeia um pedido de decisão prejudicial: saber, em suma, se o direito da União e, em especial, os direitos fundamentais garantidos pela Carta dos Direitos Fundamentais permitem que um órgão jurisdicional nacional adote, sob a forma de injunção, uma medida que ordena a um fornecedor de acesso à Internet a instalação de um sistema de filtragem e de bloqueio das comunicações eletrónicas.

Na opinião do advogado-geral do TJUE, os tribunais não podem obrigar os prestadores de serviços de Internet a usar sistemas de bloqueio e de filtragem de conteúdos com o objetivo de proteger os direitos de autor, uma vez que tal sistema representa uma limitação ao direito de confidencialidade das comunicações e de proteção dos dados pessoais e ao direito à informação - direitos consagrados na Carta dos Direitos Fundamentais da União. Segundo Pedro Cruz-Villalón, o recurso aos sistemas de bloqueio e de filtragem só seria possível respeitando os requisitos de limitação do exercício dos direitos previstos na CDFU. Pelo que essa medida deveria estar consagrada, de forma clara e acessível, na legislação nacional dos vários países da União Europeia. Nas suas conclusões, o advogado-geral constata que o sistema a instalar deve garantir a filtragem de todas as comunicações de dados que circulam na rede da *Scarlet*, de forma a detetar as que implicam uma violação dos direitos de autor, e garantir o bloqueio das comunicações que impliquem efetivamente uma violação dos direitos de autor, seja ao nível do pedido seja no momento do envio.

A medida de injunção em causa revestiria a forma de uma obrigação de carácter geral destinada a ser alargada, a prazo, de forma permanente a todos os fornecedores de acesso à Internet, afetando duradouramente um número indeterminado

de pessoas coletivas ou singulares sem ter em conta a sua relação contratual com a *Scarlet* nem o seu Estado de residência. Seria aplicada em abstrato e a título preventivo, isto é, sem que se tenha verificado previamente uma violação efetiva ou mesmo um risco de violação eminente de um direito de propriedade intelectual. Além disso, a medida de injunção constituiria uma obrigação nova onerando o fornecedor de acesso de Internet com custos de instalação do sistema de filtragem e de bloqueio, e a responsabilidade jurídica e económica pelo controlo da pirataria P2P.

Pelas suas características, a instalação deste sistema de filtragem e de bloqueio constituiria uma limitação dos direitos ao respeito do segredo das comunicações e à proteção dos dados pessoais, e à liberdade de informação, valores protegidos pela Carta dos Direitos Fundamentais. Nesta ordem de ideias, o advogado-geral recordou que a limitação ao exercício destes direitos e liberdades é possível desde que, nomeadamente, esteja «prevista na lei». Em conformidade com a jurisprudência desenvolvida na matéria pelo Tribunal Europeu dos Direitos do Homem, Cruz-Villalón considera que uma limitação ao exercício dos direitos e liberdades garantidos pela Carta dos Direitos Fundamentais deve assentar numa base legal que responda às exigências relativas à «qualidade da lei» em causa. Por conseguinte, na sua opinião, uma limitação dos direitos e liberdades dos internautas como a que estava em causa só seria admissível se tivesse uma base legal nacional, acessível, clara e previsível.

Ora, segundo o advogado-geral, não se poderia considerar prevista de forma expressa, prévia, clara e precisa na disposição legal belga em questão, a obrigação de os fornecedores de acesso à Internet instalarem, inteiramente a expensas suas, o sistema de filtragem e de bloqueio. Por conseguinte, propôs que o Tribunal de Justiça declarasse que o direito da União se opõe à adoção por um tribunal nacional, com base na disposição legal belga, de uma medida que ordena a um fornecedor de

acesso à Internet a instalação, relativamente a toda a sua clientela, em abstrato e a título preventivo, exclusivamente a expensas suas e sem limitação no tempo, de um sistema de filtragem de todas as comunicações eletrónicas que passem pelos seus serviços (nomeadamente através de software *peer-to-peer*) com o fim de identificar na sua rede a circulação de ficheiros eletrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual terceiros pretendam deter direitos e seguidamente bloquear a transferência desses ficheiros, ao nível do pedido ou no momento do envio.

Tendo em conta a opinião do advogado-geral, o Tribunal de Justiça decidiu, no acórdão de 24 de novembro de 2011, que as Diretivas 2000/31, 2001/29, 2004/48, 95/46/, 2002/58, lidas conjuntamente e interpretadas à luz das exigências resultantes da proteção dos direitos fundamentais aplicáveis, devem ser interpretadas no sentido de que se opõem a uma medida inibitória que ordena a um fornecedor de acesso à Internet a instalação de um sistema de filtragem

- de todas as comunicações eletrónicas que transitam pelos seus serviços, nomeadamente através da utilização de software «peer-to-peer» (1)

- que se aplica indistintamente a toda a sua clientela (2)

- com carácter preventivo (3)

- exclusivamente a expensas suas (4) e

- sem limitação de tempo (5)

- capaz de identificar na rede desse fornecedor a circulação de ficheiros eletrónicos que contenham uma obra musical, cinematográfica ou audiovisual sobre a qual o requerente alega ser titular de direitos de propriedade intelectual (6),

- com o objetivo de bloquear a transferência de ficheiros cujo intercâmbio viole direitos de autor (7).

O Tribunal ponderou a necessidade de assegurar um justo equilíbrio entre os direitos de propriedade intelectual, por um lado, e a liberdade de empresa do FAI, a proteção dos da-

dos pessoais e a liberdade de informação dos utilizadores, por outro. Segundo o TJUE, a instalação deste sistema de filtragem implicaria que o FAI identificasse:

1º na totalidade das comunicações eletrónicas de todos os clientes, os ficheiros que fazem parte do tráfego P2P;

2º no quadro desse tráfego, os ficheiros que contêm obras sobre as quais os titulares dos direitos de propriedade intelectual alegam deter direitos;

3º que determinasse quais desses ficheiros eram trocados ilicitamente;

4º que procedesse ao bloqueio do intercâmbio de ficheiros que considerasse ilícito.

Deste modo, essa vigilância preventiva exigiria uma observação ativa da totalidade das comunicações eletrónicas efetuadas na rede do FAI em causa e, portanto, englobaria toda e qualquer informação a transmitir e todos os clientes que utilizam essa rede. Em suma,

“a medida inibitória aplicada ao FAI em causa de instalar o sistema de filtragem controvertido obrigaria a proceder a uma vigilância ativa de todos os dados relativos aos seus clientes a fim de prevenir qualquer violação futura dos direitos de propriedade intelectual. Daqui se conclui que a referida medida inibitória imporia a esse FAI uma vigilância geral que é proibida pelo art. 15.º, n.º 1, da Diretiva 2000/31. A referida medida inibitória implicaria uma violação da liberdade de empresa do FAI em causa, dado que o obrigaria a instalar um sistema informático complexo, oneroso, permanente e exclusivamente a expensas suas, o que de resto seria contrário às condições previstas no art. 3.º, n.º 1, da Diretiva 2004/48, que determina que as medidas para assegurar o respeito dos direitos de propriedade intelectual não sejam desnecessariamente complexas ou onerosas.

Acresce que os efeitos da referida medida inibitória não se limitariam ao FAI em causa, sendo o sistema de filtragem controvertido também suscetível de violar os direitos fundamentais dos clientes desse FAI, a saber, o seu direito à proteção dos dados pessoais, bem como a sua liberdade de receber ou de

enviar informações, direitos que são protegidos pelos arts. 8º e 10º da Carta. Com efeito, é ponto assente, por um lado, que a medida inibitória que ordena a instalação do sistema de filtração controvertido implicaria uma análise sistemática de todos os conteúdos e a recolha e identificação dos endereços IP dos utilizadores que estão na origem do envio de conteúdos ilícitos na rede, sendo esses endereços dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores.”

Além disso, a referida medida inibitória correria o risco de violar a liberdade de informação, dado que esse sistema poderia não distinguir suficientemente um conteúdo ilícito de um lícito, de modo que o seu acionamento poderia provocar o bloqueio de comunicações de conteúdo lícito. Sendo que a resposta à questão da licitude de uma transmissão dependeria também da aplicação de exceções legais aos direitos de autor que variam de um Estado-Membro para outro, já que em certos Estados-Membros determinadas obras podem pertencer ao domínio público ou os autores em causa optar por colocá-las gratuitamente à disposição do público na Internet.

O acórdão do Tribunal de Justiça parece ir mais longe do que a opinião do Advogado-Geral, no que respeita à substância da causa, já que este terá deixado em aberto a possibilidade de essa medida ser ordenada, ao abrigo da legislação nacional, desde que prevista em norma acessível, clara e previsível. Ao passo que o TJ afirma, claramente, que essa injunção seria contrária à proibição de sujeitar os FAI a uma obrigação de vigilância geral, aos regimes de proteção de dados pessoais e da privacidade nas comunicações eletrónicas e, ainda, ao direito fundamental de receber e trocar informação consagrado na CDFU.

O TJ recorda ainda que a violação de direitos de autor através de partilha em rede P2P depende da legislação de cada Estado-Membro. Não obstante, poderá encontrar-se neste acór-

dão do TJ uma sugestão de reflexão sobre a necessidade de maior harmonização das utilizações livres na União Europeia, visto que um tal sistema de filtragem e bloqueio de comunicações eletrónicas poderia impedir utilizações livres de obras protegidas por direitos de autor em determinados Estados-Membros.

Em conclusão, o Tribunal de Justiça erige a liberdade de informação, juntamente com a proteção dos dados pessoais e da privacidade, como valor fundamental da ordem jurídica da União Europeia, perspetivando os direitos de autor na Internet numa ótica de concorrência de direitos fundamentais segundo uma retórica argumentativa própria da metódica constitucional.⁵¹ Podemos até afirmar que, neste acórdão, o TJ afirmou-se, claramente, com jurisdição constitucional em sede de direitos fundamentais.⁵²

Não obstante, no acórdão de 27 de março de 2014⁵³, o Tribunal de Justiça pronunciou-se favoravelmente à possibilidade de uma injunção judicial contra um fornecedor de acesso, verificados certos requisitos. Nos termos do acórdão *Telekabel*,

«Os direitos fundamentais consagrados pelo direito da União devem ser interpretados no sentido de que não se opõem a que, através de uma injunção decretada por um juiz, um fornecedor de acesso à Internet seja proibido de facultar aos seus clientes o acesso a um sítio Internet em que é colocado em linha material protegido, sem a autorização dos titulares de direitos, quando essa injunção não especifica as medidas que esse fornecedor de acesso deve tomar e quando este último pode evitar, através da prova de que tomou todas as medidas razoáveis, as sanções pecuniárias compulsórias destinadas a

⁵¹ Desenvolvemos o tema da conciliação constitucional da liberdade de informação com os direitos de autor na nossa tese de doutoramento *Direitos de Autor e Liberdade de Informação*, Coimbra, Almedina, 2008, § 3.

⁵² Posteriormente, a jurisprudência do acórdão *Sabam c. Scarlet* foi confirmada no acórdão *Sabam c. Netlog*, de 16 de fevereiro de 2012 (proc. C-360/10, SABAM c. Netlog NV, ECLI:EU:C:2012:85).

⁵³ *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft GmbH*, Proc. C-314/12. ECLI:EU:C:2014:192.

reprimir a violação da referida proibição, desde que, por um lado, as medidas tomadas não impeçam desnecessariamente os utilizadores da Internet de acederem licitamente às informações disponíveis e, por outro, essas medidas tenham o efeito de impedir ou, pelo menos, de tornar dificilmente realizáveis as consultas não autorizadas de material protegido e de desencorajar seriamente os utilizadores da Internet que recorrem aos serviços do destinatário dessa mesma injunção de consultar esse material, colocado à sua disposição em violação do direito da propriedade intelectual, o que cabe às autoridades e aos órgãos jurisdicionais nacionais verificar.»

2.6. A NEUTRALIDADE TECNOLÓGICA

A neutralidade tecnológica é igualmente uma máxima do direito da União Europeia para a Internet.⁵⁴ Transpondo Diretivas da UE, a lei portuguesa das comunicações eletrónicas⁵⁵ prevê no art. 35º a eliminação de restrições às *neutralidades* tecnológica e de serviços. O novo art. 16º-A sob epígrafe “Neutralidade tecnológica e de serviços na gestão do espectro”, estabelece que compete à ARN garantir os princípios da neutralidade tecnológica e da neutralidade de serviços. O primeiro significa que “todos os tipos de tecnologia usados para os serviços de comunicações eletrónicas podem ser utilizados nas faixas de frequência declaradas disponíveis para os serviços de comunicações eletrónicas e como tal publicitadas no QNAF” (nº 1-a). O segundo significa que “nas faixas de frequências declaradas disponíveis para os serviços de comunicações eletrónicas e como tal publicitadas no QNAF podem ser prestados todos os tipos de serviços de comunicações eletrónicas” (nº 1-b).

A ARN apenas pode estabelecer restrições a estes princípios se as restrições forem proporcionais, não discriminató-

⁵⁴ ANACOM, Quadro regulamentar para as comunicações eletrónicas: União Europeia – disponível em <http://www.anacom.pt>

⁵⁵ Lei nº 5/2004, de 10 de fevereiro (com alterações posteriores).

rias e justificadas quanto à tecnologia utilizada para os serviços de comunicações eletrônicas e se forem necessárias para evitar interferências prejudiciais (a), proteger a população da exposição a campos eletromagnéticos (b), garantir a qualidade técnica do serviço (c), garantir a maximização da partilha das frequências (d), salvaguardar a utilização eficiente do espectro (e) ou assegurar o cumprimento de um objetivo específico de interesse geral definido nos termos da lei (nº 2). Além disso, a ARN pode também “estabelecer restrições proporcionais e não discriminatórias quanto aos tipos de serviços de comunicações eletrônicas a oferecer, nomeadamente, tendo em vista, sempre que necessário, o cumprimento de requisitos previstos nos regulamentos das radiocomunicações da União Internacional das Telecomunicações (UIT)” (nº 3).

Quanto a restrições à *neutralidade de serviços*, a ARN pode adotar medidas que imponham que um serviço de comunicações eletrônicas seja oferecido numa faixa de frequências específica, disponível para serviços de comunicações eletrônicas, desde que justificado com a necessidade de assegurar o cumprimento de um objetivo específico de interesse geral, por um lado, e a oferta de um determinado serviço de comunicações eletrônicas numa faixa de frequências específica com exclusão de qualquer outro serviço, desde que justificada com a necessidade de proteger serviços de segurança da vida humana ou, excepcionalmente, para satisfazer outros objetivos de interesse geral previstos na lei, por outro lado (art. 16º-A/4). Para efeitos deste regime entende-se por “objetivos específicos de interesse geral”, nomeadamente, a segurança da vida humana, a promoção da coesão social, regional ou territorial, a prevenção de utilizações ineficientes das frequências, bem como a promoção da diversidade cultural e linguística e do pluralismo dos meios de comunicação, designadamente através do fornecimento de serviços de programas televisivos ou de rádio (art. 16º-A/5). As restrições tanto à neutralidade tecnológica como à

neutralidade de serviços devem ser publicitadas no âmbito do QNAF, cabendo à ARN reavaliar, anualmente, a necessidade da sua manutenção (art. 16º-A/6).

Posteriormente, na União Europeia, foi aprovado o Regulamento 2015/2120 sobre Internet⁵⁶, consagrando o princípio da neutralidade tecnológica no sentido da não ser imposta a utilização de um tipo específico de tecnologia nem estabelecida qualquer discriminação que a favoreça (considerando 2). O Regulamento procura preservar o desenvolvimento da Internet enquanto “plataforma aberta à inovação com poucos obstáculos de acesso para os utilizadores finais, fornecedores de conteúdos, aplicações e prestadores de serviços de Internet” (considerando 3, 1ª parte). Todavia, as medidas adotadas são consideradas necessárias e adequadas tendo em conta “um número significativo de utilizadores finais é afetado por práticas de gestão do tráfego que bloqueiam ou tornam mais lentas algumas aplicações e serviços específicos. Essas tendências exigem que se estabeleçam a nível da União regras comuns que assegurem a abertura da Internet e evitem a fragmentação do mercado interno em resultado de medidas adotadas pelos Estados-Membros a título individual” (considerando 3, 2ª parte).

O princípio da neutralidade tecnológica não é consagrado, enquanto tal, na letra da lei, mas antes como garantia de acesso à internet aberta estabelecida no artigo 3º do regulamento, nos termos do qual é direito dos utilizadores finais “aceder a informações e conteúdos e de os distribuir, de utilizar e fornecer aplicações e serviços e utilizar equipamento terminal à sua escolha, através do seu serviço de acesso à Internet, independentemente da localização do utilizador final ou do fornecedor,

⁵⁶ Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) N° 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União.

ou da localização, origem ou destino da informação, do conteúdo, da aplicação ou do serviço”, sem prejuízo dos regimes legais relativos aos conteúdos, aplicações ou serviços (nº 1). Este direito de acesso aberto não pode ser limitado por “acordos entre os prestadores de serviços de acesso à Internet e os utilizadores finais sobre as condições comerciais e técnicas e sobre as características dos serviços de acesso à Internet, tais como preços, volumes de dados ou velocidade, e quaisquer práticas comerciais utilizadas por prestadores de serviços de acesso à Internet” (nº 2).

Por outro lado, sobre os prestadores de serviços de acesso à Internet impende um dever de tratar “equitativamente todo o tráfego, ao prestarem serviços de acesso à Internet, sem discriminações, restrições ou interferências, e independentemente do emissor e do recetor, do conteúdo acedido ou distribuído, das aplicações ou serviços utilizados ou prestados, ou do equipamento terminal utilizado”, sem prejuízo de medidas razoáveis de gestão do tráfego (nº 3).

O conceito de medidas razoáveis de gestão de tráfego é objeto de desenvolvimentos normativos. Com efeito, são consideradas razoáveis as medidas de gestão do tráfego que cumprem certos requisitos, a saber: transparência, não discriminação, proporcionalidade e justificação objetiva por razões de qualidade técnica. Nos termos do nº 3 do art. 3º:

“Para que possam ser consideradas razoáveis, essas medidas devem ser transparentes, não discriminatórias e proporcionadas, e não podem basear-se em questões de ordem comercial, mas sim na qualidade técnica objetivamente diferente dos requisitos de serviço de categorias específicas de tráfego. Essas medidas não podem ter por objeto o controlo de conteúdos específicos, nem podem ser mantidas por mais tempo do que o necessário. Os prestadores de serviços de acesso à Internet não podem estabelecer medidas de gestão do tráfego mais gravosas do que as medidas previstas no segundo parágrafo, e, em particular, não podem bloquear, abrandar, alterar, restringir, ou degradar conteúdos, aplicações ou serviços específicos, ou categorias específicas dos mesmos, nem estabelecer

discriminações entre eles ou neles interferir, exceto na medida do necessário, e apenas durante o tempo necessário, para:

- a) Dar cumprimento aos atos legislativos da União ou à legislação nacional conforme com o direito da União a que o prestador de serviços de acesso à Internet está sujeito, ou às medidas conformes com o direito da União que dão execução a esses atos legislativos da União ou a essa legislação nacional, incluindo decisões dos tribunais ou de autoridades públicas investidas de poderes relevantes;
- b) Preservar a integridade e a segurança da rede, dos serviços prestados através dela e dos equipamentos terminais dos utilizadores finais;
- c) Prevenir congestionamentos iminentes da rede e atenuar os efeitos de congestionamentos excepcionais ou temporários da rede, desde que categorias equivalentes de tráfego sejam tratadas equitativamente.”

Em relação aos dados pessoais, as medidas de gestão do tráfego só podem envolver o tratamento de dados pessoais se esse tratamento for necessário e proporcionado em relação à realização dos objetivos previstos no nº 3 (cumprir a lei, preservar a integridade e a segurança da rede, e prevenir ou atenuar congestionamento da rede) e respeitar o regime estabelecido pelas Diretivas 95/46/CE e 2002/58/CE (nº 4).

Por outro lado, o Regulamento ressalva expressamente a possibilidade de os prestadores de serviços de comunicações eletrónicas ao público (incluindo os prestadores de serviços de acesso à Internet) e os fornecedores de conteúdos, aplicações ou serviços oferecerem serviços diferentes dos serviços de acesso à Internet que estejam otimizados para conteúdos, aplicações ou serviços específicos, ou para uma combinação dos mesmos. Todavia, tal só é possível “*caso a otimização seja necessária para respeitar os requisitos dos conteúdos, aplicações ou serviços para um nível de qualidade específico*” (nº 5, *italico nosso*).

Além disso, os prestadores de serviços de comunicações eletrónicas ao público, incluindo os prestadores de serviços de acesso à Internet, só podem oferecer ou facilitar serviços se a

capacidade da rede for suficiente para os fornecer além dos serviços de acesso à Internet já fornecidos, e em caso algum esses serviços podem ser utilizados ou oferecidos em substituição dos serviços de acesso à Internet, ou afetar a disponibilidade ou a qualidade geral dos serviços de acesso à Internet para os utilizadores finais (nº 5, 3 e 4 per.).

Para que possam ser consideradas razoáveis, essas medidas devem ser transparentes, não discriminatórias e proporcionadas, e não podem basear-se em questões de ordem comercial, mas sim na qualidade técnica objetivamente diferente dos requisitos de serviço de categorias específicas de tráfego.

Tal como consagrado, o princípio da neutralidade da rede, enquanto garantia de acesso aberto, retira aos prestadores de serviços de acesso a possibilidade de negociarem o tráfego com os fornecedores de conteúdos, serviços e aplicações, por exemplo estabelecendo tarifários diferenciados para diferentes velocidades de transferência, já que não podem estabelecer medidas de gestão de tráfego baseadas “em questões de ordem comercial”, mas apenas por razões de qualidade técnica objetivamente diferente dos requisitos de serviço de categorias específicas de tráfego e na medida em que não tenham por objeto o controlo de conteúdos específicos. Os provedores de comunicações eletrónicas podem oferecer serviços otimizados para determinados conteúdos, aplicações ou serviços, mas apenas se a otimização for necessária para respeitar os requisitos dos conteúdos, aplicações ou serviços para um nível de qualidade específico.

Em suma, a diferenciação só é permitida quando encontrar justificação adequada em razões de qualidade técnica objetivamente diferente.

CONCLUSÃO

O Marco Civil é um passo em frente no sentido de uma

regulação da internet conforme com os padrões constitucionais. Põe fim à ideia, por vezes veiculada, de que o ciberespaço é uma ‘terra sem rei nem roque’ (*no man’s land*) e, enquanto *Magna Carta* dos usuários da Internet, reafirma a vigência dos valores constitucionais básicos no mundo digital.

O Marco Civil não trata de todas as questões jurídicas da Internet. Por exemplo, as matérias relativas à propriedade intelectual são praticamente omissas, tanto em sede de pirataria de direitos autorais na Internet, como as questões das patentes de software, das bases de dados⁵⁷, ou ainda dos nomes de domínio⁵⁸. De igual modo, o Marco Civil não regula as questões suscitadas pelo jogo em linha, em especial as apostas desportivas⁵⁹, e a problemática do tribunal competente e lei aplicável

⁵⁷ Vide, por ex., com referências, os nossos «Patentes de programas de computador e métodos de negociação na Internet» e «Pirataria e cópia privada», in *Direito da Sociedade da Informação*, org. J. Oliveira Ascensão, Vol. IX, APDI, Coimbra Editora, 2011, respetivamente p. 111-123 e p. 125-138; Id., «Internet, direito autor e acesso reservado», *As Telecomunicações e o Direito na Sociedade da Informação, Actas do Colóquio organizado pelo IJC em 23 e 24 de Abril de 1998*, Dir. António Pinto Monteiro, Instituto Jurídico da Comunicação, Coimbra, 1999, p. 263-273; Id., «Patentes de Software: Sobre a Patenteabilidade dos Programas de Computador», *Direito Industrial*, vol. I, Coimbra, Almedina, 2001, p. 385-429; «Direitos de autor, da Imprensa à Internet», *Revista da ABPI* nº 64 (2003), p. 21-28; Id., «Direito de autor, liberdade electrónica e compensação equitativa», *Boletim da Faculdade de Direito de Coimbra*, vol. 81 (2005), p. 441-509; Id., «A reprodução para uso privado no ambiente analógico e no ambiente digital», *Direito da Sociedade da Informação*, vol. VII, org. J. Oliveira ASCENSÃO, Coimbra Editora, 2008, p. 329-361; Id., «A Liberdade de Navegação na Internet: Browsers, Hyperlinks, Meta-tags», *Estudos de Direito da Comunicação*, org. A. Pinto Monteiro, Coimbra, 2002, p. 227-260; Id. «Bases de dados e direito *sui generis*», *Direito Industrial*, Vol. VII, org. J. Oliveira Ascensão, Coimbra, Almedina, 2010, p. 373-395; Id., «Fair use e direitos de autor (entre a regra e a excepção)», *Estudos em Honra do Professor Doutor José de Oliveira Ascensão*, org. António Menezes Cordeiro, Pedro Pais de Vasconcelos e Paula Costa e Silva, Volume I, Almedina, Coimbra, 2008, p. 853-869.

⁵⁸ Vide o nosso «Nomes de domínio (novo regime), firmas e marcas», *Revista de Direito Intelectual*, Nº 01, 2015, p. 145-164. Em língua inglesa, o nosso estudo com Carla VALÉRIO, «PORTUGAL (.pt)», in Torsten BETTINGER, Allegra WADDELL, *Domain Name Law and Practice – An International Handbook*, 2ª ed. Oxford University Press, Oxford, 2015, p. 733-755.

⁵⁹ Ver, por ex., o nosos «Media rights and online betting in football matches under Portuguese law», *The International Sports Law Journal*, 14 (2014), p. 167-178.

em questões de direito privado.⁶⁰

De todo o modo, não era – nem tinha que ser – o propósito do Marco Civil codificar todo o direito aplicável a litígios relacionados com a Internet, senão afirmar os princípios fundamentais que devem reger a sociedade em rede e regular alguns aspetos mais carecidos de tutela, como os dados pessoais e o papel dos provedores de internet.

Este trabalho abordou alguns aspetos dessa lei confrontando-os com as soluções vigentes no direito da União Europeia, com destaque para a problemática da proteção dos dados pessoais, o chamado direito ao esquecimento e o papel dos provedores de Internet, tendo em conta importantes acórdãos do Tribunal de Justiça da União Europeia, e cuja jurisprudência impacta não apenas diretamente os Estados-Membros da União, mas também indiretamente os países de outras partes do mundo. Será interessante, no futuro, acompanhar a jurisprudência do Brasil com referência ao Marco Civil, comparando-a com a jurisprudência do TJUE e saber se, por essa via, a globalização tecnológica vai junto com a globalização jurídica, já que para problemas semelhantes se justificam soluções semelhantes dentro de um mesmo universo cultural. Parece-nos que é por aí, e não pela criação de mais um tribunal – como já foi proposto⁶¹ –, que se deve caminhar. A cultura jurídica democrática assenta no diálogo e na colaboração entre ordens jurídicas distintas, mas ainda assim semelhantes. O futuro do direito da Internet e quem sabe da própria Internet terá muito a ganhar com um diálogo mais intenso entre o Brasil e a União Europeia.

⁶⁰ Ver, com mais indicações, os nossos «A Jurisdição na Internet segundo o Regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas)», *Boletim da Faculdade de Direito, Universidade de Coimbra*, vol. 77 (2001), p. 633-687; Idem, «Portugal», Toshiyuki KONO (ed.), *Intellectual Property and Private International Law: Comparative Perspectives*, Oxford, Hart, 2012, p. 877-939.

⁶¹ Daniel Freire e ALMEIDA, *Um Tribunal Internacional para a Internet*, Almedina, Coimbra, 2015.



REFERÊNCIAS BIBLIOGRÁFICAS

- ALMEIDA, Daniel Freire e. Um Tribunal Internacional para a Internet. Coimbra: Almedina, 2015.
- ANACOM. Quadro regulamentar para as comunicações eletrónicas: União Europeia – disponível em <http://www.anacom.pt>
- ASCENSÃO, José de Oliveira. Direito cibernético: a situação em Portugal. *Direito & Justiça* 2 (2001), p. 9.
- ASCENSÃO, José de Oliveira. O “marco civil da internet”: a lei brasileira n.º 12965, de 23 de abril de 2014. *Revista de Direito Intelectual*, 2015, No 2, p. 271-90.
- ASCENSÃO, José de Oliveira. O Direito da Internet em Portugal e no Brasil. *Direito da Sociedade da Informação*. Vol. X. Coimbra: Coimbra Editora, 2012, p. 101-126.
- BINICHESKI, Paulo Roberto. Responsabilidade civil dos provedores de Internet. *Direito comparado e perspectivas de regulamentação no direito brasileiro*. Mestrado em Ciências Jurídicas. Faculdade de Direito da Universidade de Lisboa. Lisboa, 2008.
- CANOTILHO, J.J. Gomes. *Direito Constitucional e Teoria da Constituição*. 7ª ed. Coimbra: Almedina, 2003.
- CASTRO, Catarina Sarmiento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.
- COMUNICAÇÃO DA COMISSÃO ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, Explorar plenamente o potencial da computação em nuvem na Europa. COM(2012) 529 final, Bruxelas, 27.9.2012
- COMUNICAÇÃO DA COMISSÃO. A Digital Single Market Strategy for Europe. COM(2015) 192 final.

- GONÇALVES, Maria Eduarda. *Direito da Informação - Novos Direitos e Formas de Regulação na Sociedade da Informação*. 2.^a ed. Coimbra: Almedina, 2003.
- LEMO, Ronaldo. Uma nova lei para assegurar direitos na internet no Brasil: o Marco Civil. *Propriedades intelectuais*, nº 2 (junho 2014), p. 30-4
- LENAERTS, Koen. The Case Law of the ECJ and the Internet (2004-2014). *ELTE Law Journal*. Nº 1 (2014), p. 9-26.
- MARQUES, Garcia; MARTINS, Lourenço. *Direito da Informática*. 2.^a ed. Coimbra, Almedina, 2006
- PEREIRA, Alexandre L. Dias. A Globalização, a OMC e o Comércio Electrónico. *Revista Sequencia (UFSC)* nº 45 (2002), p. 173-195.
- . A Jurisdição na Internet segundo o Regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas). *Boletim da Faculdade de Direito, Universidade de Coimbra*. Vol. 77 (2001), p. 633-687.
- . A Liberdade de Navegação na Internet: Browsers, Hyperlinks, Meta-tags. *Estudos de Direito da Comunicação*. Org. A. Pinto Monteiro. Coimbra: Instituto Jurídico da Comunicação, 2002, p. 227-260.
- . A Partilha de Ficheiros na Internet e Direito Autoral: Desenvolvimentos Legislativos e Jurisprudenciais na Europa. *Revista da ABPI*. No 123 (2013). p. 53-62.
- . A Partilha de Ficheiros na Internet e Direito Autoral: Desenvolvimentos Legislativos e Jurisprudenciais na Europa. *Revista da Associação Brasileira da Propriedade Intelectual*. Nº 123 (2013) p. 53-62.
- . A protecção jurídica do consumidor no quadro da directiva sobre o comércio electrónico. *Estudos de Direito do Consumidor*. Nº 2 (2000), p. 43-140
- . A protecção jurídica do consumidor no quadro da directiva sobre o comércio electrónico. *Estudos de Direito do Consumidor*. Nº 2 (2001), p. 281-300

- _. A reprodução para uso privado no ambiente analógico e no ambiente digital. In *Direito da Sociedade da Informação*. Vol. VII. Org. J. Oliveira Ascensão. Coimbra: Coimbra Editora, 2008, p. 329-361
- _. A via electrónica da negociação (alguns aspectos). *Estudos de Direito do Consumidor*. Nº 8 (2006/2007), p. 275-290.
- _. As licenças de software livre e *open source* (FOSS) como ferramenta de equidade tecnológica». O contrato na gestão do risco e na garantia da equidade. Coord. António Pinto MONTEIRO. Coimbra: Instituto Jurídico, 2015, p. 111-131.
- _. Bases de dados e direito *sui generis*. In *Direito Industrial*. Vol. VII. Org. J. Oliveira Ascensão. Coimbra: Almedina, 2010, p. 373-395.
- _. Comércio electrónico e consumidor. *Estudos de Direito do Consumidor*. Nº 6 (2004), p. 341-400.
- _. Comércio electrónico na sociedade da informação: da segurança técnica à confiança jurídica. Coimbra: Almedina, 1999 (com nota atualização no site da editora)
- _. Comércio electrónico de conteúdos digitais: proteção do consumidor a duas velocidades? *Estudos de Direito do Consumidor*. Nº 9 (2015), p. 177-207.
- _. Concorrência de Direitos Fundamentais na «Constituição da Informação. Estudos em Homenagem ao Prof. Doutor Jorge de Figueiredo Dias. Org. Manuel da Costa ANDRADE e Maria João ANTUNES, Vol. IV, Coimbra Editora, 2010, p. 795-831
- _. Contratos de licenças de software e de bases de dados. Contratos de Direito de Autor e de Direito Industrial. Org. Carlos Ferreira de ALMEIDA, Luís Couto GONÇALVES e Cláudia TRABUCO. Coimbra: Almedina, 2011, p. 345-368.
- _. Direito ciberespacial: ‘soft law’ ou ‘hard law’? In *Estudos*

- em Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho, Volume III - Direitos e Interconstitucionalidade: Entre Dignidade e Cosmopolitismo. Org. Fernando Alves Correia, Jónatas Machado, João Carlos Loureiro. Coimbra Editora: Coimbra, 2012, p. 685-710.
- _. Direito de autor, liberdade electrónica e compensação equitativa. Boletim da Faculdade de Direito de Coimbra. Vol. 81 (2005), p. 441-509.
 - _. Direitos de autor e acesso à Internet: uma relação tensa. Direito Autoral e Interesse Público, Anais do IV Congresso de Direito de Autor e Interesse Público. Org. Marcos WACHOWICZ e Manoel J. Pereira dos SANTOS. Florianópolis: UFSC/Fundação Boiteux, 2010, p. 98-105
 - _. Direitos de Autor e Liberdade de Informação. Coimbra: Almedina, 2008.
 - _. Direitos de autor, códigos tecnológicos e a Lei Milénio Digital. Boletim da Faculdade de Direito da Universidade de Coimbra. Vol. 75 (1999), p. 475-521.
 - _. Direitos de autor, da Imprensa à Internet. Revista da ABPI Nº 64 (2003), p. 21-28.
 - _. Empresa, comércio electrónico 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. Coord. António Pinto MONTEIRO. Vol. I - Congresso Empresas e Sociedades. Coimbra: Coimbra Editora, 2007, p. 439-478.
 - _. Fair use e direitos de autor (entre a regra e a excepção). In Estudos em Honra do Professor Doutor José de Oliveira Ascensão. Org. António Menezes Cordeiro, Pedro Pais de Vasconcelos e Paula Costa e Silva. Volume I. Coimbra: Almedina, 2008, p. 853-869.
 - _. Inovação tecnológica, propriedade intelectual e defesa da concorrência no mercado do software. Boletim da Fa-

- culdade de Direito, Universidade de Coimbra. Vol. 85 (2009), p. 237-259.
- Internet, direito autor e acesso reservado. In *As Telecomunicações e o Direito na Sociedade da Informação*. Actas do Colóquio organizado pelo IJC em 23 e 24 de Abril de 1998. Dir. António Pinto Monteiro. Coimbra: Instituto Jurídico da Comunicação, 1999, p. 263-273.
 - Media rights and online betting in football matches under Portuguese law. *The International Sports Law Journal*. Nº 14 (2014), p. 167-178.
 - Nomes de domínio (novo regime), firmas e marcas. In *Revista de Direito Intelectual*. Nº 01, 2015, p. 145-164
 - Normas abertas nos sistemas informáticos do Estado. *Revista do CEDOUA*. No 29 (2012), p. 39-43.
 - Notários, certificadores e comércio electrónico. In *Estudos Multidisciplinares sobre Integração*. Org. Fábio Luiz Gomes. Ri de Janeiro: Editora Lumen Juris, 2004, p. 5-21.
 - Patentes de programas de computador e métodos de negociação na Internet. In *Direito da Sociedade da Informação*. Org. J. Oliveira Ascensão. Vol. IX. Coimbra: Coimbra Editora, 2011, p. 111-123.
 - Patentes de Software: Sobre a Patenteabilidade dos Programas de Computador. In *Direito Industrial*. Vol. I, Coimbra: Almedina, 2001, p. 385-429.
 - Pirataria e cópia privada. In *Direito da Sociedade da Informação*. Org. J. Oliveira Ascensão. Vol. IX. Coimbra: Coimbra Editora, 2011, p. 125-138
 - Portugal. In KONO, Toshiyuki (ed.). *Intellectual Property and Private International Law: Comparative Perspectives*. Oxford: Hart, 2012, p. 877-939.
 - ; VALÉRIO, Carla. PORTUGAL (‘.pt’). In Torsten BETTINGER, Torsten; WADELL, Allegra (Ed). *Domain Name Law and Practice – An International Handbook*.

- 2ª ed. Oxford: Oxford University Press, 2015, p. 733-755.
- _. Informática, direito de autor e propriedade tecno-digital. Coimbra: Coimbra Editora, 2001.
 - _. Software Interoperability, Intellectual Property and Competition Law: Compulsory Licenses for Abuse of Market Dominance. *Computer Law & Security Review*. N° 27 (2011), p. 175-179.
- PORTUGAL. Supremo Tribunal de Justiça, acórdão de 16 de outubro de 2014. Proc. N° 679/05.7TAEVR.E2.S1 - www.dgsi.pt
- PORTUGAL. Tribunal Constitucional. Acórdão n° 174/00, Proc. 14/99. <http://www.tribunalconstitucional.pt/tc/acordaos/20000174.html>
- SPIECKER, Indra. A new framework for information markets: Google Spain. *Common Market Law Review*. Vol. 52 (2015), p. 1033-1058.
- UNIÃO EUROPEIA. Tribunal de Justiça. 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.
- _. Tribunal de Justiça. Acórdão de 16 de fevereiro de 2012. Proc. C-360/10, *SABAM c. Netlog NV*. ECLI:EU:C:2012:85.
 - _. Tribunal de Justiça. Acórdão de 20 de maio de 2003. Procs. C-465/00, 138/01 e 139/01. ECLI:EU:C:2003:294.
 - _. Tribunal de Justiça. Acórdão de 27 de março de 2014. Proc. C-314/12. *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft GmbH*. ECLI:EU:C:2014:192.
 - _. Tribunal de Justiça. Acórdão de 6 de novembro de 2003. Proc. C-101/01, *Bodil Lindqvist*. ECLI:EU:C:2003:596.

- _. Tribunal de Justiça. Acórdão de 6 de outubro de 2015. Proc. C-362/14, Maximilian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650.
 - _. Tribunal de Justiça. Acórdão de 8 de abril de 2014. Procs. C-293/12 e C-594/12, Digital Rights Ireland. ECLI:EU:C:2014:238.
 - _. Tribunal de Primeira Instância. Acórdão de 17 de setembro de 2007. Proc. T - 201/04. Microsoft Corp. v Commission of the European Communities. ECLI:EU:T:2007:289.
- WACHOWICZ, Marcos; KIST, Vitor Augusto. Marco Civil da Internet e Direito Autoral: uma breve análise crítica - <http://www.gedai.com.br/>
- WEBER, Rolf ; WEBER, Romana. Internet of Things – Legal Perspectives. Berlin: Springer, 2010.