

Informação e Direito na Era Digital: Um Novo Paradigma Jurídico?

Maria Eduarda Gonçalves

“A fundamental shift in technology is more than a change in the implements that we use, it is a change in who we are, in what we do, and how we do it.” (Cavazos e Morin, 1996)

1. Introdução

Uma das características distintivas da sociedade contemporânea consiste na penetração das novas tecnologias da informação e da comunicação na vida social, económica e política. Estas tecnologias vêm afectando profundamente os modos de organização das relações económicas e sociais e as condições da realização de valores fundamentais como a liberdade e a democracia. No centro da mudança encontra-se, de um lado, a afirmação da informação como recurso estratégico e principal fonte de riqueza na “sociedade da informação”; e, de outro lado, a centralidade da comunicação como veículo de múltiplos e variados contactos, mensagens e conteúdos informativos, no que também vem sendo justamente designado como “sociedade em rede” (Castells, 2006).

Se não é de hoje a consciência das sociedades sobre a relevância da informação e da comunicação, a escala do fenómeno permite afirmar que vivemos numa *nova era* marcada, em particular, por:

- i) uma economia baseada, crescentemente, na informação;
- ii) uma relação diferente das pessoas com o espaço, agora sem fronteiras, e com o tempo, mais acelerado dada a automatização;
- iii) uma modificação das condições de acesso e de distribuição do poder, que é cada vez mais função do acesso às redes e do controlo sobre os fluxos de informação e sobre a comunicação.

O carácter transversal e global da transformação em curso tem conduzido alguns observadores a aludir à emergência de um novo paradigma social. Fará sentido falar a este respeito de um novo paradigma jurídico? Na realidade, a sociedade da informação vem desafiando princípios e regras de há muito consolidados, pensados para uma

sociedade assente em bens físicos ou corpóreos. Os desafios situam-se, quer no plano do direito substantivo, quer no plano da aplicação do direito.

Na sociedade da informação materializa-se, desde logo, uma modificação do âmbito e do objecto das liberdades de expressão e de informação. As potencialidades de disseminação e acesso à informação expandem-se de forma extraordinária, abrindo oportunidades não só no plano cívico e político, das liberdades públicas, mas também como meios de acesso à cultura, à educação, à saúde até, abrindo, porventura, caminho à reclamação de um direito fundamental de acesso às redes e à informação digital. Estas expectativas, aliadas à maior facilidade de acesso a obras intelectuais nas redes eletrónicas, entram, porém, em choque com os exclusivos atribuídos aos criadores e editores a título de direitos de propriedade intelectual.

Um outro direito fundamental em questão é o direito à reserva da intimidade da vida privada. Quer a generalização das bases de dados contendo informação de ordem pessoal, criadas e utilizadas pelas organizações nas esferas e para os fins mais diversos, quer, ultimamente, as práticas de exposição pública da vida privada nas redes sociais na Internet, entre outras dinâmicas de idêntica natureza, são de molde a pôr em causa o princípio da reserva.

Colocam-se, do mesmo passo, dúvidas e incertezas quanto à forma mais apropriada de regular a comunicação na Internet. São dúvidas de substância – até que ponto regular, até que ponto condicionar aí o exercício das liberdades de expressão e de informação em nome do interesse público – e de procedimento – quais os métodos regulatórios mais ajustados à natureza das relações sociais que se estabelecem nesse quadro: regulação público-estatal, autorregulação, corregulação?

Acresce que as características da Internet contrariam o alcance territorial do direito e da autoridade do Estado, gerando o problema da sua aplicação num espaço sem fronteiras dificilmente vigiável e controlável. Soma-se o problema da jurisdição: qual a lei aplicável, qual o tribunal competente para intervir na resolução de litígios?

Estruturalmente conservador, o direito vê-se perante o dilema habitual perante a transformação social: conservar, adaptar ou repensar o quadro jurídico existente? No contexto da nova era, é forte o apelo à busca de soluções inovadoras que não frustrem as oportunidades de desenvolvimento e de realização sociais e individuais.

No presente capítulo, procuraremos analisar, criticamente e à luz destas considerações iniciais, algumas tensões que a sociedade da informação vem colocando a direitos fundamentais ancorados nos sistemas jurídicos europeus e a forma como a

União Europeia (UE) vem lidando com essas tensões, a saber:

i) A tensão entre a liberdade de acesso à informação e os direitos de propriedade intelectual, bem como outras formas emergentes de apropriação da informação;

ii) A tensão entre a informatização e disponibilização pública de dados relativos às pessoas individuais e a defesa da reserva da intimidade da vida privada;

iii) A proibição da difusão de conteúdos ilícitos e a dificuldade de os prevenir e reprimir nas redes electrónicas.

2. Repensar o direito de autor?

Por detrás do dilema entre liberdade e propriedade da informação reside um paradoxo. As tecnologias da informação e da comunicação propiciam a circulação virtualmente sem constrangimentos de tempo e de espaço e sem perda de qualidade de quantidades vastíssimas de informação (dados, texto, imagem, música, filmes, vídeos ...), protegida e não protegida, com inegáveis benefícios para os utilizadores e a sociedade. Elas favorecem ao mesmo tempo o que já foi qualificado como uma "explosão" da criatividade humana, abrindo espaços e oportunidades de criação e de difusão de obras como nunca até hoje. Mas, ao acentuarem o valor social e económico da informação, as novas tecnologias fazem dela, também, um sinónimo de negócio com as inerentes dinâmicas de exclusividade.

À primeira vista, dir-se-ia que na “nova era” se alarga o âmbito da informação como bem público, livremente acessível. Nunca como agora foi possível aceder a informação tão variada de forma tão ampla e célere e a custos relativamente baixos. No entanto, é também claro o desenvolvimento de um mercado da informação apoiado em direitos privatísticos com os inerentes constrangimentos ao acesso, inclusive os preços a pagar. Em que medida as oportunidades estarão, afinal de contas, a promover a informação como bem público ou em contrapartida a potenciar a sua apropriação e exploração guiadas por interesses predominantemente privados, perguntar-se-á?

Uma questão conexas decorre de a natureza da informação digitalizada, bem como a arquitetura das redes fragilizarem a protecção dos direitos de propriedade intelectual, concebidos para obras registadas em suporte físico. Como defender então os legítimos interesses dos investidores nos novos mercados da informação sem limitar indevidamente as liberdades de expressão e de informação?

Um olhar sobre o quadro jurídico atual da sociedade da informação na UE permite detetar efetivamente um movimento consistente de reforço da apropriação privada da informação e dos produtos da informação. Esta tendência é manifesta, designadamente, nas diretivas sobre proteção de programas de computador (2009/24/CE)¹, sobre proteção das bases de dados (96/9/CE)² e sobre direitos de autor na sociedade da informação (2001/29/CE)³.

A diretiva sobre proteção jurídica de bases de dados, em particular, protege estas bases por duas vias: pelo recurso ao direito de autor, no caso de se tratar de bases de dados originais, i.e. que incorporem um esforço de seleção e sistematização (por exemplo, uma enciclopédia em CD-ROM); e pelo recurso a um novo direito, o chamado “direito *sui generis*”, no caso de bases de dados não originais, desde que envolvam num investimento tido por substancial nos planos financeiro e profissional (por exemplo, uma lista telefónica acessível electronicamente).

O “direito *sui generis*”, definido pela diretiva como o “direito do fabricante de uma base de dados de proibir a extração e/ou a reutilização da totalidade ou de uma parte substancial, avaliada qualitativa ou quantitativamente, do conteúdo desta” desde que “a obtenção, verificação ou apresentação desse conteúdo representem um investimento substancial do ponto de vista qualitativo ou quantitativo”, foi já qualificado como um “*strong new right*” (Linn, 2000, p. 1). Não implica originalidade, mas tão-só investimento, privilegiando as considerações de ordem quantitativa. Constitui, assim, uma forma de ampliar, flexibilizando, a proteção jurídica de coleções de informação que nos moldes do direito de autor convencional não alcançariam proteção por não pressuporem um ato criativo.

Não surpreende que a instituição deste direito tenha ficado envolvida em polémica. Alegou-se que uma definição ampla do “direito *sui generis*” poderia resultar em formas de monopólio e bloqueios do acesso a informação de outro modo no domínio público, em prejuízo da comunidade académica e também das empresas que dependem da disponibilidade de informação para desenvolver as suas atividades⁴. A ambiguidade

¹ Diretiva 2009/24/CE do Parlamento Europeu e do Conselho, de 23 de Abril de 2009, relativa à proteção jurídica dos programas de computador.

² Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de Março de 1996, relativa à proteção jurídica das bases de dados.

³ Diretiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação.

⁴ Commission of the European Communities – DG Internal Market and Services Working Paper, *First Evaluation of Directive 96/9/EC on the legal protection of databases*, Brussels, 12 December 2005, p. 4.

deste direito e a falta de clareza de termos e expressões como “parte substancial” ou “insubstancial” do conteúdo de uma base de dados ou “investimento na obtenção, verificação e apresentação” do conteúdo de bases de dados “avaliado quantitativamente e qualitativamente”, geraram dúvidas que o Tribunal de Justiça da UE veio em parte esclarecer em acórdãos de Novembro de 2004⁵. Como consequência desta jurisprudência, o âmbito daquele direito foi de certo modo limitado (severamente, no entender de alguns⁶), abrindo passagem à reutilização por terceiros de informação contida em bases de dados. De todo o modo, se esta jurisprudência contribuiu para reduzir o efeito restritivo do direito, fê-lo em obediência a preocupações de liberalização do mercado, não da promoção de um acesso mais livre pelos utilizadores. Ironicamente, a avaliação da aplicação da diretiva publicada pela Comissão Europeia (CE) em 2005 concluiu que “está por provar o impacto económico do direito *sui generis* na produção de bases de dados”⁷.

Uma nova etapa no processo de expansão e reforço dos direitos de propriedade intelectual na Europa traduziu-se na diretiva europeia sobre a harmonização dos direitos de autor e dos direitos conexos na sociedade da informação. Guiada igualmente pelo intuito de promover a competitividade no mercado da informação na Europa, esta diretiva estendeu os poderes exclusivos dos autores e editores às reproduções “transitórias” (i.e. a visualização da obra num ecrã de computador), para além das reproduções permanentes, e redefiniu o conceito de “comunicação ao público” alargando-o à comunicação a pedido ou por iniciativa do utilizador da obra (i.e. a prática normal no acesso on-line às obras).

⁵ Acórdão do Tribunal de Justiça (Grande Secção), 9 de Novembro de 2004, Proc. C-203/02 (The British Horseracing Board Ltd and Others v. William Hill Organisation Ltd); Acórdãos do Tribunal de Justiça (Grande Secção), de 9 de Novembro de 2004, nos Proc. C-46/02 (Fixtures Marketing Ltd v. Oy Veikkaus); C-338/02 (Fixtures Marketing Limited v. AB Svenska Spel); e C-444/02 (Fixtures Marketing Ltd v. Organismos progonstikon agonon podofairou AE –“OPAP”). Todos os casos disseram respeito a bases de dados contendo informação desportiva sobre concursos hípicas e campeonatos de futebol e foram objecto de recursos a título prejudicial, de tribunais do Reino Unido, Finlândia, Suécia e Grécia.

⁶ “Evaluation of the 1996 Database Directive raises questions”, *Single Market News Article*, Issue Nr 40, January 2006, http://ec.europa.eu/internal_market/smn/smn40/docs/database-dir_en.pdf.

⁷ O estudo da Comissão indica que a produção de bases de dados decaiu mesmo para níveis pré-diretiva e que a indústria dos EUA, país onde não vigora semelhante direito, tem crescido mais depressa do que a da UE. Cf. European Commission, *First Evaluation of Directive 96/9/EC on the legal protection of databases*, DG Internal Market and Services Working Paper, Brussels, 12 December 2005. Apesar desta conclusão, a Comissão inclinou-se para a manutenção do *status quo*, não apenas por as empresas interessadas defenderem a sua manutenção, mas também para evitar reabrir o debate, incerto, acerca do nível de proteção necessário para as bases de dados.

Recorde-se que o fundamento do direito de autor repousou desde sempre na procura de uma conciliação entre, por um lado, os interesses dos autores na defesa da integridade e do reconhecimento da autoria da obra (direitos morais) e no gozo dos benefícios inerentes à sua exploração (direitos patrimoniais); e, por outro lado, o interesse da colectividade no "progresso das letras, das artes e das ciências", como proclama, por exemplo, a Constituição dos Estados Unidos da América. A fim de alcançar este equilíbrio, garantiu-se a terceiros a possibilidade de utilizar livremente as obras dentro de certos limites, nomeadamente, para fins educativos ou informativos, por exemplo, nas bibliotecas ou no exercício da atividade jornalística. Ora, como se apontou, a política europeia tende atualmente a valorizar mais a informação como mercadoria do que como bem público ou benefício colectivo. Há, contudo, um risco neste tipo de apropriação privatística pois esta restringe a disseminação de informação indispensável para permitir à sociedade retirar plena utilidade, desequilibrando os valores em causa e podendo mostrar-se até inconsistente com os fundamentos éticos em que repousa o direito de autor. Em última análise, como salienta Delmas-Marty, o risco real é o de subordinar direitos humanos às regras do mercado (Delmas-Marty, 2000, p. 173).

Na realidade, está longe de ser consensual a ideia de que a Internet justifique um reforço da proteção dos direitos de autores e editores. Algumas dinâmicas em curso abrem inclusive a porta para reequilíbrios futuros. A expansão de iniciativas de criação partilhada e de distribuição livre ou com a cedência parcial de direitos de autor - Wikipedia, "*creative commons*", "*free software*", "*public library of science*" - é indicativa de mudanças no próprio modelo económico de criação e de circulação de informação.

Nos últimos anos, também a prática dos *downloads* de obras protegidas veio colocar novos reptos ao direito do autor, sendo controversa, na Europa como nos Estados-Unidos da América (EUA), a melhor forma de lhes responder: repressão ou tolerância? Controlo judicial ou administrativo? Que responsabilidade imputar eventualmente aos distribuidores e aos operadores de telecomunicações e prestadores de serviços de acesso?

A questão encontra-se estreitamente relacionada com a da licitude dos programas de partilha de ficheiros ("*filesharing*"). Dado o seu impacto internacional, refira-se a

decisão pioneira do *United States Court of Appeals for the Ninth Circuit* no processo *A&M Records, Inc. v. Napster, Inc.*, 2001⁸. Na sua sentença sobre o caso, este tribunal confirmou decisão anterior do *United States District Court for the Northern District of California* que condenara Napster, um serviço de partilha de ficheiros na Internet no formato MP3, criado por Shawn Fanning em 1999, por violação dos direitos de autor dos queixosos. Napster permitia que os utilizadores fizessem *download* direto nos computadores de outros utilizadores, tendo gerado uma imensa comunidade global (em 2001, eram cerca de 8 milhões de utilizadores) com milhares de músicas disponíveis para toda a rede. A Justiça americana condenou NAPSTER, assim como os utilizadores do serviço, por cópia ilícita, apesar de gratuita, e ordenou o encerramento do NAPSTER. Em sentido análogo, em *Metro-Goldwyn-Mayer Studios Inc. et al. v. Grokster, Ltd. et al.*, o *Supreme Court* dos EUA pronunciou-se pela ilegalidade da utilização do serviço disponibilizado por Grokster para acesso a material protegido, designadamente ficheiros de filmes e de músicas por meio de serviços P2P não autorizados⁹.

A via repressiva tem continuado a manifestar-se em diversas iniciativas legislativas recentes. Foi o caso, no plano internacional, do *Anti-Counterfeiting Trade Agreement* (ACTA), tratado multilateral visando o estabelecimento de standards internacionais para a garantia dos direitos de propriedade intelectual. Apoiado por associações de grandes empresas da indústria filmográfica e farmacêutica (nomeadamente, a *Motion Picture Association of America* e a *Pharmaceutical Research and Manufacturers of America*), visando combater o aumento do comércio internacional de produtos contrafeitos e a pirataria de obras intelectuais protegidas, incluindo na Internet, o ACTA foi, porém, alvo de oposição ativa por parte de grupos e movimentos que reclamaram que ele seria de molde a afectar negativamente o exercício de direitos fundamentais como a liberdade de expressão e a privacidade (*privacy*). O acordo foi ainda contestado por organizações como os Médicos Sem Fronteiras que alegaram o perigo que dele adviria para o acesso a medicamentos em países menos desenvolvidos. Assinado em Outubro de 2011 pelos governos da Austrália, Canadá, Japão, Marrocos, Nova Zelândia, Singapura, Coreia do Sul e Estados- Unidos da América, e, em 2012, por México, UE e 22 dos seus Estados Membros (incluindo Portugal), o acordo acabaria por

⁸ Cf. a decisão em <https://bulk.resource.org/courts.gov/c/F3/239/239.F3d.1004.00-16403.00-16401.html>.

⁹ Cf. a decisão em <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&navby=case&vol=000&invol=04-48>.

ser rejeitado pelo Parlamento Europeu, em 4 de Julho de 2012.

Sorte semelhante tiveram, nos EUA, o projeto de lei *Stop Online Piracy Act* (SOPA), apresentado na Câmara dos Representantes dos EUA, tendo em vista incentivar os *Internet Service Providers* (ISP) a policiarem a Internet, projeto suspenso em Janeiro de 2012. Também a iniciativa legislativa *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PROTECT IP Act), de 2011, que pretendia combater, em especial, sites promotores de pirataria hospedados fora dos EUA, foi votado a idêntico desfecho.

Na Europa, cremos ser a Lei *Création et Internet*¹⁰, aprovada pelo Parlamento francês em 2009, que foi mais longe no propósito de regular e reprimir *downloads* de obras protegidas na Internet. Igualmente controversa¹¹, esta lei instituiu um sistema de resposta gradual consistindo no envio a suspeitos de *download* ilegal de um ou mais avisos apelando à cessação daquela prática. Os avisos competem a uma entidade administrativa especializada, a *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits*. Apenas em caso de não obediência aos avisos é determinado aos ISP que impeçam o acesso ao serviço por parte do infrator.¹²

Em sentido aparentemente discordante, em Portugal, o Departamento de Investigação e Ação Penal (DIAP) da Procuradoria-Geral da República arquivou, em 2012, quase 2000 queixas respeitantes a telecarregamentos ilegais, fundando-se quer num argumento de ordem substantiva - tratar-se-ia de “cópias privadas” excetuadas da proteção conferida ao autor ou editor, quer num argumento de ordem prática: nos termos do despacho de arquivamento, seria "impossível em face não só do número de IP e do que em termos do trabalho material e gastos tal pressupõe", uma investigação que esbarraria numa "séria improbabilidade de positividade de resultados", devido ao facto de muitas partilhas serem feitas através de redes sem fios (em muitos casos, os responsáveis pelos *downloads* e *uploads* de ficheiros usam o acesso à Internet de um

¹⁰ Loi N.º 2009-669 du 12 juin 2009, JO n.º 135 de 13 de Junho de 2009.

¹¹ ‘La loi “Création et Internet”, un premier pas vers le contrôle du Réseau?’ *Le Monde*, 18.06.2008.

¹² Segundo notícia do *Le Figaro* de Setembro de 2012, “L’Hadopi a presque deux ans. ... Depuis sa mise en route à l’automne 2010, elle a envoyé 1.150 million d’ e-mails de premier avertissement, et 100.000 rappels pour ceux en récidive. En juillet dernier, 340 dossiers étaient en phase 3 de « riposte graduée », susceptibles d’être transmis au parquet.” “95 % des personnes averties ont cessé leur comportement illicite après le premier e-mail”, precisou a presidente da comissão dos direitos. “A pedagogia funciona”, acrescentou.

outro utilizador, que pode não estar consciente desse facto) e "por recurso aos Cybercafés"¹³.

Reconhecendo a dificuldade, a UE tem preferido remeter a resposta aos *downloads* ilegais para instrumentos de *soft law* e para a autorregulação. Na Comunicação “Reforçar o controlo do respeito dos direitos de propriedade intelectual no mercado interno”¹⁴, a Comissão confirma o entendimento de que a defesa da propriedade intelectual deve ser reforçada tendo em consideração quer a sua importância como factor de criação, inovação e comércio, quer a necessidade de proteger a sociedade contra a violação dos direitos de autor causadora de prejuízos económicos e mesmo de riscos para a segurança e a saúde. A Comissão admite, porém, que os meios regulatórios existentes deverão ser complementados por medidas não legislativas incluindo um observatório europeu da contrafação e da pirataria e acordos voluntários entre as partes interessadas.

Note-se ainda que no âmbito de um processo opondo um ISP, Scarlet, a SABAM, entidade responsável pela gestão dos direitos de autor na Bélgica, o TJUE considerou ilegal o pedido de um juiz a uma operadora para que monitorize a Internet a fim de evitar *downloads* ilegais, alegando que tal monitorização violaria os direitos de proteção de dados e a liberdade de receber e enviar informação. Segundo o TJ, de outro modo, a própria operadora resultaria prejudicada uma vez que seria obrigada “a implementar um sistema informático complexo, permanente e exclusivamente às suas custas”¹⁵. Assim se evidenciaram uma vez mais os dilemas reinantes neste domínio.

Em suma, de um modo geral, o direito europeu tende a privilegiar os direitos de propriedade intelectual e a apropriação privada de informação em detrimento da valorização das oportunidades criativas e de difusão proporcionadas pelas novas tecnologias. A prática tem vindo, porém, a revelar a dificuldade de garantir eficazmente esses direitos no ambiente fluído e descentralizado da Internet. Na medida em que se

¹³ <http://static.publico.pt/docs/tecnologia/DespachoDIAP.pdf>. Cf. “DIAP arquiva queixa contra partilha de ficheiros por ser ‘impossível’ identificar responsáveis”, *Público*, 27.09.2012, <http://m.publico.pt/Detail/1564850>. (acedido em Dezembro de 2012)

¹⁴ COM (2009) 467 final, 11.9.2009.

¹⁵ Acórdão do Tribunal de Justiça (Terceira Secção), de 24 de Novembro de 2011, no processo C-70/10, Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:PT:HTML> (consultado em 23.11.2012).

converteu num bem de interesse geral decisivo para o progresso social e individual a informação e a comunicação suscitam hoje, mais do que anteriormente, um problema de equidade. Impõe-se, por isso, que o legislador se preocupe tanto com a garantia dos direitos de acesso dos cidadãos à informação quanto com os direitos dos autores e dos investidores, procurando equilibrá-los. A justa compensação dos autores e editores tenderá a passar, neste contexto, como a realidade está já a mostrar, por uma mudança nos termos do negócio de oferta e distribuição, criando uma oferta legal atrativa susceptível de rivalizar com o telecarregamento livre.

3. Garantir a reserva da intimidade da vida privada

Na sociedade da informação e em rede a reserva da intimidade vida privada vem sendo, gradualmente, erodida por diversas ordens de factores: a acumulação de dados pessoais decorrentes da utilização da Internet, bem como de *smart phones*, equipamentos de GPS (Global Positioning System), via verde e outros dispositivos que permitem registar e fazer convergir informação sobre os indivíduos, assim como das possibilidades técnicas crescentes de interceptação de comunicações privadas; e as práticas, em crescendo, de exposição da vida individual em redes sociais. Esta evolução tem vindo também a evidenciar o desajustamento das legislações sobre proteção de dados pessoais informatizados adoptadas desde os anos 70 na maior parte dos países europeus. Estas legislações tiveram por objetivo preservar a intimidade da vida privada por meio da imposição às entidades responsáveis pelas bases de dados pessoais do dever de respeitar um conjunto de princípios reguladores e de direitos dos titulares dos dados.

De acordo com a Diretiva 95/46/CE¹⁶, ainda em vigor, esses princípios são, em especial: o princípio da *limitação da finalidade* – os dados pessoais apenas podem ser recolhidos e tratados para fins específicos, explícitos e legítimos e não podem ser processados para fins incompatíveis com os que presidiram à sua recolha; o *da minimização dos dados* – o processamento de dados pessoais deve restringir-se ao mínimo necessário; o *princípio da qualidade* – os dados pessoais devem ser adequados, relevantes e não excessivos em relação aos fins para que foram coligidos; e o do *controlo* – a supervisão do tratamento dos dados deve ser assegurada por um conjunto de *direitos processuais* permitindo ao titular dos dados consentir, aceder e conhecer a

¹⁶ 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.

informação que sobre ele se encontra registada, retificar esses dados e opor-se ao seu processamento em determinadas circunstâncias. A Diretiva proíbe, além disso, a transferência de dados pessoais para países terceiros que não ofereçam um nível de proteção equivalente ao que confere a UE.

Importa reconhecer, desde logo, que o próprio conceito de *regime de proteção de dados pessoais* deixa presumir que o processamento dos dados é uma atividade legítima *per se*, apartando-se assim da noção original de *vida privada* entendida como uma esfera de segredo e autonomia individual. Os dados pessoais constituem *informação* que, por natureza e por definição, se destina a ser utilizada, ainda que sujeita a um conjunto de princípios e regras. Falar em *reserva da vida privada* perde, pois, algum do seu sentido neste quadro.

Mas a Diretiva 95/46/CE foi até mais longe no esvaziamento do princípio da reserva da intimidade da vida privada do que a sua predecessora, a Convenção do Conselho da Europa para a Proteção dos Indivíduos no que respeita ao Processamento Automático de Dados Pessoais, de 1981 (Convenção 108). O objectivo dessa Convenção fora definido como “a garantia, no território de cada uma das partes e para cada indivíduo, do respeito dos seus direitos e liberdades fundamentais, particularmente do *direito à intimidade da vida privada*” (art. 1º).¹⁷ A Diretiva contém, efetivamente, um catálogo de excepções aos princípios da proteção de dados não contempladas pela Convenção 108, admitindo o consentimento implícito do sujeito quando se entenda que o uso informático dos dados é necessário para a execução de um contrato no qual a pessoa em causa é parte e em diversas outras circunstâncias indicadas de modo relativamente abrangente (art. 7.º).

Nas últimas décadas, a evolução dos modos como a informação é acedida, processada e comunicada tem evidenciado as limitações deste regime. Quer a Convenção 108, quer a diretiva europeia foram elaboradas para regular o registo e tratamento de dados pessoais que se confinavam na altura às organizações. Ora, hoje em dia, poucas atividades humanas, das organizações como dos indivíduos isolados, não envolvem interação com o computador e as redes eletrónicas, incluindo as transações comerciais mais elementares. Os dados pessoais converteram-se num recurso decisivo da economia da informação. A quantidade e variedade de informação pessoal em bases

¹⁷ Convenção para a Proteção das Pessoas relativamente ao Tratamento Informatizado de Dados Pessoais, de 28.I.1981, publicada em francês, na Série des Traités Européens n° 108, Conseil de l' Europe, Strasbourg, 1982. Para uma versão em português, cf. «<http://www.cnpd.pt/Leis/leis.htm>».

de dados eletrónicas nas administrações públicas tem vindo a aumentar em larga escala, inclusive para fins de prevenção e repressão do terrorismo e do crime. A expansão do uso da Internet, incluindo de plataformas como blogues e redes sociais, conferem mais acuidade ainda à questão da proteção da vida privada e dos dados pessoais.

O Conselho da Europa e a UE empreenderam por isso processos de reflexão e revisão da legislação em vigor. Embora admitindo que o quadro vigente continua a ser válido quanto aos seus objetivos e princípios fundamentais, o Conselho da Europa definiu como objectivo “modernizar” a Convenção 108, acrescentando novos princípios, nomeadamente o da proporcionalidade (que permite lidar com as restrições a direitos fundamentais justificáveis no interesse geral) e o da “*privacy by design*”. Visa este princípio inovador a incorporação da proteção da vida privada nas especificações das tecnologias e da arquitetura dos novos sistemas e processos. O pressuposto é que, atualmente, as empresas coligem, armazenam e partilham, mais do que nunca, informação sobre os seus clientes, importando por isso que proteger melhor a “privacidade” do consumidor/utilizador¹⁸. É reveladora esta reconfiguração da reserva da intimidade da vida privada como uma proteção imbuída em soluções tecnológicas; que, importa frisar, remetem, em última análise, para responsabilidades acrescidas das organizações que processam os dados e para a autodefesa dos utilizadores (Wacks, 2010, p. 128-129)¹⁹.

Tendo em conta as alterações trazidas pelo Tratado de Lisboa e, em especial, a consagração pela Carta dos Direitos Fundamentais de um novo direito fundamental à proteção de dados pessoais²⁰, a Comissão Europeia iniciou, em 2010, o processo de revisão do regime em vigor com a publicação da Comunicação “Uma abordagem global da proteção de dados pessoais na União Europeia”²¹. A Comissão sublinha aí a prioridade a conceder ao respeito pelo novo direito fundamental em todas as políticas da

¹⁸ Cf. Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers”, March 2012.

¹⁹ Por exemplo, por via da oportunidade concedida aos consumidores “*to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism.*” (Federal Trade Commission, cit., p. i).

²⁰ A Carta consagra o direito à proteção dos dados pessoais no artigo 8.º, nos seguintes termos: 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

²¹ Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Uma abordagem global da proteção de dados pessoais na União Europeia”, COM (2010) 609 final, 4.11.2010.

UE ao mesmo tempo que pretende facilitar o livre fluxo de dados pessoais e clarificar o quadro normativo da proteção de dados nas áreas da cooperação policial e judiciária em matéria penal.

Em 25 de Janeiro de 2012, foram publicadas uma proposta de regulamento e uma proposta de diretiva da Comissão Europeia²². A proposta de regulamento²³ define um quadro geral para a proteção dos dados no Mercado Interno destinado a tomar o lugar da Diretiva de 1995, envolvendo como principais modificações a supressão dos requisitos administrativos tidos por desnecessários e uma maior responsabilização das entidades a quem incumbe o tratamento de dados, por um lado, e, por outro lado, um mais fácil acesso aos dados pelos titulares, introduzindo dois novos direitos individuais, à portabilidade dos dados e ao esquecimento.

Ao propor um instrumento normativo distinto para a proteção de dados pessoais para efeitos de prevenção e repressão de infrações penais e de actividades judiciárias conexas aplicável na área da segurança²⁴, sob a forma de uma proposta de diretiva, a Comissão sujeitou-se, porém, a um rol de críticas. No entender do Supervisor Europeu da Proteção de Dados, teria sido preferível um regime geral transversal a todas as políticas europeias para que o direito fundamental pudesse ser plenamente realizado²⁵. A própria Comissão reconheceu anteriormente a necessidade de assegurar um regime consistente em todas as áreas, abrangendo a prevenção e repressão do crime²⁶.

Recorde-se que a Diretiva 95/46/EC foi adoptada ao abrigo das regras do Tratado relativas ao Mercado Interno. O processamento de dados pessoais no domínio da política de segurança e da cooperação policial e judicial, assim como da segurança pública, da defesa, da segurança do Estado e do direito criminal foi excetuado do âmbito de aplicação da diretiva (art. 3.º). Só em 2008 seria adotada a Decisão-quadro do

²² Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI”, COM (2012) 9 final, 25.01.2012.

²³ Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM (2012) 11 final, 25.01.2012.

²⁴ Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, COM (2012) 10 final, 25.01.2012.

²⁵ Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão “Uma abordagem global da proteção de dados pessoais na União Europeia”, 22.06.2011.

²⁶ Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Realização de um espaço de liberdade, de segurança e de justiça para os cidadãos europeus, Plano de Ação de aplicação do Programa de Estocolmo”, 20.4.2010, p. 3.

Conselho 2008/977/JAI, de 27 de Novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. Por se restringir à cooperação entre Estados-Membros e por limitar a proteção dos dados por uma série de exceções aos princípios da limitação de finalidade e do consentimento, esta decisão foi considerada em geral insatisfatória (Hijmanns and Scirocco, 2009, p. 1491)²⁷; sentimento este acentuado em face da intensificação das políticas europeias de combate ao terrorismo e ao crime desencadeadas pelos ataques terroristas de Nova Iorque 2001, Madrid 2004, e Londres 2005, que geraram um investimento crescente nos sistemas de informação. A estas medidas somaram-se outras ampliando a utilização de dados pessoais, a saber: a adoção do passaporte biométrico²⁸, que causou apreensões não apenas dada a sensibilidade dos dados biométricos mas também devido à delicadeza, do ponto de vista da intimidade da vida privada, da generalização do uso de “body scanners”; os acordos sobre os registos de passageiros aéreos (PNR), celebrados com o governo dos EUA, obrigando as companhias aéreas a transmitir dados sobre os passageiros de voos em direção aos EUA ao Departamento de Segurança Interna (“Homeland Security Department”) dos EUA²⁹; e a Diretiva Retenção de Dados³⁰. Este conjunto de medidas reflete a tendência atual na UE para o armazenamento de dados pessoais independentemente da suspeita de prática de crimes, em obediência ao princípio da “disponibilização da informação” (“*the principle of availability of information*”)³¹.

²⁷ A Comissão admitiu que a Decisão-quadro 2008/977/JAI contém uma exceção demasiado ampla ao princípio da limitação do fim, afectando a possibilidade de os indivíduos exercerem os seus direitos. Cf. Comunicação “Uma Abordagem Global à Proteção dos Dados Pessoais na União Europeia”, cit., p. 14.

²⁸ Regulamento (CE) n.º 2252/2004 do Conselho, de 13 de Dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros, alterado em 2009.

²⁹ Decisão 2007/551/PESC/JAI do Conselho, de 23 de Julho de 2007, relativa à assinatura, em nome da União Europeia, do Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento. Este acordo foi revogado e substituído pelo Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna (DSI) dos Estados Unidos, Jornal Oficial da União Europeia L 215/5, 11.8.2012.

³⁰ Diretiva 2006/24/EC, impondo obrigações reforçadas aos operadores de telecomunicações no que respeita à recolha e armazenamento de dados gerados ou processados em conexão com a prestação de serviços de comunicação pública ou em redes de comunicação pública, que modificou a diretiva 2002/58/EC.

³¹ Este princípio significa no essencial que sempre que as autoridades de segurança interna num país membro ou a Europol necessitem de informação para desempenhar as suas funções devem poder obtê-la aonde ela for acessível. Cf. Comunicação ao Conselho e ao Parlamento Europeu relativa ao reforço da eficácia, da interoperabilidade e das sinergias entre as bases de dados europeias no domínio da justiça e dos assuntos internos, COM (2005) 597 final, 24.11.2005.

É um movimento que é de molde a contrariar o reconhecimento da proteção de dados pessoais como um direito fundamental (Gonçalves and Jesus, 2012). Admitindo que o carácter *fundamental* do direito implica o reconhecimento do seu estatuto moral, na linha de um entendimento alargado na doutrina (Habermas, 1996, p. 258; Moller, 2007, p. 456; Harbo, 2010, p. 165), deverão ser daí retirados corolários: designadamente, o de que a proteção da intimidade como círculo da informação que apresenta maior sensibilidade do ponto de vista dos valores individuais e da dignidade humana deverá merecer proteção reforçada³². Ironicamente, a proposta de regulamento de 25 de Janeiro de 2012 dissocia a proteção dos dados pessoais da reserva da intimidade da vida privada, omitindo mesmo esta expressão e quebrando do mesmo passo com as suas origens (Costa and Poulet, 2012, p. 255).

A nosso ver, a reserva da intimidade da vida privada deve persistir como fundamento *essencial* da proteção dos dados pessoais; de outro modo, corre-se o risco de deitar por terra a última barreira que subsiste contra a progressiva instrumentalização dos dados pessoais, quer ao serviço dos interesses económicos, quer das políticas de segurança. Nesse sentido se orienta, cremos, a sugestão do Parlamento Europeu de que seja salvaguardada a “identidade digital” contra intrusões de agentes públicos e privados, para o que se exigiria não só uma maior sensibilização dos cidadãos, mas também o consentimento informado dos utilizadores da Internet no que respeita às actividades digitais em que se envolvam e que impliquem a partilha de dados de carácter pessoal³³.

4. Regular os conteúdos ilícitos na Internet

A expansão das plataformas de informação e comunicação na Internet, ao mesmo tempo em que abrem exponencialmente as possibilidades de exercício das liberdades públicas e de participação democrática, acentua o risco de abuso dessas liberdades sob a forma de difusão de conteúdos ilícitos, difamação e ofensa ao bom nome e reputação, e outras práticas de carácter fraudulento.

³² Vai neste sentido a sugestão de P. De Hert, “Balancing security and liberty within the European human rights framework. A critical reading of the Court’s case law in the light of surveillance and criminal law enforcement strategies after 9/11”, <http://www.utrechtlawreview.org/index.php/ulr/article/viewFile/4/4>, p. 87.

³³ Cf. Recomendação do Parlamento Europeu ao Conselho, de 26 de Março de 2009, referente ao reforço da segurança e das liberdades fundamentais na Internet (2008/2160).

A Internet é efetivamente um meio de comunicação sem mediador: diferentemente dos *media* tradicionais, que operam com base na separação entre centros emissores e receptores, estes normalmente passivos e isolados, a Internet permite aceder a um dispositivo de comunicação estruturado segundo uma relação todos-todos. São precisamente a ausência de um proprietário da rede e a sua natureza descentralizada que contribuíram para o renascer do sonho de uma comunidade harmoniosa à escala planetária, a "cidade Internet", "comunidade de internautas", partilhando um conjunto de valores e de práticas (Mathias, 1997, p. 13-14). Não se rejeita, porém, que a Internet seja atravessada por uma exigência reguladora. Esta seria, no entanto, rebelde a uma normatividade externa, dada a sua especificidade técnica e os seus modos específicos de funcionamento. Foram muitos, sobretudo na origem, os defensores da ideia de que a Internet representa um espaço natural de liberdade, não refractário a qualquer regulação, mas estranho a modos de regulação que não sejam gerados nela própria.

Para além dos argumentos relacionados com a natureza do novo meio de comunicação e informação, a recusa da hetero-regulação da Internet apoiou-se em considerações pragmáticas: a sua dimensão global e a dificuldade de controlo do que se passa na rede (Slevin, 2000, p. 214). Na mesma ordem de ideias, sustentou-se que o ciberespaço se distingue do mundo real delimitado fundamentalmente pelas fronteiras e autoridade dos Estados, reclamando por isso um direito e instituições próprias assentes na *autorregulação* das actividades *on-line*. Em defesa desta tem-se invocado também o facto de apenas os utilizadores diretos da rede serem capazes de se aperceber dos riscos envolvidos em determinadas situações e de avaliar a adequação e a eficácia das sanções (Poullet, 2000, p. 159). Mas, importa também reconhecer que a resistência à regulação da Internet é indissociável do facto de ela estar sendo promovida em larga medida pelas forças do mercado.

A defesa intransigente de uma Internet regida por princípios de liberdade transversais às esferas política e pública e económico-tecnológica tem sido dominante no discurso oficial do governo dos EUA. Nele se imbricam, explicitamente, preocupações de ordem política, como a luta contra o bloqueio do acesso à rede por imposição de autoridades de alguns países, e de ordem económica, comercial e tecnológica³⁴. No que se refere especificamente aos conteúdos circulados, o governo

³⁴ Cf. "Internet rights and wrongs: Choices and challenges in a Networked World", discurso da Secretária de Estado Hillary Clinton, George Washington University, 15 de Fevereiro de 2011, in <http://www.state.gov/secretary/rm/2011/02/156619.htm> (acedido em Dezembro de 2012).

dos EUA tem-se declarado favorável a uma circulação internacional de informação o mais livre possível, quer seja cultural, quer comercial, acreditando nas potencialidades das tecnologias de filtragem e bloqueamento de acesso como formas de proteger o acesso a conteúdos ilícitos³⁵.

À defesa da ausência de regulação e da autorregulação opõe-se, porém, uma perspectiva que, na linha da tradição jurídico-política europeia, defende a *regulação pública* sob pena de serem postos em causa valores como a ordem pública e as liberdades e direitos fundamentais das pessoas. Em princípio, os governos devem, por um lado, valorizar as externalidades positivas da Internet, promovendo a realização das liberdades de expressão e de comunicação, a criação de uma esfera pública aberta, a promoção da concorrência nos mercados, a oferta de uma diversidade de informação de interesse público, o desenvolvimento do capital humano, a promoção da paz social, a oferta de infra-estruturas adequadas; e, por outro lado, defender a legalidade e os valores constitucionais eventualmente ameaçados na sociedade da informação e em rede.

Na realidade, as políticas governamentais estão já a afetar a Internet por várias vias. A rede é presentemente um espaço organizado e regulado, embora principalmente na esfera técnica (protocolos de comunicação, nomes de domínio, etc.)³⁶. Como se apontou, dada a sua estrutura interconectada de dezenas de milhares de redes e o seu modo de funcionamento, a Internet inscreve-se mal num esquema de controlo administrativo *a priori*: nenhuma autoridade única gere os fluxos de dados, podendo todos os utilizadores ser emissores e receptores de informações. Tem sido aventada, em consequência, uma abordagem à regulação ancorada no autocontrolo dos utilizadores por via, por exemplo, de sistemas de filtragem parental e da elaboração de códigos deontológicos pelos profissionais, incluindo regras de transparência, responsabilidade e respeito do direito aplicável. Na Europa, tende, no entanto, a ser admitida a necessidade de assegurar algum mecanismo de defesa contra a difusão de conteúdos ilícitos ou prejudiciais (que, não infringindo forçosamente a lei, sejam de molde a afetar grupos mais vulneráveis, como, por exemplo, as crianças). No mesmo sentido, foi sugerido um "pluralismo regulado" ou "governança plurilateral" (Grewlich, 1999, p. xiv) ou formas

³⁵ Cf. *The Framework for Global Electronic Commerce*, em <http://clinton4.nara.gov/WH/New/Commerce/> (acedido em Novembro de 2012).

³⁶ Entre as organizações que têm regulado, no plano técnico, a Internet, contam-se o *World Wide Web Consortium* (W3C), a *Internet Engineering Task Force* (IETF) e a *Internet Corporation for Assigned Names and Numbers* (ICANN).

de correção (European Commission, 2005) envolvendo as diferentes partes interessadas na regulação do ciberespaço. Se o número de códigos de conduta tende a aumentar na Europa, isso deve-se em boa parte ao encorajamento explícito do próprio legislador (Verbiest e Wéry, 2001, p. 528).

Um exemplo de recurso à correção foi, em França, o *Fórum des droits sur Internet*, instituído em 2001, mas encerrado em 2010 na sequência da retirada da subvenção que recebia do Estado francês. A missão do Fórum era informar o público e organizar a concertação entre poderes públicos, empresas e utilizadores em torno dos problemas originados pela utilização da Internet. Oferecia, designadamente, um serviço de mediação dirigido ao público. Mais de 120 organismos públicos, associações e empresas privadas haviam aderido ao Fórum³⁷.

Importa frisar que o direito europeu sempre contemplou a liberdade de expressão e de informação como integrante do seu património comum de valores e princípios. Este princípio é agora garantido pela Carta dos Direitos Fundamentais da União Europeia (art. 11º). A consideração prestada pela UE à regulação dos conteúdos circulados na Internet explica-se, pois, não apenas à luz das restrições admitidas à liberdade de expressão desde que "necessárias, numa sociedade democrática, à segurança nacional, à integridade territorial ou à segurança pública, à defesa da ordem e à prevenção do crime, à proteção da saúde e da moral, à proteção da reputação ou dos direitos de outrem, para impedir a divulgação de informações confidenciais ou para garantir a autoridade e a imparcialidade do poder judicial" (art. 10, n.º 2 da Convenção Europeia dos Direitos do Homem), mas também pela pretensão de impedir que o desenvolvimento e competitividade de um setor promissor possam ser afetados por falta de regulação de conteúdos ilícitos ou prejudiciais.

Já na sua Comunicação relativa ao seguimento do Livro Verde sobre a Proteção de Menores e da Dignidade Humana nos serviços audiovisuais e da informação, de 1996³⁸, sublinhara a Comissão a necessidade da proteção dos interesses gerais dos cidadãos europeus como condição do clima de segurança e confiança necessários ao desenvolvimento daquelas atividades, notando contudo a dificuldade de os fazer respeitar no ambiente dos serviços em linha, o que explicaria a ênfase na

³⁷

http://www.foruminternet.org/institution/espace-presse/communiqués-de-presse/IMG/pdf/CP_dissolution_FDI_-3-.pdf. (acedido em Novembro de 2012)

³⁸ Livro Verde sobre a proteção de menores e da dignidade humana nos serviços audiovisuais e de informação, COM (96) 483, 16.10.1996, e Comunicação da Comissão sobre conteúdo ilegal e prejudicial na Internet, COM (96) 487, 16.10.1996.

autorregulação. Esta tem sido, realmente, a via preferida para a prevenção e controlo dos conteúdos ilícitos na UE. A Comissão tem-se proposto fortalecer a eficácia das medidas nacionais promovendo uma coerência mínima no desenvolvimento do quadro autorregulador e da cooperação entre as partes interessadas. A responsabilização dos agentes justifica-se em parte pela dificuldade técnica de identificar os infractores, uma opção manifestamente realista.

O “Programa comunitário plurianual para a promoção de uma utilização mais segura da Internet e das novas tecnologias em linha – 2005, 2008”, do Parlamento Europeu e do Conselho³⁹, aposta na responsabilização dos agentes económicos e sociais por um *uso legal e responsável* dos serviços de informação e de comunicação. Inicialmente proposto com base no art. 157º, n.º 3, do Tratado CE (ex-Título XIII-Indústria), acabou por ser retido, para esse efeito, o art. 153º, n.º 2 (ex-Título XI, relativo à proteção dos consumidores). Na prática, isso não impediu este plano de ser orientado sobretudo para os *industriais* — é sobre eles que recai a principal responsabilidade de regulação. Os *utilizadores* são também incitados a mobilizarem-se a fim de se protegerem contra a receção de conteúdos ilícitos ou prejudiciais e contra os riscos de invasão da vida privada, entre outros. Para organizar a luta contra os conteúdos ilícitos, encoraja-se, portanto, a tomada de medidas específicas pelos atores diretamente envolvidos ou afetados, salientando, do mesmo passo, a importância de as fazer acompanhar por mecanismos de transparência e de interface, a saber: o estabelecimento de uma rede europeia de *hotlines*, isto é, de linhas directas acessíveis aos internautas permitindo assinalar a existência de conteúdos ilícitos; e a adopção de códigos de conduta dos profissionais do sector. Sugere-se que a adesão a estes códigos seja dada a conhecer mediante a atribuição aos *sites* de rótulos de qualidade. Este mecanismo deveria tornar claros os critérios de avaliação de conteúdos, ajudando os *Internet Service Providers* (ISP) a retirar os ficheiros que não respeitassem esses critérios e os fornecedores de acesso a bloquear o acesso a esses *sites*⁴⁰. Os sistemas de filtragem e de

³⁹ Cf. Decisão n.º 854/2005/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, que adota um programa comunitário plurianual para a promoção de uma utilização mais segura da internet e das novas tecnologias em linha. Esta decisão deu continuidade à Decisão 276/1999/CE do Parlamento Europeu e do Conselho, de 25 de Janeiro de 1999, adoptando um plano de ação comunitário plurianual visando promover uma utilização segura da Internet pela luta contra as mensagens de conteúdo ilícito e prejudicial difundidas nas redes mundiais.

⁴⁰ Em certos Estados-Membros, os fornecedores de acesso e prestadores de serviços da Internet começaram já a instituir mecanismos de autorregulação. No Reino Unido, por exemplo, a *Internet Services Providers Association* e o *London Internet Exchange* uniram esforços com a *Safety-Net*

classificação de conteúdos deveriam, por seu turno, ser postos em prática em cooperação com representantes dos utilizadores. De um modo mais geral, confia-se na sensibilização alargada destes quanto aos riscos inerentes à Internet.

Mas será a autorregulação suficiente? Dir-se-ia que não. Todavia, o recurso aos tribunais vem também ele causando embaraços, quer em razão da dificuldade de identificação e perseguição dos autores de alegadas infrações, quer por estar longe de ser claro o modo de determinar a jurisdição e o tribunal competentes para decidir litígios relativos a conteúdos disponibilizados em sítios Web ou a comunicações na Internet.

A cooperação dos ISP e dos *Internet Content Providers* (ICP) afigura-se crucial para que as autoridades policiais e judiciais possam cumprir as missões que lhes competem neste campo. No entanto, a tendência é, no mundo ocidental, a de isentar os ISP (“prestadores intermediários de serviços”, na formulação da UE) de qualquer dever de vigilância da informação e comunicação na Internet⁴¹. Mesmo o dever de prestar informação às autoridades sobre o IP (Internet Protocol) dos seus clientes, em caso de mandato judicial, tem sido por vezes confrontado com a proteção que lhe é conferida pela legislação sobre proteção dos dados pessoais.

Se na UE o princípio regulador é, nesta matéria, o da imunidade relativa, já nos EUA prevalece o princípio da neutralidade das redes e na China, pelo contrário, os operadores vêm sendo responsabilizados pelos conteúdos disponibilizados nas redes por eles exploradas (Liu, 2011, p. 235). Estas divergências dificultam fortemente a aplicação da lei na sociedade da informação.

Um problema conexo é o da determinação da jurisdição competente. Em teoria, cada uma das ordens jurídicas com as quais uma conexão seja estabelecida quando da consulta de um site Internet pode reclamar o exercício da sua jurisdição. A dúvida reside em saber que critério privilegiar: o local onde o dano foi produzido? Ou o local de onde emanou a informação ou comunicação contestada, i.e. o da localização do servidor?

Dois casos, que aqui tomamos como referência, servirão para ilustrar a incerteza que subsiste neste domínio. Em *Yahoo Inc. v. La Ligue Contre le Racisme et l'Antisemitisme* (2000), o *Tribunal de Grande Instance de Paris* ordenou à empresa

Foundation a fim de regularem a circulação de conteúdos ilícitos. Foi nesse quadro definido um código de conduta visando oferecer um serviço de "rating" dos "newsgroups" e uma linha directa ("hotline").

⁴¹ É o que decorre dos arts. 12º e 15º da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no Mercado Interno (Diretiva sobre comércio eletrónico).

Yahoo que bloqueasse o acesso a sítios nazis acessíveis em França, onde o dano fora produzido. *Yahoo France* obedeceu no essencial a esta decisão, resistindo, porém, a aplicá-la aos seus serviços nos EUA alegando a impossibilidade técnica de o fazer e a violação do princípio do *free speech* em que incorreria, se o fizesse⁴². Em *Dow Jones & Company v. Gutnick* (2002), um caso de difamação, o *High Court of Australia* relevou igualmente o local onde foi causado o prejuízo. *Dow Jones & Company*, editor da revista *Barron's Online*, objeto de contestação, defendera como critério de conexão a localização dos servidores (no caso, nos EUA), onde a publicação se encontrava alojada. Mas o servidor tem uma posição meramente passiva no processo, alegou o Tribunal, que considerou também o inerente perigo decorrente da hegemonia americana em matéria de publicações na Internet⁴³.

5. Conclusão

São, pois, consideráveis os reptos e as incertezas que envolvem o direito num mundo em que a informação e a comunicação se desmaterializam e as fronteiras territoriais se diluem. Princípios e direitos longamente reconhecidos são postos em causa e duvida-se da capacidade dos Estados e das suas instituições para garantirem a ordem e a justiça no novo quadro.

Estamos, decerto, perante mudanças decisivas na relação das sociedades com a informação e a comunicação. O acesso às redes eletrónicas e à informação converteu-se numa aspiração, diremos até, numa necessidade fundamental dos cidadãos. Na medida em que a informação passa a constituir um bem ou recurso indispensável para o desenvolvimento das capacidades individuais e o progresso coletivo, ela suscita um problema de equidade que apela à intervenção redistributiva da autoridade pública. Assim como no passado o desenvolvimento das redes de comunicação telefónica ou de transportes fez emergir a filosofia do serviço público universal, também na sociedade da informação é essencial que a informação não seja encarada como uma simples mercadoria sujeita às leis do mercado, desde logo, em domínios em que sempre foi tratada como bem público como os da educação, da ciência ou da cultura. Torna-se, por isso, a nosso ver, imprescindível estender a filosofia do serviço público universal aos novos meios de comunicação e de informação. Poderá ainda invocar-se a própria

⁴² Cf. a história deste caso em <http://www.internetlibrary.com/pdf/Yahoo-La-Ligue-Contre-Le-Racisme.pdf>.

⁴³ <http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html>.

natureza da sociedade da informação e da sociedade em rede, as oportunidades que proporcionam para a realização das liberdades de expressão e de informação e mesmo de efetivação de direitos sociais, como argumentos em prol de uma consagração mais alargada de direitos de acesso dos indivíduos em face quer das empresas detentoras de direitos exclusivos, no quadro de um regime reformado de propriedade intelectual, quer do Estado, no respeitante à informação do setor público. Abre-se, assim, caminho à reclamação de novos direitos e liberdades fundamentais, que sejam de molde a prolongar ou a complementar as liberdades de expressão e de informação: um *direito de acesso às redes*, contemplado já, aliás, como “livre acesso às redes informáticas de uso público” pela Constituição da República Portuguesa (art. 35.º, n.º 6) ou defendido como uma “freedom to connect” por Hillary Clinton⁴⁴. Cremos justificar-se, inclusivamente, o reconhecimento de um verdadeiro *direito fundamental à informação como direito social*, não só como liberdade civil e política, mas também como direito de acesso na medida em que este se mostre indispensável à promoção da criação do conhecimento, da educação, da cultura ou ao próprio exercício das liberdades públicas.

Esta pretensão afirma-se, porém, quando surge, como se apontou, uma pressão considerável do mercado no sentido do reforço de exclusivos sobre os produtos de informação. Talvez paradoxalmente, o direito europeu tem tendido a privilegiar a apropriação privada de informação e a proteção dos direitos de propriedade intelectual sem curar devidamente das oportunidades criativas e de difusão proporcionadas pelas novas tecnologias. A prática tem vindo, porém, a revelar a dificuldade de garantir aqueles direitos na Internet. Por tudo isto, impõe-se, julgamos, a procura de um novo equilíbrio entre acesso e proteção de autores e editores mais compatível com as circunstâncias da sociedade da informação e da sociedade em rede.

No que respeita a um outro valor jurídico fundamental, a reserva da intimidade da vida privada, concluímos que ele sofre um processo de crescente erosão. Quer o crescimento do número de bases de dados pessoais, quer o alargamento das categorias de dados que vêm sendo registados, utilizados e transmitidos entre diferentes entidades, públicas e privadas, quer ainda a expansão as práticas de exposição pública da vida privada nas redes sociais na Internet, põem, materialmente, em causa a reserva. Curiosamente, o recuo do princípio da defesa do segredo da vida privada tem sido acompanhado pelo desenvolvimento e aprofundamento dos regimes de proteção dos

⁴⁴ Cf. discurso cit. nota 35.

dados pessoais. Vem-se delegando, assim, nas organizações que tratam os dados (controladores e processadores dos dados, na linguagem mais moderna das legislações) a responsabilidade principal de defesa dos legítimos interesses e direitos dos indivíduos a que os dados se referem, sob a supervisão de entidades reguladoras. No mundo digital, estas entidades vêem, porém, diminuída as suas capacidades de vigilância e controlo. Os indivíduos sentem-se, por seu turno, desapossados de meios efetivos de defesa dos seus direitos (Klaousen, 2001).

A afirmação do direito à proteção de dados como direito fundamental na Carta dos Direitos Fundamentais da UE parece testemunhar uma revalorização dessa proteção. Mas a evolução recente da legislação europeia tem frustrado expectativas, ao admitirem-se cada vez mais exceções aos princípios e direitos que estruturaram originariamente estes regimes.

Neste contexto, é de notar a utilização da expressão “*data privacy*” na atual doutrina anglo-saxónica. Não obstante a sua ambiguidade, a expressão parece sugerir a necessidade de devolver ao indivíduo uma parte do poder de controlo que lhe tem sido retirado sobre os seus dados pessoais; o controlo *possível*, diríamos, uma vez que o seu exercício dependerá, sobretudo, dos dispositivos técnicos postos ao serviço dos utilizadores pelos operadores. Pensamos que deveria ser considerado, além disso, o alargamento da margem do poder de renúncia pelo indivíduo/cidadão a disponibilizar dados pessoais de especial sensibilidade às organizações e aos sistemas de informação, bem como uma ampliação das circunstâncias em que deverá ser requerido o seu consentimento informado para a recolha de tais dados.

Como se indicou, a natureza das redes eletrónicas, o facto de transgredirem as fronteiras territoriais do Estado e do direito, e a volatilidade da informação digital, reduzem consideravelmente a capacidade reguladora efetiva da autoridade pública e, em última análise, a possibilidade de cumprir a sua missão protetora dos direitos dos indivíduos. A relevância atribuída pelas instituições europeias à autorregulação, bem como à sensibilização dos utilizadores para a necessidade de se defenderem em face dos riscos da Internet, é indicativa do reconhecimento de que, na sociedade da informação, a insuficiência da lei terá de ser compensada pela entrada em ação de outros modos de regulação e controlo social. Se é verdade que na UE a responsabilidade dos poderes públicos não é simplesmente alienada, a ênfase na autorregulação e na corregulação por parte do discurso oficial sobre o futuro da regulação europeia revela bem a tomada de consciência política dos constrangimentos decorrentes da nova era. A sociedade de

informação torna, realmente, premente a necessidade de reconhecer a multiplicidade, diversidade e relações de interdependência entre ordenamentos normativos distintos, a lei estatal, o direito europeu e internacional, e a “legalidade” específica que se afirma na rede, baseada em códigos de conduta e em práticas autorreguladoras. Mas talvez ainda seja cedo para avaliar plenamente o efeito desta evolução sobre a lei como arquétipo da ordenação social e da realização da justiça.

Sem dúvida, as novas tecnologias da informação e da comunicação vêm revolucionando padrões e práticas sociais, interrogando concepções jurídicas surgidas num sociedade predominantemente individualista e materialista, e contestando modos hierárquicos de exercício de autoridade. Oferecem, por isso, um terreno propício à experimentação e à inovação jurídicas. A nossa visão do direito é forçada a abrir-se em face destas novas realidades.

6. Referências bibliográficas

- Castells, M. (2006), “A sociedade em rede: do conhecimento à política”, in M. Castells e G. Cardoso (orgs.), *A Sociedade em Rede. Do Conhecimento à Acção Política*, Lisboa, Presidência da República/Imprensa Nacional, pp. 18-30
- Cavazos, Edward A. and G. Morin (2006), “A New Legal Paradigm From Cyberspace? The Effect of the Information Age on the Law”, *Technology In Society*, Vol. 18, No. 3, pp. 357-371
- Costa, L. and Y. Pouillet (2012), “Privacy and the Regulation of 2012”, *Computer Law & Security Review* 28, pp. 254-262
- Delmas-Marty, Mireille (2000), "Droit et mondialisation", in Y. Michaud (dir.), *Qu'est Ce Que La Culture*, Paris, Odile Jacob, pp. 170-182
- European Commission (2005), *The Current State of Co-Regulation and Self-Regulation in the Single Market*, European Economic and Social Committee, Single Market Observatory (SMO), European Economic and Social Committee, Brussels, http://www.eesc.europa.eu/resources/docs/2018_cahier_en_smo_def.pdf
- Gonçalves, M. E. and I. A. Jesus (2012), “Security And Personal Data Protection In The European Union: Challenging Trends From A Human Rights’ Perspective”, *Human Security Perspectives Journal*, <http://www.etc-graz.at/typo3/index.php>

- Gonçalves, M. E. and M. I. Gameiro (2012), “Security, privacy and freedom, and the EU legal and policy framework for biometrics”, *Computer Law & Security Review*, 28 (3), pp. 320-327
- Grewlich, K. W. (1999), *Governance in 'Cyberspace'. Access and Public Interest in Global Communications*, Haia, Kluwer Law International
- Habermas, J. (1996), *Between Facts and Norms*, Cambridge, The MIT Press, p. 258
- Harbo, T.-I. (2010), “The Function of the Proportionality Principle in EU Law”. *European Law Journal*, 16 (2), p. 158–185
- Hijmanns, H. and Scirocco, A. (2009), “Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?”, *Common Market Law Review*, 46, pp. 1485-1525
- Klaousen, P. (2001), "L'action de l'Union Européenne en matière de lutte contre les contenus illicites et préjudiciables sur l'Internet", in A. Blandin-Obernesser, *L'Union Européenne et Internet*, Rennes, Éditions Apogée, pp. 149-186
- Linn, A. (2000), "History of data base protection: Legal issues of concern to the scientific community", ICSU, CODATA Scientific Access to Data and Information, http://www.codata.org/data_access/linn.html, pp. 1-8
- Liu, Wenqi (2011), “A Critical Review of China’s Approach to Limitation of the Internet Service Provider’s Liability: A Comparative Perspective”, *Journal of Intellectual Property Rights*, 16, May, pp 235-245
- Mathias, P. (1997), *La Cité Internet*, Paris, Presses de Sciences Po
- Möller, K. (2007), “Balancing and the structure of constitutional rights”, *International Journal of Constitutional Law*, 5 (3), pp. 453-468
- Pouillet, Y. (2000), "Some considerations on cyberspace law", in Unesco (ed.), *The International Dimensions of Cyberspace Law*, Dartmouth, Ashgate, pp. 147-187
- Slevin, J. (2000), *The Internet and Society*, Oxford, Polity Press
- Wacks, R. (2010), *Privacy*, Oxford, Oxford University Press